CIBERSECURIDAD

Comprensión del Ciberdelito: FENÓMENOS, DIFICULTADES Y RESPUESTA JURÍDICA

Informe

Sector de Desarrollo de las Telecomunicaciones

Comprensión del Ciberdelito: Fenómenos, dificultades y respuesta jurídica

Noviembre de 2014

La publicación de la UIT "Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica" ha sido preparada por el Prof. Dr. Marco Gercke. El autor desea expresar su agradecimiento al Departamento de Infraestructura, Entorno propicio y Ciberaplicaciones de la Oficina de Desarrollo de las Telecomunicaciones de la UIT.

Esta publicación está disponible en línea en: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Antes de imprimir este informe, piense en el medio ambiente.

© UIT 2014

Todos los derechos están reservados. No se puede reproducir ninguna parte de esta publicación de ninguna manera y por ningún medio sin la autorización por escrito de la UIT.

Índice

Página

1 Introducción 1
1.1 Infraestructura y servicios 1
1.2 Ventajas y riesgos 2
1.3 Ciberseguridad y ciberdelito 3
1.4 Dimensiones internacionales del ciberdelito 4
1.5 Consecuencias para los países en desarrollo 5

2 El fenómeno de la ciberdelincuencia 11
2.1 Definiciones 11
2.2 Tipología del ciberdelito 12
2.3 Evolución de los delitos informáticos y la ciberdelincuencia 13
2.4 Alcance e impacto de la ciberdelincuencia 14
2.5 Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos 17
2.6 Delitos en relación con el contenido 22
2.7 Delitos en materia de derechos de autor y marcas 30
2.8 Delitos informáticos 32
2.9 Combinación de delitos 37

3 Desafíos que suscita la lucha contra el ciberdelito 78
3.1 Oportunidades 78
3.2 Desafíos generales 80
3.3 Retos jurídicos 88

4 Creación de capacidades 103
4.1 Ciberseguridad y ciberdelito 103
4.2 Metodología aplicable a la creación de capacidades 103
4.3 Una estrategia como punto de partida 105
4.4 Relevancia de una política 107
4.5 Función de los organismos reguladores en la lucha contra el ciberdelito 110
4.6 Experiencias en materia de creación de capacidades en el Grupo de Estados de África, el Caribe y el Pacífico (ACP) 116

5 Panorama de las actividades de las Organizaciones Regionales e Internacionales 127
5.1 Enfoques internacionales 127
5.2 Enfoques regionales 139
5.3 Enfoques científicos e independientes 162
5.4 Relaciones entre los enfoques legislativos regionales e internacionales 163
5.5 Relación entre los enfoques legislativos internacionales y los nacionales 164

6 Respuesta jurídica 189
6.1 Definiciones 189
6.2 Derecho penal sustantivo 198
6.3 Evidencia digital 251
6.4 Jurisdicción 261

Página

6.5 Derecho procesal 265
6.6 Cooperación internacional..... 295
6.7 Responsabilidad de los proveedores de Internet 310

Objetivo

El objetivo del informe de la UIT *Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica* es ayudar a los países a comprender los aspectos jurídicos del ciberdelito y la ciberseguridad y a armonizar sus marcos jurídicos. Como tal, su finalidad es prestar asistencia a los países para que comprendan mejor las repercusiones nacionales e internacionales de las crecientes ciberamenazas, evaluar las necesidades de instrumentos nacionales, regionales e internacionales, y ayudar a los países a establecer unos cimientos jurídicos sólidos.

El informe ofrece un panorama completo de los temas más pertinentes relacionados con los aspectos jurídicos del ciberdelito, haciendo hincapié en las demandas de los países en desarrollo. Debido a la dimensión transnacional del ciberdelito, las herramientas jurídicas son las mismas para los países industrializados y en desarrollo. Sin embargo, las referencias han sido seleccionadas para beneficiar a los países en desarrollo, y se ha proporcionado además una amplia selección de recursos para realizar estudios más detallados de los diversos temas. Siempre que resultó posible se utilizaron fuentes públicamente disponibles, con inclusión de numerosas ediciones gratuitas de periódicos jurídicos en línea.

El informe consta de seis capítulos. Después de la Introducción (*Capítulo 1*), se proporciona un panorama general del ciberdelito (*Capítulo 2*). Este incluye descripciones del modo según el cual se cometen los delitos y explicaciones de los ciberdelitos más propagados tales como el pirateo, el robo de identidad y los ataques de denegación de servicio. Se ofrece asimismo una visión de conjunto de las dificultades inherentes a la investigación y el enjuiciamiento del ciberdelito (*Capítulos 3* y *4*). Tras un resumen de algunas iniciativas tomadas por organizaciones internacionales y regionales en la lucha contra el ciberdelito (*Capítulo 5*), prosigue con un análisis de los diferentes enfoques jurídicos en lo que respecta al derecho penal sustantivo, el derecho procesal, la evidencia digital, la cooperación internacional y la responsabilidad de los proveedores de servicios Internet (*Capítulo 6*), con inclusión de ejemplos de enfoques internacionales y de prácticas idóneas a partir de soluciones nacionales.

En este informe se aborda el primero de los siete objetivos estratégicos consignados en la Agenda sobre Ciberseguridad Global de la UIT, en el que se insta a elaborar estrategias para el desarrollo de una legislación sobre el ciberdelito que pueda aplicarse e interfuncionar a escala mundial, en armonía con las medidas legislativas nacionales y regionales en vigor, y se considera la organización de actividades nacionales tendientes a la ciberseguridad en el marco de la Cuestión 22/1 de la Comisión de Estudio 1 del UIT-D. El establecimiento de una infraestructura jurídica adecuada es un componente básico de una estrategia nacional sobre ciberseguridad. En la Resolución 130 (Rev. Guadalajara, 2010) de la Conferencia de Plenipotenciarios de la UIT, que trata del fortalecimiento del papel de la UIT en la creación de confianza y seguridad en el uso de las tecnologías de la información y la comunicación, se hizo hincapié en el mandato conexo de la UIT en lo tocante a la creación de capacidades. La adopción, por parte de todos los países, de una legislación adecuada para combatir la utilización indebida de las TIC con fines delictivos y de otra índole, incluidas las actividades tendientes a afectar la integridad de las infraestructuras nacionales de información esenciales, es un aspecto medular para el logro de la ciberseguridad global. Puesto que las ciberamenazas pueden tener su origen en cualquier lugar del planeta, el alcance de los desafíos es inherentemente internacional y exige cooperación internacional, asistencia en materia de investigación, y unas disposiciones sustantivas y de procedimiento comunes. Por consiguiente, es importante que los países armonicen sus marcos jurídicos para combatir el ciberdelito y facilitar la cooperación internacional.

Exención de responsabilidad respecto de los hiperenlaces

Este documento contiene varios cientos de enlaces con documentos disponibles públicamente. En el momento de incorporar los enlaces a las notas se verificaron todas las referencias. Sin embargo, no es posible garantizar que el contenido actualizado de la páginas a las que se refieren los enlaces sigue siendo el mismo. Así pues, la referencia también incluye información –siempre que resultó posible– sobre el autor o la institución que lo publicó, el título y en su caso el año de publicación, para que el lector pueda buscar el documento objeto del enlace si éste ya no está disponible.

1 Introducción

Bibliografía (seleccionada): *Aggarwal,* Role of e-Learning in A Developing Country Like India, Proceedings of the 3rd National Conference, INDIA, Com 2009*; Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Choudhari/Banwet/Gupta*, Identifying Risk Factors in for E-governance Projects, published in Wgarwal/Ramana, Foundations of E-government, 2007, page 270 *et. seq.*; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe, 2006; *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 *et seq.*; *European Commission,* Final Report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure, 2009; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141 *et seq.*; *Gercke*, Cybersecurity Strategy, Computer Law Review International 2013, 136 *et seq.; Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2; *Masuda*, The Information Society as Post-Industrial Society, 1980; *Molla*, The Impact of eReadingness on eCommerce Success in Developing Countries, 2004; *Ndou*, E-Government for Developing Countries, Opportunities and Challenges, DJISDC 2004, 18, page 1 *et seq.*; *Luiijf/Klaver*, In Bits and Pieces, Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society, 2000; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, 2005; *Tanebaum*, Computer Networks, 2002; *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1; *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52-56; *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2.

1.1 Infraestructura y servicios

Internet es uno de los ámbitos del desarrollo de la infraestructura técnica que crece más rápidamente.[1] Hoy en día, las tecnologías de la información y la comunicación (TIC) son omnipresentes y la tendencia hacia la digitalización va en aumento. La demanda de Internet y de conectividad informática ha conducido a la integración de la tecnología informática en productos que normalmente funcionaban sin ésta, como por ejemplo los automóviles y edificios.[2] Las fuentes de suministro de electricidad, la infraestructura del transporte, los servicios militares y la logística, es decir prácticamente todos los servicios modernos, dependen del uso de las TIC.[3]

Aunque en los países occidentales el desarrollo de nuevas tecnologías apunta principalmente a satisfacer las necesidades del consumidor, los países en desarrollo también pueden beneficiarse de las nuevas tecnologías.[4] Gracias a la disponibilidad de tecnologías de comunicaciones inalámbricas de larga distancia tales como WiMAX[5] y los sistemas informáticos que hoy en día se pueden adquirir por menos de 200 USD[6], un número muy superior de personas en los países en desarrollo debería tener acceso a Internet y a los productos y servicios conexos.[7]

La influencia de las TIC en la sociedad va mucho más allá del establecimiento de una infraestructura de información básica. La disponibilidad de TIC es un cimiento para el desarrollo en lo tocante a la creación, disponibilidad y utilización de servicios basados en redes.[8] El correo electrónico ha desplazado a las cartas tradicionales[9]; actualmente la representación web en línea es más importante para la actividad económica que los materiales de publicidad impresos;[10] y los servicios telefónicos y de comunicaciones basados en Internet están creciendo a un ritmo más acelerado que las comunicaciones cableadas.[11]

La disponibilidad de TIC y de nuevos servicios basados en redes representa algunas ventajas para la sociedad en general y en particular para los países en desarrollo.

Se considera que las aplicaciones de las TIC tales como el cibergobierno[12], el cibercomercio[13], la cibereducación[14], la cibersanidad[15] y el cibermedioambiente son habilitadores del desarrollo, por cuanto ofrecen un canal eficiente para prestar una amplia gama de servicios básicos en zonas rurales y distantes.

Las aplicaciones de las TIC pueden facilitar el logro de los objetivos de desarrollo del milenio, reducir la pobreza y mejorar la salud y las condiciones ambientales en los países en desarrollo. Si el enfoque, el contexto y los procesos de implementación son correctos, las inversiones en aplicaciones e instrumentos TIC pueden dar lugar a un aumento de la productividad y la calidad. A su vez, las aplicaciones TIC pueden liberar capacidades técnicas y humanas y permitir un mayor acceso a los servicios básicos. A este respecto, el robo de identidad en línea y la apropiación de las credenciales y/o la información personal de otra persona por Internet con la intención de reutilizarlas de manera fraudulenta con fines delictivos es hoy una de las principales amenazas al ulterior desarrollo del cibergobierno y la actividad económica virtual.[16]

Asimismo, con frecuencia el coste de los servicios Internet es muy inferior al de otros servicios comparables fuera de la red.[17] A menudo los servicios de correo electrónico están disponibles gratuitamente o su costo es muy módico en comparación con los servicios postales tradicionales.[18] La enciclopedia en línea Wikipedia[19] se puede utilizar gratuitamente, al igual que cientos de servicios de servidor en línea.[20] La reducción de los costos es importante, ya que ello permite a un mayor número de usuarios aprovechar esos servicios, incluidas personas con ingresos muy limitados. Dado que en los países en desarrollo muchas personas tienen recursos financieros limitados, Internet les permite utilizar servicios a los que, de otro modo, no tendrían acceso fuera de la red.

1.2 Ventajas y riesgos

La introducción de las TIC en muchos aspectos de la vida diaria ha llevado a acuñar el moderno concepto de sociedad de la información.[21] Este desarrollo de la sociedad de la información ofrece grandes oportunidades.[22] El acceso sin obstáculos a la información puede fomentar la democracia, pues el flujo de información queda fuera del control de las autoridades estatales (como ha ocurrido, por ejemplo, en Europa Oriental y África del Norte).[23] Los adelantos técnicos han mejorado la vida diaria; la banca y la compra en línea, el uso de servicios móviles de datos y de transmisión vocal por el Protocolo Internet (VoIP) sólo son algunos ejemplos del grado de integración de las TIC en nuestra vida diaria.[24]

No obstante, el crecimiento de la sociedad de la información va acompañado de nuevas y graves amenazas.[25] Actualmente algunos servicios esenciales como los de suministro de agua y electricidad dependen de las TIC.[26] Los automóviles, el control de tráfico, los ascensores, el acondicionamiento de aire y los teléfonos también dependen de funcionamiento armonioso de las TIC.[27] Los ataques contra la infraestructura de la información y los servicios Internet ahora pueden perjudicar a la sociedad de nuevas formas muy graves.[28]

Ya han tenido lugar ataques contra la infraestructura de la información y los servicios Internet.[29] El fraude en línea y los ataques de piratería son sólo algunos ejemplos de los delitos relacionados con la informática que se cometen cada día en gran escala.[30] Según informes, los daños financieros causados por el ciberdelito son enormes.[31] Únicamente en 2003, los software dañinos causaron pérdidas de hasta 17.000 millones USD.[32] De conformidad con algunas estimaciones, en 2007 los ingresos del ciberdelito superaron los 100.000 millones de USD, rebasando así a los correspondientes al comercio ilegal de drogas por primera vez.[33] Teniendo en cuenta un estudio publicado en 2014, las pérdidas anuales causadas por el ciberdelito en el mundo entero podrían ascender a 400.000 millones USD.[34] Casi el 60% de las empresas de los Estados Unidos estiman que el ciberdelito les resulta más costoso que el delito físico.[35] Estas estimaciones demuestran claramente la importancia que reviste la protección de las infraestructuras de la información.[36]

La mayoría de los ataques antes mencionados contra la infraestructura informática no apuntan forzosamente a la infraestructura esencial. Sin embargo, el software dañino "Stuxnet" descubierto en 2010 puso de relieve la amenaza de ataques centrados en la infraestructura esencial.[37] Este software, que posee más de 4 000 funciones[38], apuntaba a los sistemas informáticos que utilizan programas que por lo general se utilizan para controlar la infraestructura esencial.[39]

1.3 Ciberseguridad y ciberdelito

El ciberdelito y la ciberseguridad son aspectos que difícilmente pueden considerarse separados en un entorno interconectado. Esto queda demostrado por el hecho de que en la Resolución de la Asamblea General de las Naciones Unidas de 2010 sobre la ciberseguridad se aborda el ciberdelito.[40]

La ciberseguridad[41] desempeña una función importante en el desarrollo progresivo de la tecnología de la información, así como de los servicios Internet.[42] La mejora de la ciberseguridad y la protección de la infraestructura de información crítica es esencial para la seguridad y el bienestar de cualquier nación. Conferirle mayor seguridad a Internet (y proteger a sus usuarios) se ha transformado en una parte integrante del desarrollo de nuevos servicios, así como de la política gubernamental.[43] La erradicación del ciberdelito es un componente básico de una estrategia nacional de ciberseguridad y de protección de la infraestructura de la información esencial. Ello incluye en particular la adopción de una legislación adecuada contra el uso indebido de las TIC con fines delictivos o de otra índole y las actividades destinadas a afectar la integridad de las infraestructuras nacionales esenciales. A nivel nacional, esta es una responsabilidad compartida que exige una acción coordinada para la prevención, preparación, respuesta y recuperación frente a incidentes por parte de las autoridades gubernamentales, el sector privado y los ciudadanos. A nivel regional e internacional, esto entraña la cooperación y la coordinación con los correspondientes asociados. Así pues, la formulación e implementación de un marco y una estrategia nacionales de ciberseguridad exige la adopción de un enfoque completo.[44] Las estrategias de ciberseguridad –por ejemplo, el establecimiento de sistemas de protección técnica o la educación de los usuarios para evitar que sean víctimas del ciberdelitos– puede ayudar a reducir los riesgos de ciberdelito.[45] La elaboración y el fomento de estrategias de ciberseguridad son aspectos vitales de la lucha contra el ciberdelito.[46]

Las dificultades de orden jurídico, técnico e institucional que plantea la cuestión de la ciberseguridad son de naturaleza global y amplio alcance, y sólo pueden afrontarse con una estrategia coherente en la que se tenga en cuenta la función de los diferentes interesados y las iniciativas existentes, en un marco de cooperación internacional.[47] A este respecto, en la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[48] se reconocieron los riesgos reales y significativos que trae consigo una ciberseguridad insuficiente o la proliferación del ciberdelito. En las disposiciones §§ 108-110 de la *Agenda de Túnez para la Sociedad de la Información*[49], incluidos sus Anexos, se estipula un plan para llevar a la práctica entre múltiples interesados y a escala internacional el *Plan de Acción de Ginebra de la CMSI*,[50] y en éste se describe el proceso de implementación con participación de múltiples interesados en el marco de once líneas de acción y se atribuyen responsabilidades para facilitar la puesta en práctica de dichas líneas de acción. En la CMSI los dirigentes mundiales y los gobiernos designaron a la UIT para facilitar la implementación de la Línea de Acción C5 de la CMSI, que versa sobre la creación de confianza y seguridad en la utilización de las TIC.[51]

A este respecto, el 17 de mayo de 2007 el Secretario General de la UIT presentó la Agenda sobre Ciberseguridad Global , GCA)[52] junto con representantes de los gobiernos, el sector industrial, las organizaciones regionales e internacionales, las instituciones académicas y de investigación. La GCA es un marco mundial para el diálogo y la cooperación internacional con miras a coordinar la respuesta internacional ante los crecientes desafíos a la ciberseguridad y realzar la confianza y la seguridad en la sociedad de la información. Este marco se basa en los trabajos en curso, las iniciativas y asociaciones existentes, con el objetivo de proponer estrategias globales para hacer frente a las dificultades que entraña la creación de confianza y seguridad en la utilización de las TIC. En el seno de la UIT, la GCA sirve de complemento a los programas de trabajo de la UIT existentes, y facilita la realización de las actividades de los tres Sectores en la esfera de la ciberseguridad, en un marco de cooperación internacional.

La Agenda sobre Ciberseguridad Global tiene siete principales metas estratégicas, fundamentadas en cinco ámbitos de trabajo: 1) medidas jurídicas; 2) medidas técnicas y de procedimiento; 3) estructuras orgánicas; 4) creación de capacidades; y 5) cooperación internacional.[53]

La lucha contra el ciberdelito exige la adopción de un enfoque de amplio alcance. Puesto que las medidas técnicas por si solas no pueden evitar ningún delito, es indispensable que los organismos encargados de hacer cumplir la ley estén autorizados para investigar y penalizar el ciberdelito con eficacia.[54] Entre los ámbitos de trabajo de la GCA, las "medidas jurídicas" se centran en la manera de hacer frente a dificultades legislativas que plantean las actividades delictivas cometidas en las redes TIC de forma compatible a escala

internacional. Las "medidas técnicas y de procedimiento" se centran en las principales medidas encaminadas a promover la adopción de enfoques perfeccionados para mejorar la seguridad y la gestión de riesgos en el ciberespacio, con inclusión de esquemas de acreditación, protocolos y normas. Por "estructuras orgánicas" se entiende la prevención, detección, gestión de los ciberataques y respuesta frente a los mismos, incluida la protección de los sistemas de infraestructura de la información esenciales. La "creación de capacidades" consiste en elaborar estrategias sobre mecanismos tendientes a la creación de capacidades para fomentar la concientización, la transferencia de conocimientos y potenciar la ciberseguridad en el programa de políticas nacional. Por último, la "cooperación internacional" abarca la cooperación, el diálogo y la coordinación a escala internacional para hacer frente a las ciberamenazas.

El desarrollo de una legislación adecuada y el establecimiento de un marco jurídico relacionado con el ciberdelito es una parte medular de una estrategia sobre ciberseguridad. Para eso es necesario ante todo contar con disposiciones de derecho penal sustantivas para enjuiciar actos tales como el fraude informático, el acceso ilegal, la interferencia de datos, las violaciones de los derechos de autor y la pornografía infantil.[55] El hecho de que en el Código Penal existan disposiciones aplicables a actos similares cometidos fuera de la red no significa que esas disposiciones también puedan aplicarse a los actos cometidos por Internet.[56] Por consiguiente, es fundamental hacer un análisis minucioso de las leyes nacionales en vigor para identificar cualquier posible laguna.[57] Además de las disposiciones de derecho penal sustantivas[58], los organismos encargados de hacer cumplir la ley necesitan las herramientas e instrumentos necesarios para investigar el ciberdelito.[59] Esas investigaciones plantean por si mismas algunas dificultades.[60] Los perpetradores pueden actuar prácticamente desde cualquier lugar del mundo y tomar medidas para enmascarar su identidad.[61] Las herramientas e instrumentos necesarios para investigar el ciberdelito pueden ser muy diferentes de los utilizados para investigar delitos comunes.[62]

1.4 Dimensiones internacionales del ciberdelito

Con frecuencia el ciberdelito posee una dimensión internacional.[63] A menudo los correos electrónicos con contenido ilegal pasan a través de cierto número de países durante la transferencia desde el remitente al destinatario, o el contenido ilegal se almacena fuera del país.[64] En las investigaciones de ciberdelitos es muy importante que haya estrecha cooperación entre los países involucrados.[65] Los acuerdos de asistencia jurídica mutua en vigor están basados en procedimientos oficiales complejos y que a menudo consumen mucho tiempo, y además con frecuencia no abarcan las investigaciones informáticas.[66] Por consiguiente, es vital establecer procedimientos para una respuesta rápida frente a incidentes, además de solicitar la cooperación internacional.[67]

En algunos países el régimen de asistencia jurídica mutua está basado en el principio de "doble incriminación".[68] Por lo general las investigaciones a escala mundial están limitadas a los delitos que se penalizan en todos los países participantes. Aunque algunos delitos –como la distribución de pornografía infantil– pueden penalizarse en la mayoría de las jurisdicciones, las diferencias regionales son importantes.[69] Constituyen ejemplos de ello otros tipos de contenido ilegal, como la incitación al odio. La penalización de los contenidos ilegales puede ser diferente según el país[70]; contenidos que en un país pueden distribuirse legalmente tal vez sean ilegales en otro país.[71]

La tecnología informática que se utiliza hoy en día es básicamente la misma en todo el mundo.[72] Salvo por los aspectos lingüísticos y los tipos de enchufe, existen muy pocas diferencias entre los sistemas informáticos y los teléfonos celulares que se venden en Asia y en Europa. Una situación análoga surge en relación con Internet. Debido a la normalización, los protocolos de red utilizados en los países africanos son los mismos que se usan en los Estados Unidos.[73] La normalización permite a los usuarios de todo el mundo acceder a los mismos servicios por Internet.[74]

La cuestión es determinar cuáles son los efectos de la armonización de las normas técnicas globales en el desarrollo del derecho penal nacional. En lo tocante al contenido ilegal, los usuarios de Internet tienen acceso a información procedente de todo el mundo, lo que les permite acceder a información que en el extranjero es legal y en su país puede ser ilegal.

Teóricamente, la normalización técnica va mucho más allá de la mundialización de las tecnologías y servicios y podría conducir a la armonización de las legislaciones nacionales. Sin embargo, tal como pusieron de

relieve las negociaciones sobre el Primer Protocolo al Convenio del Consejo de Europa sobre la Ciberdelincuencia ("Convenio sobre la Ciberdelincuencia"),[75] los principios de la legislación nacional evolucionan a un ritmo mucho más lento que los progresos técnicos.[76]

Aunque Internet no reconozca los controles fronterizos, existen medios para limitar el acceso a ciertos tipos de información.[77] En general el proveedor de acceso puede bloquear ciertos sitios web y el proveedor de servicio que almacena un sitio web puede impedir el acceso a la información a esos usuarios sobre la base de las direcciones IP vinculadas a cierto país ("IP-targeting").[78] Si bien es posible eludir ambas medidas, éstas igual se pueden utilizar para mantener ciertas diferencias territoriales en una red mundial.[79] Según la OpenNet Initiative[80], aproximadamente dos docenas de países aplican este tipo de censura.[81]

1.5 Consecuencias para los países en desarrollo

Encontrar estrategias de respuesta y soluciones para la amenaza del ciberdelito es un gran desafío, especialmente para los países en desarrollo. Por lo general una estrategia completa de lucha contra el ciberdelito contiene medidas de protección técnica e instrumentos jurídicos.[82] El desarrollo y la implementación de esos instrumentos exige tiempo. Las medidas de protección técnica son particularmente costosas.[83] Los países en desarrollo deben integrar las medidas de protección desde el momento en que comienzan a desplegar Internet, pues aunque esto puede hacer aumentar inicialmente el costo de los servicios Internet, las ganancias a largo plazo que supone evitar los costos y los daños inherentes al ciberdelito son vastos y compensan con creces cualquier desembolso inicial en medidas de protección técnica y salvaguardias de red.[84]

De hecho, los riesgos que entrañan unas medidas de protección débiles pueden afectar en mayor medida a los países en desarrollo, ya que su protección y sus salvaguardias son menos estrictas.[85] La capacidad de proteger a los clientes, así como a las empresas, es un requisito fundamental no sólo para las actividades económicas normales, sino también para las que se realizan en línea o por Internet. A falta de seguridad en Internet, los países en desarrollo pueden tropezar con importantes dificultades para promover la actividad económica virtual y participar en las industrias de servicios en línea.

La adopción de medidas técnicas para promover la ciberseguridad y el establecimiento de una legislación adecuada sobre el ciberdelito son vitales tanto para los países en desarrollo como para los desarrollados. En comparación con los costos que supone injertar salvaguardias y medidas de protección en las redes informáticas en una fase tardía, es probable que si esas medidas se adoptan desde el principio resulten menos onerosas. Los países en desarrollo deben poner sus estrategias de lucha contra el ciberdelito en consonancia con las normas internacionales desde un principio.[86]

1 On the development of the Internet, see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52 – 56; The World Information Society Report 2007, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information, see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

2 Regarding the threat of attacks against computer systems integrated in cars, see: BBC News, Cars safe from computer viruses, 11.05.2005, available at: http://news.bbc.co.uk/1/hi/technology/4536307.stm.

3 See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1. *Bohn/Coroama/Langheinrich/Mattern/Rohs,* "Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications", Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf. A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[4] Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: www2007.org/workshops/paper_106.pdf.

[5] WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services (such as access to the Internet) over long distances. For more information, see: The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

[6] Under the "One Laptop per Child" initiative, inexpensive laptop computers should be distributed to children, especially those in developing countries. The project is organized by the United States-based non-profit organization OLPC. For more information, see the official OLPC website at www.laptop.org. Regarding the technology of the laptop, see Heise News, Test of the 100 dollar laptop, 09.05.2007, available at: www.heise.de/english/newsticker/news/89512.

[7] Current reports highlight that around 11 per cent of the African population has access to the Internet. See www.internetworldstats.com/stats1.htm.

[8] Regarding the impact of ICT on society, see the report Sharpening Europe's Future Through ICT – Report from the information society technologies advisory group, 2006, available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf.

[9] Regarding the related risks of attacks against e-mail systems, see the report that United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[10] Regarding the ability to block Internet-based information services by denial-of-service attacks, see below: § 2.5.5.

[11] Regarding the related difficulties of lawful interception of Voice over IP communication, see: *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[12] Related to risks and challenges see for example: *Choudhari/Banwet/Gupta*, Identifying Risk Factors in for E-governance Projects, published in Wgarwal/Ramana, Foundations of E-government, 2007, page 270 et. seq; *Ndou*, E-Government for Developing Countries, Opportunities and Challenges, DJISDC 2004, 18, page 1 et seq.

[13] See for example: *Molla*, The Impact of eReadingness on eCommerce Success in Developing Countries, 2004.

[14] See for example: *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 et seq.

[15] See for example: *Aggarwal,* Role of e-Learning in A Developing Country Like India, Proceedings of the 3rd National Conference, INDIA, Com 2009.

[16] *ITU*, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February 2009, 2009, available at: www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%20&%20Cybersecurity.pdf.

[17] Regarding the possibilities of low-cost access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in developing countries, available at: www2007.org/workshops/paper_106.pdf.

[18] Regarding the number of users of free-or-charge e-mail services, see: *Graham*, Email carriers deliver gifts of ninety features to lure, keep users, USA Today, 16.04.2008, available at: www.usatoday.com/tech/products/2008-04-15-google-gmail-webmail_N.htm. The article mentions that the four biggest webmail providers have several hundred million users – Microsoft (256 million), Yahoo (254 million), Google (91 million) and AOL (48 million). For an overview on e-mail statistics, see: *Brownlow*, e-mail and web statistics, April 2008, available at: www.email-marketing-reports.com/metrics/email-statistics.htm.

[19] www.wikipedia.org

[20] Regarding the use of free-of-charge services in criminal activities, see for example: Symantec Press Release, Symantec Reports Malicious Web Attacks Are on the Rise, 13.05.2008, available at: www.symantec.com/business/resources/articles/article.jsp?aid=20080513_symantec_reports_malicious_web_attacks_are_on_the_rise.

[21] Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information

Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

[22] See for example: Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Challenges for the European Information Society beyond 2005, page 3, available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf.

[23] Regarding the impact of ICT on the development of the society, see: *Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Yang*, Between Democracy and Development: The impact of new information technologies on civil societies in China, available at: http://programs.ssrc.org/itic/publications/civsocandgov/yangpolicyrevised.pdf; *White*, Citizen Electronic: Marx and Gilder on Information Technology and Democracy, Journal of Information Technology impact, 1999, Vol. 1, page 20, available at: www.jiti.com/v1n1/white.pdf.

[24] Regarding the extent of integration of ICTs into the daily lives and the related threats, see: § 3.2.1 below, as well as *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[25] See UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211, page 1; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, page 212; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[26] See *Suter*, A Generic National Framework For Critical Information Infrastructure Protection, 2007, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

[27] *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[28] See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, page 1; *Wilshusen*, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf.

[29] Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf. Regarding the attacks against major online companies in the United States in 2000, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

[30] The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 219 million incidents were reported in one month (November 2010). Source: www.hackerwatch.org. Regarding the necessary differentiation between port scans and possible attempts to break into a computer system, see: *Panjwani/Tan/Jarrin/Cukier*, An Experimental Evaluation to Determine if Port Scans are Precursors to an Attacks, available at: www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf.

[31] See *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[32] CRS Report for Congress on the Economic Impact of Cyber-Attacks, April 2004, page 10, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[33] See: *O'Connell*, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882.

[34] Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014.

[35] IBM survey, published 14.05.2006, available at: www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

[36] *Wilshusen*, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf. For more information on the economic impact of cybercrime, see below: § 2.4.

[37] Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[38] Cyber Security Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

[39] *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

[40] UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[41] The term "Cybersecurity" is used to summarize various activities and ITU-T Recommendation X.1205 "Overview of cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberenvironment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: *ITU*, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

[42] With regard to development related to developing countries, see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[43] See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cybersecurity, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[44] For more information, references and links, see: the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009), 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[45] For more information, see: *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

[46] See: *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, available at: www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf; see also: Pillar One of the ITU Global Cybersecurity Agenda, available at: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html. With regard to the elements of an anti-cybercrime strategy, see below: §4.

[47] See in this context: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[48] For more information on the World Summit on the Information Society (WSIS), see: www.itu.int/wsis/

[49] The WSIS Tunis Agenda for the Information Society, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

[50] The WSIS Geneva Plan of Action, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0

[51] For more information on WSIS Action Line C5: Building confidence and security in the use of ICTs, see: www.itu.int/wsis/c5/

[52] For more information on the Global Cybersecurity Agenda (GCA), see: www.itu.int/cybersecurity/gca/

[53] For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[54] For an overview of the most important instruments in the fight against cybercrime, see below: § 6.5.

[55] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

[56] See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 *et seq.*

[57] For an overview of cybercrime-related legislation and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[58] See below: § 6.2.

[59] See below: § 6.5.

[60] For an overview of the most relevant challenges in the fight against cybercrime, see below: § 3.2.

[61] One possibility to mask the identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Design, 2005.

[62] Regarding legal responses to the challenges of anonymous communication, see below: § 6.5.12 and § 6.5.13.

[63] Regarding the transnational dimension of cybercrime, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[64] Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management, 2005.

[65] Regarding the need for international cooperation in the fight against cybercrime, see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[66] See below: § 6.5.

[67] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141.

[68] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf; *Plachta*, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 *et seq.*, available at: www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

[69] See below: § 5.5. See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An

Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

70 The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Council of Europe Convention on Cybercrime, but addressed in an additional protocol. See below: § 5.2.1.

71 With regard to the different national approaches towards the criminalization of child pornography, see for example: *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

72 Regarding network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

73 The most important communication protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks, 2002; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006.

74 Regarding technical standardization, see: OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: www.itu.int/dms_pub/itu-t/oth/06/15/T061500000A0015PDFE.pdf. Regarding the importance of single technical as well as single legal standards, see: *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

75 Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189), available at: www.conventions.coe.int.

76 Since parties participating in the negotiation could not agree on a common position on the criminalization of the dissemination of xenophobic material, provisions related to this topic were integrated into a First Protocol to the Council of Europe Convention on Cybercrime.

77 See: *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.,* available at: http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

78 This was discussed for example within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: www.juriscom.net/en/uni/doc/yahoo/poullet.htm; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

79 A possibility to circumvent geo-targeting strategies is the use of proxy servers that are located abroad.

80 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

81 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

82 See below: § 4.

83 See, with regard to the costs of technical protection measures required to fight against spam: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at www.oecd.org/dataoecd/5/47/34935342.pdf.

84 Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

85 One example is spam. The term "spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: "ITU Survey on Anti-Spam Legislation Worldwide 2005", page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialized countries. See: OECD, Spam Issue in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

86 For more details about the elements of an anti-cybercrime strategy, see below: § 4.

2 El fenómeno de la ciberdelincuencia

2.1 Definiciones

Bibliografía (seleccionada): *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et seq., *Chawki*, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Forst*, Cybercrime: Appellate Court Interpretations, 1999, page 1; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No.2, page 144; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at:

www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

La mayoría de los informes, guías y publicaciones sobre la ciberdelincuencia comienzan definiendo los términos[87] "delito informático" y "ciberdelincuencia".[88] En este contexto, la definición precisa de estos dos términos se ha enfocado de diversas maneras durante las últimas décadas.[89] Antes de pasar a describir el debate y evaluar esos enfoques, resulta útil determinar la relación que existe entre la "ciberdelincuencia" y los "delitos informáticos". [90] Sin entrar en detalles por ahora, cabe señalar que el término "ciberdelincuencia" es más restrictivo que el de delito informático, dado que implica una red informática. Los delitos informáticos comprenden incluso a los que afecta a sistemas informáticos autónomos, que no están conectados a una red.

En el taller que tuvo lugar con ocasión del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente se elaboraron dos definiciones:[91] Ciberdelincuencia en sentido estricto (delito informático) comprende cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y de los datos que éstos procesan. En sentido general, ciberdelincuencia (delitos relacionados con los computadores) comprende cualquier comportamiento ilícito cometido por medio de un sistema informático o una red de computadores, o relacionado con éstos, incluidos delitos tales como la posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadores.[92]

Una definición bastante común de ciberdelincuencia es cualquier actividad delictiva en la que se utilizan como herramienta computadores o redes, o en la que éstos son las víctimas de la misma o el medio desde donde se efectúa dicha actividad delictiva.[93] Esta definición general plantea diversas dificultades. Abarca, por ejemplo, delitos tradicionales tales como el homicidio, si acaso el autor utiliza un teclado para golpear y matar a la víctima. En el Artículo 1.1 del Convenio Internacional para la Protección contra la Ciberdelincuencia y el Ciberterrorismo (el "Proyecto Stanford") [94] se da otra definición general en el que por ciberdelincuencia se refiere a los actos relativos a los cibersistemas.[95]

Algunas definiciones tratan de integrar los objetivos o intenciones y de definir el término con mayor precisión[96], como "la actividad realizada mediante un computador que es *ilícita* o que algunas Partes *consideran ilícita* y que puede realizarse *a través de las redes electrónicas mundiales*".[97] Estas definiciones más detalladas excluyen los casos en los que se utilizan herramientas físicas para cometer delitos ordinarios, pero corren el riesgo de excluir delitos que se consideran ciberdelincuencia en ciertos acuerdos internacionales, tales como la Legislación Modelo de la Commonwealth sobre la delincuencia informática y relacionada con los computadores o el Convenio del Consejo de Europa sobre la Ciberdelincuencia.[98] Por

ejemplo, una persona que produce software pernicioso para dispositivos USB[99] que destruye los datos del computador cuando se le conecta el dispositivo está cometiendo un delito definido en el Artículo 4 del Convenio del Consejo de Europa sobre la Ciberdelincuencia.[100] Ahora bien, el acto de borrar datos utilizando un dispositivo físico que copia código pernicioso, al efectuarse a través de las redes electrónicas mundiales, no quedaría comprendido por la limitada definición de ciberdelito anterior. Este acto sólo podría calificarse como ciberdelito con una definición más general de éste, que incluya actos como la manipulación ilícita de datos.

Los diversos enfoques y los problemas que entrañan, hacen que las definiciones de los términos "delito informático" y "ciberdelito" presentan dificultades considerables.[101] El término "ciberdelito" se utiliza para describir una gran variedad de delitos en particular los informáticos y de red tradicionales. Dado que la naturaleza de estos delitos son muy distintas, no existe un único criterio que comprenda todos los actos mencionados en los diferentes enfoques jurídicos regionales e internacionales adoptados para abordar este asunto y que a su vez excluya los delitos que se cometen exclusivamente por medios físicos. El hecho de que no haya una única definición de "ciberdelito" no es importante siempre y cuando el término no se utilice como término jurídico.[102] En lugar de referirse a una definición, en los capítulos siguientes se enfoca la cuestión desde una perspectivo tipológica.

2.2 Tipología del ciberdelito

Bibliografía: Big Data for Development: Challenges & Opportunities, UN Global Pulse, 2012; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf; *Hartmann/Steup,* The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment, published in Podins/Stinissen/Maybaum, 5th International Conference on Cyber Conflicts, 2013; *Kim/Wampler/Goppert/Hwang/Aldridge,* Cyber attack vulnerabilities analysis for unmanned aerial vehicles, American Institute of Aeronautics and Astronautics, 2012; *Sircar*, Big Data: Countering Tomorrow's Challenges, Infosys Labs Briefings, Vol. 11, No. 1, 2013; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004.

El término "ciberdelito" abarca muy diversos tipos de delitos.[103] Los delitos reconocidos comprenden una gran variedad de infracciones, lo que dificulta su tipología o clasificación.[104] Un sistema de clasificación interesante es el definido por el Convenio sobre la Ciberdelincuencia[105], en el que se distinguen cuatro tipos diferentes de infracciones [106]:

1. delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos;[107]
2. delitos informáticos;[108]
3. delitos relacionados con el contenido;[109] y
4. delitos relacionados con el derecho de autor.[110]

Esta clasificación no es totalmente coherente, ya que no se basa en un sólo criterio para diferenciar las categorías. Tres de las categorías se refieren al objeto de la protección jurídica: "delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" [111]; delitos relacionados con el contenido[112]; y delitos relacionados con el derecho de autor.[113] La cuarta categoría "delitos informáticos"[114] no se refiere al objeto de la protección jurídica sino al método. Esta incoherencia genera cierta coincidencia entre las categorías.

Por otra parte, algunos términos que se utilizan para describir actos criminales ("ciberterrorismo"[115] o "peska" ("phishing"[116])) quedan comprendidos por varias categorías. No obstante, las categorías descritas en el Convenio sobre la Ciberdelincuencia resultan útiles para debatir acerca del fenómeno de la ciberdelincuencia.

2.3 Evolución de los delitos informáticos y la ciberdelincuencia

La utilización de la tecnología de la información con fines delictivos y la necesaria reacción jurídica son cuestiones que se debaten desde los albores de esta tecnología. En los últimos 50 años se han adoptado diversas soluciones en los planos nacional y regional. Una de las razones por las que el tema sigue siendo desafiante es la constante evolución técnica, así como la variedad y diversidad de los métodos que se emplean para cometer los delitos.

2.3.1 El decenio de 1960

En el decenio de 1960, la aparición de los sistemas informáticos basados en el transistor, que eran más pequeños y económicos que las máquinas basadas en tubos de vacío, dio lugar a un aumento en la utilización de tecnología informática.[117] En esta primera fase, los delitos consistían en causar daños físicos a los sistemas informáticos y a los datos almacenados.[118] Se informó sobre este tipo de incidentes en, por ejemplo, Canadá, donde en 1969 una revuelta estudiantil causó un incendio que destruyó los datos informatizados en la universidad.[119] A mediados del decenio de 1960, en Estados Unidos se inició un debate sobre la creación de una entidad de almacenamiento de datos de todos los ministerios.[120] En este contexto, se deliberó acerca de los delitos contra bases de datos[121] y los riesgos que entrañan para la privacidad[122].[123]

2.3.2 El decenio de 1970

En el decenio de 1970 siguió aumentando la utilización de los sistemas y datos informáticos.[124] A finales de la década, se estimó que el número de computadores centrales en Estados Unidos ascendía a 100 000.[125] Con la caída de los precios, se produjo una generalización de la tecnología informática tanto en la administración y las empresas, como en el público. El decenio de 1970 se caracterizó por una transición desde los delitos tradicionales contra los sistemas informáticos[126] que predominaba en el decenio de 1960, hacia nuevas formas de delincuencia.[127] Si bien los daños físicos siguieron siendo una forma importante de delincuencia contra los sistemas informáticos,[128] aparecieron nuevos tipos de delitos informáticos, en particular la utilización ilícita de sistemas informáticos[129] y la alteración[130] de datos electrónicos.[131] La transición de las transacciones manuales a las informáticas dio lugar a una nueva forma de delito, a saber, el fraude informático.[132] Ya en esas fechas el fraude informático causó pérdidas de varios millones de dólares.[133] El fraude informático fue, en particular, un verdadero desafío y las fuerzas de seguridad tuvieron que investigar un número creciente de casos.[134] Las dificultades[135] que surgieron al aplicar la legislación en materia de delitos informáticos abrieron el debate acerca de las soluciones jurídicas en diferentes partes del mundo.[136] En Estados Unidos se deliberó un proyecto de ley concebido concretamente para la ciberdelincuencia.[137] La Interpol examinó este fenómeno y las posibles medidas jurídicas.[138]

2.3.3 El decenio de 1980

En el decenio de 1980 se popularizaron los computadores personales. De este modo, aumentó el número de sistemas informáticos y, por ende, el número de posibles objetivos de ataque. Por primera vez los objetivos eran también una amplia variedad de infraestructura esencial.[139] Uno de los efectos secundarios de la proliferación de sistemas informáticos fue un aumento del interés en el software, lo que dio lugar a la aparición de las primeras formas de piratería informática y de delitos relacionados con las patentes.[140] La interconexión de sistemas informáticos dio lugar a nuevos tipos de delitos.[141] Las redes permitieron a los delincuentes entrar en sistemas informáticos sin estar presentes en el lugar del delito.[142] Además, la posibilidad de distribuir software a través de redes permitió a los delincuentes divulgar software maligno y el número de virus informáticos descubiertos fue en aumento.[143] Los países iniciaron un proceso de actualización de su legislación para adaptarse al nuevo y evolutivo entorno de delincuencia.[144] Las organizaciones internacionales también participaron en ese proceso. La OCDE[145] y el Consejo de Europa[146] crearon comisiones de estudio para analizar este fenómeno y evaluar las posibilidades de respuesta jurídica.

2.3.4 El decenio de 1990

La aparición de la interfaz gráfica ("WWW") en el decenio de 1990 y su consecuente rápido crecimiento del número de internautas dio lugar a nuevos problemas. La información puesta a disposición legalmente en

un país era accesible en el mundo entero – incluso en países donde la publicación de esa información estaba penalizada.[147] Otro problema relacionado con los servicios en línea que dificultaba especialmente la investigación de delitos transnacionales era la velocidad del intercambio de información.[148] Por último, la distribución de pornografía infantil pasó del intercambio físico de libros y cintas de vídeo a la distribución en línea mediante sitios web y servicios Internet.[149] Internet transformó los delitos informáticos, que eran de ámbito local, en delitos electrónicos de alcance internacional. Por ese motivo, la comunidad internacional afrontó la cuestión con mayor intensidad. Como ejemplos cabe citar la Resolución 45/121 adoptada por la Asamblea General de las Naciones Unidas en 1990[150] y el manual para la prevención y el control de delitos informáticos publicado en 1994.[151]

2.3.5 El siglo XXI

Al igual que en la década precedente, en el siglo XXI aparecieron nuevas tendencias en los delitos informáticos y la ciberdelincuencia. En la primera década del nuevo milenio predominaron métodos nuevos y muy sofisticados para cometer delitos, tales como ataques de "*peska*" (*phishing*),[152] y "redes zombi",[153] y la aparición de tecnologías que son más difíciles de perseguir jurídicamente e investigar, por ejemplo la comunicación de "voz por IP (VoIP)"[154] y la "computación en nube".[155] No sólo han cambiado los métodos, sino también el impacto. El número de delitos aumentó a medida que los delincuentes comenzaron a automatizar los ataques. Los países y las organizaciones regionales e internacionales han reaccionado a las dificultades crecientes y han conferido gran prioridad a la ciberdelincuencia. Es muy probable que, debido a nuevos adelantos, como los "grandes volúmenes de datos" (*big data*) [156], los "drones" [157] y los "dispositivos corporales" (*wearables*), se atribuya aún más importancia en el futuro a la acción de los delincuentes.

2.4 Alcance e impacto de la ciberdelincuencia

Bibliografía (seleccionada): Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Hyde-Bales/Morris/Charlton, The police recording of computer crime, UK Home Office Development and Practice Report, 2004; Maguire in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 et seq., available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf; Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Osborne/Wernicke, Introduction to Crime Analysis, 2003, page 1 et seq. available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

Los sectores académicos y los legisladores pueden emplear las estadísticas sobre delincuencia en sus deliberaciones y para el ulterior proceso de adopción de decisiones.[158] Por otra parte, el acceso a información fidedigna sobre el verdadero alcance de la ciberdelincuencia permitiría a las entidades encargadas de hacer cumplir la ley mejorar las estrategias contra la ciberdelincuencia , disuadir los posibles ataques y promulgar una legislación más adecuada y eficaz. Ahora bien, resulta difícil cuantificar la incidencia de la ciberdelincuencia en la sociedad a partir del número de delitos cometidos en un determinado periodo de tiempo.[159] Por lo general, estos datos se obtiene de estadísticas y estudios sobre delitos,[160] pero estas dos fuentes resultan problemáticas cuando se quieren utilizar para formular recomendaciones de política.

2.4.1 Estadísticas sobre delincuencia

Las cifras que se presentan a continuación se han obtenido de estadísticas nacionales sobre delincuencia. Como se indica más adelante, no se pretende que sean representativas del desarrollo mundial de la ciberdelincuencia ni de la verdadera amplitud de la misma en el plano nacional, por lo que presenta exclusivamente a título informativo sobre el país.

- El centro de reclamaciones de Internet de los Estados Unidos informa que, en 2013, se ha producido un aumento del 48,8 por ciento en las pérdidas consignadas respecto de 2012.[161]
- La Oficina de Estadísticas de Delincuencia de Alemania indica que el número general de delitos relacionados con Internet ha aumentado en 2013 un 12,2 por ciento respecto de 2012.[162]

No está claro cuán representativas son las estadísticas y en qué medido proporcionan información fiable sobre la amplitud de la delincuencia.[163] La determinación de la amenaza global que supone los ciberdelitos a partir de estadísticas sobre ciberdelincuencia plantea diversas dificultades.[164]

En primer lugar, las estadísticas sobre delincuencia se elaboran generalmente a escala nacional por lo que no ponen de manifiesto la dimensión internacional de este problema. Aunque teóricamente sea posible conjugar los datos disponibles, el resultado no generaría información fiable debido a las diferencias en la legislación y la recopilación de datos.[165] Para poder reunir y comparar estadísticas nacionales sobre delincuencia se requiere cierto grado de compatibilidad[166] de la que se carece en el ámbito de la ciberdelincuencia. Aun cuando se recaben datos sobre ciberdelitos, éstos no siempre figuran en cifras separadas.[167] Además, las estadísticas sólo indican los delitos detectados y denunciados.[168] Suscita preocupación el número de casos no denunciados, especialmente en el ámbito de la ciberdelincuencia.[169] Las empresas temen una publicidad negativa que pueda dañar su reputación.[170] Si una empresa anuncia que piratas informáticos han accedido a su servidor, puede perder la confianza de sus clientes. El coste total y las consecuencias podrían ser mayores que las pérdidas causadas por el ataque de los piratas. Por otra parte, si no se les denuncia ni enjuicia, los delincuentes seguirán actuando. Las víctimas no confían en que las fuerzas de seguridad puedan identificar a los delincuentes.[171] Al comparar el gran número de ciberdelitos con el reducido número de investigaciones con resultados, las víctimas pierden el interés en denunciar los delitos.[172] Con la automatización de los ataques, que permite a los ciberdelincuentes adoptar la estrategia de obtener grandes beneficios a partir de numerosos ataques destinados a obtener pequeñas sumas (por ejemplo, el caso de estafa de pago por adelantado[173]), la posible incidencia de delitos no denunciados podría ser considerable. Las víctimas optan por no iniciar los prolongados procedimientos de denuncia por sumas tan pequeñas. Los casos que se denuncian suelen ser los que implican sumas muy importantes.[174]

En resumen, la información estadística es útil para poner de manifiesto la creciente y constante importancia de esta cuestión, y resulta necesaria para subrayar que una de las principales dificultades relacionadas con la ciberdelincuencia es la falta de información fiable sobre la magnitud del problema, así como sobre los arrestos, enjuiciamientos y condenas. Como ya se ha indicado, las estadísticas sobre delincuencia no suelen estar desglosadas por tipo de delito, y las estadísticas disponibles sobre la incidencia de la ciberdelincuencia son en general incapaces de suministrar información fiable sobre la amplitud o magnitud de los delitos a un nivel suficiente para los legisladores.[175] Sin dichos datos, resulta difícil cuantificar el impacto de la ciberdelincuencia en la sociedad y elaborar estrategias para resolver este problema.[176] No obstante, las estadísticas pueden servir para determinar las tendencias, por comparación de los resultados a lo largo de varios años, y servir de orientación sobre el procedimiento de comunicación de ciberdelitos.[177]

2.4.2 Estudios

Las cifras que figuran a continuación se han obtenido de diferentes estudios. Como se describe más adelante, no son necesariamente representativas y, por consiguiente, los resultados se presentan exclusivamente a título informativo.

- La información sobre tarjetas de crédito y cuentas bancarias es la más popular anunciada en los servicios de economía sumergida. Los precios oscilan entre 0,85- 30 USD (información por tarjeta de crédito) y 15-850 USD (información por cuenta bancaria).[178]
- En 2007, el fraude por subastas fue uno de los principales timos por Internet en Estados Unidos, con pérdidas en promedio de más de 1 000 USD por caso.[179]
- En 2005, las pérdidas debidas a delitos relacionados con la identidad en Estados Unidos ascendieron a 56 600 millones USD.[180]

- En Irlanda el coste financiero y personal de la ciberdelincuencia varía considerablemente de un incidente a otro, generando en conjunto un coste de más de 250 000 €.[181]
- Una sola empresa de seguridad informática creó más de 450 000 nuevas firmas de código maligno en sólo un trimestre.[182]
- La cuarta parte de todas las empresas que respondieron a un cuestionario en 2010 informaron de pérdidas operativas debidas a la ciberdelincuencia.[183]
- Los profesionales de la seguridad informan que entre 2004 y 2008 se ha producido una reducción de ataques de denegación del servicio y de virus informáticos.[184]
- En 2009, los países que denunciaron mayor número de actividades delictivas fueron Estados Unidos, China, Brasil, Alemania e India.[185]
- En 2014, las pérdidas anuales debidas al ciberdelito en el mundo entero fueron estimadas entre 375.000 y 575.000 millones USD. [186]
- Dada la estimación de una pérdida equivalente al 1,6 por ciento del PIB, Alemania es el país más afectado por el ciberdelito.[187] En los Estados Unidos, las pérdidas se calculan en un 0,64 por ciento del PIB; en Brasil, del 0,32 por ciento y en Kenya, del 0,01 por ciento.[188]
- El costo medio de los robos de datos asciende a 136 USD por persona.[189] A raíz de un simple ataque pirata causado a la base de datos de un cliente, la empresa Sony afrontó costos directos por un valor de 170.000.000 USD.[190]

La utilización de estos estudios para determinar la amplitud e incidencia de la ciberdelincuencia suscita cierta inquietud.

Es muy difícil proporcionar estimaciones fiables de las pérdidas financieras. Algunas fuentes calculan que las pérdidas para empresas e instituciones en Estados Unidos[191] debidas a la ciberdelincuencia pueden alcanzar los 67 000 millones USD en un solo año; sin embargo, no está claro si se puede justificar la extrapolación de los resultados de este estudio por muestreo.[192] Las críticas a la metodología se aplican no solamente a las pérdidas, sino también al número de delitos reconocidos.

Otra dificultad relacionada con la información estadística es el hecho de que muy a menudo se cita sin cesar información poco fiable o imposible de verificar. Un ejemplo es la información estadística sobre los aspectos comerciales de la pornografía infantil en Internet. Varios análisis citan, por ejemplo, que según los cálculos de TopTenReviews la pornografía infantil en Internet genera unos 2 500 millones USD al año en todo el mundo.[193] Sin embargo, TopTenReviews no ha facilitado información sobre cómo ha llevado a cabo esa investigación. Habida cuenta de que TopTenReview afirma en su sitio web que la empresa "*ofrece la información que usted necesita para comprar de manera inteligente. Recomendamos el mejor producto en cada categoría. Nuestros gráficos comparativos, noticias, artículos y vídeos simplifican el proceso de compra para el consumidor*", utilizar dichos datos puede ser motivo de profundas preocupaciones. Otro ejemplo de cifras que se citan sin disponer de una referencia fiable fue descubierto por el Wall Street Journal en 2006.[194] Al investigar un cita en la que se afirma que la pornografía infantil es un negocio de miles de millones de dólares (20 000 millones al año), el periodista comunicó que dos de los principales documentos que contienen información sobre los ingresos de 3.000 a 20.000 millones USD –una publicación de NCMEC y otra del Consejo de Europa– se refieren a instituciones que no han confirmado las cifras.

Dado que los estudios suelen contar únicamente los incidentes sin proporcionar mayor información o detalles, es difícil sacar conclusiones sobre las tendencias. Como ejemplo puede citarse el estudio sobre ciberdelitos y seguridad informática de 2007 realizada por el CSI [195] de Estados Unidos, en la que se analiza la tendencia del número de delitos informáticos cometidos y otras tendencias.[196] El estudio se basa en las respuestas de 494 profesionales en el campo de la seguridad informática de empresas, organismos gubernamentales e instituciones financieras del país.[197] En el estudio se recoge el número de delitos notificados por los encuestados entre 2000 y 2007. Se observa que desde 2001 ha disminuido la proporción de encuestados que han experimentado y reconocido ataques de virus o accesos no autorizados a la información (o irrupción en el sistema). En el estudio no se explica las razones de esta disminución del número de delitos reconocidos.

Las estadísticas sobre ciberdelitos no proporcionan información fiable sobre la escala o magnitud de los delitos.[198] . Debido a la incertidumbre acerca de cuál es la proporción de delitos que denuncian los afectados[199], y al hecho de que no se ha encontrado una explicación a la reducción del número de ciberdelitos registrados, estas estadísticas están abiertas a interpretación. Por el momento, no existen pruebas suficientes para predecir la tendencia y la evolución en el futuro.

2.5 Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Bibliografía (seleccionada): Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; Hackworth, Spyware, Cybercrime & Security, IIA-4; Kabay, A Brief History of Computer Crime: An Introduction for Students, 2008; Ollmann, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; Paxson, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; Sieber, Council of Europe Organised Crime Report 2004; Szor, The Art of Computer Virus Research and Defence, 2005; Urbas/Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.250; Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 et seq.

Los delitos comprendidos en esta categoría están dirigidos contra (al menos) uno de los tres principios jurídicos siguientes: confidencialidad, integridad y disponibilidad. A diferencia de los delitos contemplados por la legislación penal desde hace siglos (por ejemplo, robo u homicidio), la integración de los delitos informáticos en la legislación es relativamente reciente, dado que los sistemas y datos informáticos aparecieron hace apenas sesenta años.[200] Para poder interponer una acción judicial contra estos actos es preciso que estén contemplados en las disposiciones del derecho penal no sólo como elementos tangibles y documentos físicos protegidos contra manipulación, sino también para incluir estos nuevos principios jurídicos.[201] En esta sección se expone una descripción general de los delitos de esta categoría que se producen con mayor frecuencia.

2.5.1 Acceso ilícito (piratería de sistemas y programas)[202]

Los delitos clasificados como "piratería" se refieren al acceso ilícito a un sistema informático[203], uno de los delitos más antiguos en este campo.[204] Con el advenimiento de las redes de computadores (especialmente Internet), este delito se ha convertido en un fenómeno popular.[205] Los objetivos más conocidos de los ataques de piratería son la Administración Nacional de Aeronáutica y del Espacio (NASA), las Fuerzas Aéreas de Estados Unidos, el Pentágono, Yahoo, Google, Ebay y el Gobierno de Alemania.[206]

Ejemplos de delitos de piratería son la irrupción en sitios web protegidos con contraseña [207] y la burla de la protección de contraseña en un computador. Pero los actos relacionados con la "piratería" también comprenden actos preparatorios tales como utilización de equipos o programas para obtener una contraseña e irrumpir en el sistema informático[208], Creación de sitios web "falsos" para lograr que el usuario revele su contraseña[209] y la instalación por hardware o software de interceptores de teclado ("keyloggers") que registran cada una de las teclas pulsadas y, por consiguiente, todas las contraseñas que se utilizan en el computador y/o dispositivo.[210]

Los motivos de los delincuentes son diversos. Algunos se limitan a burlar las medidas de seguridad para probar sus capacidades.[211] Otros actúan por motivos políticos (conocido como piratería activista o "hacktivism"[212]) – como es el caso del incidente reciente acaecido en el sitio web de las Naciones Unidas.[213] En muchos casos, el móvil del delincuente no se limita al acceso ilícito al sistema informático, sino que éste

es un medio para perpetrar otros delitos, como el espionaje o la manipulación de datos y los ataques de denegación del servicio.[214] En muchos casos el acceso ilícito al sistema informático, aunque esencial, es tan solo el primer paso.[215]

Muchos analistas reconocen un aumento en el número de intentos de obtener acceso ilícito a sistemas informáticos: sólo en el mes de agosto de 2007 se registraron más de 250 millones de incidentes en todo el mundo.[216] Este aumento del número de ataques de piratería se debe a tres factores principales: la protección inadecuada e incompleta de los sistemas informáticos, la aparición de herramientas informáticas que automatizan los ataques y la creciente función de los computadores privados en las estrategias de piratería.

Protección inadecuada e incompleta de los sistemas informáticos:

Cientos de millones de computadores están conectados a Internet, muchos de los cuales carecen de la protección adecuada contra el acceso ilícito.[217] Según un análisis realizado por la Universidad de Maryland todo sistema informático sin protección que se conecte a Internet es probable que sea el objeto de un ataque en menos de un minuto.[218] Si bien la instalación de medidas preventivas puede disminuir el riesgo, las medidas técnicas de protección no pueden en ningún caso detener completamente los ataques, dado que incluso los sistemas informáticos bien protegidos han sido objeto de ataques satisfactorios.[219]

Aparición de herramientas informáticas que automatizan los ataques:

Últimamente se ha comenzado a utilizar herramientas software que permiten automatizar los ataques.[220] Con la ayuda de programas instalados previamente, un mismo pirata puede atacar miles de computadoras en un sólo día utilizando sólo un computador.[221] Si además el pirata tiene acceso a más computadores por ejemplo, una red zombi [222] – puede atacar a mayor escala. Dado que la mayoría de estas herramientas informáticas utilizan métodos de ataque preprogramados, no todos los ataques resultan exitosos. Los usuarios que actualizan con regularidad sus sistemas operativos y aplicaciones informáticas reducen el riesgo de convertirse en víctimas de estos ataques generalizados, ya que las empresas que elaboran el software de protección analizan las herramientas de ataque y se preparan para contrarrestarlas.

Los ataques de gran resonancia suelen ser ataques concebidos para tal fin, y a menudo su éxito no radica en métodos muy sofisticados, sino en el número de sistemas informáticos atacados. Las herramientas para efectuar estos ataques se encuentran fácilmente disponibles en Internet[223] – algunas son gratuitas, pero las más eficientes cuestan fácilmente del orden de miles de USD.[224] Como ejemplo puede citarse una herramienta de pirateo que permite al delincuente definir una gama de direcciones IP (por ejemplo, de 111.2.0.0 a 111.9.253.253) que el software explora para encontrar puertos no protegidos de todos los computadores que utilizan una de las direcciones IP definidas.[225]

La creciente función de los computadores privados en las estrategias de piratería:

El acceso a un sistema informático no suele ser la principal motivación de los ataques.[226] Dado que los computadores de las empresas están por lo general mejor protegidos que los privados, es más difícil atacar a los primeros utilizando herramientas informáticas configuradas de antemano.[227] En los últimos años los delincuentes han concentrado sus ataques en los computadores privados, muchos de los cuales no están adecuadamente protegidos. Además, los computadores privados suelen contener información delicada (por ejemplo, datos bancarios o de tarjetas de crédito). Otra razón por la que atacan a los computadores privados es que, si el ataque resulta satisfactorio, los delincuentes pueden incluir dicho computador en su red zombi y, por ende, utilizarlo para otras actividades delictivas.[228]

El acceso ilícito a sistemas informáticos puede considerarse equivalente al acceso ilícito a un edificio, que en muchos países es un delito.[229] Del análisis de las diferentes formas de penalizar el acceso a computadores se desprende que en algunos casos las disposiciones promulgadas confunden el acceso ilícito con los delitos que se cometen después o se trata de limitar la penalización del acceso ilícito a los casos muy graves únicamente. Algunas disposiciones consideran delito el acceso inicial, mientras que otras lo limitan exclusivamente a los casos en que los sistemas accedidos están protegidos por medidas de seguridad [230], el

autor tiene malas intenciones [231] o se obtienen, modifican o dañan datos. Otros sistemas jurídicos no consideran delito el mero acceso, sino que se concentran en los delitos derivados.[232]

En un análisis más reciente se observa la tendencia a ataques más sofisticados y selectivos, aparte de los ataques más generales y a gran escala que han dominado en decenios anteriores.[233] En tanto que los ataques a gran escala responden a un criterio oportunista y pueden llevarse fácilmente a cabo, los ataques selectivos exigirán mayor energía por parte del delincuente pero serán notablemente más eficaces y dañinos[234] para la víctima.[235]

2.5.2 Adquisición ilícita de datos (Espionaje de datos)

Los sistemas informáticos contienen con frecuencia información confidencial. Si están conectados a Internet, los delincuentes pueden tratar de obtener acceso a dicha información por Internet desde prácticamente cualquier lugar del planeta.[236] Internet se utiliza cada vez más para obtener secretos comerciales.[237] El valor de la información confidencial y la capacidad de acceder a la misma a distancia hacen que el espionaje de datos resulte muy interesante. En el decenio de 1980, varios piratas alemanes consiguieron entran en los sistemas informáticos militares y del gobierno de Estados Unidos, y vendieron la información así obtenida a agentes de otro país.[238]

Los delincuentes recurren a diversas técnicas para acceder a los computadores de sus víctimas[239], entre las que cabe citar software para explorar los puertos desprotegidos [240] o para burlar las medidas de protección,[241] e ""ingeniería social".[242] Resulta especialmente interesante este último método, a saber, la "ingeniería social", por su carácter no técnico por cuanto se refiere a una intromisión basada en la interacción humana y que a menudo consiste en un ardid para engañar a las personas con el fin de obviar los procedimientos normales de seguridad.[243] En el contexto de acceso ilícito consiste en la manipulación de seres humanos con la finalidad de obtener acceso a sistemas informáticos.[244] La ingeniería social en general suele ser un método muy eficaz, dado que el punto débil de la seguridad informática reside en los usuarios del sistema. Por ejemplo, la *peska* de datos ("phishing") se ha convertido en un delito esencial en el ciberespacio [245] y consiste en tratar de obtener por fraude información confidencial (por ejemplo, contraseñas) haciéndose pasar por una persona o empresa de confianza (por ejemplo, una institución financiera) a través de una comunicación electrónica de apariencia oficial.

Si bien es cierto que la vulnerabilidad humana de los usuarios es una fuente de peligro de estafas, también existen soluciones. Los usuarios con conocimientos informáticos no son presa fácil de los delincuentes. La educación de los usuarios es una parte esencial de toda estrategia contra el ciberdelito.[246] Por otra parte, pueden adoptarse medidas técnicas para impedir el acceso ilícito. La OCDE subraya la importancia que reviste la criptografía para los usuarios, por cuanto aumenta la protección de los datos.[247] Si la persona u organización decide almacenar la información con los mecanismos de protección adecuados, la protección criptográfica puede resultarle más eficiente que la protección física.[248] El éxito de los delincuentes en la obtención de información confidencial suele radicar en la ausencia de mecanismos de protección. Dado que la información importante se almacena cada vez más en sistemas informáticos, es fundamental evaluar si las medidas de protección técnicas que aplican los usuarios son adecuadas, o si los legisladores necesitas establecer protección adicional para penalizar el espionaje de datos.[249]

Aunque por lo general los delincuentes buscan secretos comerciales, cada vez más dirigen sus ataques a computadores privados.[250] Los usuarios privados suelen guardar información sobre sus cuentas bancarias y tarjetas de crédito en sus computadores.[251] Los delincuentes pueden utilizar esta información para sus propios fines (por ejemplo, los datos bancarios para efectuar transferencias monetarias) o para venderla a terceros.[252] Por ejemplo, el precio de venta de datos de una tarjeta de crédito puede alcanzar los 60 USD.[253] En principio puede parecer sorprendente que los piratas se dediquen a los computadores privados cuando los beneficios que pueden obtener de secretos comerciales son por lo general muy superiores a los que pueden obtener de, por ejemplo, obtener o vender información de una sola tarjeta de crédito. Sin embargo, como los computadores privados suelen estar menos protegidos, el espionaje de datos en computadores privados es probable que resulte en última instancia más rentable.

Existen dos métodos para obtener información. Los autores pueden acceder a sistemas informáticos o a un dispositivo de almacenamiento y extraer la información; o tratar de manipular a los usuarios para que revelen la información o los códigos de acceso que les permitan acceder a la información ("peska").

Los delincuentes suelen utilizar herramientas informáticas instaladas en los computadores de las víctimas o software pernicioso denominados programas espía (spyware) para transmitirse datos.[254] En los últimos años se han detectado diversos tipos de programas espía, por ejemplo los interceptores de teclado (keyloggers).[255] Estos interceptores son herramientas informáticas que registran cada una de las teclas pulsadas en el teclado del computador infectado.[256] Algunos de éstos envían toda la información registrada al delincuente en cuanto el computador se conecta a Internet. Otros realizan una clasificación y un análisis inicial de los datos registrados (por ejemplo, para encontrar información relativa a tarjetas de crédito[257]) con el fin de transmitir únicamente los datos más importantes. También existen dispositivos físicos similares que se conectan entre el teclado y el sistema informático para registrar las teclas pulsadas. Obviamente los dispositivos físicos son más difíciles de instalar y detectar, dado que requieren el acceso físico al sistema informático.[258] Por ese motivo, los programas antivirus y antiespías clásicos son en general incapaces de identificarlos.[259]

Aparte del acceso a los sistemas informáticos, los delincuentes pueden obtener datos mediante la manipulación del usuario. Últimamente los delincuentes se han ingeniado timos muy eficaces para obtener información confidencial (por ejemplo, datos bancarios y de tarjetas de crédito) que consisten en manipular al usuario mediante técnicas de ingeniería social.[260] La "peska" se ha convertido recientemente en uno de los crímenes más importantes en el ciberespacio.[261] El término "*peska*" se utiliza para describir un tipo de delito que se caracteriza por tratar de obtener información confidencial de manera fraudulenta, por ejemplo conseguir contraseñas haciéndose pasar por una persona o empresa de confianza (por ejemplo, una institución financiera) en una comunicación informática de apariencia oficial.[262]

Adelantos como los "*big data*", que permiten a las empresas recopilar grandes cantidades de datos con objeto de realizar análisis más elaborados, han modificado la importancia del robo de datos en el panorama de las amenazas. Si los delincuentes acceden a grandes bases de datos con datos personales de los clientes, el mero robo de datos puede entrañar costos considerables para la empresa afectada, aún cuando no los utilicen para cometer otros delitos.[263] El costo medio de los robos de datos asciende a 136 USD por persona.[264] A raíz de un simple ataque pirata causado a la base de datos de un cliente, la empresa Sony afrontó costos directos por un valor de 170.000.000 USD.[265]

En un estudio publicado en 2014 se indica que los datos disponibles en el cibermercado negro, obtenidos por medio del robo de datos, contemplan credenciales de hasta 360 millones de cuentas.[266]

2.5.3 Intervención ilícita

Los delincuentes pueden intervenir las comunicaciones entre usuarios [267] (como mensajes de correo electrónico) o interceptar transferencias de datos (cuando los usuarios suben datos a los servidores web o acceden a medios de almacenamiento externos por la web[268]) con el fin de registrar el intercambio de información. Los delincuentes pueden atacar cualquier infraestructura de comunicaciones (por ejemplo, líneas fijas o inalámbricas) y cualquier servicio Internet (por ejemplo, correo electrónico, charlas o comunicaciones VoIP[269]).

La mayoría de los procesos de transferencia de datos entre proveedores de infraestructura de Internet o proveedores de servicios Internet están debidamente protegidos y son difíciles de intervenir.[270] Sin embargo, los delincuentes buscan los puntos débiles del sistema. Las tecnologías inalámbricas gozan de mayor popularidad y anteriormente eran vulnerables.[271] Hoy en día, muchos hoteles, restaurantes y bares ofrecen acceso Internet a sus clientes a través de puntos de acceso inalámbrico. Ahora bien, las señales en el intercambio de datos entre el computador y el punto de acceso pueden recibirse dentro de un radio de hasta 100 metros.[272] Los delincuentes que desean pinchar las comunicaciones de datos pueden hacerlo desde cualquier lugar situado en el interior de dicho radio (Figura 3). Aun cuando las comunicaciones inalámbricas estén cifradas, los delincuentes son capaces de descifrarlas y guardar los correspondientes datos.[273]

Para conseguir acceder a la información confidencial, algunos delincuentes configuran puntos de acceso cerca de los lugares donde hay gran demanda de acceso inalámbrico [274] (por ejemplo, cerca de bares y hoteles). Suelen elegir el nombre de la estación de tal forma que los usuarios que buscan un punto de acceso a Internet acaben seleccionando probablemente el punto de acceso fraudulento. Si los usuarios confían en el proveedor de acceso para garantizar la seguridad de su comunicación sin aplicar sus propias medidas de seguridad, los delincuentes pueden interceptar fácilmente las comunicaciones.

La utilización de líneas fijas no impide a los piratas pinchar las comunicaciones.[275] Al pasar a través de un cable las transmisiones de datos emiten energía electromagnética.[276] Con un equipo adecuado, es posible detectar y registrar dichas emisiones [277] y es posible registrar transferencias de datos entre los computadores y el sistema conectado, así como las transmisiones internas del sistema informático.[278]

La mayoría de los países han decidido proteger la utilización de los servicios de telecomunicaciones mediante la penalización de la intervención ilícita de conversaciones telefónicas. Ahora bien, con la creciente popularidad de los servicios IP, es posible que los legisladores tengan que evaluar hasta qué punto se ofrece una protección similar a los servicios IP.[279]

2.5.4 Manipulación de datos

Los datos informáticos son esenciales para los usuarios privados, las empresas y las administraciones, lo que depende de la integridad y disponibilidad de los datos.[280] La carencia de acceso a los datos puede causar daños (económicos) considerables. Los infractores pueden atentar contra la integridad de los datos y borrarlos, suprimirlos o alterarlos.[281] Los virus son un ejemplo bastante común de supresión de datos.[282] Desde los albores de la tecnología informática, los virus han constituido una amenaza para los usuarios que no tienen instalada la debida protección.[283] Con el tiempo el número de virus informáticos ha aumentado considerablemente.[284] Aunque no sólo ha aumentado el número de ataques mediante virus, sino que además han evolucionado las técnicas y las funciones de los virus (carga útil[285]).

Anteriormente, los virus informáticos se distribuían por dispositivos de almacenamiento, tales como disquetes, mientras que hoy en día los virus se distribuyen por Internet anexos a los mensajes de correo electrónico o a los ficheros que descargan los usuarios de Internet.[286] Estos nuevos y eficientes métodos de distribución han acelerado de manera generalizada la infección por virus y han aumentado sobremanera el número de sistemas informáticos infectados. Según las estimaciones, el gusano informático SQL Slammer[287] infectó el 90 por ciento de los sistemas informáticos vulnerables en los 10 minutos posteriores a su distribución.[288] Las pérdidas económicas causadas por ataques de virus en 2000 se calculó en 17 000 millones USD aproximadamente.[289] En 2003 esta cifra fue superior a los 12 000 millones USD.[290]

La mayoría de los virus informáticos de primera generación se limitaban a borrar información o mostrar mensajes. Recientemente, los efectos se han diversificado.[291] Los virus modernos son capaces de abrir puertas traseras por las que los piratas pueden tomar el control del computador o cifrar los ficheros del mismo de modo que las víctimas no puedan acceder a sus propios ficheros, a no ser que paguen para obtener la clave.[292]

Según informes publicados por empresas de seguridad, el número de virus informáticos y otras modalidades de software dañinos aumenta permanentemente, habiéndose registrado hasta 30 millones de nuevos programas malintencionados por año.[293] Kaspersky indica que en 2013 se detectaron más de 300.000 nuevos ficheros dañinos cada día.[294] El hecho de que la mayor parte de esas cifras hayan sido publicadas por empresas de seguridad que venden programas antivirus plantea desde luego un dilema cuando se determina la fiabilidad de esos datos. Pero su repercusión indica que, aunque han pasado decenios desde que se descubrió el primer virus informático, los software dañinos siguen siendo un problema fundamental para la seguridad de Internet.

2.5.5 Ataques contra la integridad del sistema

Los ataques a los sistemas informáticos suscitan las mismas preocupaciones que los ataques a los datos informáticos. Cada vez hay más empresas que incorporan servicios Internet en sus procesos de producción, con lo que se benefician de una disponibilidad de 24 horas al día desde cualquier lugar del mundo.[295] Al

impedir que los sistemas informáticos funcionen correctamente, los infractores consiguen causar grandes pérdidas económicas a sus víctimas.[296]

También es posible realizar ataques físicos a los sistemas informáticos.[297] Si el delincuente tiene acceso físico al sistema informático, puede destruir los equipos. En la mayoría de las legislaciones penales, el daño físico no plantea mayores problemas, dado que son similares a los casos clásicos de daño o destrucción de propiedad. Ahora bien, en el caso de empresas de comercio electrónico muy rentables, las pérdidas económicas causadas a los sistemas informáticos son mucho mayores que el costo de los equipos informáticos.[298]

Desde el punto de vista jurídico, resulta mucho más problemático el tema de los timos por la web. Ejemplos de ataques a distancia contra sistemas informáticos son los gusanos informáticos [299] y los ataques de denegación del servicio (DoS).[300]

Los gusanos informáticos [301] son un tipo de software pernicioso (similares a los virus informáticos). Los gusanos informáticos son programas informáticos que se reproducen de manera autónoma y que inician múltiples procesos de transferencia de datos con objeto de dañar la red. Su incidencia sobre los sistemas informáticos consiste en impedir el buen funcionamiento del sistema informático y utilizar los recursos del sistema para reproducirse a sí mismo por Internet, o en generar de tráfico de red adicional que puede reducir la disponibilidad de ciertos servicios (por ejemplo, sitios web).

Aunque los gusanos informáticos suelen afectar a la red en su conjunto sin dirigirse contra sistemas informáticos específicos, los ataques de DoS sí que se dirigen contra sistemas informáticos concretos. Un ataque de DoS hace que los usuarios previstos no puedan disponer de sus recursos informáticos.[302] Al dirigir a un sistema informático más solicitudes de las que éste puede gestionar, los infractores son capaces de impedir a los usuarios acceder al sistema informático, comprobar su correo electrónico, leer las noticias, reservar un vuelo o descargar archivos. En el año 2000, se lanzaron, en un breve lapso de tiempo, ataques contra varias empresas conocidas tales como CNN, eBay y Amazon.[303] Se informó de ataques similares en 2009 contra sitios web gubernamentales y comerciales de los Estados Unidos y Corea del Sur.[304] Como resultado de ello, algunos de los servicios dejaron de estar disponibles durante varias horas e incluso días.[305]

La persecución por la vía penal de los ataques de DoS y de gusanos informáticos plantea serios desafíos a la mayoría de los sistemas de derecho penal, ya que es posible que dichos ataques no tengan un impacto físico sobre los sistemas informáticos. Dejando aparte la necesidad básica de considerar como delito los ataques basados en la web,[306] se está discutiendo la cuestión de si la prevención y persecución de los ataques contra la infraestructura esencial requiere un enfoque legislativo separado.

Pese a la elaboración de herramientas técnicas de prevención del ciberdelito y de estrategias para la atenuación de sus consecuencias, los ataques de denegación del servicio no han dejado de ser aún una dificultad para las empresas e instituciones gubernamentales. Ciertos estudios indican el aumento de la amenaza de esos ataques y los costos que representan.[307]

2.6 Delitos en relación con el contenido

Bibliografía (seleccionada): *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in Governing the Internet Freedom and Regulation in the OSCE Region; *Carr*, Child Abuse, Child Pornography and the Internet, 2004; *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144 *et seq.*; *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Healy*, Child Pornography: An International Perspective, 2004; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001; *Lanning*, Child Molesters: A Behavioral Analysis, 2001; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*; *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Wortley/Smallbone*, Child Pornography on the

Internet, Problem-Oriented Guides for Police, USDOJ, 2006; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/.

Esta categoría abarca los contenidos que se consideran ilegales, incluida la pornografía infantil, el material xenófobo o los insultos relacionados con símbolos religiosos.[308] La elaboración de instrumentos legales para tratar esta categoría de delitos se ve mucho más influida por los enfoques nacionales, que pueden tomar en consideración principios culturales y jurídicos fundamentales. En lo que respecta al contenido ilícito, los sistemas de valores y los sistemas jurídicos varían sobremanera entre las sociedades. La divulgación de material xenófobo es ilegal en muchos países de Europa,[309] mientras que en Estados Unidos queda protegido por el principio de libertad de expresión [310] en los Estados Unidos.[311] La utilización de comentarios despectivos al referirse al Sagrado Profeta se considera un acto criminal en muchos países islámicos,[312] pero no en algunos países europeos.

Los criterios jurídicos para la persecución por vía penal de los contenidos ilegales no deberían interferir con el derecho a la libertad de expresión. Dicho derecho se define, por ejemplo, en el Principio 1 (b) de los Principios de Johannesburgo sobre la Seguridad Nacional y la Libertad de Expresión.[313] Ello no obstante, en el Principio 1 (c) se aclara que el derecho a la libertad de expresión puede quedar sujeto a restricciones. En consecuencia, aunque la persecución por vía penal de los contenidos ilegales no se excluye *per se*, debe quedar estrictamente limitada. Tales límites se discuten especialmente en lo que respecta a la persecución penal de la difamación.[314] En la Declaración conjunta del Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión y otros, se indica que no deberían perseguirse por vía penal nociones vagas tales como el hecho de facilitar servicios de comunicaciones y la glorificación o promoción del terrorismo o el extremismo.[315]

Estos problemas jurídicos son complejos, dado que la información publicada por un usuario en un determinado país es accesible desde prácticamente cualquier lugar del mundo.[316] Si los "infractores" crean contenido que es ilícito en algunos países, pero no en el país donde operan, la interposición de una acción judicial a los "infractores" resulta difícil, cuando no imposible.[317]

Por otra parte, no existe un consenso acerca del contenido de material o de hasta qué punto pueden penalizarse determinados actos. La divergencia en las perspectivas nacionales y las dificultades que entraña el enjuiciar los delitos cometidos fuera del territorio del país que efectúa la investigación han contribuido al bloqueo de ciertos tipos de contenido en Internet. Cuando existen acuerdos para impedir el acceso a sitios web con contenido ilícito situados fuera del país, el Estado puede aplicar leyes estrictas, bloquear sitios web y filtrar contenido.[318]

Existen diversos métodos para filtrar sistemas. Una solución consiste en que los proveedores de acceso instalen programas que analizan los sitios web visitados y bloquean los que figuran en una lista negra.[319] Otra solución es instalar software de filtrado en los computadores del usuario (método que resulta muy práctico para los padres que desean controlar el contenido que pueden ver sus hijos, y también en el caso de bibliotecas y de terminales públicos de Internet).[320]

Los intentos de controlar el contenido en Internet no se han limitado a ciertos tipos de contenido generalmente reconocido como ilícito. Algunos países recurren a tecnologías de filtrado para restringir el acceso a sitios web dedicados a temas políticos. Según la iniciativa OpenNet[321] cerca de dos docenas de países practican la censura actualmente.[322]

2.6.1 Material erótico o pornográfico (excluida la pornografía infantil)

El contenido sexual fue de los primeros en comercializarse por Internet, dado que presenta ventajas a los distribuidores minoristas de material erótico y pornográfico, en particular:

- El contenido sexual fue de los primeros en comercializarse por Internet, dado que presenta ventajas a los distribuidores minoristas de material erótico y pornográfico, en particular:[323]
- acceso mundial [324] , que permite llegar hasta un número considerablemente mayor de clientes que en una tienda al por menor;

- Internet suele considerarse un medio anónimo (lo que a menudo es un error [325]) – una característica que aprecian los consumidores de pornografía, en vista de las opiniones sociales preponderantes.

Según los estudios recientes, el número de sitios web dedicados a pornografía en Internet a los que se puede acceder en cualquier momento asciende hasta 4,2 millones.[326] Además de los sitios web, el material pornográfico puede distribuirse a través de sistemas de intercambio de ficheros y sistemas de mensajería instantánea.[327]

La penalización del material erótico y pornográfico varía según el país. Algunos países permiten el intercambio de material pornográfico entre adultos pero penalizan los casos en que los menores acceden a este tipo de material,[328] a los efectos de protección del menor.[329] Según los estudios, el acceso a material pornográfico puede afectar negativamente el desarrollo del menor.[330] Para hacer cumplir estas leyes, se han creado "sistemas de verificación de la edad".[331] En otros países se penaliza todo intercambio de material pornográfico incluso entre adultos,[332] sin tener en cuenta grupos específicos (tales como menores).

Para los países que penalizan la interacción con material pornográfico, resulta difícil impedir el acceso al mismo. Fuera de Internet las autoridades pueden detectar y enjuiciar las infracciones a la prohibición de material pornográfico. En cambio en Internet el material pornográfico suele figurar en servidores situados fuera del país, por lo que la aplicación de la ley resulta difícil. Aun cuando las autoridades lleguen a identificar los sitios web que contienen el material pornográfico, no tienen la facultad de obligar a los proveedores a retirar el contenido ofensivo.

Por lo general, el principio de *soberanía nacional* no permite a un país realizar investigaciones dentro del territorio de otro país sin el permiso de las autoridades locales.[333] Incluso si las autoridades tratan de obtener la ayuda de los países en los que se encuentran ubicados los sitios web ofensivos, el principio de "doble incriminación" puede dificultar el éxito de la investigación y la interposición de sanciones penales.[334]

Para impedir el acceso a contenido pornográfico, los países con legislación extremadamente estricta se suelen limitar al bloqueo del acceso (mediante, por ejemplo, tecnología de filtrado [335]) a determinados sitios web.[336]

2.6.2 Pornografía infantil

Internet se ha convertido en un canal principal para la distribución de pornografía infantil. En los decenios de 1970 y 1980, los infractores implicados en el intercambio de pornografía infantil se enfrentaban a graves consecuencias.[337] En aquel momento, el mercado de la pornografía infantil comercial se centraba principalmente en Europa y los Estados Unidos,[338] y el material tenía que elaborarse localmente, resultaba oneroso y era difícil de obtener.[339] Los criterios para comprar o vender pornografía infantil conllevaban una serie de riesgos que, al menos en parte, han dejado de existir en la actualidad. En el pasado, los productores no disponían de capacidad para revelar las fotografías y las películas.[340] Dependían de los servicios ofrecidos por empresas, lo cual incrementaba las posibilidades de que agentes de la autoridad identificaran casos de pornografía infantil a través de informes facilitados por empresas que se ocupaban del revelado.[341] La disponibilidad de las cámaras de video cambió por primera vez esta situación.[342] Pero los riesgos no se limitaban a la fase de producción. La obtención del acceso a pornografía infantil conllevaba riesgos para el infractor. Los pedidos se hacían respondiendo a anuncios que aparecían en la prensa de papel.[343] En consecuencia, los medios de comunicación entre el vendedor y el coleccionista, y a menudo el propio mercado, eran limitados.[344] Hasta mediados del decenio de 1990, la pornografía infantil circulaba fundamentalmente a través de los servicios postales, y el éxito de las investigaciones permitió detectar a un número importante de delincuentes.[345] En opinión de los expertos, en aquel entonces las autoridades encargadas de velar por el cumplimiento de la ley eran capaces de responder a los desafíos.[346]

La situación cambió drásticamente con el acceso a aplicaciones de intercambio de bases de datos a través de Internet. Mientras que en el pasado, las autoridades se enfrentaban a material analógico, en la actualidad la inmensa mayoría del material descubierto es digital.[347] Desde mediados del decenio de 1990, los infractores han venido utilizando cada vez más los servicios de las redes para la distribución de este tipo de material.[348] Se han reconocido los problemas resultantes en términos de detección e investigación de

casos de pornografía infantil.[349] Internet es en la actualidad el principal canal para el comercio habitual de pornografía[350] y de pornografía infantil.[351]

Cabe destacar varios motivos para el paso de la distribución analógica a la digital. Internet da a los usuarios menos cualificados técnicamente la impresión de que pueden actuar de manera invisible para los demás. Si el infractor no emplea tecnología de la comunicación anónima, esta impresión es errónea. Pero el hecho de que la utilización de medios sofisticados de comunicación anónima pueda dificultar la identificación del infractor es un motivo de preocupación en lo que respecta al intercambio de pornografía infantil en línea.[352] Además, esta evolución se ha visto favorecida por la disminución del precio de los aparatos y servicios técnicos utilizados para alojar servicios.[353] Dado que los sitios web y los servicios de Internet están al alcance de cerca de 2.000 millones de usuarios de Internet, el número de clientes potenciales también ha aumentado.[354] Existe inquietud por el hecho de que la facilidad de acceso atraiga más fácilmente a personas que no hubieran corrido el riesgo de verse atrapados tratando de obtener pornografía infantil fuera de Internet.[355] Con el paso de los medios analógicos a los medios digitales, se informa de un número creciente de imágenes de pornografía infantil descubiertas a través de las investigaciones.[356] Otro aspecto que probablemente ha contribuido a esta evolución es el hecho de que la información digital pueda duplicarse sin perder calidad.[357] Mientras que, en el pasado, los consumidores de pornografía infantil que deseaban comercializar el material se enfrentaban al obstáculo de la pérdida de calidad resultante de la reproducción, en la actualidad un archivo descargado puede convertirse en fuente de nuevas copias. Una de las consecuencias de esta situación es que, aún en el caso de que se detenga al infractor que produjo el material en primer lugar y se confisquen sus archivos, resulta difícil "eliminar" los archivos una vez que se han comercializado a través de Internet.[358]

Frente a la división de opiniones que suscita la pornografía adulta, la pornografía infantil es objeto de una condena general, y las infracciones relacionadas con la pornografía infantil se reconocen en general como actos criminales.[359] Las organizaciones internacionales se han implicado en la lucha contra la pornografía infantil en línea,[360] con varias iniciativas legales internacionales entre las que figuran: la Convención de las Naciones Unidas sobre los Derechos del Niño, de 1989;[361] la Decisión marco del Consejo de la Unión Europea relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil de 2003;[362] y el Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación Sexual y el Abuso Sexual de 2007, entre otros.[363]

Lamentablemente, estas iniciativas para tratar de controlar la distribución de pornografía a través de la red han demostrado ser poco disuasorias para los infractores, que utilizan Internet para comunicar e intercambiar pornografía infantil.[364] El incremento del ancho de banda ha contribuido al intercambio de películas y archivos fotográficos.

Según las investigaciones sobre el comportamiento de los infractores en materia de pornografía infantil, el 15 por ciento de los detenidos por delitos de pornografía infantil a través de Internet guardaban en su computador más de 1 000 imágenes; el 80 por ciento de las cuales de niños con edades comprendidas entre 6 y 12 años;[365] el 19 por ciento tenían imágenes de niños menores de 3 años [366]; y el 21 por ciento de imágenes con escenas violentas.[367]

La venta de material de pornografía infantil es muy lucrativa,[368] dado que los coleccionistas están dispuestos a pagar grandes cantidades por películas e imágenes que muestren niños en un contexto sexual.[369] Los motores de búsqueda permiten encontrar este tipo de material con rapidez.[370] La mayor parte de este material se intercambia en foros cerrados protegidos con contraseña, a los que difícilmente pueden acceder los usuarios ordinarios de Internet y las fuerzas de seguridad. Así pues, las operaciones secretas son esenciales para luchar contra la pornografía infantil[371]

Hay dos factores básicos de la utilización de las TIC que plantean dificultades en la investigación de delitos relacionados con el intercambio de pornografía infantil, a saber:

1 La utilización de divisas virtuales y pagos anónimos [372]

El pago en metálico por ciertas mercancías permite al comprador ocultar su identidad, razón por la cual es el modo de pago predominante muchas actividades delictivas. La demanda de pagos anónimos ha dado lugar a la aparición de sistemas de pago virtual y divisas virtuales.[373] Al pagar con divisas virtuales no se

exige la identificación y la validación, lo que impide a las fuerzas de seguridad rastrear el intercambio de divisas para encontrar a los delincuentes. Las recientes investigaciones sobre pornografía infantil han conseguido dar con los infractores siguiendo la pista de los pagos efectuados por éstos.[374] Sin embargo, cuando los infractores efectúan pagos anónimos resulta difícil rastrearlos. [375] Cuando los delincuentes utilizan estas divisas anónimas, ello limita la capacidad de las autoridades encargadas de velar por la aplicación de la ley para identificar a sospechosos a partir de las transferencias de dinero [376]– por ejemplo en los casos relacionados con la pornografía infantil de carácter comercial.[377]

2 La utilización de tecnología de cifrado [378]

Los autores de estos delitos recurren cada vez más al cifrado de sus mensajes. Las fuerzas de seguridad se han percatado de que los infractores utilizan técnicas de cifrado para proteger la información almacenada en sus discos duros,[379] lo que dificulta sobremanera las investigaciones penales.[380]

Además de una penalización general de los actos relacionados con la pornografía infantil, se está estudiando la posibilidad de recurrir a otros métodos, tales como imponer a los proveedores de servicios Internet la obligación de registrar a los usuarios o de bloquear o filtrar el acceso a sitios web que contengan contenido de pornografía infantil.[381]

2.6.3 Racismo, lenguaje ofensivo, exaltación de la violencia

Los grupos radicales utilizan los medios de comunicación de masas, como Internet, para divulgar propaganda. [382] El número de sitios web con contenido racista y lenguaje ofensivo ha aumentado recientemente [383] – según un estudio realizado en 2005 el número de páginas web con apología del racismo, la violencia y la xenofobia aumentó en un 25 por ciento entre 2004 y 2005.[384] En 2006 existían en Internet más de 6 000 sitios web de este tipo.[385]

La distribución por Internet ofrece varias ventajas a los delincuentes, tales como los menores costes de distribución, la utilización de equipos no especializados y una audiencia mundial. Como ejemplos de sitios web de incitación a la violencia cabe citar los que contienen instrucciones para fabricar bombas.[386] Aparte de la propaganda, Internet se utiliza para vender ciertas mercancías, por ejemplo artículos relacionados con la ideología nazi, como banderas con símbolos, uniformes y libros, que se ponen a disposición en plataformas de subastas y cibertiendas especializadas.[387] También se utiliza Internet para enviar mensajes de correo electrónico y boletines informativos y para distribuir vídeos y programas de televisión por lugares populares tales como YouTube.

Estos actos no están penalizados en todos los países.[388] En algunos países, este tipo de contenido está protegido por el principio de libertad de expresión.[389] Las opiniones son divergentes respecto hasta qué punto el principio de libertad de expresión es aplicable a ciertos temas, lo que a menudo dificulta las investigaciones de ámbito internacional. Un ejemplo de conflicto de legislaciones fue el caso en que estuvo implicado el proveedor de servicios Yahoo! en 2001, cuando un tribunal francés dictó a Yahoo! (con sede en Estados Unidos) que bloqueara el acceso de usuarios franceses a material nazi.[390] En virtud de la Primera Enmienda a la Constitución de Estados Unidos, la venta de este tipo de material es legal en este país. En aplicación de la primera enmienda, un tribunal de Estados Unidos decidió que la orden dictada por el tribunal francés no podía aplicarse contra Yahoo! en Estados Unidos.[391]

La discrepancia de opiniones entre los países sobre estos asuntos quedó patente durante la redacción del Convenio del Consejo de Europa sobre la Ciberdelincuencia. La finalidad de este Convenio es armonizar la legislación en materia de ciberdelincuencia para garantizar que las investigaciones de alcance internacional no se vean obstaculizadas por la divergencia en las legislaciones.[392] Las Partes que entablaron negociaciones no pudieron llegar a un consenso acerca de la penalización del material xenófobo, de modo que este tema quedó excluido del Convenio y se aborda por separado en un Primer Protocolo.[393] De lo contrario, algunos países (con inclusión de Estados Unidos) no lo hubieran firmado.

2.6.4 Delitos contra la religión

Son cada vez más [394] los sitios web con material que algunos países consideran que atenta contra la religión, por ejemplo declaraciones antirreligiosas por escrito.[395] Si bien cierto tipo de material corresponde a los hechos objetivos y a la tendencia (por ejemplo, la disminución de la asistencia a oficios religiosos en Europa), esta información se considera ilícita en algunas jurisdicciones. Otros ejemplos son la difamación de religiones o la publicación de caricaturas.

Internet ofrece ventajas a las personas interesadas en criticar o debatir acerca de un determinado asunto, ya que se pueden formular comentarios, publicar material o artículos sin que los autores estén obligados a revelar su identidad. Muchos grupos de debate se basan en el principio de libertad de expresión.[396] La libertad de expresión es uno de los factores esenciales que explican el éxito de Internet y, de hecho, existen portales creados específicamente para el contenido generado por los usuarios.[397] Si bien es fundamental proteger este principio, incluso en los países más liberales existen condiciones y leyes que rigen la aplicación del principio de libertad de expresión.

La divergencia de normas jurídicas sobre contenido ilícito denota los problemas que entraña la reglamentación del contenido. Incluso en los países donde la publicación de contenido está contemplada en las disposiciones relativas a la libertad de expresión, es posible acceder al material publicado desde otros países con reglamentación más estricta. La polémica sobre las "caricaturas" en 2005 es un ejemplo de los posibles conflictos que pueden surgir. La publicación de doce caricaturas en el periódico danés Jyllands-Posten generó protestas generalizadas en el mundo islámico.[398]

Al igual que en el caso del contenido ilícito, la disponibilidad de cierta información o material es un delito penal en algunos países. La protección de las diferentes religiones y símbolos religiosos varía de un país a otro. Algunos países penalizan la formulación de observaciones peyorativas sobre el Sagrado Profeta[399] o la profanación de copias del Corán,[400] mientras que otros adoptan una posición más liberal y no penalizan tales actos.

2.6.5 Juegos ilegales y juegos en línea

Los juegos por Internet son uno de los campos que experimenta un mayor crecimiento en este medio.[401] Según Linden Labs, el creador del juego en línea "Segunda Vida",[402] se han abierto unos diez millones de cuentas.[403] Los Informes muestran que algunos de estos juegos se han utilizado para cometer delitos, en particular [404] el intercambio y presentación de pornografía infantil,[405] el fraude,[406] el juego en casinos en línea [407] y la difamación (por ejemplo, escribir mensajes difamatorios o calumnias).

Según las estimaciones, los ingresos en concepto de juegos en línea por Internet pasará de 3 100 millones USD en 2001 a 24 000 millones USD en 2010[408] (si bien es cierto que comparadas con las cifras que mueve el juego tradicional, éstas son relativamente pequeñas[409]). Se estima que en 2015 los ingresos alcanzarán los 28.000 millones USD.[410]

La reglamentación del juego dentro y fuera de Internet varía de un país a otro [411] – una laguna legislativa que aprovechan tanto los infractores como los negocios legales y casinos. El efecto de la diversidad legislativa resulta evidente en Macao. Tras haber sido devuelta por Portugal a China en 1999, Macao se ha convertido en una de los destinos para el juego más importantes del mundo. Los ingresos anuales en 2006 se estimaron en 6 800 millones USD, llegando a superar a Las Vegas (6 600 millones USD).[412] El éxito en Macao se debe al hecho de que el juego es ilegal en China [413] por lo que miles de ludópatas de la China continental se desplazan a Macao para jugar.

Internet permite a las personas burlar las prohibiciones de juego.[414] Los casinos en línea han proliferado, la mayoría de los cuales se encuentran en países con legislación liberal o sin normativa sobre el juego por Internet. Los usuarios pueden abrir cuentas en línea, transferir dinero y participar en juegos de azar[415] Los casinos en línea también pueden utilizarse para lavar dinero y financiar el terrorismo.[416] Al efectuar los jugadores apuestas en casinos en línea que no mantienen registros o que están ubicados en países sin legislación contra el lavado de activos, resulta difícil para las fuerzas de seguridad determinar el origen de los fondos.

Resulta difícil a los países con restricciones de juego controlar la utilización o las actividades de los casinos en línea. Internet está socavando las restricciones jurídicas de los países sobre el acceso por los ciudadanos a los juegos en línea.[417] Ha habido varios intentos de impedir la participación en los juegos en línea:[418] en particular la Ley de 2006 de prohibición del juego por Internet en Estados Unidos cuya finalidad es limitar el juego en línea ilícito mediante la incriminación de proveedores de servicios financieros que se encargan de la liquidación de transacciones relacionadas con el juego ilícito.[419]

2.6.6 Difamación e información falsa

Internet puede utilizarse para divulgar información errónea con la misma facilidad que la información fidedigna.[420] Los sitios web pueden contener información falsa o difamatoria, especialmente en los foros y salas de charla donde los usuarios pueden publicar sus mensajes sin la verificación de los moderadores.[421] Los menores utilizan cada vez más los foros web y los sitios de relaciones sociales donde también puede publicarse este tipo de información.[422] El comportamiento delictivo [423] puede consistir, por ejemplo, en la publicación de fotografías de carácter íntimo o información falsa sobre hábitos sexuales.[424]

En muchos casos, los infractores se aprovechan de que los proveedores que ofrecen la publicación económica o gratuita no exigen la identificación de los autores o no la verifican,[425] lo que complica la identificación de los mismos. Además, los moderadores de foros controlan muy poco o nada el contenido publicado. No obstante, ello no es óbice para que se hayan desarrollado proyectos interesantes tales como Wikipedia, una enciclopedia en línea creada por los usuarios,[426] , que cuenta con procedimientos estrictos de control de contenido. Ahora bien, los delincuentes pueden utilizar esta misma tecnología para publicar información falsa (por ejemplo sobre la competencia)[427] o revelar información confidencial (por ejemplo, publicar secretos de Estado o información comercial confidencial).

Cabe destacar el creciente peligro que representa la información falsa o errónea. La difamación puede dañar la reputación y la dignidad de las víctimas en un grado considerable, dado que las declaraciones en línea son accesibles por la audiencia mundial. Desde el momento en que se publica la información en Internet el autor o autores pierden el control de la información. Aunque la información se corrija o se suprima poco después de su publicación, puede haber sido duplicada ("en servidores espejo") y esté en manos de personas que no desean retirarla o suprimirla. En tal caso, la información permanecerá en Internet aunque la fuente original de la misma se haya suprimido o corregido.[428] Como ejemplo puede citarse el caso de mensajes de correo electrónico "fuera de control", que reciben millones de personas con contenido obsceno, erróneo o falso acerca de personas u organizaciones, que quizá nunca puedan reponerse del daño causado a su reputación, con independencia de la veracidad o falsedad del mensaje original. Por consiguiente, es preciso llegar a un equilibrio apropiado entre la libertad de expresión[429] y la protección de las posibles víctimas de calumnias.[430]

2.6.7 Correo basura y amenazas conexas

Por "correo basura" o "spam" se entiende el envío masivo de mensajes no solicitados.[431] Aunque existen diversos tipos de timos, el más común es el correo basura. Los infractores envían millones de mensajes de correo electrónico a los usuarios, que normalmente contienen anuncios de productos y servicios y con frecuencia software pernicioso. Desde que se enviara el primer mensaje de correo basura en 1978,[432] la oleada de este tipo de mensajes ha experimentado un aumento espectacular.[433] Según informan las organizaciones proveedoras de correo electrónico, en la actualidad entre el 85 y el 90 por ciento de todos los mensajes son correo basura.[434] Las principales fuentes de correo basura en 2007 eran: Estados Unidos (19,6 por ciento del total); la República Popular de China (8,4 por ciento); y la República de Corea (6,5 por ciento).[435] Seis años después, las tres fuentes principales de correo basura continúan siendo las mismas: la República Popular China (22,97 por ciento), Estados Unidos (17,6 por ciento del total registrado) y la República de Corea (12,67 por ciento).[436]

La reacción de la mayoría de los proveedores de correo electrónico ante este aumento del correo basura ha sido la instalación de tecnologías de filtrado de correo basura. Esta tecnología identifica el correo basura gracias al filtrado de palabras clave o listas negras de direcciones IP de los remitentes de este tipo de correo (spammers).[437] Aunque la tecnología de filtrado sigue desarrollándose, los remitentes siempre encuentran

la forma de burlar estos sistemas por ejemplo, evitando utilizar palabras clave. Los remitentes de correo basura han encontrado muchas formas de describir "Viagra", uno de los productos más populares que se ofrecen en este tipo de correo, sin nombrar la marca.[438]

El éxito en la detección de correo basura depende de los cambios en la forma de distribución. En lugar de enviar mensajes desde un solo servidor de correo (que para los proveedores del servicio de correo electrónico sería muchos más fácil de identificar, al tratarse de un número reducido de fuentes[439]), muchos infractores utilizan redes zombi (*botnets*)[440] para distribuir correo electrónico no solicitado. Al recurrir a redes zombi (o robot) constituidas por miles de sistemas informático,[441] cada computador envía sólo unos cientos de mensajes. Por ese motivo, resulta más difícil a los proveedores de este servicio analizar la información sobre los remitentes y a las fuerzas de seguridad seguir la pista de los delincuentes.

El correo basura es una actividad muy lucrativa ya que el costo de enviar miles de millones de correo es bajo, y aún menor cuando se utilizan redes zombi.[442] Algunos expertos opinan que la única solución real en la lucha contra el correo indeseado es aumentar el costo de envío para los remitentes.[443] En un Informe publicado en 2007 se analizan los costes y beneficios del correo basura y se llega a la conclusión de que el costo de enviar unos 20 millones de mensajes de correo electrónico es de unos 500 USD.[444] Dado que para los infractores aún resulta más económicos, el envío de correo basura es muy lucrativo, especialmente si los infractores son capaces de enviar miles de millones de mensajes. Un distribuidor de correo basura holandés informó haber obtenido un beneficio de 50 000 USD por enviar un mínimo de 9 000 millones de mensajes de correo basura.[445]

En 2005, la OCDE publicó un Informe en que se analiza la incidencia del correo basura en los países en desarrollo.[446] Estos países opinan que sus usuarios de Internet se ven más afectados por el correo basura y otros abusos por Internet. El correo basura es un problema grave en los países en desarrollo, donde la anchura de banda y el acceso a Internet son más escasos y caros que en los países industrializados.[447] El correo basura consume tiempo y recursos en los países donde los recursos de Internet son más escasos y costosos.

2.6.8 Extorsión

Aunque la extorsión no es considerada un ciberdelito típico sino un delito tradicional, la nueva utilización de las TIC ha dado lugar a ataques conocidos a menudo con el apelativo "ciberextorsión".[448] En los últimos años, grandes y pequeñas empresas han sido el blanco de ese tipo de ataques.[449] Los delincuentes recurren cada vez con mayor frecuencia a las diversas ventajas que ofrecen las TIC en comparación con las formas tradicionales en que se comete ese delito. Además de utilizar tecnologías de comunicaciones anónimas para cometer el delito, un número creciente de delincuentes utilizan monedas virtuales en vez de pagos en efectivo de transferencias por cable.[450] Ciertos estudios revelan que las empresas subestiman aún la amenaza de extorsión.[451]

Un tipo más automatizado de extorsión es el llamado "*ransomware*", un software dañino que infecta el sistema informático, lo bloquea e inserta un mensaje indicando que sólo se desbloqueará si la víctima paga un rescate. Al parecer, se trata de una modalidad de extorsión que suscita cada vez más inquietud.[452] Para ser más persuasivos, los delincuentes aseguran por lo general que el bloqueo de la computadora responde a la aplicación de la ley por actividades ilícitas del usuario.[453]

2.6.9 Otras formas de contenido ilícito

Internet no sólo se utiliza para ataques directos, sino también como foro para solicitar, ofrecer e incitar el crimen ,[454] la venta ilegal de productos; y dar información e instrucciones para actos ilícitos (por ejemplo, sobre cómo construir explosivos).

Muchos países han reglamentado el comercio de ciertos productos. Cada país aplica distintas reglamentaciones nacionales y restricciones al comercio de los diversos productos, por ejemplo, el material militar.[455] La situación es similar en el caso de los medicamentos algunos medicamentos pueden comprarse sin restricciones en unos países mientras que en otros se precisa receta médica.[456] El comercio transfronterizo dificulta el control de ciertos productos restringidos en un territorio.[457] Dada la popularidad

de Internet, este problema va en aumento. Las tiendas por la web situadas en países sin restricción alguna pueden vender productos a clientes de otros países, menoscabando así esas limitaciones.

Antes de que apareciera Internet, era difícil conseguir instrucciones sobre construcción de armas. La información estaba disponible (por ejemplo, en libros sobre los aspectos químicos de los explosivos), pero conseguirla llevaba mucho tiempo. Hoy en día, la información sobre cómo construir explosivos está disponible en Internet[458] y cuanto más fácil es el acceso a esta información mayor es la probabilidad de que se produzcan atentados.

2.7 Delitos en materia de derechos de autor y marcas

Bibliografía (seleccionada): Androutsellis-Theotokis/Spinellis, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; Bakken, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf; Clarke/Sandberg/Wiley/Hong, Freenet: a distributed anonymous information storage and retrieval system, 2001; Cunard/Hill/Barlas, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; Fischer, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002; Johnson/McGuire/Willey, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf; Lohmann, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; Penn, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2; Rayburn, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001; Schoder/Fischbach/Schmitt, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Sifferd, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93.

Una de las funciones esenciales de Internet es la difusión de información. Las empresas utilizan Internet para dar información sobre sus productos y servicios. En términos de piratería, empresas prósperas pueden encontrar en Internet problemas comparables a los que existen fuera de la red. Los falsificadores pueden utilizar la imagen de marca y el diseño de una determinada empresa para comercializar productos falsificados, copiar logotipos y productos, y registrar su nombre de dominio. Las empresas que distribuyen sus productos directamente por Internet[459] pueden tener problemas de carácter jurídico con las violaciones de los derechos de autor puesto que sus productos se pueden teledescargar, copiar y distribuir.

2.7.1 Delitos en materia de derechos de autor

Con el paso de los sistemas analógicos a los digitales,[460] la digitalización[461] ha permitido a la industria del ocio incorporar en las películas en DVD nuevos servicios y prestaciones tales como idiomas, subtítulos, avances y material complementario (bonus). Los CD y los DVD han resultado ser más duraderos que los discos y las videocasetes.[462]

La digitalización ha dado paso a nuevas violaciones de los derechos de autor fundadas en la reproducción rápida y exacta. Antes de la digitalización, en la copia de un disco o una videocasete se perdía calidad. Actualmente, se pueden duplicar fuentes digitales sin ninguna pérdida de calidad y también, por ese motivo, hacer copias de copias. Entre las violaciones de los derechos de autor más comunes cabe mencionar el intercambio de archivos, de programas informáticos, archivos y temas musicales protegidos con derechos de autor a través de sistemas de compartición de archivos [463] o a través de sistemas de intercambio de archivos y la elusión de los sistemas de gestión de derechos en el ámbito digital.[464]

Los sistemas de intercambio de archivos son servicios de red entre pares [465] que habilitan a los usuarios a compartir archivos, [466] a menudo con otros millones de usuarios. [467] Una vez instalado el software correspondiente, los usuarios pueden seleccionar los archivos que van a intercambiar, utilizar el software

para buscar otros archivos colocados por los demás usuarios y teledescargarlos desde centenares de fuentes. Antes de que se crearan los sistemas de intercambio, los usuarios copiaban e intercambiaban discos y casetes, pero gracias a estos sistemas se intercambian copias entre muchos más usuarios.

El tráfico entre tecnologías pares (P2P) desempeña un papel esencial en Internet. En la actualidad, más del 50 por ciento del tráfico Internet se genera por redes entre pares.[468] El número de usuarios crece sin cesar – según un Informe publicado por la OCDE, aproximadamente el 30 por ciento de usuarios franceses de Internet ha teledescargado música o archivos mediante sistemas de intercambio de archivos,[469] y una tendencia similar se observa en otros países de la OCDE.[470] Estos sistemas pueden utilizarse para intercambiar todo tipo de datos informáticos, en especial, música, películas y software.[471] Históricamente se han utilizado ante todo para intercambiar música, pero el intercambio de vídeo es cada vez más importante.[472]

La tecnología empleada en los servicios de intercambio de archivos, sumamente compleja, permite intercambiar grandes archivos en cortos periodos de tiempo.[473] Como los sistemas de la primera generación dependían de un servidor central, las autoridades competentes podían intervenir contra el intercambio ilegal en la red Napster.[474] A diferencia de los sistemas de la primera generación (especialmente, el famoso servicio Napster), los de las segunda generación ya no dependen de un servidor central que proporciona una lista de archivos disponibles entre usuarios.[475] Con la descentralización de las redes de intercambio de archivos de la segunda generación resulta más difícil impedir su funcionamiento. Sin embargo, debido a las comunicaciones directas, es posible seguir el rastro de los usuarios de una red gracias a sus direcciones IP.[476] En la investigación de violaciones de los derechos de autor en sistemas de intercambio de archivos, las autoridades competentes han logrado algunos buenos resultados. Las versiones más recientes de estos sistemas propician formas de comunicación anónima y harán más difíciles las investigaciones.[477]

La tecnología de intercambio de archivos no sólo es utilizada por los ciudadanos de a pie y los delincuentes, sino también por las empresas.[478] No todos los archivos intercambiados con estos sistemas violan los derechos de autor. Hay ciertos usos legítimos como, por ejemplo, el intercambio de obras de arte o de copias autorizadas dentro del dominio público.[479]

Con todo, la utilización de los sistemas de intercambio de archivos plantea problemas a la industria del ocio.[480] No se sabe a ciencia cierta hasta qué punto la reducción en las ventas de CD/DVD y de entradas para el cine se debe al intercambio de títulos mediante dichos sistemas. Según estudios realizados, se han identificado millones de usuarios que intercambian archivos [481] y miles de millones de archivos teledescargados.[482] En sistemas de intercambio de archivos han aparecido copias de películas antes de su estreno oficial en los cines [483] a costa de los titulares de derechos de autor. La reciente creación de sistemas de intercambio de archivos anónimos hará más difícil la labor de los titulares de derechos de autor, y también la de las autoridades competentes.[484]

La respuesta de la industria del ocio a este problema ha sido la implantación de tecnologías que impidan a los usuarios hacer copias de CD y DVD, por ejemplo los sistemas de aleatorización de contenido (CSS, Content Scrambling Systems),[485] una tecnología de encriptación que impide la copia de contenidos en DVD.[486] Esta tecnología es un elemento esencial de los nuevos modelos comerciales que procuran otorgar más precisamente derechos de acceso a los usuarios. La gestión de derechos en el ámbito digital (DRM)[487] describe la implantación de tecnologías que permitan a los titulares de derechos de autor restringir la utilización de medios digitales, donde los usuarios adquieran únicamente derechos limitados (por ejemplo, el derecho a reproducir un tema musical durante una fiesta). La DRM, que ofrece la posibilidad de aplicar nuevos modelos comerciales que reflejen con mayor precisión los intereses de los titulares de derechos de autor y de los usuarios, podría convertir la menor utilización de esos medios en beneficios.

Una de las mayores dificultades de estas tecnologías destinadas a la protección de los derechos de autor es que pueden eludirse.[488] Los delincuentes han diseñado herramientas informáticas que permiten a los usuarios colocar en Internet, en forma gratuita o a precios muy bajos, archivos protegidos contra las copias.[489] Una vez que la protección DRM se ha eliminado de un archivo, se pueden hacer copias y reproducirlas sin límite.

Los intentos de proteger el contenido no se limitan a los temas musicales y a las películas. Algunos canales de televisión (en especial, los canales de pago) encriptan programas para que únicamente puedan recibirlos los clientes que han pagado por ellos. Pese al avance de las tecnologías de protección, los delincuentes han logrado falsificar equipos utilizados como control de acceso o eliminar la encriptación a través de herramientas informáticas.[490]

Sin herramientas informáticas, los usuarios habituales tienen menos posibilidades de cometer delitos. Los debates sobre la conveniencia de tipificar como delito las violaciones de los derechos de autor no sólo dan prioridad a los sistemas de intercambio de archivos y a la elusión de la protección técnica, sino también a la elaboración, venta y propiedad de "dispositivos ilegales" o herramientas concebidos para que los usuarios puedan llevar a cabo ese tipo de violaciones.[491]

2.7.2 Delitos en materia de marcas comerciales

Las violaciones de marcas y de los derechos de autor son similares y constituyen un aspecto bien conocido del comercio mundial. Las violaciones en materia de marcas se han incorporado al ciberespacio y, en el marco de diferentes Códigos Penales, su tipificación como delito presenta diversos grados.[492] Los delitos más graves son, entre otros, la utilización de marcas en actividades delictivas con el propósito de engañar a los usuarios, y los delitos en materia de dominios y nombres.

La buena reputación de una empresa está relacionada por lo general a su marca. Los delincuentes utilizan nombres genéricos y marcas de forma fraudulenta en numerosas actividades, por ejemplo la *peska*,[493] en las que se envían a los usuarios de Internet millones de correos electrónicos similares a los de empresas legítimas, por ejemplo consignando su marca.[494]

Otro aspecto de las violaciones de marcas son los delitos en materia de dominios,[495] por ejemplo la ciberocupación ilegal,[496] que describe el procedimiento ilegal de registrar un nombre de dominio idéntico o similar al de la marca de un producto o de una empresa.[497] En la mayoría de los casos, los delincuentes intentan vender el dominio a la empresa a un precio más elevado [498] o utilizarlo para vender productos o servicios engañando a los usuarios con su supuesta conexión a la marca comercial. [499] Otro ejemplo de infracción en materia de dominio es la "apropiación indebida de dominio" o registro de nombres de dominio que han caducado accidentalmente.[500]

2.8 Delitos informáticos

Bibliografía (seleccionada): *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*; *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf; *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005; *Gercke*, Internet-related Identity Theft, 2007; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270; *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004; *Paget*, Identity Theft – McAfee White Paper, page 10, 2007; *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1; *Sieber*, Council of Europe Organised Crime Report 2004; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*

Esta categoría abarca numerosos delitos para cuya realización se necesita disponer de un sistema informático. A diferencia de las categorías anteriores, estos delitos generales, que no suelen ser tan estrictos en la protección de principios jurídicos. Se enmarcan en esta categoría el fraude informático, la falsificación informática, la peska, el robo de identidad y el uso indebido de dispositivos.

2.8.1 Fraude y fraude informático

El fraude informático es uno de los delitos más populares cometidos en Internet,[501] puesto que con la automatización [502] y herramientas informáticas se pueden encubrir las identidades de los delincuentes.

Gracias a la automatización, los delincuentes obtienen importantes beneficios a partir de un cierto número de pequeñas acciones. [503] Aplican una estrategia que consiste en asegurar que la pérdida financiera de cada víctima esté por debajo de un cierto límite. Si tienen una "pequeña" pérdida, es menos probable que las víctimas inviertan tiempo y energía en dar a conocer e investigar esos delitos.[504] Un ejemplo de este timo es la estafa nigeriana, que consiste en el pago de una suma por adelantado.[505]

Aunque estos delitos se cometen utilizando tecnologías informáticas, la mayoría de los regímenes de derecho penal no los consideran delitos informáticos sino fraudes de carácter común.[506] . La distinción principal entre fraude informático y fraude tradicional consiste en el objetivo que se persigue. Si el estafador trata de manipular a una persona, se considera por lo general que el delito es un fraude; si su objetivo apunta a los sistemas informáticos o de procesamiento de datos, el delito suele catalogarse de fraude informático. Los regímenes de derecho penal que abarcan el fraude pero no contemplan aún la manipulación de sistemas informáticos con propósitos fraudulentos, también pueden a menudo entablar una acción judicial contra los delitos mencionados más arriba. Los fraudes más habituales son, entre otros, los siguientes: subasta en línea y estafa nigeriana.

Subasta en línea [507]

Las subastas en línea constituyen actualmente uno de los servicios más difundidos de cibercomercio. Ya en 2006, se vendieron por eBay, el mercado de subastas en línea más importante del mundo[508], mercancías por un valor superior a los 20 000 millones USD. Los compradores tienen acceso a mercancías de los segmentos de mercado más especializados y variados del mundo entero. Los vendedores se complacen de tener una cartera internacional de clientes, lo cual estimula la demanda e incrementa los precios.

Quienes cometen delitos a través de plataformas de subastas pueden explotar la ausencia del contacto cara a cara entre vendedores y compradores[509]. Debido a la dificultad de hacer una distinción entre usuarios genuinos y estafadores, el fraude de la subasta se ha convertido en uno de los ciberdelitos más populares[510]. Los dos timos más comunes son[511]: ofrecer mercancías no disponibles para la venta y exigir su pago antes de la entrega[512]; o adquirir mercancías y solicitar su envío, sin intención de pagar por ellas.

En respuesta a esta situación, los organizadores de subastas han creado sistemas de protección como, por ejemplo, el sistema de intercambio de información/comentarios. Después de cada transacción, compradores y vendedores formulan comentarios que ponen a disposición de otros usuarios[513] en calidad de información neutral sobre la fiabilidad de ambos. En este caso, "la reputación es esencial" y sin un número adecuado de comentarios positivos, es más difícil que los estafadores convenzan a las víctimas de pagar por mercancías inexistentes o, por el contrario, de enviar mercancías sin recibir antes su pago. Sin embargo, los delincuentes eluden esta protección recurriendo a cuentas de terceros[514]. Con este timo, que se conoce como "apropiación de cuenta"[515], tratan de apropiarse de nombres de usuario y de contraseñas de usuarios legítimos para comprar o vender mercancías de forma fraudulenta, resultando más difícil su identificación.

Estafa nigeriana [516]

En este tipo de fraude, los delincuentes envían mensajes electrónicos pidiendo ayuda a los destinatarios para transferir importantes cantidades de dinero a terceros con la promesa de darles un porcentaje si aceptan hacer esa operación a través de sus cuentas personales[517]. Piden también que les transfieran a su nombre una pequeña cantidad de dinero para verificar los datos de la cuenta bancaria con la que se hará la transacción (la idea es la misma que en el juego de la lotería: los que participan están dispuestos a perder una cantidad de dinero pequeña pero segura a cambio de ganar otra más importante pero improbable) o que simplemente les envíen los datos de la cuenta bancaria. Una vez que envíen el dinero, las víctimas no volverán a saber nunca más nada de esos estafadores. Si envían los datos de su cuenta bancaria, los delincuentes pueden utilizarlos para actividades fraudulentas. Hay pruebas que sugieren que esos mensajes

electrónicos reciben miles de respuestas[518]. Según estudios en curso, y pese a diversas iniciativas y campañas de información, el número de víctimas y de pérdidas totales de dinero a causa de la estafa nigeriana sigue aumentando.[519]

2.8.2 Falsificación informática

Por falsificación informática se entiende la manipulación de documentos digitales[520], por ejemplo: crear un documento que parece provenir de una institución fiable; manipular imágenes electrónicas (por ejemplo, imágenes aportadas como pruebas materiales en los tribunales); o alterar documentos.

La falsificación de correo electrónico comprende la *peska*, que constituye un grave problema para las autoridades competentes en todo el mundo[521]. Este timo consiste en lograr que las víctimas revelen información personal o secreta[522]. Por regla general, los delincuentes envían correos electrónicos que se asemejan a mensajes de instituciones financieras legítimas conocidas por la víctima[523] y están redactados de tal forma que resulta difícil creer que son falsos[524]. En ellos se pide al destinatario que revele y/o verifique cierta información confidencial. Muchas víctimas siguen el consejo y revelan datos, gracias a los cuales los delincuentes pueden efectuar transferencias en línea y otras operaciones[525].

En el pasado, las acciones judiciales contra la falsificación informática resultaban poco habituales dado que la mayoría de documentos jurídicos eran tangibles. Los documentos digitales, que desempeñan una función cada vez más importante, se utilizan con mayor frecuencia. La utilización de documentos digitales, en sustitución de documentos clásicos, se sustenta por medios jurídicos como, por ejemplo, la legislación que reconoce las firmas digitales.

Los delincuentes siempre han intentado manipular documentos. Con la falsificación informática, se puede ahora copiar documentos digitales sin ninguna pérdida de calidad y manipularlos fácilmente. A los expertos forenses les resulta difícil comprobar las manipulaciones digitales a menos que se apliquen medios técnicos de protección[526] para evitar la falsificación de un documento.[527]

2.8.3 Robo de identidad

La expresión "robo de identidad", que no se ha definido ni utilizado coherentemente, alude al acto delictivo de obtener y adoptar de forma fraudulenta la identidad de otra persona[528]. Estos actos pueden cometerse sin recurrir a medios técnicos[529] o también en línea utilizando la tecnología Internet[530].

A partir de la gran cantidad de información que puede encontrarse en la prensa[531], resultado de diversas encuestas que analizan las pérdidas causadas por el robo de identidad[532], así como la amplitud del fenómeno, y de los numerosos análisis[533] jurídicos y técnicos publicados en los últimos años se llega fácilmente a la conclusión de que los delitos relacionados con la identidad son un fenómeno del siglo XXI[534]. Sin embargo, esa afirmación es falsa, pues la suplantación y la falsificación y utilización indebida de documentos de identidad son delitos que llevan practicándose más de un siglo[535]. Ya en la década de 1980 se denunciaba ampliamente en la prensa la utilización indebida de la información de identidad[536]. La aparición de la identidad digital y la tecnología de la información sólo ha modificado los métodos y las víctimas de los delincuentes[537]. La creciente utilización de la información digital ha abierto todo un campo de posibilidades para que los delincuentes puedan acceder a la información privada[538]. Así, la transformación de los países industrializados en sociedades de la información[539] ha tenido una gran influencia en la evolución de los delitos de robo de identidad. No obstante, a pesar de la gran cantidad de robos de identidad relacionados con Internet constatados, la digitalización no sólo ha supuesto un cambio fundamental para el timo mismo, sino que ha creado nuevos objetivos y ha facilitado la utilización de nuevos métodos[540]. Parece haberse sobrestimado la repercusión que ha tenido el creciente uso de la tecnología Internet. De acuerdo con los resultados de un análisis metodológico de los delitos relacionados con la identidad, el robo de identidad sigue siendo en gran medida un delito que se comete por medios distintos de los informáticos[541]. En 2007, los timos y los robos de datos en línea[542] representaron el 20 por ciento de los delitos en Estados Unidos[543]. Pese a los últimos adelantos, el robo de identidad por medios no informáticos sigue siendo sumamente importante. Es sorprendente que se siga cometiendo tantos delitos por medios no informáticos cuando la digitalización y aún más la globalización de los servicios de red hacen que cada vez se utilice más la información de identidad digital[544]. La información de identidad es cada vez

más importante tanto en las interacciones económicas como sociales. En el pasado, el "buen nombre" y las buenas relaciones personales dominaban el comercio y las actividades cotidianas[545]. El comercio electrónico difícilmente permite la identificación presencial, por lo que la información de identidad ha adquirido mucha importancia para las personas que interactúan social y económicamente[546]. Este proceso puede describirse como una instrumentalización[547], donde la identidad se traduce en información de identidad cuantificable. Este proceso, junto con la distinción entre el aspecto más filosófico del término "identidad" (definido[548] como el conjunto de características de una persona) y la información de identidad cuantificable que permite reconocer a una persona, es de gran importancia. El proceso de transformación no sólo atañe a los aspectos relacionados con Internet del robo de identidad, pues su repercusión va mucho más allá de las redes informáticas. Hoy en día los requisitos de las transacciones no presenciales, como la confianza y la seguridad[549], dominan la economía en general y no sólo el comercio electrónico. Un ejemplo puede encontrarse en la utilización de tarjetas de pago con NIP (número de identificación personal) para la adquisición de productos en un supermercado.

Por lo general, este delito consta de tres etapas diferentes[550]. En la primera etapa, el delincuente obtiene información relativa a la identidad mediante, por ejemplo, programas informáticos dañinos o ataques destinados a la *peska*. La segunda etapa se caracteriza por la interacción con la información obtenida antes de utilizarla en el marco de una actividad delictiva[551], como ocurre con la venta de ese tipo de información[552]. Se venden, por ejemplo, listas de tarjetas de crédito a un precio de hasta 60 USD[553]. La tercera etapa consiste en la utilización de la información relativa a la identidad en relación con una actividad delictiva. En la mayoría de los casos, con el acceso a esos datos los delincuentes pueden perpetrar nuevos delitos[554] y, por ese motivo, dan menos prioridad al conjunto de datos propiamente dicho que a la capacidad para utilizarlos en actividades delictivas. Pueden citarse como ejemplo la falsificación de documentos de identidad o el fraude de las tarjetas de crédito[555].

Los métodos aplicados para obtener datos, en el marco de la primera etapa, abarcan una gran variedad de acciones. El delincuente puede utilizar métodos físicos y, por ejemplo, robar dispositivos informáticos de almacenamiento con datos de identidad, revisar la "basura" ("recolección de desechos")[556] o proceder al robo de correo[557]. También puede utilizar motores de búsqueda para identificar ese tipo de datos. "*Googlehacking*" o "*Googledorks*" son términos que describen la formulación de preguntas complejas al motor de búsqueda con la finalidad de obtener un gran número de resultados con información relativa a cuestiones de seguridad informática así como datos personales que podrían ser utilizados en delitos vinculados al robo de identidad. El delincuente puede tener como finalidad, por ejemplo, buscar sistemas de protección de contraseñas poco seguros para obtener datos[558]. Algunos Informes ponen de relieve los peligros que se corren debido a la utilización legal de motores de búsqueda con fines ilegales[559]. Se han dado a conocer también problemas similares con respecto a los sistemas de intercambio de archivos. El Congreso de los Estados Unidos mantuvo recientemente un debate sobre los sistemas de intercambio de archivos y sus posibilidades de obtener información personal que puede servir para cometer el delito de robo de identidad[560]. Por otra parte, los delincuentes pueden obtener esa información recurriendo a iniciados, que tienen acceso a datos de identidad almacenados. En la Encuesta sobre Seguridad y Delitos Informáticos de 2007 realizada por el CSI[561] se observa que más del 35 por ciento de los encuestados atribuye un porcentaje superior al 20 por ciento de las pérdidas de su organización a la acción de los iniciados. En una encuesta realizada en 2013 se muestra que el 23 por ciento de los delitos por medios electrónicos se debe a los iniciados y que el 53 por ciento de los encuestados estima que esos ataques son más perjudiciales que los cometidos por extraños.[562] Por último, los delincuentes pueden emplear técnicas de ingeniería social para convencer a las víctimas de revelar información personal. En los últimos años, los delincuentes han concebido ardides ingeniosos para obtener información secreta (como datos de cuentas bancarias o de tarjetas de crédito) manipulando a los usuarios con técnicas de ingeniería social[563].

Hay varios tipos de datos que interesan a los delincuentes[564], siendo los más importantes los números de la seguridad social o del pasaporte; la fecha de nacimiento, dirección y números de teléfono, y las contraseñas.

Número de la seguridad social (SSN) o número de pasaporte

El SSN (equivalente al número del documento nacional de identidad) utilizado en los Estados Unidos es un ejemplo clásico del tipo de dato de interés para los delincuentes. Aunque se creó con objeto de mantener

un registro exacto de los ingresos, el SSN se utiliza actualmente con fines de identificación personal[565]. Los delincuentes pueden utilizarlo, de la misma forma que el número de pasaporte, para abrir cuentas financieras o apropiarse de las ya existentes, solicitar créditos o acumular deudas.[566]

Fecha de nacimiento, dirección y números de teléfono

Por lo general, estos datos sólo pueden utilizarse para el robo de identidad si van acompañados de otro tipo de información (por ejemplo, el SSN)[567]. El acceso a la información complementaria que representa la fecha de nacimiento y la dirección, puede servirle al delincuente para eludir procedimientos de verificación. Uno de los más graves peligros de este tipo de información es que actualmente puede encontrarse sin mayores problemas en Internet, ya sea porque se ha incorporado voluntariamente en alguno de los numerosos foros de contacto social[568] o porque responde a requisitos legales, como los pies de imprenta de las páginas web.[569]

Contraseña de cuentas no financieras

Si conocen la contraseña de una cuenta, los delincuentes pueden modificar sus particularidades y utilizarla para sus propios fines[570]. Por ejemplo, podrían apropiarse de una cuenta de correo electrónico y enviar mensajes con contenidos ilegales o apoderarse de la cuenta del usuario de una plataforma de subastas y utilizarla para vender mercancías robadas.[571]

Contraseña de cuentas financieras

Como ocurre con los SSN, la información relativa a las cuentas financieras es un objetivo muy difundido en lo que atañe al robo de identidad, y se refiere a cuentas bancarias y de ahorro, tarjetas de crédito y de débito, así como a datos sobre planificación financiera. Este tipo de información constituye una fuente importante para que el ladrón de identidad cometa ciberdelitos de carácter financiero.

El robo de identidad es un problema grave y que está en aumento[572]. Según cifras recientes, en el primer semestre de 2004, el 3 por ciento de los hogares estadounidenses fue víctima de ese delito[573]. El Bureau of Justice Statistics de Estados Unidos anunció en 2012 que, en el curso de ese año, el 7 por ciento de los habitantes a partir de 16 años había sido víctima de al menos un incidente de robo de identidad.[574] En el Reino Unido, se calculó que el costo que representa el robo de identidad para la economía británica asciende a 1,3 billones de libras esterlinas por año[575]. Las estimaciones de pérdidas causadas por el robo de identidad en Australia varían entre menos de 1 000 millones USD a más de 3 000 millones USD anuales[576]. En la Encuesta sobre Fraude de Identidad de 2006 se estimó que las pérdidas registradas en los Estados Unidos alcanzaron los 56 600 millones USD en 2005[577]. Según el Informe sobre Fraude de Identidad de 2013, se registraron pérdidas por valor de 20.900 millones en 2012. Las pérdidas no sólo son financieras ya que contemplan también las estimaciones por daños y perjuicios[578]. En realidad, muchas víctimas no denuncian este tipo de delitos y las instituciones financieras, por lo general, prefieren no dar a conocer las malas experiencias de sus clientes. Es probable que la incidencia real del robo de identidad supere con creces el número de pérdidas comunicadas[579].

Se puede cometer este delito debido al escaso número de instrumentos necesarios para verificar la identidad de los usuarios por Internet. Resulta fácil identificar a las personas en el mundo real, pero la mayoría de los métodos de identificación en línea son más complejos. Las herramientas de identificación más modernas (por ejemplo, las que utilizan datos biométricos) son costosas y no están muy difundidas. Las actividades en línea tienen pocos límites y, por ello, el robo de identidad es fácil y rentable.[580]

La evolución hacia los "big data" está estrechamente vinculada al creciente aumento de la cantidad de información de identidad disponible en los "mercados negros". Si logran acceder a bases de datos que contienen millones de registros de los clientes, los delincuentes podrían vender un número considerable de esos datos. En un estudio publicado en 2014 se indica, por ejemplo, que la información de identidad que puede hallarse en los cibermercados negros y que ha sido obtenida mediante el robo de datos, abarca credenciales de hasta 360 millones de cuentas.[581]

2.8.4 Utilización indebida de dispositivos

Para cometer un ciberdelito sólo hace falta un equipo sumamente básico[582]. Delitos como la difamación o el fraude en línea no necesitan más que una computadora y el acceso a Internet, y pueden llevarse a cabo en un cibercafé. Pueden cometerse otros delitos más refinados utilizándose en ese caso herramientas informáticas especiales.

Todas las herramientas necesarias para cometer delitos más refinados pueden encontrarse en Internet[583] y, generalmente, en forma gratuita. Las más modernas cuestan varios miles de dólares[584]. Con ellas, los delincuentes pueden atacar otros sistemas informáticos pulsando tan sólo una tecla. Los ataques más habituales son ahora menos eficaces ya que las empresas de programas informáticos de protección analizan las herramientas actualmente disponibles y se preparan para ese tipo de piratería. Los ataques de mayor resonancia suelen diseñarse exclusivamente para objetivos específicos [585] . Pueden encontrarse herramientas informáticas para [586] cometer ataques por denegación de servicio (DoS) [587], diseñar virus informáticos, desencriptar información y acceder en forma ilegal a sistemas informáticos.

Con las actuales herramientas informáticas de la segunda generación se ha logrado la automatización de muchos ciberdelitos, y los delincuentes pueden llevar a cabo numerosos ataques en muy poco tiempo. Además, las herramientas informáticas simplifican los ataques, de modo que hasta los usuarios menos experimentados pueden cometerlos. Con las herramientas disponibles para el correo basura, casi todos pueden enviar ese tipo de correo[588]. Se cuenta también con herramientas para descargar archivos de los sistemas de intercambio de archivos o para colocarlos en ellos. Debido a la gran disponibilidad de herramientas informáticas especialmente concebidas, el número de posibles delincuentes ha aumentado de forma espectacular. Se están formulando diferentes iniciativas nacionales e internacionales en materia de legislación para combatir las herramientas informáticas que propician ciberdelitos, por ejemplo, tipificando como delito su producción, venta o propiedad.[589]

2.9 Combinación de delitos

Bibliografía (seleccionada): *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001; *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf; *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006; *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001); *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45, page 1033 *et seq.*; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996; *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007; *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27; *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008; *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010; *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

Se utilizan varios términos para describir delitos complejos que abarcan numerosas actividades delictivas diferentes. Pueden citarse como ejemplo los siguientes: ciberterrorismo, ciberblanqueo de dinero y peska.

2.9.1 Ciberterrorismo

Ya durante el decenio de 1990 el debate sobre la utilización de la red por organizaciones terroristas giraba en torno a los ataques cometidos en la red contra infraestructuras esenciales como el transporte o el suministro de energía ("ciberterrorismo") y al uso de la tecnología de la información en conflictos armados ("guerra informática")[590]. El éxito alcanzado por ataques con virus y redes robot son una prueba clara de las deficiencias de la seguridad en la red. Se pueden cometer, y con buenos resultados, ataques terroristas por Internet[591], pero resulta difícil evaluar la importancia de las amenazas[592]; en ese momento, la interconexión no había alcanzado la difusión actual, siendo ése probablemente -aparte del interés de los Estados de mantener en secreto el gran éxito de esos ataques- uno de los principales motivos de que poquísimos incidentes de este tipo se hayan hecho públicos. Por consiguiente, al menos en el pasado, la caída de un árbol planteaba más riesgos para el suministro de energía que un ataque pirata afortunado[593].

La situación cambió después de los atentados del 11 de septiembre. Se entabló a partir de entonces un intenso debate sobre la utilización de las TIC por los terroristas[594], propiciado por Informes[595] que revelaban el uso de Internet en la preparación del ataque[596]. Aunque no fueron ciberataques, puesto que el grupo que perpetró los atentados no cometió ataques por Internet, ésta se utilizó en la preparación de los mismos[597]. En el marco de este contexto, se descubrió que las organizaciones terroristas utilizan Internet de distintas formas[598]. Hoy ya se sabe que los terroristas recurren a las TIC y a Internet para los siguientes fines:

- propaganda
- recopilación de información
- preparación de ataques al mundo real
- publicación de material de capacitación
- comunicación
- financiación de actividades terroristas
- ataques contra infraestructuras esenciales.

Este giro del debate tuvo consecuencias positivas para los estudios sobre ciberterrorismo puesto que puso de relieve esferas de las actividades terroristas desconocidas hasta entonces. Sin embargo, a pesar de la importancia de tener en cuenta un enfoque exhaustivo, convendría que la amenaza de los ataques contra infraestructuras esenciales a través de Internet no dejara de ser el centro del debate. Debido a la vulnerabilidad de las tecnologías de la información y a la creciente subordinación a ellas[599], los ataques por Internet contra infraestructuras esenciales deben incluirse en estrategias concebidas para evitar el ciberterrorismo y combatirlo.

Pese a una investigación más intensiva, el combate contra el ciberterrorismo sigue siendo difícil. Cuando se comparan los diferentes enfoques adoptados según los países, se observan muchas similitudes con respecto a las estrategias[600]. Uno de los motivos es el reconocimiento de la comunidad internacional de que las amenazas del terrorismo internacional exigen soluciones a escala mundial[601]. Pero lo que no se sabe todavía a ciencia cierta es si este enfoque es favorable o si diferentes sistemas jurídicos y características culturales diferentes requieren soluciones distintas. Una evaluación de este problema conlleva dificultades singulares dado que, aparte de los Informes sobre los principales incidentes, hay muy pocos datos disponibles que podrían servir para efectuar análisis científicos. Se plantean las mismas dificultades en lo que concierne a la determinación del grado de amenaza relativo a la utilización de las tecnologías de la información por parte de organizaciones terroristas. Por regla general, esa información es confidencial y, por lo tanto, está únicamente en manos de los servicios de inteligencia[602]. No se ha logrado siquiera llegar a un consenso con respecto a la definición de "terrorismo"[603]. En un Informe del CRS al Congreso de los Estados Unidos, por ejemplo, se afirma que el hecho de que un terrorista adquiera por Internet un billete de avión a los Estados Unidos es una prueba de que los terroristas recurren a Internet para preparar sus ataques[604]. Parece un argumento un poco vago puesto que la compra de un billete de avión no se convierte en actividad terrorista sólo porque la lleve a cabo un terrorista.

Propaganda

En 1998, sólo 12 de las 30 organizaciones terroristas internacionales consignadas en el Departamento de Estado de los Estados Unidos disponían de páginas web para dar a conocer públicamente sus actividades[605]. En 2004, según el Instituto de los Estados Unidos para la Paz, prácticamente todas las organizaciones terroristas tenían páginas web, entre ellas Hamas, Hezbollah, PKK y Al Qaida[606]. Los terroristas también han comenzado a participar en comunidades vídeo (como YouTube) para distribuir mensajes y propaganda[607]. La utilización de páginas web y otros foros es una señal de la importancia que atribuyen los grupos subversivos a relaciones públicas más profesionales[608]. La finalidad de recurrir a páginas web y otros medios reside en distribuir propaganda[609], dar una justificación[610] de sus actividades y reclutar[611] nuevos miembros y donantes así como establecer contacto con los ya existentes[612]. En algunas páginas web se han difundido recientemente vídeos de ejecuciones.[613]

Recopilación de información

En Internet puede hallarse información considerable sobre posibles objetivos[614]. Por ejemplo, los arquitectos publican en sus páginas web planos de edificios públicos en cuya construcción participan (véase la Figura 19). A través de diversos servicios Internet y de forma gratuita pueden obtenerse actualmente imágenes de satélite de alta resolución que años atrás sólo estaban a disposición de un puñado de instituciones militares de todo el mundo[615]. Asimismo, en un programa de ciberaprendizaje, se han hallado instrucciones para la construcción de bombas y hasta campos de entrenamiento virtuales que dan instrucciones para la utilización de armas[616]. Por otra parte, se ha encontrado información delicada o confidencial, no protegida adecuadamente contra robots de búsqueda, a la que se puede tener acceso a través de motores de búsqueda[617]. En 2003, el Departamento de Defensa de los Estados Unidos tuvo conocimiento de la existencia de un manual de capacitación vinculado a Al Qaeda con información que fuentes públicas podrían utilizar para obtener detalles sobre posibles objetivos[618]. En 2006, el New York Times informó que se había publicado información básica relativa a la fabricación de armas nucleares en una página web del Gobierno que presentaba pruebas sobre la capacidad de Iraq para fabricar dichas armas[619]. Un incidente similar tuvo lugar en Australia, cuando en páginas web del Gobierno apareció información detallada sobre posibles objetivos de atentados terroristas[620]. En 2005, según la prensa alemana, un grupo de investigadores descubrió que dos sospechosos de ataques al transporte público con bombas de fabricación casera, habían teledescargado de Internet en sus computadores manuales con instrucciones para la fabricación de explosivos.[621]

Preparación de ataques al mundo real

Para preparar un ataque, los terroristas pueden utilizar las tecnologías de la información de diferentes maneras. El envío de correo electrónico o la participación en foros para dejar mensajes son dos ejemplos que se analizarán en el contexto de la comunicación. Actualmente se examinan formas más directas de actividades de preparación en línea. Según algunos Informes publicados, los terroristas están utilizando juegos en línea para preparar sus atentados[622]. Hay numerosos y diversos juegos disponibles en línea que simulan el mundo real y, para participar en él, sus usuarios pueden encarnar a diversos personajes. En teoría, esos juegos podrían servir para simular ataques pero no podría descartarse aún que hayan contribuido de alguna manera a esa actividad.[623]

Publicación de material de capacitación

A través de Internet se propaga material de capacitación, por ejemplo, instrucciones para utilizar armas y seleccionar objetivos. Ese tipo de material puede obtenerse a gran escala de diferentes fuentes en línea[624]. En 2008, los servicios secretos occidentales descubrieron un servidor de Internet que facilitaba el intercambio de material de capacitación y la comunicación[625]. Según se informó, las organizaciones terroristas se sirven de diferentes páginas web para coordinar sus actividades.[626]

Comunicación

Las organizaciones terroristas no se limitan a utilizar las tecnologías de la información para crear páginas web o buscar información en las bases de datos. En el marco de las investigaciones realizadas después de

los atentados del 11 de septiembre, se afirmó que los terroristas se comunicaban por correo electrónico para coordinar sus ataques[627]. Los diarios informaron acerca del intercambio de instrucciones detalladas sobre los objetivos y el número de atacantes a través del correo electrónico[628]. Si los terroristas utilizan tecnologías de encriptación y medios de comunicaciones anónimas, resulta más difícil identificarlos y controlar su comunicación.

Financiación de actividades terroristas

La mayoría de las organizaciones terroristas dependen de los recursos financieros que reciben de terceros. Seguir el rastro de esas transacciones financieras se ha constituido en una estrategia importante en la lucha contra el terrorismo después de los atentados del 11 de septiembre. Una de las principales dificultades al respecto reside en que los recursos financieros requeridos para cometer atentados no son necesariamente elevados[629]. Con miras a la financiación terrorista, los servicios de Internet pueden utilizarse de varias formas. Las organizaciones terroristas pueden recurrir a sistemas de pago electrónico para favorecer las donaciones en línea[630]. También pueden utilizar páginas web para explicar la forma de hacer una donación, por ejemplo qué cuenta bancaria utilizar en las transacciones. A título de ejemplo, la organización "Hizb al-Tahrir" publicó los datos de una cuenta bancaria destinada a posibles donantes[631]. También se pueden efectuar donaciones en línea mediante tarjetas de crédito. El Ejército Republicano Irlandés (IRA) fue una de las principales organizaciones terroristas que propuso este tipo de donación[632]. En ambos casos se corre el riesgo de que se descubra la información publicada utilizándola para rastrear transacciones financieras. Es probable por tanto que los sistemas de pago electrónico anónimo alcancen mayor difusión. Para evitar que las descubran, las organizaciones terroristas tratan de ocultar sus actividades implicando a quienes no despiertan sospechas, como las organizaciones caritativas. Otro método (relacionado con Internet) es utilizar tiendas web falsas. Resulta relativamente fácil crear una tienda virtual en Internet. Una de las principales ventajas de la red es la posibilidad de efectuar actividades comerciales en todo el mundo. Es muy difícil demostrar que las transacciones financieras realizadas en esos sitios no se deben a compras habituales sino a donaciones. Habría que investigar cada transacción, operación nada fácil si la tienda virtual está en funcionamiento en una jurisdicción diferente o si se utilizaron sistemas de pagos anónimos.[633]

Ataques contra infraestructuras esenciales

Además de los ciberdelitos habituales, como el fraude y el robo de identidad, los ataques contra infraestructuras esenciales de la información también podrían convertirse en un objetivo terrorista. Dada la dependencia incesante en las tecnologías de la información, la infraestructura esencial es más vulnerable a los ataques[634]. Es lo que ocurre especialmente con los ataques contra sistemas interconectados a través de computadoras y redes de comunicación[635], puesto que los trastornos ocasionados por un ataque a la red no se limitan a los fallos de un solo sistema. Hasta breves interrupciones en los servicios podrían causar enormes daños financieros a las actividades del cibercomercio, y no sólo en relación con la administración pública sino también con los servicios e infraestructuras militares[636]. Investigar o incluso impedir esos ataques supone desafíos singulares[637]. A diferencia de los ataques físicos, los delincuentes no necesitan estar presentes en el lugar afectado[638]. Y mientras llevan a cabo el ataque, pueden utilizar medios de comunicaciones anónimas y tecnologías de encriptación para ocultar su identidad[639]. Como ya se indicó anteriormente, la investigación de este tipo de ataques exige instrumentos de procedimiento especiales, una tecnología aplicada a la investigación y personal capacitado[640].

Muchos reconocen que la infraestructura esencial es un posible objetivo de atentado terrorista puesto que, por definición, resulta vital para la estabilidad y perdurabilidad del Estado[641]. Una infraestructura se considera esencial si su incapacidad o destrucción puede afectar negativamente la defensa o seguridad económica de un Estado[642]. Se trata, en particular, de sistemas de energía eléctrica y de suministro de agua, sistemas de telecomunicaciones, sistemas de almacenamiento y transporte de gas y petróleo, servicios bancarios y financieros, sistemas de transporte y servicios de emergencia. Los trastornos ocasionados por la interrupción de servicios a causa del huracán Katrina en los Estados Unidos es un ejemplo de la dependencia de la sociedad en esos servicios[643]. El software maligno "Stuxnet" pone de manifiesto la nueva amenaza que suponen los ataques por Internet a la infraestructura esencial[644]. En 2010, una empresa de seguridad de Belarús descubrió un nuevo software maligno [645]. Aún se están investigando las

manipulaciones efectuadas por el software, así como la identidad de su creador y los motivos que lo movieron, pero aún no se han descubierto todos los hechos, en particular en lo que concierne al diseñador y su motivación[646]. No obstante, el software mismo y sobre todo su funcionamiento se conocen ya bastante bien.

Se sabe que es un software complejo con más de 4 000 funciones[647] cuyo objetivo son los sistemas de control industrial (ICS)[648], en particular los de la empresa tecnológica Siemens[649]. Su distribución se realizó a través de dispositivos extraíbles y se utilizó en cuatro ocasiones para infectar los sistemas informáticos[650]. Se ha constatado la infección de sistemas informáticos en Irán, Indonesia y Pakistán, además de Estados Unidos y algunos países europeos[651]. Aunque una de las características de los software malignos es su gran sofisticación, en algunos informes este punto se pone en tela de juicio[652].

Como ya se ha indicado, determinar quién ha creado el software y por qué es mucho más difícil y no se sabe nada con certidumbre. Recientes informes y estudios manejan la hipótesis de que el programa puede haber estado destinado a las instalaciones de enriquecimiento de Uranio de Irán y haber retrasado el programa nuclear de ese país[653].

Del descubrimiento de este software maligno se desprenden dos conclusiones. En primer lugar, el incidente pone de manifiesto que la infraestructura esencial depende en gran medida de la informática y que es posible atacarla. En segundo lugar, su distribución, entre otros, mediante dispositivos extraíbles demuestra que no basta con desconectar los sistemas informáticos de Internet para prevenir los ataques.

La vulnerabilidad de la infraestructura esencial ante los ataques perpetrados en la red puede demostrarse con algunos incidentes vinculados al transporte aéreo, que en muchos países también se considera parte de la infraestructura esencial. El sistema de facturación puede ser objetivo de ataques. Los servicios de facturación de la mayoría de los aeropuertos del mundo ya disponen de sistemas informáticos interconectados[654]. En 2004, el virus informático Sasser[655] infectó millones de computadoras en todo el mundo, incluidos los sistemas informáticos de las principales compañías aéreas, con la consiguiente cancelación de vuelos[656].

Otro posible objetivo son los sistemas de venta de billetes en línea. Actualmente, se compran en línea un número importante de billetes de avión. Las compañías aéreas utilizan las tecnologías de la información para diversas operaciones, y las principales compañías ofrecen a sus clientes la posibilidad de adquirir billetes en línea. Como sucede con otras actividades de cibercomercio, estos servicios en línea pueden convertirse en un objetivo para los delincuentes, que recurren habitualmente a una técnica conocida como ataques por denegación de servicio (DoS)[657]. En 2000, durante un plazo muy breve, se cometieron varios ataques de ese tipo contra empresas bien conocidas como CNN, Ebay y Amazon[658], a raíz de los cuales algunos servicios fueron interrumpidos durante varias horas e incluso días[659]. Las compañías aéreas también han sido víctimas de ataques DoS, como el cometido contra la página web de Lufthansa en 2001[660].

Por último, otro posible objetivo de los ataques contra la infraestructura esencial del transporte aéreo consumados por Internet es el sistema de control de los aeropuertos. La vulnerabilidad de los sistemas informáticos de control aéreo se puso de manifiesto en el ataque pirata cometido contra el aeropuerto de Worcester de los Estados Unidos en 1997[661], durante el cual dejaron de funcionar los servicios telefónicos de la torre de control y el sistema de control de luces de la pista de aterrizaje[662]

2.9.2 Guerra informática

Tras los ataques contra los sistemas informáticos de Estonia en 2007 y Georgia en 2008, y el descubrimiento del virus "Stuxnet"[663], el término guerra informática se emplea con frecuencia para describir tal situación, aunque, como se verá más adelante, la utilización de este término resulta problemática.

Terminología y definiciones

No hay una terminología unificada ni una definición ampliamente aceptada del concepto de guerra informática. Otros términos utilizados son guerra de información, guerra electrónica, ciberguerra, guerra en red, operaciones informáticas[664]. Esos términos suelen emplearse para describir la utilización de las TIC para actividades bélicas en Internet. Otras definiciones más restrictivas consideran esas actividades como

un tipo de conflicto armado centrado en la gestión y utilización de la información en todas sus modalidades y a todos los niveles para obtener una ventaja militar decisiva, en particular en el entorno mixto y combinado[665]. Otras definiciones más amplias abarcan todo conflicto electrónico donde la información es un activo estratégico que merece ser conquistado o destruido.[666]

Evolución del debate

Este tema ha sido objeto de controversia durante décadas[667]. En un principio la atención se centró en la sustitución de las actividades bélicas convencionales por ataques informáticos o ejecutados con ordenadores[668], donde la capacidad de derribar a un enemigo sin siquiera entrar en batalla era uno de los elementos clave del debate[669]. Además, los ataques por la red son generalmente más baratos que las operaciones militares tradicionales[670] y hasta los países más pequeños pueden llevarlos a cabo. Quitando algunos casos concretos objeto de todas las citas, este debate sigue llevándose a cabo principalmente en términos hipotéticos[671]. Los dos casos más frecuentemente mencionados son los ataques informáticos sufridos por Estonia y Georgia. Sin embargo, la clasificación de un ataque como un acto de guerra requiere que se cumplan determinados criterios.

En 2007, Estonia sufrió una fuerte controversia acerca de la destrucción de un memorial de la Segunda Guerra Mundial, que dio lugar a disturbios callejeros en la capital[672]. Además de las protestas tradicionales, Estonia se vio sometida a varias olas de ataques informáticos contra los sitios web y los servicios en línea del gobierno y algunas empresas privadas[673], que comprendieron la supresión de sitios web[674], ataques contra servidores de nombre dominio y ataques de denegación de servicio (DDoS) distribuidos para los que se utilizaron redes robot[675]. Con respecto a estos últimos, los expertos explicaron posteriormente que el éxito de los ataques contra el sitio web oficial del gobierno de Estonia[676] sólo se podía explicar por la inadecuación de las medidas de protección[677]. Las repercusiones de los ataques, así como su origen, fueron objeto de un controvertido debate. Si en las noticias[678] y artículos[679] se decía que los ataques estuvieron a punto de acabar con la infraestructura digital del país, fuentes más fiables demuestran que las consecuencias de los ataques fueron limitadas tanto en términos de sistemas informáticos afectados como de duración de la indisponibilidad de los servicios[680]. Un debate parecido se llevó a cabo sobre el origen del ataque. Si durante el ataque se indicó que su origen se encontraba en territorio de la Federación de Rusia[681], un posterior análisis demostró que, en realidad se vieron involucrados más de 170 países[682]. Aunque las motivaciones sean políticas, un ataque no es necesariamente un acto bélico. Por consiguiente, el caso de Estonia se ha de excluir de la lista. Aunque se trate de ataques informáticos contra los sitios web y los servicios en línea del gobierno y las empresas privadas[683], incluida la supresión de los sitios web[684] y los ataques de denegación de servicio distribuidos (DDoS)[685], tales ataques no pueden considerarse como guerra informática, pues no son una demostración de fuerza ni tuvieron lugar durante un conflicto entre dos Estados soberanos.

De los dos ataques citados, el ataque de 2008 contra los sistemas informáticos de Georgia es el que más se asemeja a un acto bélico. En el contexto de un conflicto armado convencional[686], entre la Federación de Rusia y Georgia, se constataron varios ataques informáticos contra sitios web estatales y empresas de Georgia[687] (incluida la supresión de sitios web y los ataques de denegación de servicio distribuidos)[688]. Al igual que en el caso de Estonia, mucho se ha hablado desde entonces del origen del ataque contra Georgia. Aunque nuevas informaciones [689] parecían haber encontrado el origen geográfico del ataque, las investigaciones tecnológicas indican que se utilizaron redes robot, lo que dificulta en gran medida la determinación del origen [690]. La incapacidad de determinar el origen de los ataques y que los actos constatados difieren notablemente de las actividades bélicas tradicionales hacen que difícilmente se puedan considerar como guerra informática.

Si bien todo el debate acerca de este fenómeno reviste una cierta importancia, hay que señalar que estos ataques no fueron los primeros. La difusión de propaganda por Internet y los ataques contra los sistemas informáticos de alianzas militares son bastante comunes. Ya durante la guerra de Yugoslavia los sistemas informáticos de la OTAN sufrieron ataques desde Serbia[691]. En respuesta, los Estados miembros de la OTAN dijeron haber participado en ataques similares contra sistemas informáticos serbios[692]. A fin de minar al enemigo se utilizaron masivamente la propaganda informática y operaciones psicológicas (PSYOPS) de otro tipo[693]

Importancia de la diferenciación

Las acciones potencialmente bélicas guardan muchas semejanzas con otros tipos de abuso de las TIC, como la ciberdelincuencia y el terrorismo en Internet. Por consiguiente, los términos "ciberdelincuencia", "terrorismo en Internet" y "guerra informática" suelen utilizarse indistintamente; motivo por el cual es muy importante establecer una diferencia, pues los marcos jurídicos aplicables no son en absoluto los mismos. Si bien la ciberdelincuencia suele tener como respuesta otros actos que la consideran una actividad delictiva, las reglas y procedimientos aplicables a la guerra dependen en su mayoría del derecho internacional y, en concreto, de la Carta de las Naciones Unidas.

2.9.3 Ciberblanqueo de dinero

El cese de actividades del proveedor de moneda electrónica "Liberty Reserve" fue noticia en 2013. [694] Con una cifra estimada en 6.000 millones USD, podría considerarse el caso de ciberblanqueo de dinero más importante de la historia. [695] En 2013, el Departamento del Tesoro de Estados Unidos publicó una información completa al respecto. Internet está transformado los métodos de blanqueo de dinero.[696] Pese a que, cuando se trata de cantidades importantes, las técnicas tradicionales proporcionan todavía un cierto número de ventajas, Internet facilita también varias ventajas. Los servicios financieros en línea ofrecen la opción de efectuar con gran rapidez numerosas transacciones financieras en todo el mundo. Internet ha contribuido a suprimir la dependencia de transacciones con dinero en efectivo. Las transferencias por cable sustituyeron el transporte de dinero en efectivo como primer paso para poner fin a esa dependencia, pero la implantación de normas más estrictas para detectar transferencias por cable dudosas ha obligado a los delincuentes a elaborar nuevas técnicas. La detección de transacciones sospechosas en la lucha contra el blanqueo de dinero se basa en obligaciones de las instituciones financieras que intervienen en las transferencias[697].

El ciberblanqueo de dinero se divide por lo general en tres etapas: depósito, estratificación e integración.

Con respecto al depósito de grandes cantidades de dinero en efectivo, Internet no podría quizás ofrecer esas numerosas ventajas tangibles[698], pero recurrir a ella resulta especialmente interesante para los delincuentes en la etapa de estratificación (u ocultamiento). En este contexto, la investigación es particularmente difícil cuando los blanqueadores de dinero utilizan casinos en línea[699].

Las normas que se aplican a las transferencias de dinero son por ahora limitadas e Internet ofrece a los delincuentes la posibilidad de realizar transferencias internacionales de dinero poco costosas y libres de impuestos. Las dificultades actuales en la investigación de técnicas de blanqueo de dinero por Internet emanan por lo general de la utilización de moneda virtual y de casinos en línea.

Utilización de moneda virtual

Uno de los motores fundamentales de la difusión de moneda virtual fue el micropago en operaciones (por ejemplo, teledescarga de artículos en línea que costaban 10 centavos USD o menos) en las que no podían utilizarse tarjetas de crédito. Con la demanda creciente de micropagos, se implantó la moneda virtual, incluidos los "valores en oro virtuales", siendo éstos sistemas de pago por cuenta cuya cuantía está respaldada por los depósitos en oro. Los usuarios pueden abrir cuentas virtuales en oro, generalmente sin tener que registrarse. Algunos proveedores autorizan incluso transferencias directas entre pares (persona a persona) o extracciones en efectivo[700]. Los delincuentes pueden abrir este tipo de cuentas en diferentes países y combinarlas, lo cual complica la utilización de instrumentos financieros para el blanqueo de dinero y la financiación de actividades terroristas. Además, en el momento de registrarse, los titulares de esas cuentas podrían facilitar información inexacta con objeto de ocultar su identidad[701].

Además de la moneda virtual simple, hay también monedas que combinan la virtualidad con el anonimato. Ejemplo de ello es la *Bitcoin*, moneda virtual utilizada en la tecnología punto a punto[702]. Aunque se trata de sistemas descentralizados que no requieren intermediaros centrales para garantizar la validez de las transacciones, los ataques llevados a cabo con éxito en 2011 ponen de manifiesto las debilidades/riesgos de tales monedas virtuales descentralizadas[703]. Si los delincuentes utilizan tales monedas anónimas,

resultará mucho más difícil para las fuerzas del orden identificar a los sospechosos gracias a las transferencias de dinero[704], por ejemplo en los casos relacionados con la pornografía infantil[705]

Utilización de casinos en línea

En contraposición al establecimiento de un verdadero casino, no se necesitan importantes inversiones para crear casinos en línea[706]. Por otra parte, la reglamentación de los casinos en línea y fuera de línea suele ser diferente según los países[707]. Sólo se pueden localizar las transferencias de dinero y demostrar que los fondos no son ganancias de lotería sino dinero blanqueado, si los casinos tienen constancia de ellas y lo ponen en conocimiento de las autoridades competentes.

La reglamentación jurídica actual de los servicios financieros por Internet no es tan estricta como la reglamentación tradicional. Dejando de lado ciertas lagunas en la legislación, los problemas que se encuentran a la hora de reglamentar son las dificultades en la verificación del cliente, pues la precisión de una verificación puede correr peligro si el proveedor del servicio financiero y el cliente no se han conocido nunca[708]. Además, la falta de contacto personal hace que resulte difícil aplicar procedimientos tradicionales del tipo "conozca a su cliente". Además, en las transferencias por Internet suelen participar proveedores de diversos países. Por último, la supervisión de las transacciones es particularmente complicada cuando los proveedores autorizan a los clientes a efectuar transferencias de valores con arreglo al modelo "de par a par".

2.9.4 Peska

Los ciberdelincuentes han elaborado técnicas para obtener información personal de los usuarios que van desde los programas espía[709] hasta los ataques destinados a la "*peska*"[710]. El término "*peska*" describe una serie de actos llevados a cabo para que las víctimas revelen información personal y/o secreta[711]. Aunque hay diferentes tipos de ataques de este último tipo[712], la *peska* a través de mensajes electrónicos consta de tres etapas importantes. En la primera, los delincuentes identifican empresas legítimas que proponen servicios en línea y mantienen una comunicación electrónica con clientes que pueden constituir su objetivo, por ejemplo, instituciones financieras. Proceden entonces a diseñar páginas web similares a las legítimas ("sitios pirata") solicitando a las víctimas que entren normalmente en ellas. De esta forma, los delincuentes obtienen datos personales (por ejemplo, números de cuentas y contraseñas de transacciones bancarias en línea).

Con objeto de guiar a los usuarios hacia sitios pirata, los delincuentes envían mensajes electrónicos similares a los de una empresa legítima[713], que con frecuencia dan lugar a violaciones en materia de marcas[714]. En esos mensajes piden a los destinatarios que entren en una determinada página web para actualizar datos o proceder a verificaciones de seguridad, o bien profieren amenazas (por ejemplo, cancelar la cuenta) si los usuarios no colaboran. El mensaje electrónico falso contiene generalmente un enlace que conduce a la víctima hacia el sitio pirata, evitando de esta forma que acceda manualmente a la dirección web correcta del banco legítimo. Los delincuentes han concebido técnicas avanzadas para impedir que los usuarios descubran que no se trata de la página web auténtica[715].

En cuanto la información es revelada, los delincuentes entran en las cuentas de sus víctimas para cometer delitos, como la transferencia de dinero, la solicitud de pasaportes y de nuevas cuentas, etc. El número creciente de ataques realizados es una prueba de las posibilidades que ofrece la *peska*[716]. Más de 55 000 sitios de *peska* exclusivos se pusieron en conocimiento del APWG[717] en abril de 2007[718]. En enero de 2014 ascendían a casi 43.000 los sitios exclusivos de *peska* detectados.[719] Las técnicas de *peska* no se limitan únicamente al acceso a las contraseñas de transacciones bancarias en línea. Los delincuentes también pueden tratar de acceder a códigos de computadoras, plataformas de subastas y números de la seguridad social (SSN), que tienen particular importancia en los Estados Unidos y pueden dar lugar a delitos de "robo de identidad".[720]

87 Other terminology used includes information technology crime and high-tech crime. See, in this context: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No. 2, page 144.

88 Regarding approaches to define and categorize cybercrime, see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the Council of Europe Convention on Cybercrime, No. 8; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf; Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at: www.aph.gov.au/Senate/Committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1.

89 *Nhan/Bachmann* in Maguire/Okada (eds), Critical Issues in Crime and Justice, 2011, page 166.

90 Regarding this relationship, see also: *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004, page 86.

91 Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

92 With regard to the definition, see also: *Kumar*, Cyber Law, A view to social security, 2009, page 29.

93 See, for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 *et seq.*; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

94 The Stanford Draft International Convention was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Stanford Draft is published in: The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

95 Article 1, Definitions and Use of Terms,

For the purposes of this Convention:

1. "cyber crime" means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;

[...]

96 See: *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

97 *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

98 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002,

No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq.*

99 Universal serial bus (USB)

100 Article 4 – Data Interference:

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

101 For difficulties related to the application of a cybercrime definition to real-world crimes, see: *Brenner*, Cybercrime Metrics: Old Wine, New Bottles?, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

102 In civil law countries, the use of such a legal term could lead to conflicts with the principle of certainty.

103 Some of the most well-known cybercrime offences are illegal access, illegal interception of computer data, data interference, computer-related fraud, computer-related forgery, dissemination of child pornography. For an overview see: *Sieber*, Council of Europe Organised Crime Report 2004; ABA International Guide to Combating Cybercrime, 2002; *Williams*, Cybercrime, 2005, in Miller, Encyclopaedia of Criminology.

104 *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

105 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. Regarding the Convention on Cybercrime see: *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

106 The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

107 Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences, see below: § 6.2.

108 Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences, see below: § 6.2.

109 Art. 9 (Offences related to child pornography). For more information about the offences, see below: § 6.2.

110 Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences, see below: § 6.2.

111 See below: § 2.5.

112 See below: § 2.6.

113 See below: § 2.7.

114 See below: § 2.8.

115 See below: § 2.9.1

[116] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

[117] Regarding the related challenges, see: *Slivka/Darrow*; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, page 217 *et seq.*

[118] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[119] See: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[120] *Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman*, Report of the Committee on the Preservation and Use of Economic Data, 1965, available at: www.archive.org/details/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965.

[121] *Miller*, The Assault on Privacy-Computers, 1971.

[122] *Westin/Baker*, Data Banks in a Free Society, 1972.

[123] For an overview about the debate in the US and Europe, see: *Sieber*, Computer Crime and Criminal Law, 1977.

[124] *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 48.

[125] *Stevens*, Identifying and Charging Computer Crimes in the Military, Military Law Review, Vol. 110, 1985, page 59.

[126] *Gemignani*, Computer Crime: The Law in '80, Indiana Law Review, Vol. 13, 1980, page 681.

[127] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[128] For an overview about cases see: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[129] *Freed*, Materials and cases on computer and law, 1971, page 65.

[130] *Bequai*, The Electronic Criminals – How and why computer crime pays, Barrister, Vol. 4, 1977, page 8 *et seq.*

[131] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, page 225 *et seq.*; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

[132] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Bequai*, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, page 22.

[133] *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 527.

[134] Regarding the number of the cases in early cybercrime investigations, see: *Schjolberg*, Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, page 6, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

[135] *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 58, Notes – A Suggested Legislative Approach to the Problem of Computer Crime, Washington and Lee Law Review, 1981, page 1173.

[136] *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976.

[137] Federal Computer Systems Protection Act of 1977. For more information, see: *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 2, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf; *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 531.

[138] Third Interpol Symposium on International Fraud, France 1979.

[139] Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, page 73.

[140] *BloomBecker*, The Trial of Computer Crime, Jurimetrics Journal, Vol. 21, 1981, page 428; *Schmidt*, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, Vol. 21, 1981, 345 *et seq.*; *Denning*, Some Aspects of Theft of Computer Software, Auckland University Law Review, Vol. 4, 1980, 273 *et seq.*; *Weiss*, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983, page 1 *et seq.*; *Bigelow*, The Challenge of Computer Law, Western England Law Review, Vol. 7, 1985, page 401; *Thackeray*, Computer-Related Crimes, Jurimetrics Journal, 1984, page 300 *et seq.*

[141] *Andrews*, The Legal Challenge Posed by the new Technology, Jurismetrics Journal, 1983, page 43 *et seq.*

[142] *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

[143] *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

[144] *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 4, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

[145] Computer-related criminality: Analysis of Legal Politics in the OECD Area, 1986.

[146] Computer-related crime: Recommendation No. R. (89) 9.

[147] Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

[148] Regarding the impact of the speed of data exchange on cybercrime investigation, see: § 3.2.10.

[149] Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

[150] A/RES/45/121 adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm

[151] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at: www.uncjin.org/Documents/EighthCongress.html.

[152] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. For more information, see: § 2.9.4.

[153] Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

[154] *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006.

[155] *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

[156] See for example: Big Data for Development: Challenges & Opportunities, UN Global Pulse, 2012; *Sircar*, Big Data: Countering Tomorrow's Challenges, Infosys Labs Briefings, Vol. 11, No. 1, 2013;

[157] *Hartmann/Steup,* The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment, published in Podins/Stinissen/Maybaum, 5th International Conference on Cyber Conflicts, 2013; *Kim/Wampler/Goppert/Hwang/Aldridge,* Cyber attack vulnerabilities analysis for unanned areal vehicles, American Institute of Aeronautics and Astronautics, 2012.

[158] *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[159] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[160] Regarding the emerging importance of crime statistics, see: *Osborne/Wernicke*, Introduction to Crime Analysis, 2003, page 1 *et seq.*, available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

[161] 2013 Internet Crime Report, Internet Crime Complaint Center, 2014, available at: www.ic3.gov/media/annualreport/2013_IC3Report.pdf.

[162] German Crime Statistics 2013, available at www.bka.de. As this number also includes traditional crimes that involved Internet technology at any stage of the offence, the increase of cases cannot necessarily be used to determine the specific development in the typology-based crime fields.

[163] Regarding the related difficulties, see: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 229, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[164] Regarding challenges related to crime statistics in general, see: *Maguire* in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 *et seq.* available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf.

[165] See in this context: Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009, page 9, available at: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

[166] *Alvazzi del Frate*, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

[167] Computer Crime, Parliamentary Office of Science and Technology, Postnote No. 271, Oct. 2006, page 3.

[168] Regarding the related challenges, see: *Kabay*, Understanding Studies and Surveys of Computer Crime, 2009, available at: www.mekabay.com/methodology/crime_stats_methods.pdf.

[169] The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, – available at: www.heise-security.co.uk/news/80152. See also: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, page 660.

[170] See *Mitchison/Urry*, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

[171] See *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; *Smith*, Investigating Cybercrime: Barriers and Solutions, 2003, page 2, available at: www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

[172] In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp.

[173] See SOCA, International crackdown on mass marketing fraud revealed, 2007, available at: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[174] In the 2006 NW3C Internet Crime report, only 1.7 per cent of the reported total USD losses were related to the Nigerian Letter Fraud, but those cases that were reported had an average loss of USD 5 100 each. The number of reported offences is very low, while the average loss of those offences is the high.

[175] With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[176] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[177] See in this context: *Hyde-Bales/Morris/Charlton*, The police recording of computer crime, UK Home Office Development and Practice Report, 2004.

[178] Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport, page 15.

[179] National Fraud Information Center, 2007 Internet Fraud Statistics, 2008, available at: www.fraud.org/internet/intstat.htm.

[180] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report.

181 2nd ISSA/UCD Irish Cybercrime Survey, 2008, available at: www.issaireland.org/2nd%20ISSA%20UCD%20Irish%20Cybercrime%20Survey%20-%20Results%2017DEC08.pdf.

182 Symantec Intelligence Quarterly, April-June 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport.

183 2010 CSO CyberSecurity Watch Survey, 2010.

184 2008 CSI Computer Crime and Security Survey, 2009, page 15.

185 Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at: www.symantec.com/business/theme.jsp?themeid=threatreport, page 7,

186 Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 2.

187 Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 8.

188 Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 8.

189 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

190 Goodin, PlayStation Network breach will cost Sony $ 171m, The Register, 24.05.2011, available at: www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/.

191 See 2005 FBI Computer Crime Survey, page 10.

192 See: § 2.4.

193 *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62; ECPAT, Violence against Children in Cyberspace, 2005, page 54; Council of Europe Organized Crime Situation Report 2005, Focus on Cybercrime, page 41.

194 *Bialik*, Measuring the Child-Porn Trade, The Wall Street Journal, 18.04.2006.

195 Computer Security Institute (CSI), United States.

196 The CSI Computer Crime and Security Survey 2007 is available at: www.gocsi.com/

197 See CSI Computer Crime and Security Survey 2007, page 1, available at: www.gocsi.com/. Having regard to the composition of the respondents, the survey is likely to be relevant for the United States only.

198 With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22, available at: www.gao.gov/new.items/d07705.pdf. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

199 See below: § 2.4.

200 Regarding the development of computer systems, see: *Hashagen*, The first Computers – History and Architectures.

201 See in this context, for example, the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

202 From a legal perspective, there is no real need to differentiate between "computer hackers" and "computer crackers" as – in the context of illegal access – both terms are used to describe persons who enter a computer system without right. The main difference is the motivation. The term "hacker" is used to describe a person who enjoys exploring the details of programmable systems, without breaking the law. The term "cracker" is used to describe a person who breaks into computer systems in general by violating the law.

203 In the early years of IT development, the term "hacking" was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term "hacking" was often used to describe a constructive activity.

204 See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61; *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985,

page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

[205] See the statistics provided by HackerWatch. The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported; *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.* in the month of August 2007. Source: www.hackerwatch.org.

[206] For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 *et seq.*; Regarding the impact, see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.*

[207] *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

[208] *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

[209] *Sieber*, Council of Europe Organised Crime Report 2004, page 66

[210] *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

[211] Hacking into a computer system and modifying information on the first page to prove the ability of the offender can – depending on the legislation in place – be prosecuted as illegal access and data interference. For more information, see below: § 6.2.1 and § 6.2.4.

[212] The term "hacktivism" combines the words hack and activism. It describes hacking activities performed to promote a political ideology. For more information, see: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf. Regarding cases of political attacks, see: *Vatis*, cyberattacks during the war on terrorism: a predictive analysis, available at: www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

[213] A hacker left messages on the website that accused the United States and Israel of killing children. For more information, see BBC News, "UN's website breached by hackers", available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm

[214] The abuse of hacked computer systems often causes difficulties for law-enforcement agencies, as electronic traces do not often lead directly to the offender, but first of all to the abused computer systems.

[215] Regarding different motivations and possible follow-up acts, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1;

[216] The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: www.hackerwatch.org.

[217] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.

[218] See Heise News, Online-Computer werden alle 39 Sekunden angegriffen, 13.02.2007, available at: www.heise.de/newsticker/meldung/85229. The report is based on an analysis from Professor Cukier.

[219] For an overview of examples of successful hacking attacks, see http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[220] Regarding threats from Cybercrime toolkits, see Opening Remarks by ITU Secretary-General, 2nd Facilitation Meeting for WSIS Action Line C5, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/sg-opening-remarks-14-may-2007.pdf. See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 29, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[221] For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[222] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

[223] Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[224] For an overview of the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[225] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9, available at: www.212cafe.com/download/e-book/A.pdf.

[226] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

[227] For an overview of the tools used to perform high-level attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; *Erickson*, Hacking: The Art of Exploitation, 2003.

[228] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: § 3.2.9.

[229] See *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[230] See in this context Art. 2, sentence 2, Convention on Cybercrime.

[231] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

[232] One example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a) until 2007, when the provision was changed. The following text is taken from the old version of Section 202a – Data Espionage:

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

[233] With regard to targeted attacks see for example: *Sood/Enbody*, Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, 2010. With regard to trends towards targeted attack see: Blurring Boundaries, Trend Micro Security Predictions for 2014 and Beyond, Trend Micro, 2014.

[234] With regard to details related to the damage of targeted attacks see: *Kaspersky*, IT Security Risks Survey 2014.

[235] Targeted Cyber Attacks, GFI White Paper, 2009, page 5.

[236] For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq.*; *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[237] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

[238] For more information about that case, see: *Stoll*, Stalking the wily hacker, available at: http://pdf.textfiles.com/academics/wilyhacker.pdf; *Stoll*, The Cuckoo's Egg, 1998.

[239] See *Sieber*, Council of Europe Organised Crime Report 2004, page 88 *et seq.*; *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[240] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

[241] Examples are software tools that are able to break passwords. Another example is a software tool that records keystrokes (keylogger). Keyloggers are available as software solutions or hardware solutions.

[242] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[243] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[244] For more information, see *Mitnick/Simon/Wozniak*, The Art of Deception: Controlling the Human Element of Security.

[245] See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See: *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

[246] Regarding the elements of an Anti-Cybercrime Strategy, see below: § 4.

[247] "Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems" – See OECD Guidelines for Cryptography Policy, V 2, available at: www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

[248] Physical research proves that it can take a very long time to break encryption, if proper technology is used. See *Schneier*, Applied Cryptography, page 185. For more information regarding the challenge of investigating cybercrime cases that involve encryption technology, see below: § 3.2.14.

[249] The Council of Europe Convention on Cybercrime contains no provision criminalizing data espionage.

[250] Regarding the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq.*

[251] Regarding the impact of this behaviour for identity theft, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

[252] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[253] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

[254] See *Hackworth*, Sypware, Cybercrime & Security, IIA-4. Regarding user reactions to the threat of spyware, see: *Jaeger/ Clarke*, The Awareness and Perception of Spyware amongst Home PC Computer Users, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Jaeger%20Clarke%20-%20The%20Awareness%20and%20Perception%20of%20Spyware%20amongst%20Home%20PC%20Computer%20Users.pdf

[255] See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

[256] For further information about keyloggers, see: http://en.wikipedia.org/wiki/Keylogger; Netadmintools Keylogging, available at: www.netadmintools.com/part215.html

[257] It is easy to identify credit-card numbers, as they in general contain 16 digits. By excluding phone numbers using country codes, offenders can identify credit-card numbers and exclude mistakes to a large extent.

[258] One approach to gain access to a computer system in order to install a keylogger is, for example, to gain access to the building where the computer is located using social engineering techniques, e.g. a person wearing a uniform from the fire brigade pretending to check emergency exits has a good chance of gaining access to a building, if more extensive security is not in place. Further approaches can be found in *Mitnick*, The Art of Deception: Controlling the Human Element of Security, 2002.

[259] Regular hardware checks are a vital part of any computer security strategy.

[260] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[261] See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606.

[262] For more information on the phenomenon of phishing, see below: § 2.9.4.

[263] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

[264] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

[265] Goodin, PlayStation Network breach will cost Sony $ 171m, The Register, 24.05.2011, available at: www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/.

[266] *Finkle*, 360 million newly stolen credentials on black market: cybersecurity firm, Reuters, 25.02.2014.

[267] *Leprevost*, Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, Development of surveillance technology and risk of abuse of economic information, 2.4, available at: http://cryptome.org/stoa-r3-5.htm.

[268] With the fall in price of server storage space, the external storage of information has become more popular. Another advantage of external storage is that information can be accessed from every Internet connection.

[269] Regarding the interception of VoIP to assist law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf. Regarding the potential of VoIP and regulatory issues, see: *Braverman*, VoIP: The Future of Telephony is now…if regulation doesn't get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47 *et seq.*, available at: www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

[270] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[271] *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

[272] The radius depends on the transmitting power of the wireless access point. See http://de.wikipedia.org/wiki/WLAN.

[273] With regard to the time necessary for decryption, see below: § 3.2.14.

[274] Regarding the difficulties in Cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

[275] *Sieber*, Council of Europe Organised Crime Report 2004, page 97.

[276] With regard to the interception of electromagnetic emissions, see: Explanatory Report to the Convention on Cybercrime, No. 57.

[277] See http://en.wikipedia.org/wiki/Computer_surveillance#Surveillance_techniques.

[278] e.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

[279] For more details on legal solutions, see below: § 6.2.4.

[280] See in this context also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[281] *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

[282] A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user, to harm the computer system. See *Spafford*, The Internet Worm Program: An Analysis, page 3; *Cohen*, Computer Viruses – Theory and Experiments, available at: http://all.net/books/virus/index.html; *Adleman*, An Abstract Theory of Computer Viruses, Advances in Cryptography – Crypto, Lecture Notes in Computer Science, 1988, page 354 *et seq.* Regarding the economic impact of computer viruses, see: *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12; Symantec Internet Security Threat Report,Trends for July-December 2006, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

[283] *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

[284] *White/Kephart/Chess*, Computer Viruses: A Global Perspective, available at: www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html.

[285] Payload describes the function the virus performs after it is installed on victims' computers and activated. Examples of the payload are displaying messages or performing certain activities on computer hardware, such as opening the CD drive or deleting or encrypting files.

[286] Regarding the various installation processes, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 21 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

[287] See BBC News, Virus-like attack hits web traffic, 25.01.2003, http://news.bbc.co.uk/2/hi/technology/2693925.stm;

[288] Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO, 2005 GAO-05-434, page 12, available at: www.gao.gov/new.items/d05434.pdf.

[289] *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[290] *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12, available at: www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[291] See *Szor*, The Art of Computer Virus Research and Defence, 2005.

[292] One example of a virus that encrypts files is the Aids Info Disk or PC Cyborg Trojan. The virus hid directories and encrypted the names of all files on the C-drive. Users were asked to 'renew their licence' and contact PC Cyborg Corporation for payment. For more information, see: *Bates*, "Trojan Horse: AIDS Information Introductory Diskette Version 2.0" in *Wilding/Skulason*, Virus Bulletin, 1990, page 3.

[293] Annual Report, Pandalabs, 2013.

[294] Kaspersky Press Release, 10.12.2013, available at: www.kaspersky.com/about/news/virus/2013/number-of-the-year.

[295] In 2000, a number of well-known United States e-commerce businesses were targeted by denial-of-service attacks. A full list of the attacks business is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[296] Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

[297] Examples include: Inserting metal objects in computer devices to cause electrical shorts, blowing hairspray into sensitive devices or cutting cables. For more examples, see *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

[298] Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

[299] *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

[300] A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

[301] The term "worm" was used by *Shoch/Hupp*, The 'Worm' Programs – Early Experience with a Distributed Computation, published in 1982. This publication is available for download: http://vx.netlux.org/lib/ajm01.html. With regard to the term 'worm', they refer to the science-fiction novel, "The Shockwave Rider" by John Brunner, which describes a program running loose through a computer network.

[302] For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP.

[303] See *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf.

[304] July, 2009 South Korea and US DDosc Attacks, Arbor Networks, 2009, available at: www.idcun.com/uploads/pdf/July_KR_US_DDoS_Attacks.pdf.

[305] July, 2009 South Korea and US DDosc Attacks, Arbor Networks, 2009, available at: www.idcun.com/uploads/pdf/July_KR_US_DDoS_Attacks.pdf.

[306] Regarding the different approaches, see below: § 6.2.6.

[307] 2012 Cost of Cyber Crime Study: United States, Ponemon, 2012, page 7.

[308] For reports on cases involving illegal content, see *Sieber*, Council of Europe Organised Crime Report 2004, page 137 *et seq.*

[309] One example of the wide criminalization of illegal content is Sec. 86a German Penal Code. The provision criminalizes the use of symbols of unconstitutional parties: Section 86a: Use of Symbols of Unconstitutional Organizations:

> (1) Whoever: 1. domestically distributes or publicly uses, in a meeting or in writings (Section 11 subsection (3)) disseminated by him, symbols of one of the parties or organizations indicated in Section 86 subsection (1), nos. 1, 2 and 4; or 2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use domestically or abroad, in the manner indicated in number 1, shall be punished with imprisonment for not more than three years or a fine.
> (2) Symbols, within the meaning of subsection (1), shall be, in particular, flags, insignia, uniforms, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in sentence 1 shall be deemed to be equivalent thereto.
>
> (3) Section 86 subsections (3) and (4), shall apply accordingly.

[310] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[311] Concerns over freedom of expression (e.g. the First Amendment to the United States Constitution) explain why certain acts of racism were not made illegal by the Convention on Cybercrime, but their criminalization was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

[312] The 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "in many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues". In 2008 the Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should desist from the further adoption of statements supporting the idea of defamation of religions.

[313] 1996 Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

[314] The 2002 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".

[315] International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, and the

ACHPR (African Commission on Human and Peoples Rights) Special Rapporteur on Freedom of Expression and Access to Information, 2008.

316 See below: §§ 3.2.6 and 3.2.7.

317 In many cases, the principle of dual criminality hinders international cooperation.

318 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/*; Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

319 Regarding this approach, see: *Stadler*, Multimedia und Recht 2002, page 343 *et seq.*; *Mankowski*, Multimedia und Recht 2002, page 277 *et seq.*

320 See *Sims*, Why Filters Can't Work, available at: http://censorware.net/essays/whycant_ms.html; *Wallace*, Purchase of blocking software by public libraries is unconstitutional, available at: http://censorware.net/essays/library_jw.html.

321 The OpenNet Initiative is a transatlantic group of academic institutions that reports on internet filtering and surveillance. Harvard Law School and the University of Oxford participate in the network, among others. For more information, see: www.opennet.net.

322 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

323 Depending on the availability of broadband access.

324 Access is in some countries is limited by filter technology. Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

325 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: § 6.5.

326 *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

327 About a third of all files downloaded in file-sharing systems contained pornography. *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

[328] One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch):

Section 184 Dissemination of Pornographic Writings
(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):

1. offers, gives or makes them accessible to a person under eighteen years of age; […]

[329] Regarding this aspect, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[330] See: *Nowara/Pierschke*, Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerterten Modellprojekten, 2008.

[331] See *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[332] One example is the 2006 Draft Law, Regulating the protection of Electronic Data and Information and Combating Crimes of Information (Egypt):

Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty.

[333] National sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[334] Regarding the principle of "dual criminality", see below: § 6.6.2.

[335] Regarding technical approaches in the fight against obscenity and indecency on the Internet, see: *Weekes*, Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

[336] Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion about filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

[337] Regarding the risk of detection with regard to non Internet-related acts, see: *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 63.

[338] *Healy*, Child Pornography: An International Perspective, 2004, page 4.

[339] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006, page, 1.

[340] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8 *et seq.*

[341] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[342] *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 62; Rights of the Child, Commission on Human Rights, 61st session, E/CN.4/2005/78, page 8; *Healy*, Child Pornography: An International Perspective, 2004, page 5; Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 19.

[343] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[344] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[345] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

[346] *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 41.

[347] Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17.

[348] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

[349] Vienna Commitment against Child Pornography on the Internet, 1st October 1999; Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 2; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 49.

[350] *Bloxsome/Kuhn/Pope/Voges*, The Pornography and Erotica Industry: Lack of Research and Need for a Research Agenda, Griffith University, Brisbane, Australia: 2007 International Nonprofit and Social Marketing Conference, 27-28 Sep 2007, page 196.

[351] Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 1; *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1. *McCulloch*, Interpol and Crimes against Children – in Quayle/Taylor, Viewing child pornography on the Internet: Understanding the offence, managing the offender, helping the victims, 2005.

[352] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29.

[353] *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29; *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62.

[354] According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[355] *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 7.

[356] See in this context, for example: *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 8.

[357] *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 64.

[358] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 12.

[359] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[360] See, for example, the "G8 Communique", Genoa Summit, 2001, available at: www.g8.gc.ca/genoa/july-22-01-1-e.asp.

[361] United Nations Convention on the Right of the Child, A/RES/44/25, available at: www.hrweb.org/legal/child.html. Regarding the importance of cybercrime legislation see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 35, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[362] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[363] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http://conventions.coe.int.

[364] *Sieber*, Council of Europe Organised Crime Report 2004, page 135. Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[365] See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

366 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 5, available at: www.missingkids.com/en_US/publications/NC144.pdf.

367 For more information, see: Child Pornography: Model Legislation & Global Review, 2010, page 3, available at: www.icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf.

368 See *Walden*, Computer Crimes and Digital Investigations, 2007, page 66.

369 It is possible to make big profits in a rather short period of time by offering child pornography – this is one way how terrorist cells can finance their activities, without depending on donations.

370 Police authorities and search engines forms alliance to beat child pornography, available at: http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/; "Google accused of profiting from child porn", available at: www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

371 See ABA, International Guide to Combating Cybercrime, page 73.

372 Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, Harvard Journal of Law & Technology, Volume 11, page 840 *et seq.*

373 For more information, see: *Wilson*, Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond., (1997) 30 Creighton Law Review 671 at 690.

374 *Smith*, Child pornography operation occasions scrutiny of millions of credit card transactions, available at: www.heise.de/english/newsticker/news/print/83427.

375 With regard to the concept see for example: *Nakamoto* (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

376 Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

377 Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at:

378 See below: § 3.2.14.

379 Based on the "National Juvenile Online Victimization Study", 12 per cent of arrested possessors of Internet-related child pornography used encryption technology to prevent access to their files. *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

380 See below: § 3.2.14.

381 For an overview of the different obligations of Internet service providers that are already implemented or under discussion, see: *Gercke*, Obligations of Internet Service Providers with regard to child pornography: legal issue, 2009, available at www.coe.int/cybercrime.

382 Radical groups in the United States recognized the advantages of the Internet for furthering their agenda at an early stage. See: *Markoff*, Some computer conversation is changing human contact, NY-Times, 13.05.1990.

383 *Sieber*, Council of Europe Organised Crime Report 2004, page 138.

384 *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in "Governing the Internet Freedom and Regulation in the OSCE Region", page 91, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

385 See: Digital Terrorism & Hate 2006, available at: www.wiesenthal.com.

386 *Whine*, Online Propaganda and the Commission of Hate Crime, available at: www.osce.org/documents/cio/2004/06/3162_en.pdf

387 See: ABA International Guide to Combating Cybercrime, page 53.

388 Regarding the criminalization in the United States, see: *Tsesis*, Prohibiting Incitement on the Internet, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.

[389] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[390] See: *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 *et seq.*; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 *et seq.*; Development in the Law, The Law of Media, Harvard Law Review, Vol. 120, page 1041.

[391] See: Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=213138298941949941944938934938937961519199 1.

[392] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144.

[393] See: Explanatory Report to the First Additional Protocol, No. 4.

[394] See: *Barkham*, Religious hatred flourishes on web, The Guardian, 11.05.2004, available at: www.guardian.co.uk/religion/Story/0,,1213727,00.html.

[395] Regarding legislative approaches in the United Kingdom see *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.192.

[396] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman,* Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[397] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[398] For more information on the "cartoon dispute", see: the Times Online, 70.000 gather for violent Pakistan cartoons protest, available at: www.timesonline.co.uk/tol/news/world/asia/article731005.ece; *Anderson*, Cartoons of Prophet Met With Outrage, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/01/30/AR2006013001316.html; *Rose*, Why I published those cartoons, Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2006/02/17/AR2006021702499.html.

[399] Sec. 295-C of the Pakistan Penal Code:

295-C. Use of derogatory remarks, etc., in respect of the Holy Prophet: Whoever by words, either spoken or written, or by visible representation or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Mohammed (Peace be Upon Him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

[400] Sec. 295-B of the Pakistan Penal Code:

295-B. Defiling, etc., of Holy Qur'an : Whoever wilfully defiles, damages or desecrates a copy of the Holy Qur'an or of an extract there from or uses it in any derogatory manner or for any unlawful purpose shall be punishable with imprisonment for life.

[401] Regarding the growing importance of Internet gambling, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf ; *Brown/Raysman*, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 *et seq.* available at: www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

[402] www.secondlife.com.

[403] The number of accounts published by Linden Lab. See: www.secondlife.com/whatis/. Regarding Second Life in general, see: *Harkin*, Get a (second) life, Financial Times, available at: www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

[404] Heise News, 15.11.2006, available at: www.heise.de/newsticker/meldung/81088; DIE ZEIT, 04.01.2007, page 19.

[405] BBC News, 09.05.2007 Second Life 'child abuse' claim, available at: http://news.bbc.co.uk/1/hi/technology/6638331.stm.

[406] *Leapman*, Second Life world may be haven for terrorists, Sunday Telegraph, 14.05.2007, available at: www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml; *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

[407] See: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[408] Christiansen Capital Advisor. See www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

[409] The revenue of United States casinos in 2005 (without Internet gambling) was more than USD 84 billion, from: *Landes*, Layovers And Cargo Ships: "The Prohibition Of Internet Gambling And A Proposed System Of Regulation", page 915, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

[410] Statista, Statistic Portal, Global Online Gambling Gross Win from 2006-2015, available at: www.statista.com/statistics/208456/global-interactive-gambling-gross-win/.

[411] See, for example, GAO, "Internet Gambling – An Overview of the Issues", available at: www.gao.gov/new.items/d0389.pdf. Regarding the WTO Proceedings "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; Article 21.5 panel concluded that the United States had failed to comply with the recommendations and rulings of the DSB.

[412] For more information, see: BBC News, Tiny Macau overtakes Las Vegas, at: http://news.bbc.co.uk/2/hi/business/6083624.stm.

[413] See Art. 300 China Criminal Code:

Whoever, for the purpose of reaping profits, assembles a crew to engage in gambling, opens a gambling house, or makes an occupation of gambling, is to be sentenced to not more than three years of fixed-term imprisonment, criminal detention, or control, in addition to a fine.

[414] Besides gambling in Macau, Chinese have started to use Internet gambling intensively. See: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[415] For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

[416] See: OSCE Report on Money Laundering Typologies 2000 – 2001, page 3, available at: www.oecd.org/dataoecd/29/36/34038090.pdf; *Coates*, Online casinos used to launder cash, available at: www.timesonline.co.uk/tol/news/politics/article620834.ece?print=yes&randnum=1187529372681.

[417] See, for example, Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[418] For an overview of the early United States legislation, see: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[419] See § 5367 Internet Gambling Prohibition Enforcement Act.

[420] See *Reder/O'Brien*, Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking The Identity Of Anonymous Employee Internet Posters, Mich. Telecomm. Tech. L. Rev. 195, 2002, page 196, available at www.mttlr.org/voleight/Reder.pdf.

[421] Regarding the situation in blogs, see*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[422] Regarding the privacy concerns related to social networks, see: *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available at: www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[423] Regarding the controversial discussion about the criminalization of defamation, see: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf.

[424] See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

[425] With regard to the challenges of investigating offences linked to anonymous services see below: § 3.2.l2.

[426] See: www.wikipedia.org

[427] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

[428] Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as www.archive.org.

[429] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[430] See in this context*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[431] For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[432] *Tempelton*, Reaction to the DEC Spam of 1978, available at: www.templetons.com/brad/spamreact.html.

[433] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[434] The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. The provider Postini published a report in 2007 identifying up to 75 per cent spam e-mail, see www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mail, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. Article in The Sydney Morning Herald, 2006: The year we were spammed a lot, 16 December 2006; www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html.

[435] 2007 Sophos Report on Spam-relaying countries, available at: www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

[436] Kaspersky Security Bulletin. Spam Evolution 2013.

[437] For more information about the technology used to identify spam e-mails, see: *Hernan/Cutler/Harris*, Email Spamming Countermeasures: Detection and Prevention of Email Spamming, available at: www.ciac.org/ciac/bulletins/i-005c.shtml. For an overview on different approaches, see: BIAC ICC Discussion Paper on SPAM, 2004, available at: www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf.

[438] *Lui/Stamm*, Fighting Unicode-Obfuscated Spam, 2007, page 1, available at: www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

[439] Regarding the filter technologies available, see: *Goodman*, Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam, ConsumerPerspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[440] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

[441] Current analyses suggest that up to a quarter of all computer systems may have been recruited to act as part of botnets, see: *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

[442] Regarding international approaches in the fight against botnets, see: ITU Botnet Mitigation Toolkit, Background Information, ICT Application and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

[443] See: *Allmann*, The Economics of Spam, available at:

http://acmqueue.org/modules.php?name=Content&pa=showpage&pid=108; *Prince*, ITU Discussion Paper "Countering Spam: How to Craft an Effective Anti-Spam Law", page 3 with further references, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

[444] Bulk discounts for spam, Heise News, 23.10.2007, available at: www.heise-security.co.uk/news/97803.

[445] *Thorhallsson*, A User Perspective on Spam and Phishing, in Governing the Internet Freedom and Regulation in the OSCE Region, page 208, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[446] Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[447] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[448] Regarding the terminology see: *Sulkowski*, Cyber-Extortion, Journal of Law, Technology & Policy, 2007, page 101 et seq.

[449] *Perlroth/Wortham*, Tech Start-Ups Are Targets of Ransom Cyberattacks, NYT, 03.04.2014; *Perlroth*, Tally of Cyber Extortion Attacks on Tech Companies Grows, NYT, 19.07.2014.

[450] *Ross*, BItcoin used for extortion demands, Examiner.com, 20.07.2014.

[451] KPMG E-Crime Study 2013, page 7.

[452] *O'Gorman/MCDonald*, Ransomware: A Growing Menace, Symantec Security Response.

[453] *Wang/Ajjan*, Ransomware: Hijacking Your Data, Sophos, 2013; *Sancho/Hacquebord*, The "Police Trojan", An In-Depth Analysis, Trend Micro Research Paper, 2012.

[454] See *Sieber*, Council of Europe Organised Crime Report 2004, page 140.

[455] See for example the United States International Traffic in Arms Regulation or the Wassenaar Agreement, which is a convention on arms control. 40 countries already participate in the agreement. For more information, see: www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement

[456] See in this context: Council of Europe, Resolution ResAP(2007)2 on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

[457] See for example *Henney*, Cyberpharmacies and the role of the US Food And Drug Administration, available at: https://tspace.library.utoronto.ca/html/1807/4602/jmir.html; *De Clippele*, Legal aspects of online pharmacies, Acta Chir Belg, 2004, 104, page 364, available at: www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, What's a Legal System to Do? The Problem of Regulating Internet Pharmacies, available at: www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

[458] See: See *Conway*, Terrorist Uses of the Internet and Fighting Back, Information and Security, 2006, page 16, United States Department of Justice 1997 Report on the availability of bomb-making information, available at: www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.

[459] E.g. by offering the download of files containing music, movies or books.

[460] Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

[461] See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, 2004, page 34 *et seq.*

[462] Besides these improvements, digitization has speeded up the production of copies and lowered the costs that were one of the key drivers for the industry to perform the transition to digital-based technologies.

[463] *Sieber*, Council of Europe Organised Crime Report 2004, page 148.

[464] Digital Rights Management describes access control technology used to limit the usage of digital media. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; *Baesler*, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

[465] Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schroder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

[466] GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement, available at: www.gao.gov/new.items/d04503.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. United States Federal Trade Commission, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, page 3, available at: www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

[467] In 2005, 1.8 million users used Gnutella. See *Mennecke*, eDonkey2000 Nearly Double the Size of FastTrack, available at: www.slyck.com/news.php?story=814.

[468] See: Cisco, Global IP Traffic Forecast and Methodology, 2006-2011, 2007, page 4, available at: www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd806a81aa.pdf.

[469] See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

[470] One example is Germany, where a regularly updated report of the Federation of the phonographic businesses pointed out that, in 2006, 5.1 million users in Germany downloaded music in file-sharing systems. The report is available at: www.ifpi.de/wirtschaft/brennerstudie2007.pdf. Regarding the United States, see: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

[471] Apart from music, videos and software, even sensitive personal documents are often found in file-sharing systems. See: *Johnson/McGuire/Willey*, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

[472] While in 2002, music files made up more than 60 per cent of all files exchanged in file-sharing systems in OECD countries, this proportion dropped in 2003 to less than 50 per cent. See: OECD Information Technology Outlook 2004, page 192, available at: www.oecd.org/dataoecd/22/18/37620123.pdf.

[473] *Schoder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005, page 11, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Cope*, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: www.computerworld.com/networkingtopics/networking/story/0,10801,69883,00.html; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

[474] Regarding Napster and the legal response, see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html; *Penn*, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol7/issue2/penn.pdf.

475 Regarding the underlying technology, see: *Fischer*, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: www.vjolt.net/vol7/issue3/v7i3_a07-Fisher.pdf; *Sifferd*, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Herndon*, Who's watching the kids? – The use of peer-to-peer programs to Cyberstalk children, Oklahoma Journal of Law and Technology, Vol. 12, 2004, available at: www.okjolt.org/pdf/2004okjoltrev12.pdf; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

476 For more information on investigations in peer-to-peer networks, see: Investigations Involving the Internet and Computer Networks, NIJ Special Report, 2007, page 49 *et seq.*, available at: www.ncjrs.gov/pdffiles1/nij/210798.pdf.

477 *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005..

478 Regarding the motivation of users of peer-to-peer technology, see: *Belzley*, Grokster and Efficiency in Music, Virginia Journal of Law and Technology, Vol. 10, Issue 10, 2005, available at: www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

479 For more examples, see: Supreme Court of the United States, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, I. B., available at: http://fairuse.stanford.edu/MGM_v_Grokster.pdf.

480 Regarding the economic impact, see: *Liebowitz*, File-Sharing: Creative Destruction or Just Plain Destruction, Journal of Law and Economics, 2006, Vol. 49, page 1 *et seq.*

481 The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80 per cent of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

482 The Recording Industry 2006 Privacy Report, page 4, available at: www.ifpi.org/content/library/piracy-report2006.pdf.

483 One example is the movie "Star Wars – Episode 3" that appeared in file-sharing systems hours before the official premiere. See: www.heise.de/newsticker/meldung/59762 drawing on a MPAA press release.

484 Regarding anonymous file-sharing systems, see: *Wiley/ Hong*, Freenet: A distributed anonymous information storage and retrieval system, in Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability, 2000.

485 Content scrambling systems (CSS) is a digital rights management system that is used is most DVD video discs. For details about the encryption used, see: *Stevenson*, Cryptanalysis of Contents Scrambling System, available at: www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

486 Regarding further responses of the entertainment industry (especially lawsuits against Internet users), see: *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

487 Digital rights management describes access control technology used to limit the usage of digital media. For more information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

488 *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, Copy Protection for DVD Videos, IV 2, available at: www.adastral.ucl.ac.uk/~icox/papers/1999/ProcIEEE1999b.pdf.

489 *Siebel*, Council of Europe Organised Crime Report 2004, page 152.

490 See: www.golem.de/0112/17243.html.

491 Regarding the similar discussion with regard to tools used to design viruses, see below: § 2.8.4.

492 See *Bakke*, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Regarding trademark violations as a consequence of online-criticism, see: *Prince*, Cyber-Criticism and the Federal Trademark Dilution act: Redefining the Noncommercial use Exemption, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf.

493 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions. See *Gecko*, The criminalization of Phishing and Identity Theft,

Computer und Resht, 2005, 606; *Ullman*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: § 2.9.4.

494 For an overview about what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

495 Regarding the connection with trademark-related offences, see for example: Explanatory Report to the Convention on Cybercrime, No. 42.

496 Another term used to describe the phenomenon is "domain grabbing". Regarding cybersquatting, see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from cybersquatters, Virginia Journal of Law and Technology, Vol. 10, Issue 6; *Binomial*, Cyberspace Technological Standardization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 *et seq.*; *Struve/Wagner*, Real space Sovereignty in Cyberspace: Problems with the Ant cybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 *et seq.*; *Travis*, The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003.

497 See: *Lipton*, Beyond cybersquatting: taking domain name disputes past trademark policy, 2005, available at: www.law.wfu.edu/prebuilt/w08-lipton.pdf.

498 This happens especially with the introduction of new top-level-domains. To avoid cybersquatting, the introduction of a new first-level domain is often accompanied by a period where only parties with trademarks can register a domain name. At the end of this phase (often called the "sunrise period"), other users can register their domain.

499 For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 112.

500 For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 113.

501 In 2006, the United States Federal Trade Commission received nearly 205 000 Internet-related fraud complaints. See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

502 Regarding the related challenges, see below.

503 In 2006, Nearly 50 per cent of all fraud complaints reported to the United States Federal Trade Commission were related to amounts paid between 0-25 US Dollars See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

504 Regarding the related automation process: § 3.2.8.

505 The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237.

506 For more information, see below: § 6.2.14.

507 The term auction fraud describes fraudulent activities involving electronic auction platforms over the Internet. Regarding auction fraud, see: *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*, available at: www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*; *Chau/Falooutsos*, Fraud Detection in Electronic Auction, available at: www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf; *Dolan*, Internet Auction Fraud: The Silent Victims, Journal of Economic Crime Management, Vol. 2, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

508 See www.ebay.com.

509 See *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1.

510 The United States Internet Crime Complaint Centre (IC3) (a partnership between the FBI and the National White Collar Crime Centre) reported that around 45 per cent of complaints refer to Auction Fraud. See: IC3 Internet Crime Report 2006, available at: www.ic3.gov/media/annualreport/2006_IC3Report.pdf.

511 Law Enforcement Efforts to combat Internet Auction Fraud, Federal Trade Commission, 2000, page 1, available at: www.ftc.gov/bcp/reports/int-auction.pdf.

[512] See: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[513] For more information, see for example: http://pages.ebay.com/help/feedback/feedback.html.

[514] Regarding the criminalization of "account takeovers", see: *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

[515] See Putting an End to Account-Hijacking Identity Theft, Federal Deposit Insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[516] The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121, available at: www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report, Vol. 21, Issue 3, 237; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[517] Advance Fee Fraud, Foreign & Commonwealth Office, available at: www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.

[518] For an overview of estimated losses, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 3 *et seq.*

[519] For more information, see: the Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.

[520] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[521] Regarding phishing, see: *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

[522] The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und REcht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

[523] "Phishing" scams show a number of similarities to spam e-mails. It is likely that those organized crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: § 2.6.7.

[524] Regarding related trademark violations, see above: § 2.7.2.

[525] For more information about phishing scams, see below: § 2.9.4.

[526] One technical solution to ensure the integrity of data is the use of digital signatures.

[527] For case studies, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 94.

[528] *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding the different definitions of identity theft, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[529] One of the classic examples is the search for personal or secret information in trash or garbage bins ("dumpster diving"). For more information about the relation to identity theft, see: Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

[530] Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15 per cent obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at:

www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

531 See for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006; *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007.

532 See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

533 See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000.

534 *Hoar*, Identity Theft: The Crime of the New Millennium, Oregon Law Review, Vol. 80, 2001, page 1421 *et seq.*; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, British Journal of Criminology, 2008, page 8.

535 See: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, page 5.

536 See *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003, page 1.

537 Identity Fraud, Prevalence and Links to Alien Illegal Activities, GAO, 2002, GAO-02-830T, page 6; *Paget,* Identity Theft, McAfee White Paper, 2007, page 6. For an overview of Internet-related phishing, see: *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, page 8 *et seq.*l

538 *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270.

539 Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

540 *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 51.

541 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 5.

542 35 per cent of the overall number of cases.

543 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 6.

544 Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07_935T, page 4.

545 *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

546 See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 555.

547 *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science Technology Society, 2007, Vol. 27, 2008, page 20.

548 See Encyclopaedia Britannica 2007.

549 *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, 533.

550 *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[551] In some cases perpetrators used the data they obtained to hide their real identity. Regarding this aspect, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[552] *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[553] See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

[554] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[555] Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[556] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

[557] This method is not considered as an Internet-related approach.

[558] For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

[559] See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

[560] See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.

[561] The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of cybercrime businesses. It is based on the responses of 494 computer security practitioners from in US corporations, government agencies and financial institutions. The survey is available at: www.gocsi.com/

[562] 2013 US State of Cybercrime Survey, How Bad is the Insider Threat, Carnegie Mellon University, 2013.

[563] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[564] For more details, see: *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

[565] *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[566] See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[567] *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005, page 6; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[568] Examples is the online community Facebook, available at www.facebook.com.

[569] See for example Art. 5 of the Directive 2000/31/Ec Of The European Parliament And Of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[570] Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[571] Regarding forensic analysis of e-mail communication, see: *Gupta*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[572] Identity Theft, Prevalence and Cost Appear to be Growing, GAO-02-363.

[573] United States Bureau of Justice Statistics, 2004, available at www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

574 Press release from the Bureau of Justice Statistics, 12.12.2013, available at: www.bjs.gov/content/pub/press/vit12pr.cfm.

575 See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.

576 *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

577 See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.

578 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

579 The United States Federal Bureau of Investigation (FBI) requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. The Head of the FBI office in New York is quoted as saying: "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack". See: Heise News, available at: www.heise-security.co.uk/news/80152.

580 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

581 *Finkle*, 360 million newly stolen credentials on black market: cybersecurity firm, Reuters, 25.02.2014.

582 The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: § 3.2.3.

583 Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

584 For an overview about the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (USD 200-500), see: *Paget*, Identity Theft, White Paper, McAfee, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

585 See above: § 2.5.1.

586 For more examples, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 23 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law-enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

587 DoS is an acronym for denial-of-service attack. For more information, see above: § 2.5.5.

588 These generally contain two elements: Software that automates the process of sending out e-mails by avoiding techniques that enable e-mail providers to identify spam e-mails and a database with thousands or even millions of e-mail addresses. For more information, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 25, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

589 For more details, see below: § 6.2.14.

590 *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*

591 *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 10, available at: www.fas.org/sgp/crs/terror/RL33123.pdf.

592 The CIA pointed out in 2002 that attacks against critical infrastructure in the United States will become an option for terrorists. Regarding the CIA position, see: *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 13, available at: www.fas.org/sgp/crs/terror/RL33123.pdf. However, the FBI has stated that there is presently a lack of capability to mount a significant cyberterrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, A Framework for Understanding Terrorist Use of the Internet, 2006, available at: www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp.

593 See: Report of the National Security Telecommunications Advisory Committee – Information Assurance Task Force – Electric Power Risk Assessment, available at: www.aci.net/kalliste/electric.htm.

[594] See: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 et seq.; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf

[595] See: *Roetzer*, Telepolis News, 4.11.2001, available at: www.heise.de/tp/r4/artikel/9/9717/1.html.

[596] The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; *Zeller*, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position;

[597] CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html.

[598] For an overview, see: *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*

[599] *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[600] Regarding different international approaches as well as national solutions, see: *Sieber* in Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

[601] One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.

[602] Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyberattacks During the War on Terrorism, page 14ff.; *Clark*, Computer Security Officials Discount Chances of "Digital Pearl Harbour", 2003; USIP Report, Cyberterrorism, How real is the threat, 2004, page 2; *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

[603] See, for example: *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.

[604] *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

[605] ADL, Terrorism Update 1998, available at: www.adl.org/terror/focus/16_focus_a.asp.

[606] *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes, see also: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

[607] Regarding the use of YouTube by terrorist organizations, see: Heise News, news from 11.10.2006, available at: www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

[608] *Zanini/Edwards*, The Networking of Terror in the Information Age, in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

[609] United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

[610] Regarding the justification, see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

[611] *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 *et seq.*

612 See: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16.

613 Videos showing the execution of American citizens Berg and Pearl were made available on websites. See *Weimann* in the USIP Report: How Terrorists use the Internet, 2004, page 5.

614 Regarding the related challenges, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.

615 *Levine*, Global Security, 27.06.2006, available at: www.globalsecurity.org/org/news/2006/060627-google-earth.htm. Regarding the discovery of a secret submarine on a satellite picture provided by a free-of-charge Internet service, see: Der Standard Online, Google Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: www.derstandard.at/?url/?id=2952935.

616 For further reference, see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.

617 For more information regarding the search for secret information with the help of search engines, see: *Long, Skoudis, van Eijkelenborg*, Google Hacking for Penetration Testers.

618 "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy." For further information, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information & Security, 2006, page 17.

619 See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.

620 *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18.

621 See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

622 See US Commission on Security and Cooperation in Europe Briefing, 15.05.2008, available at: http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecordType=B&CFID=18849146&CFTOKEN=53; *O'Brian*, Virtual Terrorists, The Australian, 31.07.2007, available at: www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html; *O'Hear*, Second Life a terrorist camp?, ZDNet.

623 Regarding other terrorist related activities in online games, see: *Chen/Thoms*, Cyberextremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 *et seq.*

624 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008, page 215 *et seq.*

625 *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

626 *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

627 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

628 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position.

629 The Commission analysing the 9/11 attacks calculated that the costs for the attack could have been between USD 400 000 and 500 000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved, the cost per person was relatively small. Regarding the related challenges, see also: *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

630 See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

631 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.

632 See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4.

633 Regarding virtual currencies, see: *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

634 *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

635 *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats, Center for Strategic and International Studies, December 2002.

636 *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

637 *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 *et seq.*

638 *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.

639 CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

640 Law Enforcement Tools and Technologies for Investigating Cyberattacks, DAP Analysis Report 2004, available at: www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.

641 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

642 United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17, 1996. Vol. 61, No. 138.

643 Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: www.gao.gov/new.items/d07706r.pdf.

644 Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

645 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

646 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

647 Cybersecurity Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

648 *Falliere/Murchu/Chien*, W32.Stuxnet Dossier, Symantec, November 2010, page 1; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

649 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

650 Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

651 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1; Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

652 See for example: *Leyden*, Lame Stuxnet Worm: "Full of Errors" says Security Consultant, The Register, 19.02.2011.

653 *Albright/Brannan/Walrond*, Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 22.12.2010; *Broad/Markoff/Sanger*, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times, 15.01.2011; *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 2; *Timmerman*, Computer Worm Shuts Down Iranian Centrifuge Plant, Newsmax, 29.11.2010. al

654 *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: www.pp.bme.hu/tr/2003_1/pdf/tr2003_1_03.pdf; *Merten/Teufel*, Technological Innovations in the Passenger Process of the Airline Industry: A Hypotheses Generating Explorative Study in O'Conner/Hoepken/Gretzel, Information and Communication Technologies in Tourism 2008.

655 Sasser B Worm, Symantec Quick reference guide, 2004, available at: http://eval.symantec.com/mktginfo/enterprise/other_resources/sasser_quick_reference_guide_05-2004.en-us.pdf.

656 *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; The Sasser Event: History and Implications, Trend Micro, June 2004, available at: http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp02sasserevent040812us.pdf.

657 *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP, 1997; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

658 *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence? available at: www.projects.ncassr.org/hackback/ethics00.pdf.

659 *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html.

660 *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

661 Improving our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center, Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary United States Senate One Hundred Seventh Congress First Session, July 2001, Serial No. J–107–22, available at: http://cipp.gmu.edu/archive/215_S107FightCyberCrimeNICPhearings.pdf.

662 Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: www.cio.com/article/print/30933.

663 Regarding the Stuxnet software, see: *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1.000 Centrifuges at the Nataz Enrichment Plant? Preliminary Assessment, Institute for Science and International Security, 2010.

664 *Wilson*, Information Operations and Cyberwar, Capabilities and related Policy Issues, CRS Report for Congress, RL21787, 2006; *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

665 *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

666 *Schwartau*, Information Warfare: Chaos on the Electronic Superhighway, 1994, page 13.

667 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

668 Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

669 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

670 *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

671 *Libicki*, Sub Rosa Cyberwar, COEP, 2010.

672 *Myers*, Estonia removes Soviet-era war memorial after a night of violence, The New York Times, 27.04.2007; Estonia removes Soviet memorial, BBC News, 27.04.2007; *Tanner*, Violence continues over Estonia's removal of Soviet war statue, The Boston Globe, 28.04.2007.

673 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

674 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

675 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

676 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf

677 See: *Waterman*: Analysis: Who cybersmacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

678 See for example: *Landler/Markoff*, Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007.

679 *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27, page 193.

680 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18-20.

681 Estonia hit by Moscow cyberwar, BBC News, 17.05.2007; *Traynor*; Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17.05.2007.

682 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

683 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

684 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

685 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

686 Regarding the background to the conflict, see: Council of Europe Parliamentary Assembly Resolution 1633 (2008), The consequences of the war between Georgia and Russia.

687 *Tikk/Kaska/Rünnimeri/Kert/Talihärm/Vihul*, Cyberaattacks Against Georgia: Legal Lessons Identified, 2008, page 4; *Hart*, Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar, Washington Post, 14.08.2008; Cybersecurity and Politically, Socially and Religiously Motivated Cyberattacks, European Union, Policy Department External Policies, 2009, page 15; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

688 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

689 See for example: *Partitt,* Georgian blogger Cyxymu blames Russia for cyberattack, The Guardian, 07.08.2009.

690 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 75; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

691 See *Walker*, Information Warfare and Neutrality, *Vanderbilt Journal of Trans-national Law* 33, 2000; *Banks*, Information War Crimes: Mitnick meets Milosevic, 2001, AU/ACSC/019/2001-04.

692 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyberforce, Alb. Law Journal of Science and Technology, Vol. 18, page 315.

693 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 61.

694 *Rushton*, Liberty Reserve shut down in $6bn money laundering case, The Telegraph, 28.05.2013.

695 Santora/Rashbaum/Perlroth, Online Currency Exchange Accused of Laundering $ 6 Billion, NYT.

696 Notice of Finding, Departement of the Treasury, 2013, available at: www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf.

697 One of the most important obligations is the requirement to keep records and to report suspicious transactions.

698 Offenders may tend to make use of the existing instruments, e.g. the services of financial organizations to transfer cash, without the need to open an account or transfer money to a certain account.

699 For case studies, see: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000-2001", 2001, page 8.

700 See: *Woda*, Money Laundering Techniques With Electronic Payment Systems, Information & Security, Vol. 18, 2006, page 40.

701 Regarding the related challenges, see below: § 3.2.I.

702 Regarding the fundermental concept see: Nakamoto (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

703 Regarding the attacks see: Cohen, Speed Bumps on the Road to Virtual Cash, NYT, 3.7.2011, available at: www.nytimes.com/2011/07/04/business/media/04link.html.

704 Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

[705] Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at: www.missingkids.com/en_US/documents/FCACPTrendsInOnlineCrimePaper2011.pdf

[706] The costs of setting up an online casino are not significantly larger than other e-commerce businesses.

[707] Regarding approaches to the criminalization of illegal gambling, see below: § 6.2.12.

[708] See: Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000-2001, 2001, page 2.

[709] Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

[710] Regarding the phenomenon of phishing, see: *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

[711] The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, "The Phishing Guide Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

[712] The following section describes e-mail-based phishing attacks, compared to other phishing scams, which may, for example, be based on voice communications. See: *Gonsalves*, Phishers Snare Victims with VoIP, 2006, available at: www.techweb.com/wire/security/186701001.

[713] "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organized crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see above: § 2.6.7.

[714] Regarding related trademark violations, see above: § 2.7.2.

[715] For an overview of what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

[716] In some phishing attacks, as many as 5 per cent of victims provided sensitive information on fake websites. See *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, page 1, that refers to *Loftesness*, Responding to "Phishing" Attacks, Glenbrook Partners (2004).

[717] Anti-Phishing Working Group. For more details, see: www.antiphishing.org.

[718] Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[719] Phishing Activitiy Trends Report, 1st Quarter 2014, WPWG, 2014.

[720] See above: § 2.8.3.

3 Desafíos que suscita la lucha contra el ciberdelito

Bibliografía (seleccionada): *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV; *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142; *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 291 *et seq.*; *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2; *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19; *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*; *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001; *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago. edu/Papers/PickerCyber.200.pdf; *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004; *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003; *Wallsten*, Regulation and Internet Use in Developing Countries, 2002.

El reciente desarrollo de las TIC ha redundado no sólo en nuevos ciberdelitos y métodos delictivos, sino también en nuevas formas de investigar el delito cibernético. Los avances logrados en el campo de las TIC han permitido ampliar en gran medida las capacidades de las entidades encargadas de hacer cumplir la ley. Ahora bien, los delincuentes pueden utilizar las nuevas herramientas para impedir su identificación y obstaculizar las investigaciones. En el presente Capítulo nos centraremos en los desafíos que supone el combate contra el ciberdelito.

3.1 Oportunidades

Aunque el desarrollo de algunos servicios TIC, como los servidores de comunicación anónimos o las herramientas antiforenses, puede obstaculizar seriamente las investigaciones, los avances técnicos también sirven para impulsar investigaciones más avanzadas.

3.1.1 Automatización general de las investigaciones

Años atrás, la búsqueda de la evidencia pertinente en las computadoras de los sospechosos se realizaba principalmente por medios manuales. La elaboración de herramientas forenses avanzadas ha modificado completamente esta situación. Las fuerzas del orden pueden utilizar ya la potencia cada vez mayor de los sistemas informáticos y los complejos programas forenses para acelerar las investigaciones y automatizar los procedimientos de búsqueda.[721] No todos los métodos de investigación se pueden automatizar.

Aunque es posible realizar fácilmente una búsqueda de contenido ilegal basada en contraseñas, no sucede otro tanto con la identificación de fotografías ilegales. Los métodos que entrarían en la obtención de valores segmentados sólo tienen éxito cuando las fotografías se han clasificado anteriormente por notas, los valores segmentados se almacenan en una base de datos y la fotografía que se analiza no se modifica.[722]

El soporte lógico forense es capaz de buscar automáticamente imágenes de pornografía infantil, comparando los ficheros mantenidos en el disco duro de los sospechosos con información acerca de imágenes conocidas. Así, a fines de 2007, las autoridades descubrieron una serie de fotografías de abuso sexual a niños. Para impedir cualquier posibilidad de identificación, el delincuente del caso modificó digitalmente la parte de las fotografías en que aparecía su rostro, antes de publicar éstas en Internet. Los expertos en informática forense pudieron deshacer las modificaciones y reconstruir el rostro del sospechoso.[723] Si bien el éxito de esta investigación demuestra con claridad las posibilidades de la ciencia informática forense, no se puede alegar este caso como prueba de un avance definitivo en la investigación de la pornografía infantil, ya que si el delincuente se hubiera limitado a cubrirse el rostro con una mancha blanca, no habría sido posible identificarlo.

3.1.2 Creación de datos en servicios en línea

Como ya se ha indicado, los servicios TIC han logrado una gran difusión. Facebook, YouTube, Instagram y Twitter son apenas algunos ejemplos de servicios con centenares de millones de usuarios.[724] Y la mayoría de ellos efectúa un rastreo intensivo de las actividades de sus usuarios,[725] lo cual forma parte del modelo comercial de esas empresas. Al mismo tiempo, esos datos pueden revestir gran importancia para los investigadores. Cuando se puede solicitar esa información y recurrir a ella por medios legales, los investigadores llegan a realizar investigaciones sumamente complejas y, por ejemplo, verificar con quién se comunicó el sospechoso antes de cometer un delito que difícilmente puede llevar a cabo una sola persona. La geoinformación creada por empresas de telefonía celular puede revestir la misma importancia, pues se puede tener conocimiento de ese tipo de datos si el teléfono celular del sospechoso estaba localizado cerca de la escena del delito en el preciso momento en que éste se cometió.[726]

3.1.3 Creación de datos en el marco de la digitalización de procesos no informáticos

Dada la intensa utilización actual de las TIC en los procesos cotidianos, hay una creación incesante de datos que, dependiendo de la autorización para acceder a ellos y aplicarlos en investigaciones penales, podrían ser utilizados por los organismos encargados de velar por el cumplimiento de la ley. No sólo los nuevos servicios íntegramente digitales, como las redes sociales, suscitan la atención de los usuarios y el almacenamiento de datos. También los servicios no informáticos tradicionales están sometidos a fases de digitalización. A título de ejemplo: la utilización creciente de las TIC en los servicios postales.[727] Con escáneres de alta velocidad se escanean las direcciones convirtiéndolas en datos electrónicos.[728] Ese tipo de tecnología ya había sido adoptada en los Estados Unidos en el decenio de 1980.[729]

En 2013 los diarios informaron que los servicios postales estadounidenses efectuaban un registro de todos los envíos con fines de investigación. En el marco del programa Mail Isolation Control and Tracking (MICT), creado en 2011 tras los atentados con ántrax perpetrados en el país, se guardó una foto de cada carta y cada paquete enviado por correo.[730] Ese tipo de información fue utilizada en la investigación de delitos.[731]

3.2 Desafíos generales

3.2.1 Dependencia con respecto a las TIC

Muchas de las comunicaciones diarias exigen recurrir a las TIC y a los servicios basados en Internet; entre otras, las llamadas VoIP y las comunicaciones por correo electrónico[732]. Las TIC se utilizan en nuestros días para ejecutar funciones de control y gestión en edificios[733], vehículos y el campo de los servicios de aviación[734]. El suministro de energía, agua potable y servicios de comunicación se apoya en las TIC y es probable que prosiga la integración de estas tecnologías en nuestras vidas diarias[735]. La creciente dependencia con respecto a las TIC aumenta la vulnerabilidad de los sistemas y servicios ante los ataques que se llevan a cabo contra infraestructuras vitales[736]. Una breve interrupción de un servicio puede ocasionar grandes daños financieros en los mercados de cibercomercio[737] y las comunicaciones civiles no son las únicas que pueden quedar interrumpidas por ataques, pues depender de las TIC es uno de los grandes riesgos de las comunicaciones militares[738].

La infraestructura técnica existente presenta una serie de insuficiencias en el plano de la seguridad; por ejemplo, la monocultura o la homogeneidad de los sistemas operativos. Un gran número de usuarios privados y de pequeñas y medianas empresas utilizan el sistema operativo de Microsoft[739], por lo cual los delincuentes pueden diseñar ataques eficaces, concentrándose únicamente en este objetivo[740].

La sociedad depende de las TIC y dicha dependencia no se limita a los países occidentales[741], como demuestra el hecho de que los países en desarrollo deban afrontar los ataques lanzados contra sus infraestructuras y usuarios[742]. El desarrollo de tecnologías de infraestructura baratas, tales como WiMAX[743], ha hecho posible que los países en desarrollo ofrezcan servicios Internet a un mayor número de consumidores. Los países en desarrollo están en condiciones de evitar el error cometido por varios países occidentales, que se concentraron esencialmente en maximizar la accesibilidad, sin invertir lo suficiente en protección. Algunos expertos estadounidenses han señalado que la falta de medidas apropiadas de protección explica que tuvieran éxito los ataques emprendidos contra sitios oficiales de entidades públicas de Estonia[744, 745]. A los países en desarrollo se les brinda la gran oportunidad de integrar las medidas de seguridad en una fase temprana. Esto puede exigir la realización de inversiones considerables por anticipado, pero de no proceder así la ulterior integración de las medidas de seguridad necesarias puede resultar más onerosa a largo plazo[746].

Habrá que definir estrategias para impedir dichos ataques y preparar contramedidas, que incluyen la preparación y el fomento de medios técnicos de protección, así como la promulgación de legislación idónea y suficiente que permita a las autoridades encargadas de hacer cumplir la ley luchar eficientemente contra el ciberdelito.[747]

3.2.2 Número de usuarios

La popularidad de Internet y de sus servicios van en rápido aumento, como demuestra la existencia de más de dos mil millones de usuarios de Internet en todo el mundo[748]. Los fabricantes de computadores y los proveedores de servicios Internet (PSI) tienen la mira puesta en los países en desarrollo, ya que estas naciones presentan el mayor potencial de crecimiento[749]. En 2005 el número de usuarios de Internet en los países en desarrollo sobrepasó al de usuarios en las naciones industrializadas[750], por no hablar de que el desarrollo de equipo barato y acceso inalámbrico permitirá que una mayor cantidad de personas acceda a Internet[751].

El continuo incremento de la población conectada a Internet hace que aumente también el número de víctimas en potencia y de delincuentes[752]. Es difícil calcular cuántas personas emplean Internet para efectuar actividades ilegales. En todo caso, si sólo el 0,1 por ciento de los usuarios perpetrasen actos delictivos, el número total de delincuentes ascendería a más de un millón de personas. Si bien las tasas de utilización de Internet son más bajas en los países en desarrollo, promover la ciberseguridad en dichas naciones no resulta tarea fácil, ya que los delincuentes pueden cometer delitos a partir de cualquier otro lugar en el mundo[753].

La creciente cantidad de usuarios de Internet obstaculiza la labor de las entidades encargadas de hacer cumplir la ley, ya que resulta relativamente difícil automatizar los procesos de investigación. Aunque la investigación de contraseñas de contenido ilegal pueda efectuarse fácilmente, la identificación de imágenes ilegales plantea grandes problemas. Así por ejemplo, los enfoques basados en valores desmenuzados son sólo útiles si se procede previamente a clasificar las imágenes por nota, se almacenan los valores desmenuzados en una base de datos y la imagen analizada no se ha modificado.[754]

3.2.3 Disponibilidad de dispositivos y de acceso

Para cometer delitos informáticos es preciso disponer de un sistema básico y ello exige simplemente equipos, programas y acceso a Internet.

Por lo que hace al equipo, hay que señalar que la potencia de los computadores se encuentra en continuo aumento[755] y que se han emprendido una serie de iniciativas para hacer posible que los nacionales de los países en desarrollo utilicen en mayor grado las TIC[756]. Los delincuentes pueden perpetrar delitos informáticos de consideración, recurriendo únicamente a tecnología barata de segunda mano, ya que en este contexto el conocimiento es mucho más importante que el equipo. La fecha de la tecnología de los computadores disponibles ejerce escasa influencia en la utilización de ese equipo para cometer ciberdelitos.

La perpetración de un ciberdelito se ve facilitada por el empleo de soporte lógico especializado. Cabe la posibilidad de que los delincuentes descarguen herramientas informáticas[757] diseñadas para localizar puertos abiertos o suspender la protección que procuran las contraseñas[758]. Debido a las técnicas de espejo y de intercambio entre pares, resulta difícil limitar la disponibilidad especializada de dichos dispositivos.[759]

El último elemento crucial es el acceso a Internet. El costo de dicho acceso[760] es más elevado en la mayoría de los países en desarrollo que en las naciones industrializadas, pero hay que decir que el número de usuarios de Internet en los países en desarrollo se encuentra en rápido aumento[761]. Los delincuentes no se abonan normalmente a un servicio Internet, ya que podrían ser identificados, y prefieren, por tanto, optar por servicios que utilizan sin necesidad de registro. Esto explica, que los delincuentes recurran al método denominado "*wardriving*", que consiste en localizar redes inalámbricas desde automóviles para acceder a las mismas[762]. Los métodos más comunes que emplean los delincuentes para acceder a la red de forma anónima son los terminales públicos de Internet, las redes abiertas (inalámbricas)[763], las redes pirateadas y los servicios de prepago que no requiere registro.

Las entidades encargadas de hacer cumplir la ley están tomando medidas para restringir el acceso sin control a los servicios de Internet, para evitar el abuso delictivo de tales servicios. En Italia y China, por ejemplo, la utilización de terminales públicos de Internet exige identificar a los usuarios[764]. Con todo, hay motivos que aconsejan no imponer dicha obligación de identificación[765]. Aunque restringir el acceso puede contribuir a impedir la comisión de delitos y facilita las investigaciones de las entidades encargadas de hacer cumplir la ley, la legislación necesaria podría obstaculizar el crecimiento de la sociedad de la información y el desarrollo del comercio electrónico[766].

Se ha sugerido que esta limitación del acceso a Internet podría violar ciertos derechos humanos[767]. Así por ejemplo, en una serie de casos de radiodifusión, el Tribunal Europeo determinó que el derecho a la libertad de expresión se aplicaba no sólo al contenido de la información, sino también a los medios de transmisión o recepción. En el caso de Autronic contra Suiza[768], el Tribunal señaló que era necesario interpretar el caso en sentido amplio, ya que cualquier restricción que se impusiera a los medios de comunicación interferiría necesariamente con el derecho a recibir y transmitir información. Si estos principios se aplican a las limitaciones que puedan imponerse al acceso a Internet, dichos enfoques legislativos podrían entrañar la violación de derechos humanos.

3.2.4 Disponibilidad de información

Internet consta de millones de páginas web[769] que contienen información actualizada y a tales páginas puede acceder cualquier persona que publique o mantenga una página web. Un ejemplo del éxito obtenido

por las plataformas generadas por usuarios es Wikipedia[770], que es una enciclopedia en línea en la cual cualquier persona puede publicar[771].

El éxito de Internet se basa, igualmente, en motores de búsqueda de gran potencia que hacen posible que los usuarios busquen millones de páginas web en unos cuantos segundos. Dicha tecnología puede utilizarse tanto con propósitos legítimos como delictivos. El pirateo a través de Google "*Googlehacking*" o las personas que divulgan inadvertidamente información en Google "*Googledorks*" son términos que remiten a la utilización de motores de búsqueda complejos para filtrar un gran número de resultados de búsqueda con el fin de obtener información sobre aspectos de seguridad informática. Así por ejemplo, los delincuentes podrían proponerse buscar información sobre sistemas de protección dotados de contraseñas inseguras[772]. Se han realizado Informes en los cuales se destaca el riesgo de la utilización de motores de búsquedas con fines ilegales[773]. Hay terroristas que pueden encontrar en Internet información detallada sobre la forma de construir una bomba utilizando productos químicos disponibles en los supermercados[774]. Aunque este tipo de información estaba disponible aun antes de que se desarrollarse Internet, resultaba mucho más difícil procurársela. Hoy en día, empero, cualquier usuario de Internet puede acceder a esas instrucciones.

Por otra parte, los delincuentes están en condiciones de utilizar motores de búsqueda para analizar las características de los objetivos de sus ataques[775]. Así por ejemplo, en un manual de formación descubierto durante la investigación de miembros de un grupo de terroristas, se destacaba la gran utilidad que revestía Internet para recoger información sobre posibles objetivos[776]. Utilizando motores de búsqueda, los terroristas pueden recoger información disponible al público (por ejemplo, planes de construcción de edificios públicos) que les ayuden en sus preparativos. Se ha informado de que en Afganistán los insurgentes que lanzan ataques contra las tropas británicas utilizan para ello imágenes de satélite de Google Earth.[777]

3.2.5 Ausencia de mecanismos de control

Una administración central y un conjunto de normas técnicas son requisitos indispensables para garantizar el funcionamiento de todas las redes de comunicaciones de masas –de Internet a las redes telefónicas utilizadas para hacer llamadas vocales. El debate en curso en torno a la Gobernanza de Internet apunta al hecho de que Internet no es una red distinta de las basadas en la infraestructura de comunicaciones transnacionales e incluso nacionales[778], por lo cual Internet debería ser también objeto de legislación, y los legisladores y las entidades encargadas de hacer cumplir la ley han iniciado ya el proceso de formular normas jurídicas en las que se preconiza un cierto grado de control central.

Internet fue diseñada en un principio como una red militar[779], basada en una arquitectura centralizada de redes que tenía como propósito preservar la integridad y las posibilidades de funcionamiento de la principal funcionalidad de la red, aunque sus componentes fueran atacados. Esto hizo que la infraestructura de red de Internet resistiera contra las fuerzas de control externo. Ahora bien, Internet no fue diseñada en un principio para facilitar investigación de delitos o para impedir que se lanzaran ataques en el interior de la red.

Internet se utiliza cada vez más para prestar y solicitar servicios civiles, y el paso de los servicios militares a los civiles ha modificado la naturaleza de la demanda de instrumentos de control. Resulta lógico que, como la red se basaba en protocolos diseñados con propósitos militares, estos instrumentos de control centrales no existan, lo que hace difícil establecerlos sin volver a diseñar en grado considerable la red. La ausencia de instrumentos de control dificulta en gran medida la investigación del ciberdelito[780].

Un ejemplo de los problemas que plantea la ausencia de instrumentos de control es que los usuarios pueden soslayar los dispositivos de filtro[781] recurriendo a servicios de comunicación anónima encriptada[782]. Si los proveedores de acceso bloquean ciertos sitios web donde puede verse contenido ilegal (por ejemplo, pornografía infantil), en la mayoría de los casos los clientes no podrán acceder a dichos sitios web. Ahora bien, los clientes pueden soslayar el bloqueo del contenido ilegal utilizando un servidor de comunicaciones anónimas que encripte las comunicaciones entre los mismos y el servidor central. En este caso, es posible que los proveedores no puedan bloquear las peticiones de estos usuarios, debido a que éstas son enviadas como mensajes encriptados que los proveedores de acceso son incapaces de abrir.

3.2.6 Dimensiones internacionales

Muchos procesos de transferencia de datos afectan a más de un país[783]. Los protocolos que se utilizan para realizar transferencias de datos en Internet se basan en el encaminamiento óptimo, cuando los enlaces directos se bloquean temporalmente[784]. Aun cuando los procesos nacionales de transferencia en el país fuente sean limitados, los datos pueden salir del país, transmitidos a través de encaminadores situados fuera del territorio de ese país y dirigirse una vez más al país mencionado[785]. Además, muchos servicios de Internet se basan en servicios prestados desde el exterior y, así por ejemplo, los proveedores huéspedes pueden arrendar espacio web[786] en un país aprovechando equipo situado en otro[787].

Cuando los delincuentes y sus objetivos se encuentran situados en países distintos, los investigadores de esos ciberdelitos deben cooperar con las entidades encargadas de hacer cumplir la ley de todos los países afectados[788]. Dado que, por motivos de soberanía nacional, no se permite realizar investigaciones en el territorio de los países interesados, sin el permiso de las autoridades nacionales[789], los investigadores de ciberdelitos necesitan el apoyo y la participación de los gobiernos de los países concernidos.

Resulta difícil llevar a cabo la cooperación en materia de ciberdelito aplicando los principios tradicionales de asistencia mutua jurídica. El carácter oficial de los requisitos jurídicos y el tiempo necesario para colaborar con las entidades extranjeras encargadas de hacer cumplir la ley suelen obstaculizar las investigaciones[790], que las más de las veces se realizan en periodos muy breves[791]. Ahora bien, algunos datos que resultan indispensables para detectar delitos suelen borrarse rápidamente. El hecho de que el periodo de investigación sea corto resulta problemático, ya que toma tiempo organizar un marco de asistencia mutua dentro de los regímenes jurídicos tradicionales[792]. El principio de doble criminalidad[793] también plantea dificultades, cuando el acto considerado no se tipifica como delito en uno de los países que participan en la investigación[794]. Además, es posible que los delincuentes incluyan deliberadamente a terceros países en sus ataques para obstaculizar las investigaciones[795].

Cabe la posibilidad de que los delincuentes seleccionen deliberadamente objetivos situados fuera de su propio país y actúen a partir de países con una legislación de lucha contra el ciberdelito inadecuada[796]. La armonización de las leyes sobre el ciberdelito y de la cooperación internacional contribuiría positivamente en este contexto. Existen dos enfoques que aceleran el ritmo de la cooperación internacional para efectuar investigaciones sobre el ciberdelito: la red del G8 que funciona las 24 horas del día y 7 días por semana[797] y las disposiciones de cooperación internacional especificadas en el Convenio del Consejo de Europa sobre la Ciberdelincuencia[798].

3.2.7 Independencia respecto del lugar del delito y la presencia en el mismo

No es necesario que los delincuentes se encuentren presentes en el mismo lugar en el que esté situado su objetivo. Como el lugar en el que se encuentra el delincuente puede ser por completo distinto del lugar en el que éste comete su delito, muchos ciberdelitos son trasnacionales. La comisión de delitos internacionales requiere considerables esfuerzos y tiempo. Por otra parte, los ciberdelincuentes intentan evitar países con una estricta legislación en cuanto al delito cibernético[799].

Oponerse a los "refugios seguros" es uno de los desafíos esenciales a la hora de combatir el ciberdelito[800], puesto que mientras éstos existan los delincuentes los utilizarán para obstaculizar la investigación de sus actos. Los países en desarrollo que no han formulado aún legislación sobre el ciberdelito pueden ser vulnerables, ya que los delincuentes tenderían a establecerse en estos países para evitar su enjuiciamiento. Puede resultar difícil oponerse a la perpetración de delitos graves y que afectan a sus víctimas en todo el mundo, debido a la legislación insuficiente de los países en los que los delincuentes se hayan establecido. Esto puede llevar a ejercer presiones sobre algunos países para que promulguen legislación al respecto. En este sentido, cabe citar el gusano informático "*Love Bug*", diseñado en 2000 por un sospechoso en Filipinas[801], que infectó millones de computadores en todo el mundo[802]. Las investigaciones nacionales se vieron dificultadas por el hecho de que el diseño y la preparación de programas maliciosos no se habían tipificado penalmente de manera adecuada en Filipinas[803]. Otro ejemplo es el de Nigeria, país al que se ha presionado para que tome medidas en relación con la distribución de correos electrónicos destinados a estafar a sus destinatarios.

3.2.8 Automatización

Una de las grandes ventajas de las TIC es la posibilidad de automatizar ciertos procesos, automatización que tiene efectos apreciables: acelera los procesos, aumenta el alcance e impacto de los procesos y limita la participación de seres humanos.

La automatización reduce la necesidad de disponer de mucho personal, lo que permite a los proveedores ofrecer servicios a precios bajos[804]. Los delincuentes pueden recurrir a la automatización para intensificar sus actividades: en efecto, es posible enviar muchos millones de mensajes de correo electrónico no solicitado a granel[805], si se recurre a la automatización[806]. Actualmente los piratas suelen llevar a cabo sus ataques de forma automatizada[807] (hasta 80 millones de ataques diarios)[808], recurriendo a programas informáticos[809] que pueden atacar miles de sistemas informáticos en unas cuantas horas[810]. Los delincuentes pueden obtener grandes beneficios, automatizando procesos que les permiten llevar a cabo estafas basadas en un gran número de delitos y que entrañan una pérdida relativamente reducida para cada víctima[811]. La idea es que mientras más baja sea la pérdida menor será la probabilidad de que una víctima informe al respecto.

La automatización de los ataques afecta muy especialmente a los países en desarrollo. Dados sus recursos limitados, el correo basura puede plantear a estos países un problema de mayor consideración que a las naciones industrializadas[812]. El mayor número de delitos que cabe cometer gracias a la automatización plantea problemas a las entidades encargadas de hacer cumplir la ley en todo el mundo, ya que haría aumentar el número de víctimas en sus jurisdicciones.

3.2.9 Recursos

Los modernos sistemas informáticos que aparecen actualmente en el mercado presentan una gran potencia y pueden utilizarse para realizar actividades delictivas. Pero no es simplemente el aumento de potencia[813] de los ordenadores de usuario lo que plantea problemas a las investigaciones. La mayor capacidad de las redes también es un tema de gran importancia.

En ese sentido, cabe citar los ataques cometidos recientemente contra sitios web del Gobierno de Estonia[814]. El análisis de estos ataques cometidos por miles de computadores dependientes de una red robot[815] o grupo de computadores comprometidos que ejecutan programas bajo el control de una fuente exterior[816]. En muchos casos, los computadores son infectados por programas maliciosos que instalan en ellos herramientas que permiten a los delincuentes hacerse con el control de los mismos. La red robot se utiliza para tener información acerca de objetivos y para realizar ataques de alto nivel[817].

En los últimos años las redes robot se han convertido en una gran amenaza para la ciberseguridad[818]. El tamaño de las redes robot es variable, ya que va de unos cuantos computadores a más de un millón de máquinas[819]. Los analistas sugieren que hasta una cuarta parte de todos los computadores conectados a Internet pueden estar infectados con programas informáticos que los obligan a formar parte de una red robot[820]. La red robot puede utilizarse para realizar actividades delictivas de diverso tipo, entre otras los ataques que conllevan la denegación del servicio[821], el envío de correo basura[822], los ataques de piratas e intercambio de ficheros con derechos de propiedad protegidos.

Las redes robot brindan varias ventajas a los delincuentes. Por una parte, aumentan su capacidad en términos de computadores y redes. Utilizando miles de sistemas informáticos, los delincuentes pueden atacar sistemas de computadores que serían inmunes a un ataque realizado con sólo unas cuantas máquinas[823]. En segundo lugar, las redes robot dificultan la localización del delincuente original, ya que las pistas iniciales sólo llevan a un determinado miembro de las redes robot. A medida que los delincuentes controlan sistemas y redes informáticos de mayor potencia, aumenta el desnivel entre las capacidades de las autoridades de investigación y las de los delincuentes.

3.2.10 Velocidad de los procesos de intercambio de datos

La transferencia de un correo electrónico entre varios países sólo toma varios segundos, lo que explica, entre otras cosas, el éxito de Internet, puesto que el correo electrónico ha eliminado las barreras temporales que caracterizaban el transporte físico de mensajes y deja poco tiempo a las entidades de hacer

cumplir la ley para investigar o recoger pruebas (el proceso tradicional de investigación es mucho más largo)[824].

En este sentido, cabe dar como ejemplo el intercambio de pornografía infantil. En el pasado, los vídeos pornográficos se pasaban de mano en mano o transportaban para su entrega a los compradores. Estas dos acciones brindaban a las entidades encargadas de hacer cumplir la ley la oportunidad de llevar a cabo sus investigaciones. La principal diferencia entre el intercambio de pornografía infantil dentro y fuera de Internet es el transporte. En efecto, cuando los delincuentes utilizan Internet las películas pornográficas pueden intercambiarse en cuestión de segundos.

Los correos electrónicos demuestran la importancia de contar con herramientas de respuesta inmediata que puedan ser usadas sin tardanza. Para localizar e identificar a sospechosos, los investigadores suelen necesitar datos que pueden borrarse poco después de ser transferidos[825]. Con frecuencia para que una investigación resulte eficiente es indispensable que las correspondientes autoridades reaccionen muy rápidamente. Si la legislación y los instrumentos disponibles no permiten a los investigadores actuar inmediatamente e impedir que se borren los datos, tal vez no sea posible combatir eficazmente el ciberdelito[826].

Los procedimientos de "rápida congelación"[827] y los puntos de redes 24/7[828] son ejemplos de herramientas que pueden acelerar las investigaciones. Además, la legislación promulgada para promover la retención de datos tiene por objeto fomentar el tiempo de que disponen las entidades encargadas de hacer cumplir la ley para efectuar sus investigaciones. Si los datos necesarios para localizar a delincuentes se preservan durante un cierto tiempo, aumentará la probabilidad de que las entidades encargadas de hacer cumplir la ley puedan identificar sospechosos.

3.2.11 Rápido ritmo de desarrollo

Internet se ha desarrollado constantemente y la creación de la interfaz de usuario gráfica (WWW[829]) constituye el inicio de su expansión exponencial, ya que los servicios basados en comandos que se suministraban anteriormente eran difíciles de utilizar por el usuario. La creación de la WWW ha permitido la creación de nuevas aplicaciones y la perpetración de nuevos delitos[830], por lo cual las entidades encargadas de hacer cumplir la ley hacen grandes esfuerzos por mantenerse al día. Ahora bien, la evolución de Internet prosigue, debido en gran medida a los juegos en línea y a las comunicaciones vocales con IP (VoIP).

Los juegos en línea son cada vez más populares y no resulta claro si las entidades encargadas de hacer cumplir la ley podrán investigar y enjuiciar eficazmente los delitos cometidos en este mundo virtual[831].

El paso de telefonía vocal tradicional a la telefonía Internet supone, por su parte, nuevos desafíos para las entidades encargadas de hacer cumplir la ley. Las técnicas y rutinas creadas por estas entidades para interceptar llamadas telefónicas tradicionales no se ajustan por regla general a las comunicaciones VoIP. La intercepción de llamadas vocales tradicionales se lleva a cabo normalmente a través de los proveedores de telecomunicaciones. Si se aplicase el mismo principio a las comunicaciones VoIP, las entidades encargadas de hacer cumplir la ley actuarían por conducto de los PSI y los proveedores de servicio que suministran servicios VoIP. Con todo, si el servicio se basa en tecnología de comunicaciones entre pares, en muchos casos los proveedores de servicio no podrían interceptar comunicaciones puesto que los participantes transfieren entre sí directamente los correspondientes datos[832]. En consecuencia, se requieren nuevas técnicas[833].

Asimismo, se están desarrollando rápidamente nuevos dispositivos de equipo con tecnología de red. Los sistemas de entretenimiento en el hogar más reciente convierten el aparato de televisión en un punto de acceso a Internet, al paso que los teléfonos portátiles móviles más recientes almacenan datos y conectan a Internet a través de redes inalámbricas[834]. Además, se han incorporado a relojes, plumas y navajas de bolsillo dispositivos de memoria USB (*bus serial universal*) con una capacidad de más de 1 GB. Las entidades encargadas de hacer cumplir la ley deben tener en cuenta esta evolución al realizar sus funciones, motivo por lo cual resulta esencial educar continuamente a los funcionarios que realizan investigaciones sobre el

ciberdelito, con el fin de que éstos se mantengan al día con respecto a la tecnología más reciente y puedan identificar los correspondientes equipos y los dispositivos específicos que deban decomisarse.

Otro problema es la utilización de los puntos de acceso inalámbrico. La expansión del acceso inalámbrico a Internet en los países en desarrollo brinda oportunidades, pero también acarrea problemas para las entidades encargadas de hacer cumplir la ley[835]. Si los delincuentes utilizan puntos de acceso inalámbrico que no requieren registro, éstos dificultan las tareas que realizan las entidades encargadas de hacer cumplir la ley para rastrear la pista de los delincuentes, ya que sus investigaciones llevan únicamente a localizar puntos de acceso.

3.2.12 Comunicaciones anónimas

Determinar el origen de las comunicaciones es muy a menudo fundamental en la investigación de los ciberdelitos. Sin embargo, la naturaleza distribuida de la red[836] así como la disponibilidad de ciertos servicios de Internet, de origen incierto, complican la tarea de identificar sospechosos.[837] Las comunicaciones anónimas pueden ser únicamente un subproducto de un servicio u ofrecerse con la intención de evitar desventajas para el usuario. Ser conscientes de la incertidumbre del origen es crucial para evitar llegar a conclusiones incorrectas.[838] Entre estos servicios (que pueden combinarse incluso), cabe citar los siguientes:

- terminales públicos de Internet (por ejemplo, terminales en el aeropuerto, o cibercafés);[839]
- dispositivos de traducción de dirección de red (NAT) y redes privadas virtuales (VPN);[840]
- redes inalámbricas;[841]
- servicios móviles de prepago que no requieren registro;
- capacidades de almacenamiento de páginas ofrecidas sin registro;
- servidores de comunicación anónimos;[842]
- repetidores de correo anónimos.[843]

Los delincuentes pueden encubrir sus identidades recurriendo, entre otras cosas, a direcciones falsas de correo electrónico[844]. Muchos proveedores ofrecen gratuitamente direcciones de correo electrónico. Puede ocurrir que no se verifique la introducción de información personal, aunque sea necesario introducirla, por lo cual los usuarios estarían en condiciones de registrar direcciones de correo electrónico sin revelar su identidad. Las direcciones de correo electrónico anónimas resultan útiles, por ejemplo, cuando los usuarios desean inscribirse en grupos de discusión política sin identificarse. Aunque es posible que las comunicaciones anónimas generen conductas antisociales, permiten, por otra parte, a los usuarios, actuar con mayor libertad.[845]

Habida cuenta de que los usuarios dejan rastros, huelga decir que es preciso habilitar instrumentos que impidan que sus características personales sean identificadas por terceros[846]. Así pues, varios Estados y organizaciones han apoyado el principio de la utilización anónima de los servicios de correo electrónico de Internet como demuestra el hecho de que se haya preconizado, entre otras cosas, en la Directiva sobre la privacidad y las comunicaciones electrónicas[847]. Un enfoque jurídico para proteger la privacidad del usuario es especificado en el Artículo 37 del Reglamento relativo a la protección de datos de la Unión Europea[848]. No obstante, algunos países abordan los desafíos suscitados por las comunicaciones anónimas, aplicando restricciones jurídicas[849]; por ejemplo, Italia, país que exige a los proveedores de acceso público a Internet identificar a los usuarios antes de comenzar a prestar servicio a éstos[850].

Si bien estas medidas están encaminadas a ayudar a identificar sospechosos a las entidades encargadas de hacer cumplir la ley, pueden ser soslayadas fácilmente, cuando los delincuentes recurren a redes inalámbricas privadas no protegidas o utilizan tarjetas SIM de países que no exigen registro alguno. No resulta claro si la limitación de las comunicaciones anónimas y del acceso anónimo a Internet debería desempeñar un cometido de mayor alcance en las estrategias de ciberseguridad[851].

3.2.13 Fallo de los instrumentos de investigación tradicionales

La investigación y persecución del ciberdelito exige el empleo de herramientas e instrumentos específicos de Internet que permitan a las autoridades competentes llevar a cabo dichas investigaciones.[852] En este contexto, resultan esenciales los instrumentos para identificar al delincuente y recoger la evidencia oportuna a fin de desencadenar los procedimientos jurídicos penales correspondientes.[853] Estos instrumentos pueden ser los mismos utilizados en las investigaciones contra el terrorismo tradicionales no relacionadas con la tecnología informática, pero en un número cada vez mayor de casos relativos a Internet, los instrumentos de investigación tradicionales no son suficientes para identificar al delincuente. Un ejemplo es la intercepción de las comunicaciones voz sobre IP (VoIP).[854] En las últimas décadas los Estados han desarrollado instrumentos de investigación tales como escuchas telefónicas que les permiten interceptar comunicaciones telefónicas de línea fija y de telefonía móvil.[855] La intercepción de llamadas vocales tradicionales se realiza normalmente a través de los proveedores de telecomunicaciones.[856] Aplicando el mismo principio a VoIP, las entidades encargadas de hacer cumplir la ley operarían a través de los proveedores de servicio Internet (PSI) y de los proveedores de servicio que ofrecen servicios de VoIP. Sin embargo, si el servicio se basa en una tecnología entre pares, los proveedores de servicio generalmente serán incapaces de interceptar las comunicaciones puesto que los datos relevantes se transfieren directamente entre las partes comunicantes.[857] Por tanto, es necesario recurrir a nuevas soluciones técnicas junto con los instrumentos jurídicos pertinentes.

3.2.14 Tecnología de encriptado

Otro factor que puede complicar la investigación del ciberdelito es la tecnología de encriptado[858], que protege la información contra el acceso por parte de personas no autorizadas y es una solución técnica esencial en la lucha contra el ciberdelito.[859] El encriptado es una técnica que convierte un texto legible en un formato ilegible mediante un algoritmo.[860] Al igual que el anonimato, la encriptación no es un concepto novedoso[861], pero la tecnología informática ha transformado la situación. Durante mucho tiempo estaba sujeta al secreto pero en un entorno interconectado ese secreto es difícil de mantener.[862]

La amplia disponibilidad de herramientas informáticas de fácil uso y la integración de la tecnología de encriptado en los sistemas operativos[863] hace posible actualmente encriptar los datos informáticos con el "clic" de un ratón y ello aumenta, por tanto, las posibilidades de que las entidades encargadas de hacer cumplir la ley deban enfrentarse a material encriptado.[864] Existen varios programas informáticos que permiten a los usuarios proteger los ficheros contra el acceso no autorizado.[865] No está claro en qué medida los delincuentes utilizan ya tecnología de encriptado para encubrir sus actividades.[866] Una encuesta realizada sobre pornografía infantil apunta el hecho de que sólo el 6% de los poseedores de esta pornografía utilizan tecnología de encriptado[867], pero los expertos subrayan la amenaza que supone un mayor uso de la tecnología de encriptado en los casos de ciberdelito.[868]

Existen diversas estrategias técnicas para cubrir los datos encriptados y se dispone de algunas herramientas informáticas para automatizar estos procesos.[869] Las estrategias van desde el análisis[870] de la debilidad de la herramienta informática utilizada para encriptar los ficheros,[871] buscando frases clave del encriptado[872] e intentando contraseñas típicas, hasta ataques masivos complejos y de gran duración. El término "ataque masivo" se emplea para describir el procedimiento de identificación de un código probando todas las posibles combinaciones.[873] Dependiendo de la técnica de encriptación y la magnitud de la llave utilizadas, podría tomar décadas descifrar un encriptado.[874] Así por ejemplo, si un delincuente utiliza soporte lógico de encriptación con una capacidad de 20 bits de encriptación, la magnitud del espacio de la llave se situaría en torno al millón de operaciones. Utilizando un computador de último modelo con capacidad para procesar un millón de operaciones por segundo, un encriptado podría descifrarse en menos de un segundo. Con todo, si los delincuentes utilizan un encriptado de 40 bits, podrían transcurrir dos semanas antes de poder descifrarlo.[875] Por ejemplo, en 2002, el Wall Street Journal pudo decriptar ficheros hallados en un ordenador de Al Quaeda encriptados con una encripción de 40 bits.[876] Si se utiliza un encriptado que conste de 56 bits, podrían pasar 2 285 años antes de poder descifrarlo con un solo computador. Si los delincuentes recurren a un encriptado de 128 bits, mil millones de sistemas de computadores podrían consagrar miles de millones de años de cómputo antes de poder descifrarlo.[877] La última versión del popular soporte lógico de encriptación PGP permite realizar encriptados de 1 024 bits.

Los actuales programas de encriptación van más allá de la encriptación de ficheros individuales. Por ejemplo, la última versión del sistema operativo de Microsoft permite la encriptación de todo un disco duro[878]. Los usuarios podrían instalar fácilmente soporte lógico de encriptación. Aunque algunos expertos de informática forense estiman que esta función no supone una amenaza para ellos[879], la disponibilidad generalizada de esta tecnología entre los usuarios podría redundar en un mayor empleo de la encriptación. Existen herramientas para encriptar comunicaciones, tales como correos electrónicos y llamadas telefónicas[880] que pueden enviarse utilizando VoIP[881]. Recurriendo a la tecnología de encriptación VoIP, los delincuentes podrían proteger conversaciones vocales contra su intercepción[882].

Por otra parte, cabe la posibilidad de combinar diversas técnicas. Utilizando herramientas de soporte lógico, los delincuentes podrían encriptar mensajes y transformarlos en fotografías o imágenes, tecnología denominada esteganografía[883]. Resulta difícil que las autoridades de investigación puedan distinguir el intercambio inocuo de fotografías de vacaciones del intercambio de fotografía con mensajes encriptados ocultos[884].

La disponibilidad y empleo de las tecnologías de encriptación por delincuentes es un desafío que afrontan las entidades encargadas de hacer cumplir la ley. Actualmente se están discutiendo diversos enfoques jurídicos para abordar el problema[885]; entre otros: obligar posiblemente a los diseñadores de soporte lógico a instalar una puerta trasera que puedan utilizar las entidades encargadas de hacer cumplir la ley; limitar la potencia de las llaves; obligar a revelar el contenido de las llaves, cuando se efectúen investigaciones sobre actos delictivos[886]. Con todo, la tecnología de encriptación no sólo es utilizada por delincuentes, pues dicha tecnología puede emplearse de distintas formas con propósitos legales. Si no es posible acceder adecuadamente a una tecnología de encriptación, puede resultar difícil proteger información delicada. Dado el creciente número de ataques[887], la autoprotección es un importante elemento de la ciberseguridad.

3.2.15 Resumen

La investigación y enjuiciamiento del delito cibernético plantea algunos problemas a las entidades encargadas de cumplir la ley y si bien es cierto que resulta indispensable educar a las personas que participan en la lucha contra el ciberdelito, también lo es preparar legislación idónea y éticas contra el mismo. En esta sección se analizaron los principales desafíos que supone promover la ciberseguridad y una serie de esferas donde los instrumentos existentes pueden resultar insuficientes, por lo cual habría necesidad de implementar dispositivos especiales.

3.3 Retos jurídicos

3.3.1 Retos a la hora de elaborar las leyes penales nacionales

Una legislación adecuada es la base para la investigación y procesamiento del ciberdelito. Sin embargo, los legisladores deben responder constantemente a los desarrollos de Internet y supervisar la eficacia de las disposiciones existentes, especialmente teniendo en cuenta la velocidad de desarrollo de las tecnologías de redes.

Históricamente, la introducción de servicios informáticos o tecnologías de Internet ha dado lugar a nuevas formas de delito, poco después de que se introdujese la tecnología. Un ejemplo es la aparición de las redes informáticas en los años 70; el primer acceso no autorizado a estas redes informáticas se produjo poco después[888]. De forma similar, los primeros delitos de software aparecieron al poco tiempo de la introducción de los ordenadores personales en los años 80, cuando estos sistemas se utilizaron para copiar productos de software.

Lleva algún tiempo actualizar las leyes penales para procesar nuevas formas de ciberdelito en línea y algunos países aún no han finalizado este proceso de ajuste. Los delitos que han sido criminalizados con arreglo a las leyes penales nacionales deben revisarse y actualizarse, por ejemplo, la información digital debe tener un carácter equivalente a las firmas y los listados impresos tradicionales[889]. Sin la integración de los ciberdelitos no pueden procesarse estas infracciones.

El reto principal de los sistemas jurídicos penales nacionales es el retraso existente entre el reconocimiento de abusos potenciales de las nuevas tecnologías y las modificaciones necesarias que deben introducirse en las leyes penales nacionales. Este reto sigue siendo tan importante y fundamental como siempre, puesto que cada vez es mayor la velocidad en la innovación de las redes. Muchos países están trabajando intensamente para introducir los ajustes jurídicos pertinentes[890]. Por regla general, el proceso de ajuste consta de tres etapas: ajustes a las leyes nacionales, identificación de lagunas en el Código Penal y redacción de la nueva legislación.

Ajustes a las leyes nacionales

Esos ajustes deben empezar con el reconocimiento de una utilización delictiva de la nueva tecnología. Es necesario que las autoridades nacionales competentes cuenten con departamentos específicos cualificados para investigar los posibles ciberdelitos. La creación de equipos de respuesta de emergencia informática (CERT) [891], de equipos de respuesta a incidencias informáticas (CIRT), de equipos de respuesta a incidentes de seguridad informática (CSIRT) y de otros mecanismos de investigación ha mejorado la situación.

Identificación de lagunas en el Código Penal

Para garantizar unas bases jurídicas eficaces, es necesario comparar la situación de las disposiciones jurídicas penales en las leyes nacionales con los requisitos que surgen debido a los nuevos tipos de delitos. En muchos casos, las leyes existentes pueden cubrir nuevas variedades de delitos existentes (por ejemplo, las leyes relativas a la falsificación pueden aplicarse fácilmente a documentos electrónicos). La necesidad de introducir modificaciones legislativas se limita a los delitos omitidos o insuficientemente contemplados por las leyes nacionales.

Redacción de la nueva legislación

Basándose en la experiencia, puede ser difícil para las autoridades nacionales llevar a cabo el proceso de redacción relativo a los ciberdelitos sin la cooperación internacional, debido al rápido desarrollo de las nuevas tecnologías y a sus complejas estructuras[892]. Una legislación sobre el ciberdelito por separado puede dar lugar a una duplicación significativa y a un derroche de recursos, y también es necesario verificar el desarrollo de la normativa y estrategias internacionales. Sin la armonización internacional de las disposiciones jurídicas penales nacionales, la lucha contra el ciberdelito transnacional tropezará con serias dificultades debido a la incoherencia o a la incompatibilidad de las legislaciones nacionales. En consecuencia, cada vez adquieren más importancia los intentos internacionales para armonizar las diferentes leyes penales nacionales [893]. Las leyes nacionales pueden beneficiarse enormemente de la experiencia de otros países y de la asesoría jurídica de expertos internacionales.

3.3.2 Nuevos delitos

En muchos casos, los delitos cometidos utilizando las TIC no son delitos nuevos sino estafas modificadas para ser cometidas en línea. Un ejemplo es el fraude; no hay demasiada diferencia entre alguien que envía una carta con la intención de engañar a otra persona y un correo electrónico con la misma intención[894]. Si el fraude ya es un delito, puede que no sea necesario ajustar las leyes nacionales para perseguir dichos actos.

La situación es distinta si los delitos ya no son contemplados por las leyes nacionales. En el pasado, algunos países contaban con disposiciones adecuadas para atacar el fraude regular pero no podían abordar los delitos en los que intervenían sistemas informáticos en vez de seres humanos. Para estos países ha sido necesario adoptar nuevas leyes que penalicen el fraude informático, además del fraude convencional. Varios ejemplos demuestran cómo la amplia interpretación de las disposiciones existentes no puede sustituir la adopción de nuevas leyes.

Además de los ajustes para los fraudes habituales, los legisladores deben analizar continuamente los nuevos tipos de ciberdelito en constante evolución para garantizar su efectiva penalización. Un ejemplo de ciberdelito que aún no ha sido penalizado en todos los países es el robo y el fraude en los juegos por ordenador y en línea[895]. Durante mucho tiempo, las discusiones sobre los juegos en línea se han centrado en temas relativos a la protección de los jóvenes (por ejemplo, el requisito de verificar la edad) y al

contenido ilegal (por ejemplo, acceso a pornografía infantil en el juego en línea "Segunda Vida")[896]. Se están descubriendo constantemente nuevas actividades delictivas; en los juegos en línea pueden "robarse" divisas virtuales y comercializarse en subastas[897]. Algunas divisas virtuales tienen valor en términos de moneda real (basándose en el tipo de cambio), dando al delito una dimensión "real"[898]. Tales delitos puede que no sean perseguidos en todos los países. A fin de evitar la aparición de paraísos seguros para los delincuentes es fundamental supervisar los desarrollos en todo el mundo.

3.3.3 Incremento en la utilización de las TIC y necesidad de nuevos instrumentos de investigación

Los delincuentes utilizan las TIC de diversas formas para preparar y llevar a cabo sus delitos[899]. Las autoridades competentes necesitan disponer de instrumentos adecuados para investigar los posibles actos delictivos. Algunos instrumentos (tales como la retención de datos)[900] podrían interferir con los derechos de los usuarios de Internet inocentes[901]. Si la gravedad del delito no guarda proporción con la intensidad de la interferencia, la utilización de instrumentos de investigación podría estar injustificada o ser ilegal. En consecuencia, aún no se han introducido en un cierto número de países algunos instrumentos que podrían mejorar la investigación.

La introducción de instrumentos de investigación siempre es el resultado de una solución de compromiso entre las ventajas que ello supone para las autoridades competentes y la interferencia que afecta los derechos de los usuarios de Internet inocentes. Es fundamental supervisar las actividades delictivas en curso para evaluar si varían los niveles de amenaza. A menudo, la introducción de nuevos instrumentos se ha justificado basándose en la "lucha contra el terrorismo", pero esto es más una motivación de largo alcance que una justificación específica *per se*.

3.3.4 Desarrollo de procedimientos para la evidencia digital

Especialmente debido a los bajos costes[902] comparados con los que supone el almacenamiento de documentos físicos, el número de documentos digitales es cada vez mayor[903]. La digitalización y la nueva utilización de las TIC tienen una gran influencia en los procedimientos relativos a la recopilación de evidencias y su utilización en los tribunales[904]. Como consecuencia de estos desarrollos, la evidencia digital se introdujo como una nueva fuente de evidencia[905]. Se define como cualquier dato almacenado o transmitido utilizando tecnología informática que soporte la teoría sobre la manera en que se ha producido un delito[906]. El manejo de la evidencia digital viene acompañado por retos peculiares y requiere la aplicación de procedimientos específicos[907]. Uno de los aspectos más difíciles consiste en mantener la integridad de esta evidencia digital[908]. Los datos digitales son extremadamente frágiles y pueden borrarse o modificarse fácilmente[909]. Esto es especialmente importante si se trata de información almacenada en la memoria RAM del sistema que se borra automáticamente cuando se desconecta el sistema[910] y, por consiguiente, requiere la utilización de técnicas de mantenimiento especiales[911]. Además los nuevos desarrollos pueden tener una fuerte repercusión en la forma de tratar la evidencia digital. Un ejemplo lo constituye la informática en nube ("*cloud-computing*"). En el pasado, los investigadores podían centrarse en los locales de los sospechosos buscando los datos que almacenaban en sus ordenadores. Hoy en día deben tener en cuenta que la información digital puede almacenarse en el exterior y sólo se puede acceder a ella a distancia, si es necesario.[912]

La evidencia digital desempeña un papel importante en varias fases de las investigaciones del ciberdelito. En general es posible distinguir cuatro fases[913]. La primera fase es la identificación de la evidencia pertinente[914]. Va seguida de una recopilación y mantenimiento de la evidencia[915]. La tercera fase incluye el análisis de la tecnología informática y la evidencia digital. Por último, la evidencia debe ser presentada ante los tribunales.

Además de los procedimientos relativos a la presentación en los tribunales de la evidencia digital, la forma en que dicha evidencia se recoge exige especial atención. Su recopilación está vinculada a los procedimientos forenses informáticos. El término "procedimientos forenses informáticos" describe el análisis sistemático de los equipos de TI con objeto de buscar la evidencia digital[916]. El hecho de que el volumen de datos almacenados en formato digital aumenta constantemente pone en evidencia los retos

logísticos que suponen tales investigaciones [917]. Los enfoques de los procedimientos forenses automatizados, por ejemplo realizando búsquedas basadas en los valores de troceo para localizar imágenes de pornografía infantil[918] o búsqueda por teclado[919], desempeñan un papel importante además de las investigaciones manuales[920].

Dependiendo del requisito de la investigación específica, los procedimientos forenses informáticos podrían por ejemplo incluir el análisis del hardware y el software utilizados por un sospechoso[921], el apoyo a los investigadores para identificar la evidencia pertinente[922], la recuperación de los ficheros suprimidos[923], el decriptado de ficheros[924] y la identificación de los usuarios de Internet analizando los datos de tráfico.[925]

721 See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf ; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

722 Regarding hash-value based searches for illegal content, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

723 For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp.

724 In 2014 Facebook alone reported 829 million daily active users and 1.32 billion monthly active user. Source: http://newsroom.fb.com/company-info/.

725 See for example: *Chaabane/Kaafar/Boreli*, Big Friend is Watching You: Analyzing Online Social networks Tracking Capabilities, Proceedings of the 2012 ACM workshop on online social networks, page 7 et seq.

726 See in this regard: *Daniel*, Cellular Location Evidence for Legal Professionals, 2014.

727 Regarding the development see: The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

728 Regarding the process see: *Rlamondon/Srihari*, On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey, ICC Transactions on pattern Analysis and machine Intelligence, Vol. 22, No.1, 2000, page 63 et seq.

729 The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

730 *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

731 *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

732 It was reported that the United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

733 Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

734 See *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

735 *Bohn/Coroama/Langheinrich/Mattern/Rohs,* Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications, Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[736] Regarding the impact of attacks, see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[737] A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[738] *Shimeall/Williams/Dunlevy*, Countering cyber war, NATO review, Winter 2001/2002, page 16, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

[739] One analysis by "Red Sheriff" in 2002 stated that more than 90 per cent of users worldwide use Microsoft`s operating systems (source: www.tecchannel.de – 20.09.2002).

[740] Regarding the discussion on the effect of the monoculture of operating systems on cybersecurity, see *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; Warning: Microsoft 'Monoculture', Associated Press, 15.02.2004, available at www.wired.com/news/privacy/0,1848,62307,00.html; *Geer and others*, CyberInsecurity: The Cost of Monopoly, available at: http://cryptome.org/cyberinsecurity.htm.

[741] With regard to the effect of spam on developing countries, see: Spam issues in developing countries, 2005, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[742] Regarding the integration of developing countries in the protection of network infrastructure, see: Chairman's Report on ITU Workshop On creating trust in Critical Network Infrastructures, available at: www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[743] WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services over long distances. For more information, see: The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX Technology for Broadband Wireless Access.

[744] Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[745] See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

[746] Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[747] See below: § 4.

[748] According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[749] See *Wallsten*, Regulation and Internet Use in Developing Countries, 2002, page 2.

[750] See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[751] An example for new technology in this area is WiMAX (Worldwide Interoperability for Microwave Access), a standards-based wireless technology that provides broadband connections over long distances. Each WiMAX node could enable high-speed Internet connectivity in a radius of up to 50 km. For more information, see: The WiMAX Forum at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

[752] Regarding the necessary steps to improve cybersecurity, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[753] The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: § 2.9.4.

754 Regarding hash-value based searches, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

755 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law). For more information, see *Moore*, Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law, available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.

756 "World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr/.

757 "Websense Security Trends Report 2004", page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

758 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

759 In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime. See below: § 6.2.15.

760 Regarding the costs, see: The World Information Society Report, 2007, available at: www.itu.int/wisr/

761 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

762 For more information, see: *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

763 With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

764 One example of an approach to restrict the use of public terminals for criminal offences is Art. 7 of the Italian Decree-Law No. 144. Decree-Law 27 July 2005, No. 144 – "Urgent measures for combating international terrorism". For more information about the Decree-Law, see for example the article "Privacy and data retention policies in selected countries", available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

765 See below: § 6.5.13.

766 Regarding the impact of censorship and control, see: *Burnheim*, The right to communicate, The Internet in Africa, 1999, available at: www.article19.org/pdfs/publications/africa-internet.pdf.

767 Regarding the question whether access to the Internet is a human right, see: *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; Regarding the declaration of Internet Access as a human right in Estonia, see: Information and Communications Technology, in UNDP Annual Report 2001, page 12, available at: www.undp.org/dpa/annualreport2001/arinfocom.pdf; Background Paper on Freedom of Expression and Internet Regulation, 2001, available at: www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

768 Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument.

769 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 a total of nearly 130 million websites at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

770 www.wikipedia.org

771 In the future development of the Internet, information provided by users will become even more important. "User generated content" is a key trend among the latest developments shaping the Internet. For more information, see: *O'Reilly*, What Is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software, 2005, available at: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

[772] For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

[773] See *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

[774] One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

[775] See *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003, page 112 *et seq*., available at: www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf; *Brown/Carlyle/Salmerón/Wood*, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530, available at: www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

[776] "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 per cent of all information required about the enemy". Reports vary as to the source of the quotation: The British High Commissioner Paul Boateng mentioned in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: *Boateng*, The role of the media in multicultural and multifaith societies, 2007, available at: www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624. The United States Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites, see: *Knezo*, "Sensitive but Unclassified" Information and Other Controls: Policy & Options for Scientific and Technical Information, 2006, page 24, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

[777] See Telegraph.co.uk, news from 13 January 2007.

[778] See for example, *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004, available at: www.internetpolicy.net/governance/20040315paper.pdf;

[779] For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff*, A Brief History of the Internet, available at: www.isoc.org/internet/history/brief.shtml.

[780] *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[781] Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/ *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et. seq*., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq*.; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

[782] For more information regarding anonymous communications, see below: § 3.2.l2.

[783] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[784] The first and still most important communication protocols are: Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[785] See *Kahn/Lukasik*, Fighting Cyber Crime and Terrorism: The Role of Technology, presentation at the Stanford Conference, December 1999, page 6 *et seq.*; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[786] One example of the international cooperation of companies and delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system of the mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, page 429 *et seq.* (with notes *Sieber*).

[787] See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

[788] Regarding the need for international cooperation in the fight against Cybercrime, see: *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[789] National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[790] See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[791] See below: § 3.2.10.

[792] See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142.

[793] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

[794] Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, page 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[795] See: *Lewis*, Computer Espionage, Titan Rain and China, page 1, available at: www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

[796] Regarding the extend of cross-border cases related to computer fraud, see: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 9, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[797] See below: § 6.6.12.

[798] See below: § 6.6.

[799] One example is phishing. Although most sites are still stored in the United States (32%), which has strong legislation in place, countries such as China (13%), Russia (7%) and the Republic of Korea (6%), which may have less effective instruments in the field of international cooperation in place, are playing a more important role. Apart from the United States, none of them has yet signed and ratified cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

[800] This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: § 5.1.

[801] For more information, see http://en.wikipedia.org/wiki/ILOVEYOU. Regarding the effect of the worm on critical information infrastructure protection, see: *Brock*, ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: www.gao.gov/archive/2000/ai00181t.pdf.

802 BBC News, Police close in on Love Bug culprit, 06.05.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. Regarding the technology used, see: http://radsoft.net/news/roundups/luv/20000504,00.html.

803 See for example: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

804 One example of low-cost services that are automated is e-mail. The automation of registration allows providers to offer e-mail addresses free of charge. For more information on the difficulties of prosecuting cybercrime involving e-mail addresses, see: § 3.2.I2.

805 The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

806 For more details on the automation of spam mails and the challenges for law-enforcement agencies, see: *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

807 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

808 The Online-Community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). Source: www.hackerwatch.org.

809 Regarding the distribution of hacking tools, see: CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

810 See CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

811 Nearly 50 per cent of all fraud complains reported to the United States Federal Trade Commission are related to an amount paid between USD 0 and 25. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

812 See Spam Issue in Developing Countries, Page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

813 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

814 Regarding the attacks, see: Lewis, Cyber Attacks Explained, 2007, available at: www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; A cyber-riot, The Economist, 10.05.2007, available at: www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007, available at: www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

815 See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

816 See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf.

817 See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, available at: www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, An Inside Look at Botnets, available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, BotNets: Detection and Mitigation.

818 See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf.

819 *Keizer*, Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, 21.10.2005, available at: www.techweb.com/wire/172303160.

820 See *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

821 E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[822] "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: www.ic3.gov/media/initiatives/BotRoast.pdf.

[823] *Staniford/Paxson/Weaver*, How to Own the Internet in Your Space Time, 2002, available at: www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

[824] *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International, 2006, page 142.

[825] *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[826] Regarding the necessary instruments, see below: § 6.5. One solution that is currently being discussed is data retention. Regarding the possibilities and risks of data retention, see: *Allitsch*, Data Retention on the Internet – A measure with one foot offside?, Computer Law Review International 2002, page 161 *et seq.*

[827] The term "quick freeze" is used to describe the immediate preservation of data on request of law-enforcement agencies. For more information, see below: § 6.5.4.

[828] The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country. For more information, see below: § 6.6.8.

[829] The graphical user interface called World Wide Web (WWW) was created in 1989.

[830] The development of the graphical user interface supported content-related offences in particular. For more information, see above: § 2.6.

[831] For more information see above: § 2.6.5.

[832] Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[833] With regard to the interception of peer-to-peer based VoIP communications, law-enforcement agencies need to concentrate on carrying out the interception by involving the access provider.

[834] Regarding the implications of the use of cell phones as storage media for computer forensics, see: *Al-Zarouni*, Mobile Handset Forensic Evidence: a challenge for Law Enforcement, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Al-Zarouni%20-%20Mobile%20Handset%20Forensic%20Evidence%20-%20a%20challenge%20for%20Law%20Enforcement.pdf.

[835] On the advantages of wireless networks for the development of an IT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries", 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[836] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[837] Regarding the challenges related to anonymous communication, see: *Sobel*, The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity, Virginia Journal of Law and Technology, Symposium, Vol. 5, 2000, available at: www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

[838] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[839] Regarding legislative approaches requiring identification prior to the use of public terminals, see Art. 7 of the Italian Decree-Law No. 144. For more information, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.* and below: § 6.5.14.

[840] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[841] Regarding the difficulties that are caused if offenders use open wireless networks, see above: § 3.2.3.

[842] Regarding technical approaches in tracing back users of anonymous communication servers based on the TOR structure, see: *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

[843] See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[844] Regarding the possibilities of tracing offenders using e-mail headers, see: *Al-Zarouni*, Tracing Email Headers, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

[845] *Donath*, Sociable Media, 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

[846] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Regarding the benefits of anonymous communication see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

[847] "(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services [...]". Source: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[848] Article 37 – Traffic and billing data "1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection". – Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[849] See below: § 6.5.13.

[850] Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[851] Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[852] This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

[853] Regarding user-based approaches in the fight against cybercrime, see: *Goerling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[854] The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols. For more information, see: *Swale*, Voice Over IP: Systems and Solutions, 2001; *Black*, Voice Over IP, 2001.

[855] Regarding the importance of interception and the technical solutions, see: *Karpagavinayagam/State/Festor*, Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection – ICIMP 2007. Regarding the challenges related to interception of data communication, see*: Swale/Chochliouros/Spiliopoulou/Chochliouros*, Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response, in *Janczewski/Colarik*, Cyber Warfare and Cyber Terrorism, 2007, page 424.

[856] Regarding the differences between PSTN and VoIP communication, see: *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq.*

[857] Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*,

Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq*.

858 Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the mathematical background, see: *Menezes*, Handbook of Applied Cryptography, 1996, page 49 *et seq.*

859 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: 2006 E-Crime Watch Survey, page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

860 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

861 *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

862 *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58, page 143.

863 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

864 Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

865 Examples include the software Pretty Good Privacy (see www.pgp.com) or True Crypt (see www.truecrypt.org).

866 Regarding the use of cryptography by terrorists, see: *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

867 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

868 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

869 Regarding the most popular tools, see: *Frichot*, An Analysis and Comparison of Clustered Password Crackers, 2004, page 3, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf. Regarding practical approaches in responding to the challenge of encryption see: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

870 See: Data Encryption, Parliament Office for Science and Technology No. 270, UK, 2006, page 3, available at: www.parliament.uk/documents/upload/postpn270.pdf.

871 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

872 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

873 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

874 *Schneier*, Applied Cryptography, page 185; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005, page 36, available at: www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

875 1 099 512 seconds.

876 *Usborne*, Has an old computer revealed that Reid toured world searching out new targets for al-Qaida?, The Independent, 18.01.2002, available at: www.independent.co.uk/news/world/americas/has-an-old-computer-revealed-that-reid-toured-world-searching-out-new-targets-for-alqaida-663609.html; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf. With further reference to the case: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

877 Equivalent to 10790283070806000000 years.

878 This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.

879 See *Leyden*, Vista encryption 'no threat' to computer forensics, The Register, 02.02.2007, available at: www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

880 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, Skype Security Evaluation, 2005, available at: www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

881 Phil Zimmermann, the developer of the encryption software PGP, developed a plug-in for VoIP software that can be used to install added encryption, in addition to the encryption provided by the operator of the communication services. The difficulty arising from the use of additional encryption methods is the fact that, even if the law-enforcement agencies intercept the communications between two suspects, the additional encryption will hinder the analysis. For more information on the software, see: *Markoff*, "Voice Encryption may draw US Scrutiny", New York Times, 22.05.2006, available at: www.nytimes.com/2006/05/22/technology/22privacy.html?ex=1305950400&en=ee5ceb136748c9a1&ei=5088. Regarding the related challenges for law-enforcement agencies, see: *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

882 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

883 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; *Labs*, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

884 For practical detection approaches, see: *Jackson/Grunsch/Claypoole/Lamont*, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, page 1 *et seq.*; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001.

885 See below: § 6.5.11.

886 See below: § 6.5.11.

887 See above: § 3.2.8.

888 See BBC News, Hacking: A history, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

889 An example of the integration of digital sources is Section 11, Subsection 3 of the German Penal Code: "Audio & visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection."

890 Within this process, the case-law based Anglo-American law system has advantages in terms of reaction time.

891 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 per cent of Internet systems to a halt in November 1988. For more information on the history of the CERT CC, see: www.cert.org/meet_cert/; *Goodman*, Why the Police don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.

892 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and UN Resolution 55/63.

893 See below: § 5.

894 See above: § 2.8.1.

895 Regarding the offences recognized in relation to online games, see above: § 2.6.5.

896 Regarding the trade of child pornography in Second Life, see for example BBC, Second Life "child abuse" claim, 09.05.2007, at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: http://secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy/.

897 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 *et seq.*

898 *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

899 Regarding the use of ICTs by terrorist groups, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16; *Hutchinson*, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf; *Gercke*, Cyberterrorism, Computer Law Review International 2007, page 64.

900 Data retention describes the collection of certain data (such as traffic data) through obliged institutions, e.g. access providers. For more details, see below: § 6.5.5.

901 Relating to these concerns, see: Advocate General Opinion, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

902 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

903 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

904 *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

905 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historic development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

906 *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

907 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq*.

908 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1.

909 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

910 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

911 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

912 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

913 Regarding the different models of cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also: *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

914 This includes the development of investigation strategies.

915 The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

916 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

917 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

918 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

919 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

920 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

921 This includes for example the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

922 This includes for example the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

923 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

924 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

925 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

4 Creación de capacidades

Bibliografía (seleccionada): *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141*; Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf*; Henten/Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1; *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003*; Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf; *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et seq.*; *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

El número cada vez mayor de ciberdelitos reconocidos y de víctimas, incluso en países en desarrollo con escasa conexión, sitúa los temas de la ciberseguridad y el ciberdelito en los primeros lugares de la agenda del sector privado y los poderes públicos. Puesto que las TIC evolucionan con tanta rapidez, especialmente en los países en desarrollo, es importante la creación e implementación de medidas anticiberdelito eficaces. En el capítulo siguiente se presenta un panorama general de las cuestiones que deben tener frecuentemente en cuenta los países al elaborar ese tipo de medidas paliativas.

4.1 Ciberseguridad y ciberdelito

Una de las primeras cuestiones que se plantea en general cuando los países empiezan a abordar el ciberdelito es si hay que hacerlo en el marco de la observancia de la ley o de la ciberseguridad. La distinción entre ambos aspectos no es fácil,[926] dado que indudablemente están relacionados entre sí, como lo indica el hecho de que en la Resolución sobre seguridad cibernética[927] de la Asamblea General de las Naciones Unidas de 2010 se estima que el ciberdelito constituye un problema importante. Por lo tanto, aunque puede estimarse que el ciberdelito es un elemento integral [928] de todo enfoque destinado a aumentar la ciberseguridad, no cabe duda que es apenas uno de los componentes de una estrategia en materia de ciberseguridad. Al tener esto en cuenta se pone de relieve el carácter interdisciplinario de ambos aspectos y, por consiguiente, la necesidad de lograr la participación de diferentes instancias gubernamentales interesadas en el proceso. Elaborar una respuesta nacional ante el ciberdelito supone muchas veces la participación de diferentes ministerios (como el Fiscal General, el Ministerio de Comunicaciones o el Ministerio de Educación).

4.2 Metodología aplicable a la creación de capacidades

Al analizar los diferentes enfoques que permitirán crear las capacidades nacionales necesarias para combatir el ciberdelito en cada país, se observan ciertos elementos básicos fundamentales de un enfoque basado en prácticas óptimas.

4.2.1 Puesta en marcha

El punto de partida es un debate a fondo en el país (y con organizaciones internacionales de apoyo) para comprender plenamente las demandas y estar en condiciones de elaborar el plan de proyecto o la propuesta correspondiente. En ese debate se tratan diversos asuntos, por ejemplo: ¿Se contemplará en el proyecto una estrategia, una política, una legislación, o sólo elementos de ellas? ¿Existen ya estructuras que convendría utilizar de base? ¿Qué normas nacionales, regionales o internacionales habría que utilizar para realizar un análisis comparativo? ¿Qué temas habría que tratar (por ejemplo, la protección de los niños en línea, la protección de datos, el ciberdelito, las transacciones electrónicas)? ¿Tendría el proyecto que contemplar además la capacitación de expertos y/o la elaboración de material didáctico? ¿Recibe actualmente el país otro tipo de apoyo? A fin de coordinar las diferentes actividades de apoyo, es sumamente importante comprender la situación de las diferentes actividades.

4.2.2 Elaboración de un plan de proyecto

Teniendo en cuenta los resultados del debate inicial, puede elaborarse un plan de proyecto provisional que describa las actividades, los expertos participantes, los resultados esperados y el calendario previsto.

4.2.3 La evaluación como punto de partida

Poner en marcha un proyecto con una evaluación adecuada es un factor esencial para obtener los resultados deseados. Únicamente si todos los funcionarios y expertos que participan en él están al tanto de la situación de los componentes existentes (por ejemplo, leyes o políticas) y de ciertos detalles, como los instrumentos jurídicos concretos de un país, es posible un apoyo adaptado a las necesidades específicas. Esa evaluación debería tener en cuenta la capacidad institucional y la determinación de los principales interesados (expertos gubernamentales, asociaciones empresariales y grupos de interés, como los grupos de defensa de los derechos civiles).

4.2.4 Análisis comparativo

Los resultados de la evaluación muestran la situación actual, pero la evaluación no puede visualizar cómo está situado un país en comparación con ciertos indicadores. El análisis comparativo se funda en los resultados de la evaluación, pero podría añadir un componente analítico. La base de la comparación será la determinación de los criterios que se utilizan para determinar posibles lagunas y hacer hincapié en las prácticas más óptimas. Si el país beneficiario es un pequeño país insular del Pacífico y forma parte de la Commonwealth, se podría comparar su legislación nacional o sus proyectos de ley vigentes con la Ley modelo de la Commonwealth sobre delitos informáticos y delitos conexos y con la estructura del modelo regional ICB4PAC para los países del Pacífico. Podrían añadirse a la lista otra serie de normas, como la Directiva de la Unión Europea sobre ataques contra los sistemas de información o el Convenio del Consejo de Europa sobre la Ciberdelincuencia. El resultado será un informe complejo en el que se comparan o enumeran los elementos nacionales que se hayan determinado y los elementos comparables de la evaluación, se indican las diferencias y semejanzas y se formulan recomendaciones.

4.2.5 Consultas con los interesados

Otra práctica óptima de los enfoques aplicables a la creación de capacidades es la celebración de consultas con los interesados. La experiencia de muchos años sobre creación de capacidades en el ámbito de la estrategia, la política y la ley, indica que las consultas con los interesados pueden fortalecer considerablemente el proceso de elaboración necesario. Es indudable que requiere mucha más energía examinar los elementos de una política nacional y de un proyecto de ley cuando intervienen numerosos interesados. Sin embargo, la ausencia de contratiempos en el proceso legislativo que siguió a las consultas con los interesados en esos países, que ya fueron sometidos al procedimiento de transposición, es un indicio de las ventajas que supone mantener intensos debates en el marco del proceso de elaboración con el fin de lograr que se tengan en cuenta los diferentes intereses.

Durante el curso de esas consultas en el país, varios interesados nacionales (por ejemplo, el público en general, políticos, funcionarios gubernamentales, la comunidad empresarial del sector, proveedores de servicios Internet y grupos de defensa de los derechos civiles) serán invitados a diferentes reuniones de consulta en las que se examinarán los resultados de los análisis realizados y las acciones a seguir. Se tomará nota de las aportaciones de los interesados, que serán contempladas en el momento de elaborar las políticas y leyes correspondientes.

4.2.6 Proceso de elaboración

Sobre la base del análisis comparativo y las consultas con los interesados, se podrán elaborar o modificar estrategias, políticas y leyes. Por lo general, el proceso de elaboración incluye también la redacción de notas explicativas y otros documentos (por ejemplo, documentos informativos para el gabinete).

4.2.7 Actividades de capacitación, formación y seguimiento

Las estrategias, políticas y leyes más óptimas no serán por sí solas suficientes para luchar eficazmente contra el ciberdelito. Hay otras medidas igualmente importantes, como la capacitación de los profesionales y la educación del público en general. Las actividades de capacitación pueden comprender la formación en escuelas sobre prevención del delito por edad y simulacros de ciberincidentes en tiempo real para altos funcionarios gubernamentales, cuyo propósito es ayudarlos a evitar ataques. Las actividades de seguimiento también contemplan habitualmente una evaluación del proyecto.

4.3 Una estrategia como punto de partida

Como se ha indicado anteriormente, la ciberseguridad[929] desempeña un papel importante en el desarrollo de la tecnología de la información en curso así como en el de los servicios de Internet[930]. Hacer que Internet sea más segura (y proteger a los usuarios de Internet) se ha convertido en parte integrante del desarrollo de nuevos servicios así como de la política gubernamental[931]. Las estrategias de ciberseguridad, por ejemplo el desarrollo de sistemas de protección técnica o la educación de los usuarios para evitar que sean víctimas de ciberdelitos, pueden ayudar a disminuir el riesgo del ciberdelito.[932]

Una estrategia anticiberdelito debe ser un elemento integrante de una estrategia de ciberseguridad. La Agenda sobre Ciberseguridad Global de la UIT[933], como marco global para el diálogo y la cooperación internacional a fin de coordinar la respuesta internacional a los retos cada vez mayores que plantea la ciberseguridad y para mejorar la confianza y seguridad en la sociedad de la información, se ha basado en los trabajos, iniciativas y asociaciones existentes con el objetivo de proponer estrategias a escala mundial que aborden estos retos afines. Todas las medidas necesarias, indicadas en los cinco pilares de la Agenda sobre Ciberseguridad Global, son pertinentes a cualquier estrategia de ciberseguridad. Además, la capacidad de luchar de manera eficaz contra los ciberdelitos requiere tomar medidas en el marco de los cinco pilares.[934]

4.3.1 Implementación de las estrategias existentes

Una posibilidad consiste en que las estrategias anticiberdelito establecidas en los países industrializados puedan introducirse en los países en desarrollo, lo que ofrece las ventajas de un menor coste y menos tiempo de desarrollo. La implementación de las estrategias existentes podría permitir a los países en desarrollo beneficiarse de los conocimientos y experiencias actuales.

No obstante, la implementación de una estrategia anticiberdelito ya existente plantea varias dificultades. Aunque los países en desarrollo y desarrollados se enfrentan a retos similares, las soluciones óptimas que podrían adoptarse dependen de los recursos y capacidades de cada país. Los países industrializados pueden promover la ciberseguridad de manera distinta y más flexible; por ejemplo, centrándose en temas de protección técnica más onerosos.

Existen otros temas que deben tener en cuenta los países en desarrollo que adopten estrategias anticiberdelito existentes. Entre ellos cabe citar la compatibilidad de los respectivos sistemas jurídicos, la situación de las iniciativas de apoyo (por ejemplo, educación de la sociedad), la amplitud de las medidas de

autoprotección existentes así como el grado de soporte por parte del sector privado (por ejemplo, a través de asociaciones públicas/privadas).

4.3.2 Diferencias regionales

Dado el carácter internacional del ciberdelito, la armonización de las leyes nacionales y de las técnicas resulta indispensable para combatirlo. Sin embargo, esta armonización debe tener en cuenta la demanda y capacidad regionales. La importancia de los aspectos regionales en la implementación de las estrategias anticiberdelito viene realzada por el hecho de que muchas normas jurídicas y técnicas hayan sido acordadas entre países industrializados sin incluir varios aspectos importantes para los países en desarrollo[935]. Por lo tanto, es necesario incluir los factores y diferencias regionales cuando se vayan a implementar en algún otro lugar.

4.3.3 Relevancia de los temas relativos al ciberdelito en los pilares de la ciberseguridad

La Agenda sobre Ciberseguridad Global tiene siete objetivos estratégicos principales basados en cinco áreas de trabajo: 1) Medidas legales; 2) Medidas técnicas y de procedimiento; 3) Estructuras institucionales; 4) Creación de capacidades, y 5) Cooperación internacional. Como se ha indicado anteriormente, los temas relativos al ciberdelito desempeñan un papel importante en los cinco pilares de la Agenda sobre Ciberseguridad Global. Entre estas áreas de trabajo, las medidas legales se centran en la forma de abordar los retos legislativos planteados por las actividades delictivas que se conducen por las redes TIC procurando mantener la compatibilidad internacional.

4.3.4 Adopción de estrategias no limitada a la formulación de futuros planes

Varios países han elaborado en los últimos años una serie de estrategias en materia de ciberseguridad y ciberdelito. [936] Lo mismo ha ocurrido en las organizaciones internacionales e instituciones intergubernamentales. [937] Al comparar estos diferentes planteamientos, se observan similitudes considerables.

La mayoría de las estrategias en materia de ciberseguridad y ciberdelito se condensan en documentos muy breves (de 10 a 20 páginas) que no ofrecen una información demasiado completa. Se consagran por lo general a destacar la importancia del tema, a confirmar la voluntad de actuar y a formular decisiones generales sobre lo que convendría hacer para mejorar la ciberseguridad. La mayoría de las estrategias no proponen soluciones ni medidas concretas. Se considera que una estrategia debe aportar una solución a un determinado obstáculo o problema. No es necesario que se refiera a un caso específico, pero podría servir de guía en la confrontación de problemas.[938] La estrategia sobre ciberseguridad formulada en Alemania[939], por ejemplo, indica que el gobierno tiene previsto organizar iniciativas y examinar aún más las responsabilidades de los proveedores. La estrategia, sin embargo, no determina quién tomará la iniciativa ni de qué manera se alcanzarán los objetivos.

Una estrategia muy básica tiene la ventaja de que su elaboración requiere poco tiempo. Los límites impuestos por la definición de principios sumamente generales también reducen notablemente la necesidad de llevar a cabo una actualización periódica. [940] Una estrategia muy general podría seguir en pie durante años antes de que sea necesario ponerla al día. Pero este enfoque también plantea dificultades. Es indudable que la elaboración de un enfoque exhaustivo no exige medidas ni actividades que deban combinarse en un documento. Sin embargo, la existencia de numerosos documentos puede ocasionar la falta de compatibilidad de diferentes medidas. La experiencia indica que, en lo que respecta a la complejidad de las amenazas, incluso pequeños conflictos o incoherencias entre las diferentes medidas pueden reducir considerablemente la eficacia de la prevención de un incidente y la respuesta ante el mismo. Sólo gracias a la plena armonización y complementariedad recíproca de todos sus componentes, una estrategia podrá lograr su máxima eficacia.

Una solución sería combinar una estrategia muy general con planes de acción concretos (y, por lo tanto, más detallados) en el marco de las actividades de seguimiento. Este enfoque ofrece la posibilidad de demostrar públicamente los esfuerzos que se llevan a cabo dando a conocer una estrategia de ciberdelito y ciberseguridad pero, al mismo tiempo, manteniendo el carácter confidencial de las medidas concretas.

Los gobiernos pueden tener una necesidad urgente de presentar un panorama general de actividades en el ámbito del ciberdelito y la ciberseguridad, y los países pueden necesitar una estrategia nacional de ciberseguridad para atraer a los inversores. Al mismo tiempo, no en todos los casos podría aceptarse que se revelaran detalles sobre las medidas adoptadas para aumentar la seguridad e identificar a los delincuentes puesto que daría a estos información que podrían utilizar para constatar deficiencias.

4.4 Relevancia de una política

El desarrollo de una legislación que tipifique como delito ciertas conductas o introduzca instrumentos de investigación, constituye un procedimiento bastante insólito en la mayor parte de los países. El procedimiento habitual consiste en la introducción inicial de una política[941]. Una política es comparable a una estrategia que defina los distintos instrumentos utilizados para abordar un problema. A diferencia de una estrategia más genérica de lucha contra el ciberdelito que pueda implicar a varios interesados, el papel de la política consiste en definir la respuesta pública del gobierno a un determinado problema[942]. Esta respuesta no se limita forzosamente a la legislación, ya que los gobiernos pueden recurrir a diversos instrumentos para alcanzar las metas de la política. Incluso admitiendo la necesidad de aplicar legislación, no es forzosamente necesario ceñirse al código penal ya que también puede incorporarse legislación más orientada a la prevención de la delincuencia. A este respecto, el desarrollo de una legislación permite al gobierno definir exhaustivamente su respuesta al problema. Dado que la lucha contra el ciberdelito no puede limitarse exclusivamente a la introducción de la oportuna legislación, sino que debe constar de diversas estrategias con distintas medidas, la política puede lograr que las diferentes medidas no provoquen conflicto alguno.

En los diferentes planteamientos para la armonización de la legislación contra el ciberdelito, se ha otorgado escasa prioridad a la integración de la legislación en el marco jurídico nacional, en la política existente e incluso en el desarrollo inicial de dicha política. Por este motivo, ciertos países que se limitaron a introducir legislación contra el ciberdelito sin desarrollar previamente una estrategia para combatirlo ni políticas a nivel gubernamental, han tenido que arrostrar graves dificultades que se han debido principalmente a la falta de medidas de prevención del ciberdelito y al solapamiento de las diferentes medidas.

4.4.1 Responsabilidad en el ámbito gubernamental

La política permite ajustar las competencias sobre un determinado asunto en el ámbito gubernamental. El solapamiento entre los diversos ministerios es bastante común y, en lo que respecta al Ciberdelito, se produce con cierta frecuencia dado el carácter interdisciplinario de este tema.[943] Algunos aspectos relacionados con la lucha contra el ciberdelito tienen relación con los mandatos del Ministerio de Justicia, del Ministerio de Comunicaciones y del Ministerio del Interior, por citar tres. En el proceso de desarrollo de la política, puede definirse el papel de las distintas instituciones gubernamentales.

Esto se expresa, por ejemplo, en el Proyecto de Modelo de Política contra el Ciberdelito ICB4PAC.[944]

> *A este respecto resulta imprescindible definir con toda claridad las responsabilidades de los distintos interesados. Esto es especialmente importante por el carácter transectorial del ciberdelito que podría implicar a los mandatos de diversas instituciones tales como la Fiscalía General o el Ministerio de Comunicaciones.*

4.4.2 Definición de los diversos componentes

Como se ha indicado anteriormente, la política puede servir para definir los diversos componentes del planteamiento. Esto podría ir del fortalecimiento de la capacidad institucional (por ejemplo, la policía y la represión) a enmiendas legislativas específicas (tales como la introducción de legislación más avanzada).

Ésta es otra de las cuestiones expresadas en el Proyecto de Modelo de Política contra el Ciberdelito ICB4PAC[945]:

Responder a los retos multidimensionales de la lucha contra el ciberdelito exige un planteamiento de amplio alcance que incluya políticas globales, legislación, educación y sensibilización, creación de capacidades e investigación así como soluciones de índole técnica.

Lo ideal sería que la política se utilizase para coordinar las diversas actividades, incluso si son competencia de distintos ministerios y órganos gubernamentales. El hecho de que, por lo general, las políticas tengan que ser aprobadas por el consejo de ministros, no sólo permite identificar los distintos órganos gubernamentales y ministerios implicados en este asunto sino que facilita la armonización de sus actividades.[946]

4.4.3 Determinación de los interesados

La política no sólo sirve para identificar las instituciones gubernamentales implicadas, sino también los interesados con los que hay que contar. Por ejemplo, puede que sea necesario elaborar directrices con respecto a la implicación del sector privado.

La cuestión de los interesados que deben implicarse y con los que hay que contar se expresa, por ejemplo, en el Proyecto de Modelo de Política contra el Ciberdelito ICB4PAC.[947]

Además, este planteamiento exige la implicación de los diversos interesados tales como el gobierno, los ministerios y los organismos gubernamentales, el sector privado, los colegios y universidades, los dirigentes tradicionales, la comunidad, los organismos internacionales y regionales, los cuerpos y fuerzas de seguridad, los jueces, los servicios aduaneros, los fiscales, los abogados, la sociedad civil y las ONG.

4.4.4 Identificación de los elementos de referencia

Como se subraya más adelante, las distintas organizaciones regionales consideran que la importancia de la armonización de la legislación marca una de las prioridades clave[948]. La necesidad de armonización, no obstante, no se limita a la legislación, sino que incluye cuestiones tales como la estrategia y la formación de expertos.[949] La política puede servir para identificar ámbitos en los que debería aplicarse la armonización así como para definir las normas internacionales y/o regionales que deberían implantarse.

La importancia de la armonización se expresa por ejemplo en el Proyecto de Modelo de Política contra el Ciberdelito ICB4PAC.[950]

En lo tocante a la dimensión mundial del ciberdelito así como a la necesidad de proteger a los usuarios de Internet de la Región para que no se conviertan en víctimas del ciberdelito, las medidas orientadas a aumentar la capacidad de lucha contra el ciberdelito deben tener la máxima prioridad. Las estrategias y especialmente la legislación desarrollada para responder a los retos del ciberdelito deben, en primer lugar, ajustarse a las normas internacionales y, en segundo lugar, reflejar las peculiaridades de la Región.

Otro ejemplo lo constituye el Modelo HIPCAR de Política contra el Ciberdelito [951]:

Se establecerán disposiciones que contemplen las formas de ciberdelito más comunes y con una aceptación internacional más amplia, así como los delitos que revistan un interés particular para la región (como por ejemplo el correo basura).
Para facilitar la cooperación con los cuerpos y fuerzas de seguridad de los países de la región y fuera de ésta, la legislación deberá será compatible, en la medida de lo posible, con las normas internacionales, las prácticas óptimas y las normas regionales y prácticas óptimas existentes.

4.4.5 Definición de los temas clave para la legislación

La política puede utilizarse para definir ámbitos clave que deban contemplarse en la legislación. El nivel de detalle podría descender hasta la pormenorización de las disposiciones que vayan a incorporarse a la legislación sobre Ciberdelincuencia.

Un ejemplo lo constituye el Modelo HIPCAR de Política contra el Ciberdelito[952]:

> *Debería incluirse una disposición que penalice la producción, venta y demás actividades, deliberadas e ilegales, relacionadas con la pornografía infantil. A este respecto, deben tenerse especialmente en cuenta las normas internacionales. Además, la legislación debe contemplar la penalización de la posesión de pornografía infantil y el acceso a sitios web que contengan pornografía infantil. Debe incluirse una cláusula de exención que permita a las fuerzas y cuerpos de seguridad realizar sus labores de investigación.*

4.4.6 Definición de los marcos legales que necesitan enmendarse, actualizarse o modificarse

La introducción de la legislación contra el ciberdelito no es una tarea fácil, ya que hay varios ámbitos que deben ser objeto de reglamentación. Además del derecho sustantivo penal y procesal, la legislación aplicable a la lucha contra el ciberdelito puede abarcar temas relativos a la cooperación internacional, las evidencias electrónicas y la responsabilidad de los proveedores de servicios de Internet (PSI). Es posible que, en la mayor parte de los países, ya existan elementos de dicha legislación, a menudo en marcos jurídicos diferentes. Las disposiciones relativas a los ciberdelitos no tienen por qué integrarse por fuerza en una única ley. En lo que respecta a las estructuras existentes durante el proceso de introducción de nueva legislación, tal vez sea necesario actualizar varias leyes (por ejemplo, introduciendo enmiendas a una Ley de Evidencia para que sea aplicable a la admisión de evidencias electrónicas en los procesos penales) o suprimir disposiciones de una legislación más antigua (por ejemplo en una Ley de Telecomunicaciones).

El planteamiento de aplicar la legislación contra el ciberdelito respetando las estructuras existentes, es ciertamente más problemático que la simple plasmación literal de una norma regional o práctica óptima internacional en una sola ley independiente. Debe señalarse no obstante el hecho de que este proceso de adaptación permite la subsistencia de las tradiciones jurídicas nacionales, por lo que muchos países son partidarios de este planteamiento.

La política puede servir para definir los diversos componentes que deben integrarse así como para identificar las leyes existentes que necesitan actualizarse.

4.4.7 Pertinencia de la prevención de la delincuencia

A pesar de que la amenaza de un castigo evite potencialmente los delitos, el objeto de la legislación penal no es la prevención del delito sino la sanción del mismo. Sin embargo, la prevención de la delincuencia se identifica como un componente clave para la eficacia de la lucha contra el ciberdelito.[953] Las medidas pueden comprender desde soluciones técnicas (tales como cortafuegos para evitar los accesos ilegales a un sistema informático y software antivirus que dificulte la instalación de programas informáticos malintencionados) hasta el bloqueo del acceso a contenidos ilegales. [954]

La importancia de la prevención del delito se expresa por ejemplo en el Proyecto de Modelo de Política contra el Ciberdelito ICB4PAC.[955]

Además de la penalización del ciberdelito y la mejora de la capacidad de los cuerpos y fuerzas de seguridad para luchar contra el ciberdelito, es necesario desarrollar medidas de prevención del delito. Durante el desarrollo de dichas medidas, que pueden comprender desde soluciones técnicas hasta actividades orientadas a la concienciación de los usuarios, es importante identificar los grupos que exigen una atención específica tales como la juventud, las personas con algún tipo de discapacidad tecnológica (tales como las que residen en aldeas aisladas y carecen de conocimientos tecnológicos) y las mujeres. No obstante, las medidas para la prevención del delito deben aplicarse también a usuarios avanzados y a los actores iniciados en la tecnología tales como los proveedores de infraestructuras críticas (por ejemplo, de los sectores turístico o financiero). En el debate sobre las medidas necesarias debe tenerse en cuenta también toda la gama de instrumentos tales como la sensibilización, la entrega gratuita y promoción de tecnología de protección (como el software antivirus) y la implementación de soluciones que permitan a los padres limitar el acceso a ciertos contenidos. Lo ideal sería que estas medidas estuviesen disponibles cuando se introdujera un servicio/tecnología y se mantuviesen durante su explotación. Para una mayor difusión de estas medidas, debe implicarse a una gama más amplia de interesados, desde proveedores de servicios de Internet hasta gobiernos y organismos regionales, y buscar diversas fuentes de financiación.

4.5 Función de los organismos reguladores en la lucha contra el ciberdelito

En los últimos decenios, las soluciones debatidas para acabar con la ciberdelincuencia se han centrado en la legislación. Como ya se ha señalado en el Capítulo dedicado a la estrategia anticiberdelito, los componentes esenciales de una solución de amplio alcance para luchar contra el ciberdelito son considerablemente más complejos. Últimamente, ha cobrado protagonismo la función de los organismos reguladores en la lucha contra el ciberdelito.

4.5.1 De la reglamentación de las telecomunicaciones a la de las TIC

La función de los organismos reguladores en el contexto de las telecomunicaciones está ampliamente reconocida.[956] Con la desaparición del antiguo modelo de división de las responsabilidades entre el gobierno y el sector privado, favorecida por Internet, se ha observado una transformación de la función tradicional de los organismos reguladores de las TIC y un cambio en los objetivos de la reglamentación de las TIC. [957] En la actualidad, los organismos reguladores ya se encuentran inmersos en toda una gama de actividades vinculadas a la lucha contra el ciberdelito. Esto reviste una importancia especial en ámbitos tales como el de la reglamentación de contenidos, la seguridad de la red y la protección del consumidor, dada la vulnerabilidad de los usuarios[958]. La implicación de los organismos reguladores es, por consiguiente, consecuencia del hecho de que el ciberdelito sea una rémora para el desarrollo de la industria de las TIC y de los productos y servicios relacionados.

Los nuevos deberes y responsabilidades de los organismos reguladores de las TIC en la lucha contra el ciberdelito pueden considerarse parte de una tendencia más amplia hacia la conversión de los modelos centralizados de reglamentación del ciberdelito en estructuras flexibles. En algunos países, los organismos reguladores de las TIC ya han explorado la posibilidad de transferir el ámbito de los deberes reglamentarios desde la esfera de las cuestiones de la competencia y autorización en el seno de la industria de la telecomunicación a un ámbito más amplio en el que tengan cabida la protección del consumidor, el desarrollo de la industria, la ciberseguridad, la participación en el desarrollo y aplicación de políticas contra el ciberdelito en las que se inserte una utilización más amplia de las TIC y por consiguiente, cuestiones relacionadas con el ciberdelito. A pesar de la reciente creación de nuevos organismos reguladores con mandatos y responsabilidades entre los que figura la lucha contra el ciberdelito, [959] los organismos reguladores de las TIC con más años de existencia han ampliado sus competencias para dar cabida a nuevas actividades destinadas a hacer frente a las amenazas de origen informático.[960] No obstante, el grado de esta implicación y sus limitaciones siguen siendo objeto de debate.

4.5.2 Modelos para la ampliación de la responsabilidad del Organismo Regulador

Existen dos modelos diferentes para establecer el mandato de los organismos reguladores en la lucha contra el ciberdelito, a saber: la ampliación de la interpretación del mandato en vigor o la creación de un nuevo mandato.

Dos de los ámbitos de competencia tradicionales de los organismos reguladores son la protección del consumidor y la seguridad de la red. Con el paso de los servicios de telecomunicación a los servicios relacionados con Internet, se ha modificado el objetivo principal de la protección al consumidor. Además de las amenazas tradicionales, hay que tener en cuenta la repercusión del correo basura, los programas informáticos malintencionados y las redes robot. Un ejemplo de ampliación del mandato es del Organismo Autónomo de Correos y Telecomunicaciones de los Países Bajos (OPTA). En el mandato[961] de este organismo regulador figuran la prohibición del correo basura [962] y la prevención de la difusión de programas maliciosos.[963] Durante el debate del mandato de la OPTA, esta organización manifestó su apoyo a la construcción de un puente entre la ciberseguridad, como ámbito de actividad tradicional, y el ciberdelito, para poder abordar con eficacia ambos problemas.[964] Si el ciberdelito se considera un fallo de la ciberseguridad, es lógico que el mandato del organismo regulador se amplíe automáticamente.

La posibilidad de ampliar el mandato del organismo regulador para asumir el problema del ciberdelito depende también del diseño institucional del organismo regulador y de si éste tiene competencia sobre varios sectores (como las comisiones de suministros públicos), sobre un sector específico o se trata de un organismo regulador convergente. Aunque cada modelo de diseño institucional tiene sus ventajas e inconvenientes desde el punto de vista de la reglamentación de la industria de las TIC[965], debe tenerse en cuenta el tipo de diseño institucional a la hora de evaluar cómo y en qué ámbitos debe implicarse el organismo regulador de las TIC. Los organismos reguladores convergentes con responsabilidad sobre medios y contenidos así como los servicios TIC, suelen tener que hacer frente a los retos que plantea la complejidad de su carga de trabajo. No obstante, su amplio mandato puede constituir una ventaja a la hora de afrontar los problemas relacionados con los contenidos, tales como la pornografía infantil u otros contenidos ilegales o perniciosos.[966] En un entorno convergente en el que los organismos reguladores tradicionales pueden luchar por resolver diversos problemas, tales como el de la consolidación de los proveedores de contenidos de medios y los de servicios de telecomunicación, el operador de telecomunicaciones parece estar en mejores condiciones para afrontar los problemas de redes y contenidos. Además, el regulador convergente puede contribuir a evitar las incoherencias y la incertidumbre de la reglamentación y la desigualdad de la intervención reglamentaria con respecto a los diferentes contenidos distribuidos por las diversas plataformas.[967] No obstante, el debate de las ventajas de un organismo regulador convergente no debe restar importancia a las actividades de los organismos reguladores monosectoriales. Por ejemplo, mientras que a finales de 2009 en la Unión Europea sólo había cuatro organismos reguladores convergentes, [968] eran muchos más los implicados en la lucha contra el ciberdelito.

Cuando se considera la ampliación de la interpretación de los mandatos actuales, debe tenerse en cuenta la capacidad del organismo regulador y la necesidad de evitar el solapamiento con los mandatos de otras organizaciones. Estos conflictos potenciales pueden resolverse más fácilmente si se definen con claridad los nuevos mandatos.

El segundo planteamiento consiste en la definición de nuevos mandatos. Ante la posibilidad de que se produzcan conflictos, algunos países como Malasia han optado por volver a definir los mandatos a fin de evitar confusiones y solapamientos. La Comisión de Comunicaciones y Multimedios de Malasia (MCMC), en calidad de organismo regulador convergente, ha establecido un departamento especial[969] para tratar los problemas relativos a la seguridad de la información y la fiabilidad de la red, la integridad de las comunicaciones y las infraestructuras de comunicaciones críticas.[970] Un planteamiento similar es el adoptado en la República de Corea, donde en 2008, se instituyó la Comisión de Comunicaciones de Corea (KCC) por fusión del Ministerio de Información y de Comunicación y la Comisión de Radiodifusión de Corea. Entre otros cometidos, la KCC es responsable de la protección de los usuarios de Internet frente a contenidos ilegales o perniciosos.[971]

4.5.3 Ejemplos para la implicación de los Organismos Reguladores en la lucha contra el Ciberdelito

Siguen pendientes de definición tanto el modelo de definición del mandato del organismo regulador como el ámbito de actuación de los organismos reguladores de las TIC en este campo. Sólo unos pocos organismos reguladores tienen competencias efectivas para ir más allá de la reglamentación de las telecomunicaciones y abordar problemas más amplios del sector de las TIC. Al desenvolverse en un sector en acelerado cambio y en desarrollo, los organismos reguladores se ven expuestos a nuevos ámbitos que se han considerado tradicionalmente dominio de otros departamentos y organismos gubernamentales, e incluso tierra de nadie.[972] Aunque el organismo regulador posea de hecho suficiente competencia y experiencia técnica en el sector para implicarse en la solución de problemas específicos relacionados con el ciberdelito, la existencia de un mandato claro en el que se definan sin ambigüedad las áreas exactas de implicación es clave para la eficacia de los organismos reguladores. Las esferas de implicación potencial de los organismos reguladores se especifican a continuación:

Estrategias de política mundial

El principio de la división de poderes dentro del Estado[973] establece la separación entre el proceso de formulación de políticas y la aplicación de éstas.[974] A pesar de la importancia de este concepto, la complejidad de la cuestión puede exigir que los organismos reguladores se impliquen en el asesoramiento en materia de políticas.[975] Por sus conocimientos técnicos y los canales de comunicación existentes con otros interesados, los organismos reguladores de las TIC de muchos países desempeñan una importante función en la determinación de políticas y estrategias para el desarrollo de la industria de las TIC.[976] En algunos países, la función de ofrecer contribuciones a la formulación de políticas de las TIC se considera una de los principales cometidos del organismo regulador de las TIC.[977] Aunque esta práctica habitual se centra en el asesoramiento en materia de telecomunicaciones, este mandato podría ampliarse a la lucha contra el ciberdelito. En Finlandia, el Gobierno ha instituido un Comité Asesor para la Seguridad de la Información (ACIS) en el seno del Organismo Regulador de las Comunicaciones de Finlandia (FICORA) con el fin de desarrollar la estrategia de información de este país.[978] En la propuesta publicada por el ACIS en 2002, se definen metas y medidas para promover la estrategia de la seguridad de la información. Hay varias medidas que pueden considerarse relacionadas con el ciberdelito y subrayan la importancia de desarrollar y mejorar la legislación adecuada, la cooperación internacional y la sensibilización del usuario- final al problema de la seguridad de la información.[979]

Implicación en el desarrollo de la legislación contra el ciberdelito

El organismo competente para adoptar la legislación es el legislador, no la autoridad de reglamentación. No obstante, el organismo regulador de las TIC puede desempeñar una importante función en el proceso de desarrollo de la legislación contra el ciberdelito. Dada la experiencia de los organismos reguladores en protección de datos, confidencialidad de la transmisión de datos, prevención de la difusión de los programas malintencionados, otros aspectos de la protección del consumidor y responsabilidades de los PSI, su implicación en estos campos es especialmente controvertida.[980] Por otra parte, el derecho penal no es precisamente algo desconocido para los organismos reguladores ya que hay muchos países en los que la infracción grave de obligaciones el ámbito tradicional del trabajo reglamentario puede ser objeto de sanción penal. Además de su función asesora en materia de estrategias globales, como se ha señalado anteriormente, los organismos reguladores pueden implicarse en el proceso de desarrollo de la legislación. Por ejemplo, la Comisión de Comunicaciones de Uganda se implicó en el proceso de desarrollo de la legislación contra el ciberdelito en calidad de asesora.[981] La Comisión de Comunicaciones de Uganda forma parte, a través del Grupo Especial de Uganda para legislación contra el ciberdelito, de una iniciativa regional denominada Grupo Especial de los Países del África Oriental para la Legislación Informática, dedicado al continuo proceso de desarrollo y armonización de la legislación contra el ciberdelito en la región de África Oriental.[982] En Zambia, el Organismo Regulador de las Comunicaciones[983] ha colaborado, según se informa, en la elaboración de nueva legislación contra el ciberdelito,[984] concretamente, la Ley de Comunicaciones y Transacciones Electrónicas de 2009.[985] Otro ejemplo es el de Bélgica, país en el que, en 2006, el organismo regulador de las TIC belgas (BIPT) participó en el proceso de redacción de la legislación contra el ciberdelito.

El proyecto de ley se redactó en cooperación con el Servicio Público Federal de Justicia y la Unidad Federal de Delitos Informáticos.[986]

Detección e investigación del ciberdelito

Los equipos de respuesta ante incidentes informáticos (CIRT) desempeñan una importante función en la supervisión, detección, análisis e investigación de las ciberamenazas y los ciberincidentes.[987] Dada la naturaleza multisectorial del problema del ciberdelito, se han instituido distintos CIRT por parte de toda una gama de interesados, entre los que cabe destacar los gobiernos, las empresas, los operadores de telecomunicación y los sectores académicos, con objeto de llevar a cabo una serie de funciones.[988] En algunos países, los organismos reguladores de las TIC tienen la responsabilidad de crear y dirigir los CIRT nacionales. Estos CIRT suelen ser considerados no sólo entidades importantes encargadas de la detección e investigación de los incidentes relacionados con la ciberdelincuencia a nivel nacional, sino también participantes clave en las acciones orientadas a mejorar la cooperación internacional contra el ciberdelito. Uno de los primeros CIRT constituidos a iniciativa del organismo regulador de las TIC ha sido el Equipo Finlandés de Respuesta a los Incidentes Informáticos que comenzó su andadura en enero de 2002 formando parte del Organismo Regulador de las Comunicaciones de Finlandia (FICORA).[989] Hay otros ejemplos en Suecia,[990] los Emiratos Árabes Unidos[991] y Qatar.[992]

Facilitación de las funciones de fiscalización

El organismo regulador de las TIC sólo puede emprender las investigaciones y, a tal efecto, actuar como organismo de fiscalización, con arreglo a un mandato explícito que la hayan otorgado para ejercer y fiscalizar disposiciones legales específicas. Algunos países han autorizado al regulador de las TIC a actuar como organismo de fiscalización en ámbitos relacionados con el ciberdelito tales como la lucha contra el correo basura, la reglamentación de contenidos o la fiscalización de medidas reglamentarias conjuntas. En lo que al correo basura se refiere, algunos organismos europeos reguladores de las TIC ya se han integrado en una red de contactos de autoridades de fiscalización del correo basura establecida por la Comisión Europea en 2004 para combatir el correo basura a nivel paneuropeo.[993] El Grupo Especial de la OCDE para la lucha contra el correo basura también considera a los organismos reguladores de las TIC como coordinadores de las instituciones de fiscalización.[994] También existen acuerdos de cooperación entre los organismos reguladores de las TIC y las unidades de lucha contra el ciberdelito a nivel policial en los Países Bajos y Rumania.[995]

4.5.4 Medidas legales

De los cinco pilares de la Agenda sobre Ciberseguridad Global, el de las medidas legales es probablemente el más relevante para una estrategia contra el ciberdelito.

Derecho penal sustantivo

Lo primero que se necesita es una serie de disposiciones del Derecho penal sustantivo para penalizar actos tales como los del fraude informático, los accesos ilegales, la interferencia de los datos, la violación de los derechos de autor y la pornografía infantil.[996] El hecho de que haya disposiciones en el Código Penal aplicables a actos semejantes cometidos fuera de la red no quiere decir que puedan aplicarse también a actos cometidos por Internet.[997] Por consiguiente el análisis exhaustivo de las leyes nacionales vigentes es indispensable para identificar los posibles vacíos legales.[998]

Derecho penal procesal

Además de las disposiciones del Derecho penal sustantivo,[999] las autoridades competentes necesitan disponer de las herramientas e instrumentos suficientes para investigar los ciberdelitos[1000]. Esta investigación presenta a su vez una serie de problemas.[1001] Los delincuentes pueden actuar prácticamente desde cualquier lugar del mundo adoptando medidas para enmascarar su identidad.[1002] Las herramientas e instrumentos de investigación de los ciberdelitos pueden ser radicalmente distintas de las utilizadas en la investigación de los delitos ordinarios.[1003] Dada la dimensión internacional[1004] del ciberdelito, resulta

además necesario desarrollar el marco jurídico del país para poder cooperar con las autoridades competentes en el extranjero.[1005]

Evidencias electrónicas

En sus esfuerzos por combatir el ciberdelito, las autoridades competentes en la investigación, así como los tribunales de justicia, necesitan recurrir a evidencias electrónicas. El recurso a este tipo de evidencias plantea una serie de problemas [1006] aunque también abre un nuevo abanico de posibilidades a la investigación y el trabajo de los forenses y tribunales.[1007] En los casos en los que no hay otra fuente de evidencias, la posibilidad de identificar y procesar al delincuente puede depender de la correcta recogida y evaluación de las evidencias electrónicas.[1008] Esto influye en el modo en que las autoridades competentes y los tribunales estudian estas evidencias.[1009] Mientras que los documentos tradicionales se introducen por distribución manual de los originales en los tribunales, las evidencias digitales requieren en determinados casos procedimientos específicos que no permiten su conversión a evidencias tradicionales, por ejemplo, presentando la salida de impresora de archivos u otros datos de la investigación.[1010] Por consiguiente, la existencia de legislación que apoye la admisión de evidencias se considera indispensable en la lucha contra el ciberdelito.

Cooperación Internacional

Dada la dimensión transnacional de Internet y la mundialización de los servicios, cada vez es mayor el número de ciberdelitos con una dimensión internacional.[1011] Los países que deseen cooperar con otros en la investigación de los delitos transfronterizos necesitarán utilizar instrumentos de cooperación internacional. [1012] La movilidad de los delincuentes, la independencia de la presencia de éstos y la repercusión del delito ponen de manifiesto el problema y la necesidad de cooperación de las autoridades competentes y las judiciales.[1013] Dadas las diferencias entre la legislación de los diversos países y el carácter limitado de los instrumentos jurídicos, se considera que la cooperación internacional es uno de los mayores retos de la mundialización de la delincuencia.[1014] Dentro de un planteamiento de amplio alcance para resolver el problema del ciberdelito, es necesario que los países fortalezcan su capacidad de cooperación con otros países para mejorar la eficacia del proceso.

Responsabilidad del proveedor de servicios

Es difícil que los ciberdelitos se cometan sin recurrir a los servicios de un proveedor de servicios de Internet (PSI). Los correos electrónicos de contenido amenazador se envían gracias a los servicios de un proveedor de correo electrónico, y la descarga de contenidos ilegales de un sitio web supone entre otras cosas, contratar los servicios de un Proveedor de alojamiento y de un Proveedor de acceso. Esto se traduce en que los PSI suelan ser el centro de las investigaciones penales sobre los infractores que utilizan los servicios de los PSI para comete sus delitos.[1015] Teniendo en cuenta que, por una parte, los ciberdelitos no pueden cometerse sin la implicación de los ISP y que, por otra, los proveedores no tienen forma de evitar estos delitos, se plantea la cuestión de si es necesario limitar la responsabilidad de los proveedores de Internet.[1016] Esta cuestión puede abordarse en el marco de un planteamiento jurídico de amplio alcance del ciberdelito.

4.5.5 Medidas técnicas y de procedimiento

Las investigaciones relativas al ciberdelito a menudo tienen una fuerte componente técnica[1017]. Además, el requisito de mantener la integridad de la evidencia durante una investigación exige la aplicación de procedimientos precisos. Por consiguiente, el desarrollo de las capacidades y procedimientos necesarios es un requisito esencial en la lucha contra el ciberdelito.

Otro tema es el desarrollo de los sistemas de protección técnica. Los sistemas informáticos bien protegidos son más difíciles de atacar. Un primer paso de gran importancia es la mejora de la protección técnica estableciendo las adecuadas normas de seguridad. Por ejemplo, los cambios en el sistema bancario en línea (el paso de TAN[1018] a ITAN[1019]) han eliminado la mayoría de los peligros planteados por los actuales ataques de usurpación de identidad ("phishing"), demostrando la importancia fundamental que tiene el adoptar las soluciones técnicas [1020]. Las medidas de protección técnica deben incluir todos los elementos de la infraestructura técnica; la infraestructura de red básica, así como los diversos ordenadores conectados de

forma individual en todo el mundo. Pueden identificarse dos grupos objetivo potenciales para la protección de los usuarios y las actividades comerciales de Internet: usuarios finales y comerciales (método directo); y proveedores de servicios y empresas de software.

Desde un punto de vista logístico puede ser más sencillo centrarse en la protección de la infraestructura básica (por ejemplo, red básica, encaminadores, servicios esenciales), en vez de integrar millones de usuarios en una estrategia anticiberdelito. La protección del usuario puede lograrse de manera indirecta, ofreciendo seguridad a los servicios que utiliza el consumidor; por ejemplo, servicios bancarios en línea. Este método indirecto de protección de los usuarios de Internet puede reducir el número de personas e instituciones necesarias que deben incluirse en las etapas para promover la protección técnica.

Aunque limitar el número de personas necesarias que deben incluirse en el sistema de protección técnica puede parecer conveniente, los usuarios de servicios informáticos y de Internet a menudo constituyen el eslabón más débil y el objetivo principal de los delincuentes. Generalmente es más sencillo atacar ordenadores privados para obtener información sensible que los sistemas de ordenadores bien protegidos de una institución financiera. A pesar de estos problemas logísticos, la protección de la infraestructura del usuario final es fundamental para lograr la protección técnica de toda la red.

Los proveedores de servicios de Internet y los fabricantes de productos para Internet (por ejemplo, las empresas de software) desempeñan un papel muy importante en el soporte de las estrategias anticiberdelito. Debido a su contacto directo con los clientes, pueden actuar como garantes de las actividades de seguridad (por ejemplo, la distribución de herramientas de protección e información sobre la situación actual de los fraudes más recientes).[1021]

Estructuras organizativas

Una lucha eficaz contra el ciberdelito exige unas estructuras organizativas altamente desarrolladas. Sin unas estructuras adecuadas que eviten el solapamiento de competencias y se basen en una clara definición de éstas, difícilmente será posible llevar a cabo las complejas investigaciones que exigen la asistencia de distintos expertos jurídicos y técnicos.

Creación de capacidades y educación de los usuarios

El ciberdelito es un fenómeno global. Para poder investigar eficazmente estos delitos es necesario establecer una armonización de las leyes y desarrollar los medios adecuados para lograr la cooperación internacional. Con objeto de garantizar el desarrollo de las normas mundiales en los países desarrollados así como en los países en desarrollo es preciso crear capacidades[1022].

Además de crear capacidades es necesario formar a los usuarios[1023]. Algunos ciberdelitos, especialmente los relativos a fraudes tales como la usurpación de identidades ("phishing") y la falsificación de direcciones de origen o piratería ("spoofing"), no suelen producirse por un déficit de protección técnica sino a causa de una falta de conocimiento por parte de las víctimas[1024]. Existen varios productos de software que pueden identificar automáticamente direcciones web fraudulentas[1025], pero hasta ahora estos productos no pueden identificar todas las direcciones web sospechosas. La capacidad de protección de los usuarios inherente a la adopción de una estrategia basada únicamente en productos de software es bastante limitada[1026]. Aunque continúan desarrollándose medidas de protección técnica y los productos disponibles se actualizan de manera periódica, tales productos no pueden aún sustituir otros métodos.

Uno de los elementos más importantes en la prevención del ciberdelito es la formación de los usuarios[1027]. Por ejemplo, si los usuarios fueran conscientes de que sus instituciones financieras nunca se pondrán en contacto con ellos mediante correo electrónico para solicitarles sus claves o los detalles de sus cuentas bancarias, no podrían ser víctimas de un intento de usurpación de identidad o de ataques fraudulentos. La formación de los usuarios de Internet reduce el número de objetivos potenciales. Los usuarios pueden formarse mediante campañas públicas o asistiendo a clases en los colegios, bibliotecas, universidades y centros de enseñanza de TI y entidades de cooperación entre el sector público y el privado (PPP).

Un requisito importante para lograr una estrategia educativa e informativa eficaz es la comunicación abierta de las últimas amenazas de los ciberdelitos. Algunos Estados y/o empresas privadas rehúsan hacer hincapié

en el hecho de que los ciudadanos y clientes estén afectados por amenazas de ciberdelito, para evitar la pérdida de confianza en los servicios de comunicación en línea. La Oficina Federal de Investigación (FBI) de Estados Unidos de América ha pedido explícitamente a las empresas que superen su aversión a una publicidad negativa e informen sobre los ciberdelitos[1028]. Para determinar el nivel de gravedad de las amenazas y poder informar de ello a los usuarios, es fundamental mejorar la recopilación y publicación de la información pertinente.[1029]

Cooperación internacional

En muchos casos los procesos de transferencia de datos en Internet afectan a más de un país[1030]. Esto es consecuencia del diseño de la red y de la existencia de protocolos que permiten realizar las transmisiones aun cuando las líneas directas se encuentren temporalmente bloqueadas[1031]. Además, un gran número de servicios de Internet (por ejemplo los servicios de alojamiento) son ofrecidos por empresas con sede en el extranjero.[1032]

Cuando el delincuente no se encuentra en el mismo país que la víctima, la investigación requiere la cooperación entre las autoridades competentes de todos los países afectados[1033]. Las investigaciones internacionales y transnacionales sin el consentimiento de las autoridades competentes en los países correspondientes, son difíciles en lo que respecta al principio de soberanía nacional. Este principio, en general, no permite que un país lleve a cabo investigaciones dentro del territorio de otro país sin permiso de las autoridades locales[1034]. Por lo tanto, las investigaciones deben realizarse con el apoyo de las autoridades de todos los países implicados. El hecho de que en la mayoría de los casos sólo se disponga de un breve intervalo de tiempo en el que pueden llevarse a cabo con éxito las investigaciones, supone que la aplicación del clásico régimen de asistencia jurídica mutua presente evidentes dificultades cuando se trata de la investigación de ciberdelitos. Ello se debe a que, normalmente, la asistencia jurídica recíproca exige procedimientos formales muy laboriosos. En consecuencia, la mejora de los términos de ampliación de la cooperación internacional reviste una gran importancia y desempeña una función crítica para el desarrollo y aplicación de las estrategias de seguridad y las estrategias anticiberdelito.

4.6 Experiencias en materia de creación de capacidades en el Grupo de Estados de África, el Caribe y el Pacífico (ACP)

Entre 2008 y 2013, la UIT y la UE financiaron un proyecto [1035] destinado a respaldar la elaboración de políticas y leyes en el Grupo de Estados de África, el Caribe y el Pacífico (ACP), en el marco del programa "ACP - Tecnologías de la Información y la Comunicación" y del noveno Fondo de Desarrollo Europeo. La Región del África subsahariana recibió apoyo a través de la iniciativa Armonización de Políticas TIC en el África subsahariana (*HIPSSA, Harmonization of ICT Policies in Sub-Saharan Africa*). Para los países del Caribe se puso en marcha el proyecto Mejora de la competitividad en el Caribe gracias a la armonización de políticas, leyes y procedimientos reglamentarios en materia de TIC (*HIPCAR, Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures*). [1036] También se prestó apoyo a los países del Pacífico mediante el proyecto Creación de capacidades y marcos político, reglamentario y legislativo en materia de TIC para los Estados insulares del Pacífico (*ICB4PAC, Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries*). La UIT elaboró una metodología específica y logró avances importantes con respecto a la creación de capacidades en el curso de esos seis años.

4.6.1 Metodología

Uno de los principales logros de los proyectos fue la elaboración de una metodología exhaustiva de creación de capacidades en el ámbito de la estrategia, la política y la ley. El estudio de ejemplos de prácticas óptimas sobre metodologías vigentes de armonización regional de políticas y leyes formó parte de las actividades de preparación del proyecto. Sin embargo, la singularidad del proyecto con respecto al número de países participantes (más de 70 países de las tres regiones), las esferas de trabajo (hasta nueve) previstas y el tiempo consagrado (seis años) hizo necesario elaborar nuevos enfoques.

Durante la primera de las dos etapas, se elaboraron políticas modelo y leyes modelo regionales. Esta etapa se inició con una evaluación de las políticas y leyes vigentes en los países beneficiarios. Para procurar que se identificaran todas las leyes aplicables, la evaluación fue llevada a cabo por expertos internacionales y regionales con apoyo de homólogos especializados de cada país. En el informe que resumía las conclusiones se efectuó una comparación entre las normas existentes identificadas y las prácticas óptimas internacionales y regionales, dando prioridad a las que se aplicaban directamente al menos en algunos países beneficiarios (por ejemplo, la Ley modelo de la Commonwealth). No obstante, se incluyeron también prácticas óptimas de otras regiones, como la Unión Europea. Los informes de evaluación[1037] contenían una reseña de la legislación vigente, así como un análisis de derecho comparado de la legislación vigente con prácticas óptimas regionales e internacionales. Con objeto de preparar un análisis de las disparidades, el informe de evaluación definió además demandas regionales específicas que no necesariamente tienen en cuenta las prácticas óptimas internacionales. Seguidamente, el informe de evaluación fue examinado con los principales interesados de todos los países beneficiarios. Tras consultas con los interesados, se elaboraron políticas modelo, leyes modelo y notas explicativas para todas las esferas de trabajo correspondientes. Este proceso estuvo a cargo de expertos regionales (de todos los países beneficiarios) con la intención de procurar no sólo que los resultados estuvieran en armonía con prácticas óptimas regionales e internacionales sino que también fueran llevados a la práctica fácilmente.

La segunda etapa se consagró a la transposición nacional. Para ello fue igualmente necesario formular una metodología particular. El calendario limitado y el número de esferas de trabajo requerían una metodología que lograra un apoyo nacional sumamente eficaz. Tras la determinación de los paquetes de trabajo necesarios, cada país recibía un plan de proyecto destinado a obtener un apoyo adaptado a las circunstancias particulares. Con miras a asegurar el máximo apoyo de los interesados de cada país, la transposición nacional de políticas y leyes modelo contempló consultas exhaustivas con los interesados. Durante esas consultas, numerosos interesados nacionales (por ejemplo, el público en general, políticos, funcionarios gubernamentales, la comunidad empresarial, el proveedor de servicios Internet y grupos de defensa de los derechos civiles) fueron invitados a diferentes reuniones de consulta en las que se debatieron abiertamente el proceso de transposición y las políticas y leyes modelo. Las aportaciones de los interesados se tuvieron en cuenta en la redacción del proyecto, que fue llevada a cabo por expertos locales, regionales e internacionales. Por otra parte, se organizaron talleres sobre creación de capacidades destinados a diferentes grupos de interés (por ejemplo, programas de formación especial para el personal policial; sesiones consagradas a jueces, magistrados y fiscales; conferencias en escuelas y universidades; talleres para el público en general y campañas en cooperación con la prensa local).

4.6.2 Lecciones aprendidas

La intensa labor realizada con más de 70 países dio lugar a diferentes prácticas óptimas que podrían ser de utilidad en futuros proyectos de creación de capacidades.

Legislación sumada a una política

Elaborar una legislación es un requisito fundamental para crear un entorno de utilización fiable de las TIC.[1038] Sin embargo, no es habitual iniciar el proceso de elaboración de leyes antes de formular una estrategia y una política general. La mayoría de los países establecen en primer lugar una política general, cuya función consiste en definir la respuesta del gobierno a una determinada cuestión.[1039] Gracias a esa política, el gobierno logra dar una respuesta completa al problema. Además de la legislación, se pueden contemplar otras respuestas para lograr objetivos en materia de política. A diferencia de otros enfoques regionales que privilegian la armonización de las leyes, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia[1040], HIPSSA, HIPCAR e ICB4PAC contemplaron la formulación de ese tipo de política. Su resultado concreto fue facilitar la cooperación de los diferentes interesados (especialmente, ministerios) con competencias coincidentes en el ámbito de las TIC. Es probable que la combinación de política y legislación también haya disminuido el tiempo necesario en un país para adoptar una ley.

Diferencias limitadas entre legislaciones modelo

Comparar diferentes enfoques regionales (como el Convenio del Consejo de Europa sobre la Ciberdelincuencia[1041], la Decisión marco de la Unión Europea relativa a los ataques contra los sistemas de información[1042], el proyecto de Convenio de la Unión Africana sobre ciberseguridad[1043], la iniciativa HIPSSA, el proyecto HIPCAR y el proyecto ICB4PAC) para hacer frente a delitos concretos (por ejemplo, el acceso ilegal) revela un alto grado de coherencia en el enfoque y la metodología prescritos. Por consiguiente, se han seguido todas las prácticas óptimas internacionales y ha sido posible aplicar la ley modelo elaborada por expertos del Caribe como base para la elaboración del modelo marco HIPSSA e ICB4PAC.

Normas de alto nivel en los países en desarrollo

El proyecto pone de relieve que el nivel de las normas elaboradas por pequeños países y países en desarrollo no debe ser inferior al de las normas elaboradas en Europa. De hecho, diversos elementos de los marcos jurídicos trascienden incluso las normas europeas. A título de ejemplo puede mencionarse la pornografía infantil que, en el Art. 9 del Convenio del Consejo de Europa sobre la Ciberdelincuencia, alude únicamente a "material pornográfico que contenga la representación visual" y no tiene en cuenta por tanto el material audio, siendo de sobra conocido que los delincuentes también se ocupan del intercambio de ficheros audio pornográficos.[1044] Los proyectos HIPCAR, HIPSSA e ICBT adoptaron un enfoque diferente y evitaron el término "visual", incluyendo de esa manera los ficheros audio.

Ventajas de la amplia participación de expertos y de la consulta con los interesados

Dos aspectos que resultaron de gran utilidad durante la etapa de transición han sido la participación de expertos de casi todos los países beneficiarios en la elaboración de una política y una legislación modelo, así como la amplia participación de los interesados nacionales en el proceso de transición.

La evaluación puso de manifiesto que la amplia participación de expertos de todos los países beneficiarios en la elaboración de normas regionales tuvo gran éxito. El Convenio del Consejo de Europa sobre la Ciberdelincuencia, por ejemplo, fue elaborado por expertos de sólo 14[1045] de los 47 Estados miembros y cuatro expertos de Estados no miembros[1046], a diferencia de la política y legislación modelo de los proyectos HIPSSA, HIPCAR e ICB4PAC, elaboradas por expertos de casi todos los países beneficiarios.

Otra experiencia positiva resultó la celebración de consultas con los interesados. Todos ellos coincidieron en que requería muchísima más energía examinar los elementos de una política nacional y un proyecto de ley con numerosos interesados que llevar únicamente a cabo un debate interno. No obstante, el proceso legislativo que tuvo lugar sin dificultades tras la participación de los interesados es un indicio de la ventaja que supone celebrar intensos debates en el marco del proceso de elaboración con objeto de asegurar que se tengan en cuenta las diferentes inquietudes.

926 Regarding a clear distinction see for example: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1, page 3.

927 UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

928 See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cybersecurity, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

929 The term "cybersecurity" is used to summarize various activities ITU-T Recommendation X.1205 "Overview of Cybersecurity" provides a definition, description of technologies, and network protection principles: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberenvironment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see: *ITU*, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

930 With regard to developments related to developing countries, see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

931 See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008) on Cybersecurity available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; EU Communication towards a general policy on the fight against cyber crime, 2007 available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

932 For more information, see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

933 For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

934 See below: § 4.4.

935 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arab regions.

936 See for example: Austria: National ICT Security Strategy Austria, available at: www.ccdcoe.org/strategies/Austrian_Cyber_Security_Strategy.pdf; Estonia: Cyber Security Strategy, available at: www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf; Germany: Cybersecurity Strategy for Germany, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile; United Kingdom: UK Cyber Security Strategy, available at.: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf; New Zealand: www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf; For more examples see: National Cyber Security Framework Manual, NATO CCD, 2012, page 53 et seq.

937 See for example the EU Cybersecurity Strategy: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the

European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1. Regarding the activities of the UN in relation to Cybersecurity see: *Maurer*, Cyber Norm Emergence at the United Nations, An Analysis of the Activities at the UN regarding Cyber-Security, 2011.

938 See: National Cyber Security Framework Manual, NATO CCD, 2012, page 46.

939 Cybersecurity Strategy for Germany, 2011, page 7, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

940 With regard to the need of updates see below III.5.c.

941 This issue was for example taken into consideration within the EU/ITU co-funded projects HIPCAR and ICB4PAC. The model policy, as well as the model legislation, are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

942 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

943 Regarding the need for an interdisciplinary approach see: *Schjolberg/Ghernaouti-Helie*, A Global Treaty on Cybersecurity and Cybercrime, Second Edition, 2011, page 17, available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

944 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

945 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

946 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

947 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

948 See below: § 5.

949 The harmonization of training is one of the main objectives for the EU Cybercrime Centers of Excellence Network (2Centre). Information is available at: www.2centre.eu. Other examples are the European Cybercrime Training & Education Group (ECTEG) as well as the Europol Working Group on the Harmonization of Cybercrime Training (EWGHCT).

950 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

951 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

952 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf..

953 See for example: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, 2007, page 5, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf; *Pladna*, The Lack of Attention in the Prevention of Cyber Crime and How to improve it, University of East Carolina, ICTN6883, available at: www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf.

954 Regarding blocking of websites with illegal content see: *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008.

955 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

956 Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary, page 7, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf; see also ITU, World Summit on Information Society, The Report of the Task Force on Financial Mechanisms for ICT for Development, December, 2004, available at: www.itu.int/wsis/tffm/final-report.pdf; ITU/infoDEV ICT Regulation Toolkit, Chapter 4.1. What is the Role of Regulators?, available at: www.ictregulationtoolkit.org/en/Section.3109.html

[957] See GSR09 – Best Practice Guidelines on innovative regulatory approaches in a converged world to strengthen the foundation of a global information society, available at www.itu.int; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009 // available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf

[958] *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf; *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

[959] E.g. Korea Communications Commission, established in February 2008 (formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission), announced among other core regulatory duties protection of Internet users from harmful or illegal content. Korea Communications Commission: http://eng.kcc.go.kr.

[960] E.g. Swedish ICT Regulator PTS addresses cyberthreats and cybercrime under user protection mandate and network security mandate. See: *PTS*. Secure communications, available at www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

[961] *OPTA*. Regulatory areas, available at: www.opta.nl/en/about-opta/regulatory-areas/..

[962] The Dutch regulator is granted the mandate to monitor any contravention of the prohibition of unsolicited communication under its duties to provide Internet safety for consumers.

[963] OPTA has the power to take action against anyone contravening the prohibition of spam and unsolicited software by imposing fines..

[964] OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

[965] *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Henten/ Samarajiva/ Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; infoDev/ITU ICT regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

[966] See the discussions on regulation, illegal content and converged regulators: *Van Oranje et al,* Responding to Convergence: Different approaches for Telecommunication regulators TR-700-OPTA, 30 September 2008, available at: www.opta.nl/download/convergence/convergence-rand.pdf; *Millwood Hargrave, et al,* Issues facing broadcast content regulation, Broadcasting Standards Authority, New Zealand, 2006, available at: www.bsa.govt.nz/publications/IssuesBroadcastContent-2.pdf. See also: *ITU*, Case Study: Broadband, the Case of Malaysia, Document 6, April 2001, available at: www.itu.int/osg/spu/ni/broadband/workshop/malaysiafinal.pdf.

[967] See*: infoDev/ITU* ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html. See also: *Henten/ Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; *Singh/Raja*, Convergence in ICT services: Emerging regulatory responses to multiple play, June 2008, available at: http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/Convergence_in_ICT_services_Emerging_regulatory_responses_to_multiple_play.pdf; *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1.

[968] The four states which have regulators that can be regarded as converged regulatory authorities are: Finland, Italy, Slovenia and the United Kingdom. See: infoDev/ITU ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html.

[969] Information and network security (INS).

[970] See: *MCMC*, What do we Do. Information Network Security, available at: www.skmm.gov.my/what_we_do/ins/feb_06.asp.

[971] Korea Communications Commission: Important Issues, available at: http://eng.kcc.go.kr.

[972] Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary. 2009, P. 11, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

[973] See: *Haggard/McCubbins*, Presidents, Parliaments, and Policy. University of California, San Diego, July 1999, available at: http://mmccubbins.ucsd.edu/ppp.pdf. For the discussion with regard to regulatory agencies, see: *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making: a Comparative Analysis of Six Decision-Making Processes in

the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf.

974 The rationale for separating the ICT regulator from the policy-making body is to have an independent regulator that maintains a distance from the ministry or other government bodies which could remain as the major shareholder of the incumbent. An independent regulator can avoid conflict of interest that can happen if the regulator is also responsible for industry promotion. See: *OECD*, Telecommunications Regulatory Structures and Responsibilities, DSTI/ICCP/TISP(2005)6/FINAL, January, 2006, available at: www.oecd.org/dataoecd/56/11/35954786.pdf.

975 InfoDev ITU ICT Regulation toolkit. Section 6.3. Separation of Power and Relationship of Regulator with Other Entities, available at: www.ictregulationtoolkit.org/en/Section.1269.html.

976 Public Consultation Processes. InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; *Labelle*, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

977 One example is the Botswana Telecommunications Authority, which is required to provide the input to government policy-making efforts. See: Case Study Single Sector Regulator: Botswana Telecommunications Authority (BTA). InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/PracticeNote.2031.html.

978 International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich, 2009, available at www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663, P. 133.

979 National Information Security Strategy Proposal, November, 2002 // available at: www.mintc.fi/fileserver/national_information_security_strategy_proposal.pdf.

980 *Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

981 See: *Uganda Communications Commission*, Recommendations on Proposed Review of the Telecommunications Sector Policy, 2005, available at: www.ucc.co.ug/UgTelecomsSectorPolicyReview_31_Jan_2005.pdf; *Blythe*, The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control in Repositioning African Business and Development for the 21st Century, Simon Sigué (Ed.), 2009, available at: www.iaabd.org/2009_iaabd_proceedings/track16b.pdf; Uganda Computer Misuse Bill 2004, available at: www.sipilawuganda.com/files/computer%20misuse%20bill.pdf.

982 See, for example: Report of the Second EAC Regional Taskforce Meeting on Cyber Laws. June 2008, Kampala, Uganda, available at: http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf.

983 Now: Zambia Information and Communications Technology Authority.

984 *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis, Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf; *Hatyoka*, ZICTA Corner – Defining ZICTA's new mandate. Times of Zambia, 2009 // available at: www.times.co.zm/news/viewnews.cgi?category=12&id=1262768483.

985 Zambia Electronic Communications and Transactions Act 2009, available at: www.caz.zm/index.php?option=com_docman&Itemid=75. See also ZICTA. Cybercrime Penalties (Part 1), available at: www.caz.zm/index.php?option=com_content&view=article&id=76:cyber-crime-penalties-part-1&catid=34:column&Itemid=38.

986 Annual report 2008 Belgian Institute for postal service and telecommunication, BIPT, 2009, available at: http://bipt.be/GetDocument.aspx?forObjectID=3091&lang=en.

987 See: *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003, available at: www.cert.org/archive/pdf/03hb001.pdf.

988 *Scarfone/Grance/Masone,* Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61, 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf, pp. 2-2.

989 www.ficora.fi/.

990 Sweden's IT Incident Centre (Sitic) is located in the ICT regulator PTS .See: PTS. Secure communications, available at: www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

991 aeCERT created as an initiative of the UAE Telecommunications Regulatory Authority to detect, prevent and respond to current and future cybersecurity incidents in the UAE *: Bazargan*, A National Cybersecurity Strategy aeCERT Roadmap. Presentation at Regional Workshop on Frameworks for Cybersecurity and CIIP 18 – 21 Feb 2008 Doha, Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

992 The national CERT (qCERT) was established by the Qatari ICT regulator (ictQatar) and acts on behalf of ictQatar; *Lewis*, Q-CERT. National Cybersecurity Strategy Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incid ent-management-brisbane-july-08.pdf.

993 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf.

994 E.g. ICT regulators are involved in law-enforcement efforts with regard to combating spam in the following countries: Australia, Finland, Greece, Hungary, Japan, Malaysia, Mexico, Netherlands, Portugal, Turkey. See: *OECD* Task Force on Spam. Enforcement authorities contact list, available at: www.oecd-antispam.org/countrycontacts.php3.

995 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

996 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

997 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et. seq*.

998 For an overview of cybercrime-related legislation and its compliance with the standards defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

999 See below: § 6.2.

1000 See below: § 6.2.

1001 For an overview of the most relevant challenges in the fight against cybercrime, see above: § 3.1.

1002 One possibility to mask identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems, see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

1003 Regarding legal responses to the challenges of anonymous communication, see below: §§ 6.5.10 and 6.3.11.

1004 See above: § 3.2.6.

1005 See in this context below: § 6.6.

1006 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

1007 *Vaciago*, Digital Evidence, 2012.

1008 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

1009 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

1010 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

1011 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The

Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1012] See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[1013] See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[1014] *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[1015] See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

[1016] For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[1017] *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2

[1018] Transaction authentication number – for more information, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[1019] The ITAN system improves the TAN system. The financial institutions provide the customer with a number of TAN-indexed identity numbers. With regard to each relevant transaction, the online banking system requires a specific ITAN number selected at random from the list of supplied TAN. For more information, see: *Bishop*, Phishing & Pharming: An investigation into online identity theft, 2005, available at: http://richardbishop.net/Final_Handin.pdf.

[1020] Regarding various authentication approaches in Internet banking, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[1021] Regarding approaches to coordinate the cooperation of law-enforcement agencies and Internet service providers in the fight against cybercrime, see the results of the working group established by Council of Europe in 2007. For more information, see: www.coe.int/cybercrime/.

[1022] Capacity building is in general defined as the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation (of women in particular), human resources development and strengthening of managerial systems. In addition, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations, user groups, professional associations, academics and others).

[1023] At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect". Regarding user-education approaches in the fight against phishing, see: Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, Technical Trends in Phishing Attacks, available at: www.cert.org/archive/pdf/Phishing_trends.pdf. Regarding sceptical views on user education, see: *Görling*, The Myth Of User Education, 2006, available at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[1024] Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: www.cert.org/archive/pdf/Phishing_trends.pdf.

[1025] *Shaw*, Details of anti-phishing detection technology revealed in Microsoft Patent application, 2007, available at: http://blogs.zdnet.com/ip-telephony/?p=2199; Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers – Cyota Inc., Internet Identity and MarkMonitor to provide phishing Web site data for Microsoft Phishing Filter and SmartScreen Technology services, 2005, available at: www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

[1026] For a different opinion, see: *Görling*, The Myth Of User Education, 2006, at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[1027] At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[1028] "The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack, explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, available at: www.heise-security.co.uk/news/80152

[1029] Examples of the publication of cybercrime-related data include: Symantec Government Internet Security Threat Report Trends for July–December 06, 2007, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf; Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[1030] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1031] The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1032] See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network-storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

[1033] Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf..

[1034] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[1035] Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/

[1036] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

[1037] The assessment reports are available on the HIPCAR website and will be on the HIPSSA and ICB4PAC website shortly.

[1038] With regard to the relevance of legislation related to the specific topic cybercrime see: *Gercke*, CRi 2012, 81.

[1039] See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

[1040] Council of Europe Convention on Cybercrime (CETS No. 185); *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225,; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, CRi 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, page 7 *et seq.*; *Gercke*, 10 years Convention on Cybercrime, Cri 2011, 142 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing:

An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[1041] Art. 2: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

[1042] Art. 2 (1) :Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

[1043] Art. III-2: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system.

[1044] Regarding the relevance of audio files see: *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1045] Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Netherlands, Portugal, Sweden and "The Former Yugoslav Republic of Macedonia".

[1046] The decision to establish the working group was made during the 583rd Meeting of the Minister's, Decision No. CM/Del/Dec(97)583.

5 Panorama de las actividades de las Organizaciones Regionales e Internacionales

Bibliografía (seleccionada): *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009; Committee II Report, 11th UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007; *Nilsson* in *Sieber*, Information Technology Crime, page 576; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001; Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, 2001; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07.

En el presente Capítulo se traza un panorama de los enfoques legislativos internacionales[1047] y la relación de estos enfoques con los nacionales.

5.1 Enfoques internacionales

Varias organizaciones internacionales realizan constantes esfuerzos por analizar los últimos hechos registrados en materia de ciberdelito y han establecido Grupos de Trabajo para definir estrategias destinadas a combatir tales delitos.

5.1.1 El G7 (anteriormente G8)[1048]

En 1997 el Grupo de los Ocho (G8) estableció un Subcomité[1049] sobre delitos de alta tecnología, cuyo objetivo era luchar contra el ciberdelito[1050]. Durante la reunión del G8, celebrada en Washington D.C., Estados Unidos, los Ministros de Justicia y del Interior del G8 adoptaron Diez Principios y un Plan de Acción de diez puntos para combatir el delito de alta tecnología.[1051] Los Jefes de Estado apoyaron ulteriormente estos principios, entre los cuales cabe citar los siguientes:

- No puede haber refugios para aquellos que utilizan de forma abusiva las tecnologías de la información.
- Todos los Estados interesados habrán de investigar la comisión de delitos internacionales de alta tecnología, así como el enjuiciamiento de sus autores, con independencia de cual sea el país en el que se hayan producido los correspondientes daños.
- Habrá que entrenar y equipar al personal encargado de hacer cumplir la ley para abordar los delitos de alta tecnología.

En 1999 el G8 especificó la actuación que tenía prevista para luchar contra el delito de alta tecnología en la Conferencia Ministerial sobre la Lucha contra el Delito Transnacional celebrada en Moscú, Federación de Rusia.[1052] Los participantes en el G8 expresaron su preocupación acerca de delitos tales como la pornografía infantil, así como sobre la posibilidad de rastrear las transacciones y el acceso transfronterizo para almacenar datos. En el comunicado publicado con motivo de la Conferencia se consignan varios principios sobre la lucha del ciberdelito, que figuran actualmente en una serie de estrategias internacionales[1053].

Uno de los logros prácticos de las tareas efectuadas por varios Grupos de Expertos ha sido la preparación de una red internacional de contactos las 24 horas del día y 7 días por semana, red que exige que los países participantes establezcan coordinadores de las investigaciones transnacionales que se realicen, coordinadores que deberán estar accesibles las 24 horas del día y 7 días por semana[1054].

En la Conferencia del G8 organizada en París, Francia, en 2000, el G8 abordó el tema del ciberdelito e hizo un llamamiento para oponerse a la constitución de refugios digitales ilegales. Ya en esas fechas, el G8 se esforzó por ofrecer una relación entre los intentos de sus miembros por buscar soluciones internacionales en lo que concierne al Convenio del Consejo de Europa sobre la Ciberdelincuencia[1055]. El G8 debatió sobre una serie de instrumentos de procedimiento para luchar contra el ciberdelito en un taller celebrado en Tokio en 2001[1056], en el cual la atención se centró en determinar si habría que implementar la obligación de retener datos o si la preservación de los mismos podría ser una solución opcional[1057].

En 2004, los Ministros de Justicia y del Interior del G8 expidieron un comunicado en el que señalaron que había que considerar la necesidad de crear capacidades mundiales para combatir la utilización delictiva de Internet[1058]. Una vez más el G8 tomó nota del Convenio del Consejo de Europa sobre la Ciberdelincuencia[1059].

Durante la reunión que tuvo lugar en Moscú en 2006 los debates de los Ministros de Justicia y del Interior del G8 se centraron en la lucha contra el ciberdelito y los diferentes aspectos del ciberespacio, así como sobre la necesidad de adoptar contramedidas eficaces[1060]. La reunión de los Ministros de Justicia y del Interior del G8 fue seguida por la Cumbre del G8 que tuvo lugar en Moscú y en la cual se analizó[1061]la cuestión que representaba el ciberterrorismo[1062].

Durante la reunión de 2007 que se organizó en Munich, Alemania, los Ministros de Justicia y del Interior del G8 estudiaron más a fondo la utilización de Internet por grupos terroristas, y los Ministros convinieron en tipificar como delito la utilización abusiva de Internet por grupos terroristas[1063]. Hay que agregar que este acuerdo no incluía ciertos actos específicos que los Estados deberían tipificar penalmente.

Durante la reunión de los Ministros de Justicia y del Interior, celebrada en Roma, Italia, en 2009 se debatieron diversos asuntos relacionados con el ciberdelito. La declaración final indica que, en la opinión del G8, se debería establecer el bloqueo de los sitios de Internet de pornografía infantil, partiendo de una lista negra actualizada y difundida por las organizaciones internacionales.[1064] En lo que respecta al ciberdelito en general, la declaración final destaca una amenaza creciente e indica que se precisa una cooperación más estrecha entre los proveedores de servicios y el cumplimiento de la ley y que deben reforzarse las formas de cooperación existentes, como los puntos de contacto del G8 sobre delitos de alta tecnología[1065] disponibles las 24 horas del día y 7 días por semana.

Durante la Cumbre del G8 celebrada en Muskoka, Canadá, se abordó el ciberdelito sólo brevemente. La Declaración de Muskoka únicamente reconoce en lo que concierne a las actividades terroristas la preocupación del G8 por la creciente amenaza que representa el ciberdelito y que se intensificarán los trabajos para debilitar a las redes de terroristas y delincuentes.[1066]

El ciberdelito y la ciberseguridad fueron asuntos abordados por el Foro del G8, en el que las delegaciones debatieron con los dirigentes económicos[1067] asuntos relacionados con Internet. También se trataron en la cumbre del G8 de Deauville, Francia. Pero, aunque se prestó mucha atención al tema del ciberdelito, la declaración final de la cumbre no incluye, al contrario que en años anteriores, recomendaciones específicas. El G8 sólo acordó principios generales tales como la importancia de la seguridad y la protección frente a la delincuencia que está minando una Internet fuerte y pujante.[1068]

5.1.2 Las Naciones Unidas y la Oficina de las Naciones Unidas contra la Droga y el Delito[1069]

Las Naciones Unidas han promovido varios enfoques importantes para afrontar el desafío del ciberdelito. Aunque al principio su reacción se limitó a directrices de carácter general, la organización ha tratado últimamente con mayor intensidad estos retos y su respuesta judicial.

Convención de las Naciones Unidas sobre los Derechos del Niño

La Convención de las Naciones Unidas sobre los Derechos del Niño, adoptada en 1989,[1070] incluye varios instrumentos destinados a proteger a la infancia. No define la pornografía infantil, ni incluye disposición alguna que armonice la persecución por la vía penal de la distribución de pornografía infantil por Internet. No obstante, el Artículo 34 hace un llamamiento a los Estados Miembros para que eviten la explotación de los niños en sesiones pornográficas.

Resolución 45/121 de la Asamblea General de las Naciones Unidas

Tras el octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente (celebrada en La Habana, Cuba, entre el 27 de agosto y el 7 de septiembre de 1990), la Asamblea General de las Naciones Unidas adoptó una Resolución relativa a la legislación sobre delitos informáticos.[1071] Basándose en su Resolución 45/121 (1990), las Naciones Unidas publicaron un manual en 1994 sobre la prevención y el control del delito informático.[1072]

Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía

El Protocolo facultativo no sólo trata el tema de la pornografía infantil en general, sino que se refiere explícitamente al protagonismo de Internet en la distribución de ese tipo de material.[1073] La pornografía infantil se define como cualquier representación, mediante cualquier medio, de un niño comprometido en actividades sexuales explícitas reales o simuladas o en cualquier representación de las partes sexuales de un niño para fines principalmente sexuales.[1074] El Artículo 3 requiere a las partes que penalicen ciertas conductas, incluidos los actos relacionados con la pornografía infantil.

> ***Artículo 3***
> *1. Todo Estado Parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeran queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente:*
> *[….]*
> *c) Producir, distribuir, divulgar, importar, exportar, ofrecer, vender o poseer, con los fines antes señalados, material pornográfico en que se utilicen niños, en el sentido en que se define en el Artículo 2.*
> *[...]*

Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente

Durante el décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrado en Viena en 2000, se trataron las repercusiones de los delitos informáticos en un taller específico.[1075] Los debates se centraron en particular en las categorías de los delitos y en la investigación transnacional, así como en la respuesta jurídica ante este fenómeno.[1076] Las conclusiones del taller incluyen elementos importantes del debate, que no ha finalizado: se requiere la persecución por la vía penal, es preciso que la legislación contemple instrumentos procesales, la cooperación internacional resulta crucial y se deben reforzar las asociaciones público privadas.[1077] Además, se destacó la importancia de la creación de capacidades – una cuestión que vuelve a surgir a lo largo de los años.[1078] La Declaración de Viena hizo un llamamiento a la Comisión de Prevención del Delito y Justicia Penal para que emprendiera trabajos en este sentido:

> *18. Decidimos formular recomendaciones de política orientadas a la acción para la prevención y el control de los delitos relacionados con la informática e invitamos a la Comisión de Prevención del Delito y Justicia Penal a que emprenda trabajos a este respecto, teniendo en cuenta la labor en curso en otros foros. Nos comprometemos también a esforzarnos por aumentar nuestra capacidad de prevenir, investigar y enjuiciar los delitos de alta tecnología y relacionados con la informática.*

Resolución 55/63 de la Asamblea General de las Naciones Unidas

El mismo año, la Asamblea General de las Naciones Unidas adoptó una Resolución para combatir el uso incorrecto de las tecnologías de la información con fines delictivos que presenta algunas similitudes con el Plan de Acción de diez puntos del G8 de 1997.[1079] En su Resolución, la Asamblea General identificó un cierto número de medidas para evitar el uso incorrecto de la tecnología de la información con fines delictivos, entre las que cabe citar:

> *Los Estados deben velar para que en su legislación y en la práctica se eliminen los refugios seguros para quienes utilicen la tecnología de la información con fines delictivos.*
> *Debe coordinarse entre todos los Estados interesados la cooperación en lo que se refiere a la vigilancia del cumplimiento de la ley y la investigación y el enjuiciamiento de los casos en que se utilice la tecnología de la información con fines delictivos en el plano internacional.*
> *El personal encargado de hacer cumplir la ley debe contar con capacitación y equipo adecuado para hacer frente a la utilización de la tecnología de la información con fines delictivos.*

La Resolución 55/63 invita a los Estados Miembros a tomar las medidas oportunas para combatir el ciberdelito a escala regional e internacional. Esto implica la elaboración de leyes nacionales para eliminar refugios seguros para quienes utilicen las tecnologías con fines delictivos, la mejora de la capacitación para hacer cumplir las leyes, cooperando a través de las fronteras en la investigación y persecución de los casos internacionales de uso de las tecnologías con fines delictivos, la mejora de los intercambios de información y de la seguridad de los sistemas informáticos y de datos, la formación técnica para el cumplimiento de la ley con el fin de, en particular, afrontar los desafíos asociados con el ciberdelito, la creación de regímenes de asistencia mutua y el aumento de la sensibilización de los ciudadanos ante la amenaza del ciberdelito.

Resolución 56/121 de la Asamblea General de las Naciones Unidas

La Asamblea General de las Naciones Unidas adoptó en 2002 otra Resolución para luchar contra la utilización de las tecnologías de la información con fines delictivos.[1080] La Resolución plantea los enfoques internacionales existentes en la lucha contra el ciberdelito y destaca algunas soluciones.

> *Observando la labor de organizaciones internacionales y regionales en la lucha contra el delito de alta tecnología, incluida la labor del Consejo de Europa en la preparación del Convenio sobre el Delito Cibernético4, así como la labor de esas organizaciones encaminada a fomentar un diálogo entre los gobiernos y el sector privado sobre la seguridad y la confianza en el espacio cibernético:*

1. Invita a los Estados Miembros a que, al elaborar leyes y políticas nacionales y al adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos, tengan en cuenta, según proceda, la labor y los logros de la Comisión de Prevención del Delito y Justicia Penal y de otras organizaciones internacionales y regionales.
2. Toma nota del valor de las medidas enunciadas en su Resolución 55/63, e invita nuevamente a los Estados Miembros a que las tengan en cuenta en su lucha contra la utilización de la tecnología de la información con fines delictivos.
3. Decide aplazar el examen de este tema, mientras se realiza la labor prevista en el Plan de Acción contra los delitos de alta tecnología y relacionados con las redes informáticas de la Comisión de Prevención del Delito y Justicia Penal.

La Resolución 56/121 recalca la necesidad de cooperación entre los Estados en la lucha contra la utilización de las tecnologías de la información con fines delictivos y destaca el papel que pueden representar las Naciones Unidas y otras organizaciones regionales e internacionales. La Resolución invita también a los Estados a que tengan en cuenta las directrices facilitadas por la Comisión de Prevención del Delito y Justicia Penal cuando elaboren su legislación nacional.

Resoluciones 57/239 y 58/199 de la Asamblea General de las Naciones Unidas

Las Resoluciones 57/239 y 58/199 son dos Resoluciones de la Asamblea General relativas a la ciberseguridad. Sin entrar en detalles en lo que respecta al ciberdelito, citan a las Resoluciones 55/06 y 56/121. Ambas hacen hincapié además en la necesidad de la cooperación internacional en la lucha contra el ciberdelito al reconocer que las lagunas en el uso y en el acceso de los Estados a las tecnologías de la información pueden reducir la eficacia de la cooperación internacional en la lucha contra la utilización de las tecnologías con fines delictivos.[1081]

Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

El ciberdelito se debatió durante el undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en Bangkok, Tailandia, en 2005. Se consideraron, tanto en las contribuciones[1082] como en los talleres,[1083] diversos retos planteados por la utilización emergente de los sistemas informáticos para cometer delitos y su dimensión transnacional. En el marco de las reuniones preparatorias anteriores al Congreso, algunos países miembros como Egipto solicitaron la elaboración de un nuevo convenio sobre el ciberdelito y la reunión preparatoria regional de Asia occidental solicitó la negociación de este tipo de convenio.[1084] La posibilidad de negociación de un convenio se incluyó en la guía para los debates del undécimo Congreso de las Naciones Unidas sobre el prevención del delito.[1085] Sin embargo, los Estados Miembros no pudieron en ese momento decidir el inicio de una armonización de la legislación. La Declaración de Bangkok, por tanto – sin hacer mención de ningún instrumento específico – sólo considera los enfoques existentes.

16. Observamos que, en esta era de la globalización, la tecnología de la información y el rápido desarrollo de nuevos sistemas de telecomunicaciones y redes informáticas se han visto acompañados del uso indebido de esas tecnologías con fines delictivos. Por consiguiente, acogemos con beneplácito los esfuerzos por aumentar y complementar la cooperación existente para prevenir, investigar y juzgar los delitos informáticos y de alta tecnología, incluso mediante la asociación con el sector privado. Reconocemos la importante contribución de las Naciones Unidas a los foros regionales y a otros foros internacionales en la lucha contra el delito cibernético e invitamos a la Comisión de Prevención del Delito y Justicia Penal a que, teniendo en cuenta esa experiencia, examine la posibilidad de incrementar la asistencia en esa esfera bajo la égida de las Naciones Unidas y en colaboración con otras organizaciones que realicen actividades en ese sector.

Resolución 60/177 de la Asamblea General de las Naciones Unidas

Después del undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en Bangkok, Tailandia, en 2005, se adoptó una declaración, que destaca la necesidad de armonización en la lucha contra el ciberdelito,[1086] en la que se abordan, entre otros, los temas siguientes:

> *Reafirmamos la importancia fundamental de aplicar los instrumentos existentes y profundizar el desarrollo de las medidas nacionales y la cooperación internacional en asuntos penales, lo que incluye considerar la posibilidad de fortalecer e intensificar las medidas, en particular contra el delito cibernético, el blanqueo de dinero y el tráfico de bienes culturales, así como en materia de extradición, asistencia judicial recíproca y decomiso, recuperación y restitución del producto del delito.*
> *Observamos que, en esta era de la globalización, la tecnología de la información y el rápido desarrollo de nuevos sistemas de telecomunicaciones y redes informáticas se han visto acompañados del uso indebido de esas tecnologías con fines delictivos. Por consiguiente, acogemos con beneplácito los esfuerzos por aumentar y complementar la cooperación existente para prevenir, investigar y juzgar los delitos informáticos y de alta tecnología, incluso mediante la asociación con el sector privado. Reconocemos la importante contribución de las Naciones Unidas a los foros regionales y a otros foros internacionales en la lucha contra el delito cibernético e invitamos a la Comisión de Prevención del Delito y Justicia Penal a que, teniendo en cuenta esa experiencia, examine la posibilidad de incrementar la asistencia en esa esfera bajo la égida de las Naciones Unidas y en colaboración con otras organizaciones que realicen actividades en ese sector.*

La Resolución 60/177 de la Asamblea General de las Naciones Unidas respalda la Declaración de Bangkok de 2005 al estimular los esfuerzos de la comunidad internacional por mejorar y complementar la cooperación existente para prevenir el delito informático, invitando a un examen más profundo de la posibilidad de facilitar asistencia a los Estados Miembros tratando los delitos informáticos bajo la égida de las Naciones Unidas y en colaboración con otras organizaciones que realicen actividades en ese sector.

Duodécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

Durante el duodécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en Brasil en 2010 también se debatió el tema del delito cibernético.[1087] En las cuatro reuniones regionales preparatorias del Congreso para América Latina y el Caribe,[1088] Asia Occidental,[1089] Asia y el Pacífico[1090] y África,[1091] los países hicieron un llamamiento para la elaboración de un convenio internacional sobre el ciberdelito. Se plantearon llamamientos similares en el seno de las instituciones académicas.[1092]

Durante el propio Congreso los Estados Miembros hicieron progresos importantes hacia una implicación más activa de las Naciones Unidas en el debate sobre el tema del delito informático y del ciberdelito. El hecho de que las delegaciones trataran los temas durante dos días y de que se organizaran eventos paralelos destaca la importancia del asunto, que se debatió con mayor intensidad que durante los congresos anteriores.[1093] Las deliberaciones se centraron sobre todo en dos temas: cómo lograr la armonización de las normas jurídicas y cómo ayudar a los países en desarrollo a luchar contra el ciberdelito. El primer punto resulta de particular importancia en el caso en que las Naciones Unidas desarrollen normas jurídicas integrales o sugieran que los Estados Miembros apliquen el Convenio del Consejo de Europa sobre la Ciberdelincuencia. Con el fin de preparar el Congreso sobre Ciberdelito de las Naciones Unidas, el Consejo de Europa expresó su preocupación por el planteamiento de las Naciones Unidas[1094] e hizo un llamamiento para que se apoyaran su Convenio sobre la Ciberdelincuencia. Tras un intenso debate, en el que se trató en particular el limitado alcance del Convenio, los Estados Miembros decidieron no proponer su ratificación sino reforzar el papel de las Naciones Unidas en dos ámbitos importantes, como se plasmó en la Declaración del Salvador:

41. Recomendamos a la Oficina de las Naciones Unidas contra la Droga y el Delito que, en cooperación con los Estados Miembros, las organizaciones internacionales pertinentes y el sector privado, preste asistencia técnica a los Estados que lo soliciten y les imparta capacitación para mejorar su legislación nacional y reforzar la capacidad de las autoridades nacionales, a fin de que hagan frente a los delitos cibernéticos, incluso mediante la prevención, la detección, la investigación y el enjuiciamiento de esos delitos en todas sus formas, y para aumentar la seguridad de las redes informáticas.
42. Invitamos a la Comisión de Prevención del Delito y Justicia Penal a que estudie la posibilidad de convocar a un grupo intergubernamental de expertos de composición abierta para que realice un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, prácticas óptimas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas.

Por lo tanto, los Estados Miembros recomendaron un mandato exigente para la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) para que facilitara la creación de capacidades cuando se solicitara. Habida cuenta de la experiencia de la ONUDD en la creación de capacidades sobre legislación penal y de que, al contrario que el Consejo de Europa, la ONUDD dispone de una red mundial de oficinas regionales, es probable que las Naciones Unidas a través de la ONUDD juegue un papel importante en este ámbito en el futuro.

La segunda recomendación destaca que, durante el Congreso sobre delincuencia de la Naciones Unidas, los Estados Miembros fueron incapaces de decidir la elaboración o no de un texto jurídico. Esto refleja el controvertido debate durante el Congreso, en el que aquellos países europeos que habían ratificado el Convenio sobre la Ciberdelincuencia, en particular, expresaron su apoyo a ese instrumento mientras algunos países en desarrollo solicitaron un convenio de las Naciones Unidas. Sin embargo, los Estados Miembros tuvieron una respuesta diferente a la del undécimo Congreso sobre delincuencia, en el que hicieron referencia a instrumentos existentes. Esta vez no indicaron instrumentos existentes y, lo que es más importante, no decidieron recomendar que el Convenio sobre la Ciberdelincuencia se considerara una norma mundial. Al contrario, los Estados Miembros recomendaron invitar a la Comisión de Prevención del Delito y Justicia Penal a que llevara a cabo un estudio completo, que debería, entre otros, examinar las posibilidades de reforzar las medidas jurídicas nacionales e internacionales existentes y proponer otras nuevas para combatir el ciberdelito.

Resolución 64/211 de la Asamblea General de las Naciones Unidas

En marzo de 2010, la Asamblea General de las Naciones Unidas adoptó una nueva resolución[1095] como parte de la iniciativa "Creación de una cultura mundial de ciberseguridad". La Resolución 64/211 hace referencia a dos resoluciones importantes sobre el ciberdelito[1096] así como a dos resoluciones fundamentales sobre ciberseguridad.[1097] El instrumento voluntario de la autoevaluación sobre los esfuerzos nacionales para proteger las infraestructuras de información crítica, que figura en un anexo a la resolución, hace un llamamiento para que los países revisen y actualicen los textos jurídicos (incluidos los relativos al ciberdelito, la privacidad, la protección de los datos, la legislación comercial, las firmas digitales y el encriptado) que puedan estar obsoletos debido a la rápida evolución de las tecnologías de la información y de la comunicación. La Resolución hace además un llamamiento a los Estados para que utilicen los convenios, acuerdos y antecedentes regionales e internacionales en estas revisiones.

13. Examinar y actualizar las autoridades jurídicas (incluidas las relacionadas con los delitos cibernéticos, la privacidad, la protección de los datos, el derecho comercial, las firmas digitales y el cifrado) que puedan estar anticuadas u obsoletas como resultado de la rápida incorporación de las nuevas tecnologías de la información y las comunicaciones y de la dependencia de esas tecnologías, y utilizar en esos exámenes los convenios, arreglos y precedentes regionales e internacionales. Determinar si el país ha elaborado la legislación necesaria para la investigación y el enjuiciamiento de la delincuencia cibernética, indicando los marcos existentes, por ejemplo, las resoluciones de la Asamblea General 55/63 y 56/121 relativas a la lucha contra la utilización de la tecnología de la información con fines delictivos e iniciativas regionales como el Convenio del Consejo de Europa sobre la Ciberdelincuencia.
14. Determinar la situación actual de las autoridades y procedimientos nacionales que se ocupan de la delincuencia cibernética, incluidas las competencias legales y las dependencias nacionales encargadas de las cuestiones relativas a la delincuencia cibernética, y el nivel de comprensión de esas cuestiones entre los fiscales, jueces y legisladores.
15. Evaluar la idoneidad de los códigos jurídicos y las autoridades actuales para hacer frente a los desafíos presentes y futuros de la delincuencia cibernética y del ciberespacio de forma más general.
16. Examinar la participación nacional en las iniciativas internacionales para luchar contra la delincuencia cibernética, como la Red permanente de puntos de contacto.
17. Determinar los requisitos para que los organismos nacionales de imposición de la ley cooperen con sus homólogos internacionales a fin de investigar los delitos cibernéticos transnacionales en los casos en que la infraestructura o los autores del delito se encuentren en el territorio nacional pero las víctimas residan en otros lugares.

El hecho de que cuatro de las 18 cuestiones del instrumento de autoevaluación estén relacionadas con el ciberdelito destaca la importancia de disponer de capacidad para el cumplimiento de la ley para luchar con eficacia y mantener la seguridad cibernética.

Estudio mundial sobre ciberdelito

Tras la celebración de intensos debates[1098] sobre los temas y la metodología[1099] de un estudio exhaustivo de la ONUDD sobre ciberdelito, los Estados Miembros de las Naciones Unidas recibieron un cuestionario a principios de 2012. Al mismo tiempo, se elaboró un portal en línea.[1100] El complejo cuestionario contiene varias cuestiones relativas a distintos ámbitos de la legislación contra el ciberdelito, como definiciones, penalización e instrumentos procesales. Se pidió a los Estados Miembros que proporcionaran información sobre la situación en que se halla su legislación y la aplicación de diferentes normas regionales (como el Convenio sobre la Ciberdelincuencia). En 2013, esos resultados se presentaron[1101] a la Comisión de Prevención del Delito y Justicia Penal.[1102]

En 2013 la ONUDD publicó los primeros resultados del estudio[1103], el más complejo realizado hasta la fecha, que contiene los resultados de los 69 Estados Miembros que enviaron sus respuestas.[1104] Además de las respuestas de los Estados Miembros, el estudio contempla los resultados del examen de 500 documentos e informaciones de difusión pública presentados por más de 40 empresas y 16 instituciones académicas. En el estudio se hace hincapié en el alcance limitado de los instrumentos de armonización a escala regional, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia. Por otra parte, el estudio muestra que otros instrumentos regionales son igualmente importantes.[1105] El Grupo de Trabajo de Expertos se reunió en febrero de 2013 y presentó el asunto a la Comisión de Prevención del Delito y Justicia Penal.[1106]

En abril de 2013, la Comisión de Prevención del Delito y Justicia Penal examinó por primera vez los resultados del estudio.[1107] En la Resolución 22/7 se analiza la labor realizada sin entrar en detalles.[1108] En lugar de ello, la Comisión exhorta a los Estados Miembros a examinar los resultados, solicita al Grupo de Expertos que prosiga sus tareas y pide a la Secretaría que se traduzca el estudio en todos los idiomas de trabajo de las Naciones Unidas. Durante la 23ª reunión, numerosos oradores abordaron el tema del ciberdelito.[1109] A pesar de los diversos llamamientos para una armonización a escala mundial, la Comisión no adoptó una decisión al respecto. En vez de hacerlo, dio mayor prioridad a la creación de capacidades y destacó el Programa mundial de creación de capacidad a cargo de la ONUDD.[1110]

Grupo Gubernamental de Expertos

En 2013, un Grupo Gubernamental de Expertos que comprendía expertos de algunos países europeos (Estonia, Francia, Alemania y Reino Unido) presentó el informe "Development in the Field of Information and Telecommunications in the Context of International Security"[1111] (Desarrollo en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional). La ciberseguridad/seguridad de la información fue la principal actividad de ese grupo de trabajo. Además, aunque se examinaron una serie de normas, el grupo de trabajo privilegió un aspecto concreto de la ciberseguridad: la participación del Estado.[1112]

Grupo Intergubernamental de Expertos sobre Ciberdelincuencia

Tras el llamamiento de los Estados Miembros a la ONUDD para constituir un grupo de trabajo intergubernamental, se celebró la primera reunión del grupo en Viena en enero de 2011.[1113] El grupo de expertos incluía representantes de los Estados Miembros, de organizaciones intergubernamentales e internacionales, de agencias especializadas, del sector privado y de las instituciones académicas. Durante la reunión los miembros del grupo debatieron sobre un proyecto de estructura para un estudio que analizara con amplitud el tema del ciberdelito y su respuesta.[1114] En lo que respecta a la respuesta juridicial, algunos miembros resaltaron la utilidad de los instrumentos jurídicos internacionales existentes, incluidos la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC) y el Convenio del Consejo de Europa sobre la Ciberdelincuencia, y el deseo de elaborar un instrumento jurídico mundial para abordar específicamente el problema del ciberdelito. Se acordó que la decisión sobre si se debe elaborar un instrumento mundial se tomaría una vez finalizado el estudio.

Otras resoluciones y actividades

Un cierto número de decisiones, resoluciones y recomendaciones del sistema de las Naciones Unidas tratan asuntos relacionados con el ciberdelito, entre las que cabe citar que la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) y la Comisión de Prevención del Delito y Justicia Penal[1115] adoptaron una resolución sobre prevención efectiva del delito y respuestas penales para luchar contra la explotación sexual de los niños.[1116] En 2004, el Consejo Económico y Social de las Naciones Unidas[1117] adoptó una Resolución sobre cooperación internacional para la prevención, investigación, persecución y condena por fraude, abuso delictivo y falsificación de identidad y delitos conexos.[1118] En 2005 se creó un grupo de trabajo.[1119] Se estableció un grupo central de expertos sobre los delitos relacionados con la identidad para llevar a cabo un amplio estudio sobre este tema. En 2007 el Consejo Económico y Social adoptó una Resolución sobre cooperación internacional para la prevención, investigación, persecución y condena por fraude, abuso delictivo y falsificación de identidad y delitos conexos.[1120] Ninguna de estas dos Resoluciones trata explícitamente los retos de la delincuencia relacionada con Internet,[1121] pero se aplican también a esos delitos. A partir de las Resolución 2004/26[1122] y de la Resolución 2007/20[1123] del Consejo Económico y Social, la ONUDD creó un grupo central de expertos en 2007 para intercambiar puntos de vista sobre la mejor manera de proceder.[1124] El grupo ha llevado a cabo varios estudios en los que se incluyen aspectos de los delitos relacionados con Internet.[1125] En 2004, el Consejo Económico y Social adoptó una Resolución sobre la venta de drogas legales a través de Internet que tuvo explícitamente en cuenta un fenómeno relacionado con un delito informático.[1126]

Memorando de Entendimiento ONUDD/UIT

En 2011 la ONUDD y la Unión Internacional de Telecomunicaciones (UIT) firmaron un memorando de entendimiento relativo al ciberdelito.[1127] El memorando comprende la cooperación (en particular la creación de capacidades y la asistencia técnica para los países en desarrollo), la formación profesional y talleres conjuntos. En lo que respecta a las actividades de la creación de capacidades ambas organizaciones pueden disponen de una amplia red de oficinas en todos los continentes. Es más, las organizaciones acordaron una divulgación conjunta de la información y del conocimiento, así como de los análisis de los datos.

5.1.3 Unión Internacional de Telecomunicaciones [1128]

La Unión Internacional de Telecomunicaciones (UIT), como agencia especializada en el seno de las Naciones Unidas, juega un papel fundamental en la normalización y desarrollo de las telecomunicaciones y también en los temas relativos a la ciberseguridad.

Cumbre Mundial sobre la Sociedad de la Información

Entre otras actividades, la UIT ejerció de agencia líder durante la Cumbre Mundial sobre la Sociedad de la Información (CMSI) que se celebró en dos fases en Ginebra, Suiza, en 2003 y en Túnez en 2005. Gobiernos, responsables políticos y expertos de todo el mundo compartieron ideas y experiencias sobre cómo afrontar de la mejor forma posible los problemas emergentes asociados con el desarrollo de una sociedad mundial de la información, incluida la elaboración de normas y leyes compatibles. Los resultados de la cumbre figuran en la *Declaración de Principios de Ginebra*, el *Plan de Acción de Ginebra*; el *Compromiso de Túnez* y la *Agenda de Túnez para la Sociedad de la Información*.

El Plan de Acción de Ginebra destaca la importancia de las medidas en la lucha contra el ciberdelito:[1129]

> ***C5. Creación de confianza y seguridad en la utilización de las TIC***
> *12. La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información.*
> *[...]*
> *b) Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.*
> *[...]*

El ciberdelito también se consideró en 2005 durante la segunda fase de la CMSI en Túnez. La Agenda de Túnez para la Sociedad de la Información[1130] destaca la necesidad de cooperación internacional en la lucha contra el ciberdelito y hace referencia a los enfoques legislativos existentes tales como las resoluciones de la Asamblea General de las Naciones Unidas y el Convenio del Consejo de Europa sobre la Ciberdelincuencia:

> *40. Destacamos la importancia de enjuiciar la ciberdelincuencia, incluida la que se produce en una jurisdicción pero repercute en otra. Destacamos además la necesidad de concebir instrumentos y mecanismos nacionales e internacionales eficaces y eficientes, para promover la cooperación internacional, entre otros, de los organismos encargados de aplicar la ley en materia de ciberdelincuencia. Instamos a los gobiernos a que, en cooperación con otras partes interesadas, promulguen leyes que hagan posible la investigación y enjuiciamiento de la ciberdelincuencia, respetando los marcos vigentes, por ejemplo, las Resoluciones de la Asamblea General de las Naciones Unidas 55/63 y 56/121 sobre la "Lucha contra la utilización de la tecnología de la información con fines delictivos" y el Convenio sobre el Delito Cibernético del Consejo de Europa.*

Agenda sobre Ciberseguridad Global

Como resultado de la CMSI, la UIT fue designada como único facilitador de la Línea de Acción C5 consagrada a la creación de confianza y seguridad en la utilización de las TIC.[1131] En la segunda reunión de facilitación relativa a la Línea de Acción C5 convocada en 2007, el Secretario General de la UIT destacó la importancia de la cooperación internacional en la lucha contra el ciberdelito y anunció el lanzamiento de una *Agenda sobre Ciberseguridad Global de la UIT*.[1132] La Agenda se centra en siete objetivos clave,[1133] basados a su vez en cinco pilares estratégicos[1134], entre otros la elaboración de estrategias para la formulación de legislación modelo sobre el ciberdelito. Los siete objetivos son los siguientes:

1 Preparar estrategias que promuevan el desarrollo de una legislación modelo sobre ciberdelito, que resulte aplicable a escala mundial y sea compatible con las medidas legislativas ya adoptadas en los diferentes países y regiones.
2 Definir estrategias mundiales para crear las adecuadas estructuras institucionales nacionales y regionales, así como definir las correspondientes políticas para luchar contra el ciberdelito.
3 Diseñar una estrategia que permita establecer un conjunto mínimo y mundialmente aceptado de criterios de seguridad y planes de acreditación para equipos, aplicaciones y sistemas informáticos.
4 Definir estrategias para crear un marco mundial con miras a vigilar, alertar y responder ante incidentes y garantizar así la coordinación transfronteriza en lo que concierne a las iniciativas nuevas y existentes.
5 Diseñar estrategias mundiales tendentes a crear y apoyar un sistema de identidad digital genérico y universal y las correspondientes estructuras institucionales para garantizar el reconocimiento internacional de credenciales digitales.
6 Concebir una estrategia global para facilitar la creación de capacidad humana institucional con el fin de promover los conocimientos técnicos y prácticos en todos los sectores y las esferas antes mencionadas.
7 Formular propuestas para establecer un marco conducente a una estrategia mundial multipartita que fomente la cooperación, el diálogo y la coordinación internacionales en todas las esferas precitadas.

Para analizar y desarrollar medidas y estrategias relativas a los siete objetivos de la Agenda, el Secretario General de la UIT creó un Grupo de Expertos de alto nivel que reúne a representantes de los Estados Miembros, de la industria y del ámbito científico.[1135] En 2008 el Grupo de Expertos concluyó sus negociaciones y publicó el "Informe Estratégico Global".[1136] Lo más importante desde el punto de vista del ciberdelito son las medidas jurídicas incluidas en el Capítulo 1. Además de una visión general de los diferentes planteamientos regionales e internacionales sobre la lucha contra el ciberdelito,[1137] ese Capítulo ofrece un panorama de las disposiciones penales,[1138] los instrumentos de procedimiento,[1139] la reglamentación que rige la responsabilidad de los proveedores de servicios de Internet[1140] y las garantías para proteger los derechos fundamentales de los usuarios de Internet.[1141]

Creación de capacidades

En el marco de la Agenda sobre Ciberseguridad Global de la UIT, el UIT-D trabaja para ayudar a que los países lleven a cabo actividades armonizadas relacionadas con la ciberseguridad a escala nacional, regional e internacional. La Resolución 130 (Rev. Guadalajara, 2010) de la Conferencia de Plenipotenciarios de la UIT destaca el mandato de la Unión en la creación de capacidades. Según la Resolución, la UIT tiene el mandato de asistir a los Estados Miembros, en particular a los países en desarrollo, en la elaboración de medidas jurídicas adecuadas y practicables relativas a la protección frente a las amenazas informáticas.

Esto incluye actividades de creación de capacidades para el desarrollo, entre otros, de estrategias nacionales, reglamentación y cumplimiento de las leyes y estructuras organizativas (por ejemplo, vigilancia, alerta y respuesta ante incidentes). La UIT ha organizado varias conferencias regionales que han abordado específicamente, entre otros asuntos, los relativos al ciberdelito.[1142] Junto con asociados de los sectores público y privado, el UIT-D ha desarrollado instrumentos sobre ciberseguridad/CIIP para ayudar a los Estados Miembros a potenciar la sensibilización nacional, llevando a cabo autoevaluaciones nacionales sobre ciberseguridad, revisando su legislación y ampliando las capacidades de vigilancia, alerta y respuesta ante incidentes. Entre estos instrumentos figuran Comprensión del Ciberdelito: Una Guía para los países en desarrollo, el Conjunto de herramientas de la UIT para la autoevaluación nacional en materia de ciberseguridad/CIIP y el Conjunto de herramientas de la UIT para la defensa contra las redes robot.

Resoluciones

La UIT ha adoptado varias resoluciones relacionadas con la ciberseguridad que son importantes para el ciberdelito, aunque no tratan el asunto directamente con disposiciones de derecho penal.

- Resolución 130 (Rev. Guadalajara, 2010) de la Conferencia de Plenipotenciarios de la UIT sobre el fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación.

- Resolución 149 (Antalya, 2006) de la Conferencia de Plenipotenciarios de la UIT sobre el estudio de las definiciones y la terminología relativa a la creación de capacidades y la seguridad al utilizar las tecnologías de la información y las comunicaciones.
- Resolución 45 (Doha, 2006) de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT) sobre los mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo basura, e Informe de la Reunión sobre mecanismos de cooperación en materia de ciberseguridad y en la lucha contra el spam (31 de agosto - 1 de septiembre de 2006).
- Resolución 50 (Rev. Johannesburgo, 2008) de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), sobre ciberseguridad.
- Resolución 52 (Rev. Johannesburgo, 2008) de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), sobre respuesta y lucha contra el correo basura.
- Resolución 58 (Johannesburgo, 2008) de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), sobre Fomento de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo.

Proyectos para el Grupo de Estados ACP financiados por la UIT/UE

En apoyo de la elaboración de políticas y de una legislación en el Grupo de Estados de África, el Caribe y el Pacífico (ACP), la UIT y la UE decidieron financiar un proyecto [1143] en el marco del programa "ACP - Tecnologías de la Información y la Comunicación" y el noveno Fondo de Desarrollo Europeo. Teniendo en cuenta diferentes acontecimientos y prioridades anteriores en África, el Caribe y el Pacífico, el proyecto se subdividió en tres subprogramas regionales. La Región del África subsahariana recibió apoyo a través de la iniciativa Armonización de Políticas TIC en el África subsahariana (*HIPSSA, Harmonization of ICT Policies in Sub-Saharan Africa*). Para los países del Caribe se puso en marcha el proyecto Mejora de la competitividad en el Caribe gracias a la armonización de políticas, leyes y procedimientos reglamentarios en materia de TIC (*HIPCAR, Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures*).[1144] Por último, los países del Pacífico recibieron apoyo gracias al proyecto "Creación de capacidades y marcos político, reglamentario y legislativo en materia de TIC para los Estados insulares del Pacífico (*ICB4PAC, Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries*)".

Los tres proyectos constaban de dos etapas principales. En la primera etapa, se efectuó una evaluación regional de la legislación en vigor comparándola con prácticas óptimas internacionales. Teniendo en cuenta la evaluación y consultas intensivas, se elaboraron políticas modelo y leyes modelo. Durante la segunda etapa, los países obtuvieron apoyo en la transposición nacional de políticas modelo y leyes modelo.

Armonización de políticas sobre las TIC en el África subsahariana (HIPSSA)

Ya en 2004 la UIT y la Unión Europea pusieron en marcha un proyecto piloto regional para respaldar el establecimiento de un mercado integrado de las TIC en África Occidental (Armonización del mercado de las TIC de la CEDEAO/UEMAO).[1145] En 2005 se adoptaron directrices de prácticas óptimas[1146]; en calidad de actividades de seguimiento, en 2006 los Ministros de TIC de la CEDEAO adoptaron decisiones sobre una reglamentación armonizada en materia de TIC[1147], y en 2007, la Autoridad de la CEDEAO de Jefes de Estado y de Gobierno aprobó la Ley de decisiones complementaria.[1148]

La iniciativa HIPSSA fue concebida como un proyecto de crecimiento gradual respecto del proyecto piloto indicado anteriormente. Se incluyeron 42 países del África subsahariana en calidad de países beneficiarios.[1149] El objetivo del proyecto consistía en elaborar y fomentar políticas y directrices relativas a las TIC con miras al establecimiento de un mercado sostenible[1150] y a la creación de capacidades humanas e institucionales en la esfera de las TIC a través de diversas actividades de capacitación, formación e intercambio de conocimientos.

Mejora de la competitividad en el Caribe (HIPCAR)

En 2008, se puso en marcha con 15 países del Caribe el proyecto HIPCAR[1151], cuyo objetivo es ayudar a los países del Foro del Caribe (CARIFORUM)[1152] a armonizar sus políticas y marcos jurídicos en materia de TIC. En el marco de su preparación, se determinaron nueve esferas de trabajo[1153], en las cuales, durante la primera etapa del proyecto, se elaboraron políticas modelo y una legislación modelo para facilitar la elaboración y armonización de la legislación en la región. Esas esferas son las siguientes: cibertransacciones (comercio), evidencia digital, privacidad y protección de datos, interceptación de las comunicaciones, ciberdelito, acceso a la información pública/libertad de información, acceso universal, interconexión y, por último, concesión de licencias. Durante la segunda etapa, varios países (entre ellos Barbados, Granada, San Kitts y Nevis, Santa Lucía y Trinidad) recibieron apoyo en el proceso de transposición nacional.[1154]

Creación de capacidades y marcos políticos, reglamentarios y legislativos en materia de TIC para los Estados insulares del Pacífico (ICB4PAC)

A pedido de los países insulares del Pacífico, el proyecto asociado (ICB4PAC)[1155], que proponía la creación de capacidades sobre políticas y reglamentación de las TIC, daba prioridad a la creación de capacidades humanas e institucionales en el ámbito de las TIC mediante actividades de capacitación, formación e intercambio de conocimientos para 15 países insulares del Pacífico.[1156] Las esferas de trabajo abarcadas son, por ejemplo, la concesión de licencias y la numeración, el acceso universal, la interconexión, la elaboración de modelos de costos y el ciberdelito.

5.2 Enfoques regionales

Además de las organizaciones internacionales activas en el mundo, una serie de organizaciones internacionales centradas en regiones específicas han comenzado a realizar actividades relacionadas con el ciberdelito.

5.2.1 Consejo de Europa [1157]

El Consejo de Europa está representando un papel activo para afrontar los desafíos planteados por el ciberdelito.

Actividades hasta 1995

En 1976 el Consejo de Europa destacó la naturaleza internacional de los delitos informáticos y examinó este asunto en una conferencia que versaba sobre los diferentes aspectos del delito económico. Este asunto ha permanecido desde entonces en el orden del día del Consejo de Europa.[1158] En 1985 el Consejo de Europa designó a un Comité de Expertos [1159] para analizar los aspectos jurídicos de los delitos cibernéticos.[1160] En 1989 el Comité Europeo para Asuntos Delictivos adoptó el "Informe de Expertos sobre el delito cibernético",[1161] en el que se analizaban las disposiciones de derecho penal sustantivas que exigía la lucha contra nuevos tipos de delitos electrónicos, incluido el fraude cibernético y la falsificación cibernética. Reunido en 1989, el Comité de Ministros adoptó una Recomendación [1162] en la que se destacaba concretamente la índole internacional del ciberdelito:

De conformidad con el Artículo 15.b del Estatuto del Consejo de Europa y habida cuenta de que el objetivo del Consejo de Europa es lograr una mayor unidad entre sus miembros, el Comité de Ministros; reconociendo la importancia de dar rápidamente una respuesta adecuada al nuevo desafío que constituye el delito cibernético; considerando que el delito cibernético suele tener carácter transfronterizo; consciente de la necesidad concomitante de promover la armonización de la legislación y las prácticas, y de mejorar la cooperación internacional, recomienda a los Gobiernos de los Estados Miembros que:

1. Tengan en cuenta, al revisar su legislación o iniciar la promulgación de nuevas leyes, el Informe sobre el delito cibernético preparado por el Comité Europeo sobre los problemas planteados por los delitos, y en especial las directrices destinadas a los parlamentos nacionales.

2. Informar al Secretario General del Consejo de Europa durante 1993 acerca de cualquier evolución de su legislación, práctica judicial o experiencia en materia de cooperación jurídica internacional en lo que concierne al delito cibernético.

En 1995 el Comité de Ministros adoptó otra Recomendación, que versaba sobre los problemas dimanantes de los ciberdelitos transnacionales.[1163] Las directrices para preparar la legislación idónea se resumen en el Apéndice a dicha Recomendación.[1164]

Convenio del Consejo de Europa sobre la Ciberdelincuencia y Primer Protocolo Adicional

En 1996 el Comité Europeo para Asuntos Delictivos (CDPC) decidió establecer un Comité de Expertos para abordar el ciberdelito.[1165] La idea de pasar de una serie de principios a preparar otra Recomendación y redactar un Convenio se expuso durante las fechas del establecimiento del Comité de Expertos.[1166] Entre 1997 y 2000 el Comité celebró diez sesiones en Plenaria y su Grupo de Redacción de composición abierta organizó otras quince ordinarias. El Pleno adoptó el Proyecto de Convenio en la segunda parte de su sesión de abril de 2001.[1167] Una vez terminado, el Proyecto de Convenio se presentó para su aprobación al CDPC y ulteriormente el texto de dicho Proyecto se trasladó al Comité de Ministros con miras a su adopción.[1168] El Convenio se abrió a la firma en una ceremonia organizada en Budapest el 23 de noviembre de 2001 durante la cual 30 países firmaron el Convenio (incluidos cuatro Estados no miembros del Consejo de Europa, a saber: Canadá, Estados Unidos, Japón y Sudáfrica, que habían participado en las negociaciones). En junio de 2014, 47 Estados[1169] habían firmado el Convenio y 42 Estados[1170] lo habían ratificado[1171], entre ellos cuatro Estados[1172] que no lo habían firmado previamente. En total, 12 Estados[1173] fueron invitados a adherirse al Convenio, aunque todavía no lo han hecho.[1174] Actualmente, se reconoce que el Convenio es un importante instrumento internacional para luchar contra el ciberdelito y como tal ha recabado el apoyo de diferentes organizaciones internacionales.[1175]

Se aprobó el Primer Protocolo Adicional del Convenio sobre la Ciberdelincuencia.[1176] Durante las negociaciones del texto del Convenio se vio que penalizar especialmente el racismo y la distribución de material xenófobo era objeto de controversia.[1177] Algunos de los países en los que se protege apreciablemente el principio de libertad de expresión[1178] señalaron con preocupación que si se incluían disposiciones en el Convenio que violaran la libertad de expresión, no podrían firmarlo.[1179] En el cuarto borrador de 1998, el Convenio todavía incluía una disposición que requería a las partes que persiguieran por la vía penal el contenido ilegal "relativo en particular a asuntos tales como la pornografía infantil y la discriminación racial".[1180] Para evitar que los países no pudieran firmar un Convenio que violara la libertad de expresión, se suprimieron estos temas del Convenio durante la fase de elaboración y se incluyeron en un protocolo separado. En junio de 2014, 38 Estados[1181] habían firmado el Protocolo Adicional y 20 Estados[1182] lo habían ratificado.

Debate relativo al Convenio del Consejo de Europa sobre la Ciberdelincuencia

Actualmente, el Convenio del Consejo de Europa sobre la Ciberdelincuencia sigue siendo un instrumento de gran alcance apoyado por diferentes organizaciones internacionales.[1183] Sin embargo, durante el duodécimo Congreso sobre delincuencia, los debates destacaron que diez años después de la apertura a la firma, la repercusión del Convenio era limitada.[1184]

Limitaciones del alcance del Convenio del Consejo de Europa sobre la Ciberdelincuencia

A fecha de enero de 2011, Estados Unidos de América es el único país no europeo que ha ratificado el instrumento. Es cierto que los efectos del Convenio no se pueden medir únicamente a partir del número de países que lo firman o lo ratifican, puesto que países como Argentina,[1185] Pakistán,[1186] Filipinas,[1187] Egipto,[1188] Botswana[1189] y Nigeria[1190] han utilizado el Convenio como modelo y han redactado partes de su legislación a partir del Convenio sin adherirse formalmente a él. Incluso en el caso de esos países, sin embargo, no está claro hasta qué punto han utilizado el Convenio sobre la Ciberdelincuencia como modelo. Algunos de esos países también han utilizado otros textos legales, tales como la Directiva de la Unión Europea sobre ataques contra los sistemas informáticos y la Ley modelo de la Commonwealth. Puesto que estas leyes presentan ciertas similitudes con el Convenio sobre la Ciberdelincuencia y, además, las disposiciones rara vez se han reproducido literalmente, sino que se han adaptado a las necesidades de cada país, resulta casi imposible determinar hasta qué punto un país se ha inspirado en el Convenio. A pesar de todo, el Consejo de Europa reivindica que más de 100 países han firmado, ratificado o utilizado el Convenio al elaborar su propia legislación.[1191] Esta cifra, no obstante, no se podría comprobar. El Consejo de Europa no divulga los nombres de los países implicados y sólo se refiere a una "lista interna". Ni siquiera se divulga el número de países. Aunque fuera posible demostrar que 100 países han utilizado el Convenio sobre la Ciberdelincuencia, no significa forzosamente que hayan armonizado su legislación con respecto al Convenio. La imprecisa información publicada por el Consejo de Europa también deja sin respuesta la cuestión de si se han implementado todas las disposiciones del Convenio o solamente una.

Plazos para el trámite de ratificación

El alcance territorial limitado no fue la única inquietud debatida durante el undécimo Congreso sobre el Delito de las Naciones Unidas. La celeridad en el trámite de firma y ratificación sigue siendo un problema pendiente. Nueve años después de la firma inicial por 30 Estados el 23 de noviembre de 2001 sólo otros 17 Estados han firmado el Convenio sobre la Ciberdelincuencia. Ningún Estado que no sea miembro del Consejo de Europa se ha adherido durante este tiempo al Convenio, aunque se invitó a ocho países.[1192] El número de ratificaciones ha evolucionado de la forma siguiente: 2002 (2[1193]), 2003 (2[1194]), 2004 (4[1195]), 2005 (3[1196]), 2006 (7[1197]), 2007 (3[1198]), 2008 (2[1199]), 2009 (3[1200]), 2010 (4[1201]), 2011 (2[1202]), 2012 (6[1203]), 2013 (3[1204]). El proceso de implantación es tan lento como el de ratificación. En promedio, se precisan más de cinco años para que un país ratifique el Convenio después de haberlo firmado. Las diferencias entre países son importantes. Mientras Albania tardó algo más de medio año para ratificar el Convenio, Alemania necesitó casi diez años.

Evaluación de la ratificación

El Consejo de Europa hasta ahora nunca ha evaluado si los países que han presentado el instrumento de ratificación han puesto en práctica realmente el Convenio sobre la Ciberdelincuencia de conformidad con los requisitos. Existe mucha preocupación, en particular en el caso de los primeros países que ratificaron el Convenio, en relación con su total implementación. Incluso en países grandes como Alemania o los Estados Unidos es poco probable que el Convenio se implante en su totalidad. Alemania, por ejemplo, no persigue por la vía penal, en contra del Artículo 2 del Convenio, el acceso ilegal a los sistemas informáticos, sólo lo hace para el acceso ilegal a los datos informáticos.[1205] El perfil de país de la legislación contra el ciberdelito en los Estados Unidos que figura en la página Web del Consejo de Europa indica que 18 USC. § 1030(a)(1) – (5) corresponde al Artículo 2.[1206] Al contrario que el Artículo 2 del Convenio sobre la Ciberdelincuencia, sin embargo, 18 USC. § 1030(a) no persigue por la vía penal el mero acceso a un sistema informático. Además de "acceder" a un sistema informático, la disposición requiere otras actuaciones (como, por ejemplo, "obtener" información).[1207]

Debate mundial

Un aspecto del Convenio sobre la Ciberdelincuencia criticado con frecuencia es la escasa representación de los países en desarrollo durante el proceso de elaboración.[1208] A pesar de la dimensión transnacional del ciberdelito, su influencia en las diferentes regiones es dispar, lo que resulta de particular importancia para los países en desarrollo.[1209] No sólo se negoció el Convenio sin ninguna implicación importante de países en

desarrollo de Asia, África y América Latina, sino que impone condiciones restrictivas a los participantes de países que no sean miembros del Consejo de Europa, aunque se concibiera como un Convenio abierto a países no miembros. Según estipula el Artículo 37, la adhesión al Convenio requiere la consulta y el consentimiento unánime de los Estados firmantes. Además, la participación en las deliberaciones sobre futuras enmiendas está restringida a los firmantes del Convenio.[1210] Los debates durante la preparación del duodécimo Congreso sobre delitos de las Naciones Unidas mostraron que los países en desarrollo en particular se interesan por un planteamiento internacional en lugar de por la unión de iniciativas regionales. Durante las reuniones preparatorias regionales para el duodécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal para Latino América y el Caribe[1211], Asia Oriental[1212], Asia y el Pacífico[1213] y África,[1214] algunos países hicieron un llamamiento para un convenio internacional sobre el ciberdelito. Las instituciones académicas hicieron un llamamiento similar.[1215]

Falta de respuesta ante las tendencias actuales

El ciberdelito es una parte de la delincuencia que está cambiando permanentemente.[1216] En los años 90, cuando se elaboró el Convenio sobre la Ciberdelincuencia, el uso de Internet por grupos terroristas[1217], los ataques de redes robot[1218] y la usurpación de identidad[1219] o no se conocían o no tenían la importancia que tienen hoy en día[1220] y, por lo tanto, no se podían afrontar con soluciones específicas. Incluso el Consejo de Europa ha reconocido que el Convenio sobre la Ciberdelincuencia está en parte anticuado, lo que se puede demostrar comparando las disposiciones relativas a la pornografía infantil que figuran en el Convenio sobre la Ciberdelincuencia de 2001 y las del Convenio relativo a la Protección del Niño de 2007. El Artículo 20 (1)(f) de este último persigue por la vía penal acceder voluntariamente, mediante tecnologías de la información y de la comunicación, la pornografía infantil. Esto no se penaliza en el Convenio sobre la Ciberdelincuencia, aunque la referencia a las TIC hace hincapié en que se trata de un delito que se puede caracterizar como ciberdelito. A partir de los motivos expuestos en el Informe Explicativo, los redactores decidieron incluir esta disposición para cubrir los casos en los que los infractores ven imagines de niños en línea accediendo a sitios de pornografía infantil pero sin descargar nada. Esto significa, por consiguiente, que el Convenio sobre la Ciberdelincuencia no recoge este tipo de actos y, por tanto, en este aspecto ni siquiera cumple las propias disposiciones del Consejo de Europa.

Esto mismo es cierto en lo que respecta a los instrumentos de procedimiento. La interceptación de comunicaciones de voz por IP (VoIP), la admisibilidad de evidencias y procedimientos digitales para tomar en consideración el uso emergente de tecnologías de cifrado y los medios para la comunicación anónima son asuntos de suma importancia para el Convenio sobre la Ciberdelincuencia, aunque no sean tratados en él. En sus diez años de existencia, el Convenio nunca ha sido enmendado y, salvo por el Protocolo Adicional relativo al material xenófobo, no se han añadido nuevas disposiciones o instrumentos.

Es preciso adaptar las leyes a las tecnologías y a los comportamientos delictivos cambiantes. Como se ha indicado anteriormente, los requisitos respecto de la legislación sobre el ciberdelito han cambiado en los últimos diez años. Sería, por lo tanto, muy necesaria una actualización del Convenio sobre la Ciberdelincuencia. Otras organizaciones regionales, como la Unión Europea, acaban de revisar los instrumentos jurídicos en relación con el ciberdelito, que se introdujeron más recientemente hace unos cinco años. A pesar de la urgencia de una actualización, es poco probable que se realice. La Unión Europea, que ha apoyado intensamente el Convenio sobre la Ciberdelincuencia, declaró hace poco que en su opinión "actualizar el Convenio [sobre la Ciberdelincuencia] […] no se puede considerar una posibilidad factible".[1221]

Adhesión de países que facilitan infraestructuras en lugar de países en desarrollo

En los últimos diez años el Consejo de Europa no ha logrado adhesiones de países pequeños y en desarrollo. Una de las razones es que el Convenio se negoció con una escasa representación de los países en desarrollo.[1222] Asia y África estaban especialmente poco representadas y América Latina no estaba representada en absoluto. Aunque el Consejo de Europa invita a representantes de los países en desarrollo a sus principales conferencias sobre ciberdelito, estos países no pueden participar en las deliberaciones sobre posibles enmiendas puesto que esas reuniones están restringidas a los partícipes en el Convenio.[1223]

En lo que respecta a las adhesiones también se pueden observar diferencias frente a los instrumentos verdaderamente internacionales como los convenios de las Naciones Unidas. Aunque el proceso de

adhesión al Convenio estaba concebido para dar cabida a los no miembros, se aplican condiciones restrictivas. Al contrario que en el caso del Convenio de las Naciones Unidas, la adhesión al Convenio sobre la Ciberdelincuencia requiere la consulta y el acuerdo unánime de los Estados signatarios.[1224] Por consiguiente, los países en desarrollo en particular realizaron un llamamiento para un planteamiento (más) internacional durante la preparación del duodécimo Congreso sobre el delito de las Naciones Unidas. Durante las reuniones preparatorias del Congreso para América Latina y el Caribe[1225], Asia Occidental[1226], Asia y el Pacífico[1227] y África[1228] los países participantes solicitaron el desarrollo de ese instrumento internacional.

Aunque la estrategia del Consejo de Europa de centrarse en los países occidentales parece lógica puesto que son los que disponen de las infraestructuras, la participación de los países en desarrollo es crucial si hubiera que incluir a las víctimas potenciales. En 2005 la cantidad de usuarios de internet de los países en desarrollo superó al de las naciones industrializadas.[1229] Al excluir a los países en desarrollo y centrarse en los países desarrollados que (actualmente) facilitan la mayor parte de las infraestructuras y de los servicios, se ignoran dos aspectos fundamentales: la importancia de proteger a la mayoría de los usuarios de los servicios de Internet y, en segundo lugar, la cada vez mayor influencia de los países emergentes como India, China y Brasil. Si no se apoya a los países en desarrollo para que elaboren leyes que les permitan investigar casos que influyen sobre sus ciudadanos y, además, cooperar a escala internacional con otras unidades que persiguen el cumplimiento de las leyes para identificar a los infractores, las investigaciones de la ciberdelincuencia resultarán más difíciles cuando impliquen a esos países. El hecho de que en los últimos diez años no se haya adherido ningún país en desarrollo al Convenio sobre la Ciberdelincuencia muestra las limitaciones de un planteamiento regional. Si se tiene además en cuenta que en la última década el Consejo de Europa sólo ha invitado a ocho países (de los 146 Estados Miembros de las Naciones Unidas que no han firmado el Convenio) para adherirse al Convenio, quedan en evidencia los escasos esfuerzos dedicados en este asunto. Esto está seguramente relacionado con el hecho que las necesidades de los países en desarrollo relativas a la legislación y a la creación de capacidades en general está más allá de los mecanismos del Convenio. Hasta ahora el Consejo de Europa se ha centrado en ayudar a los países para que alineen su legislación con el Convenio (por ejemplo, para reducir las diferencias citadas). Además, cada vez más países podrían estar necesitando ayuda en la elaboración de su legislación puesto que las disposiciones del Convenio requieren un ajuste durante su ejecución. Los países pueden, por ejemplo, determinar quién está autorizado a ordenar ciertas investigaciones (jueces/fiscales/comisarías de policía) y sobre qué indicios (pruebas demostradas/declaración jurada/información).

Este asunto se debatió en profundidad durante el duodécimo Congreso sobre el Ciberdelito de las Naciones Unidas, lo que llevó a los Estados Miembros a tomar decisiones para reforzar el mandato sobre creación de capacidades de la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD) en el ámbito del ciberdelito.[1230] Otras organizaciones de las Naciones Unidas como la Unión Internacional de Telecomunicaciones (UIT) han recibido últimamente mandatos similares.[1231]

Abandono de los países pequeños y en desarrollo

Los países pequeños y en desarrollo se enfrentan a dificultades cuando aplican las normas del Convenio. El hecho de que los países más pequeños del Consejo de Europa no hayan ratificado[1232] el Convenio en los últimos diez años pone en evidencia que no es un desafío sólo para pequeños países fuera de Europa sino que también lo es para los países europeos pequeños.

Una de las disposiciones que plantea dificultades en este caso es la necesidad de establecer puntos de contacto durante las 24 horas todos los días de la semana. Estos puntos de contacto pueden tener un efecto muy positivo sobre la rapidez de las investigaciones y, por consiguiente, el Artículo 35 es uno de los instrumentos más importantes del Convenio.[1233] Sin embargo, hay que mencionar que recientemente el Consejo de Europa ha publicado un estudio que analiza la eficacia de la cooperación internacional frente al ciberdelito[1234] y otro sobre el funcionamiento de puntos de contacto a todas horas todos los días para luchar contra el ciberdelito[1235] y que el resultado de estos dos estudios es que no todos los países que han ratificado el Convenio han establecido este tipo de puntos de contacto y que incluso los países que han facilitado un punto de contacto a menudo lo utilizan sólo con un propósito limitado.

El principal problema para los países en desarrollo radica en que es obligatorio establecer ese punto de contacto. Mientras que para los países desarrollados establecer y mantener este tipo de punto de contacto con toda probabilidad no es problemático al utilizar una policía especializada en la ciberdelincuencia en turnos de noche y de día, si constituye un reto para países en los que esa policía especializada está formada por una sola persona. En estos casos la obligatoriedad implica una importante inversión. Que la adhesión al Convenio y su implantación no implica costes asociados para los países, como ha declarado recientemente un representante del Consejo de Europa en una conferencia en el Pacífico,[1236] es, por tanto, sólo cierto si se excluyen los costes indirectos, por ejemplo, para mantener un punto de contacto permanente o para adquirir tecnología y registrar datos de tráfico en tiempo real.

Planteamiento incompleto

Uno de los principales objetivos del Convenio fue proporcionar un planteamiento completo con el fin de tratar todos los aspectos relevantes del ciberdelito.[1237] Pero, si se compara el Convenio con otros planteamientos, en particular con la Ley modelo de la Commonwealth sobre delitos informáticos y delitos relacionados con la informática[1238] así como con instrumentos de la Unión Europea tales como la Directiva sobre comercio electrónico[1239], se observa que faltan aspectos importantes. Entre ellos se pueden citar la falta de disposiciones relativas a la admisibilidad de las pruebas electrónicas[1240] o a la responsabilidad de los proveedores de servicio. Puesto que las pruebas electrónicas se caracterizan en gran medida como una nueva categoría de prueba[1241], la falta de una disposición sobre, por lo menos, un marco reglamentario relativo a la admisibilidad de las pruebas electrónicas tiene consecuencias importantes. Y, a menos que un país disponga de otros instrumentos o que sus jueces consideren aceptables esas pruebas, no se podría condenar a ningún infractor aunque el Convenio estuviera implantado en su totalidad.

Convenio sobre la protección del niño

En su planteamiento para mejorar la protección de los menores de edad contra la explotación sexual, el Consejo de Europa introdujo en 2007 un nuevo Convenio.[1242] 23 Estados firmaron el Convenio sobre la protección del niño el primer día en que se dispuso para la firma. En junio de 2014 tenía la firma de 47 Estados,[1243] de los que 31 lo habían ratificado.[1244] Uno de los objetivos del Convenio sobre la protección del niño contra la explotación sexual es la armonización de las disposiciones de derecho penal destinadas a proteger a los niños contra la explotación.[1245] Para conseguir este objetivo, el Convenio incluye un conjunto de disposiciones relativas al derecho penal. Además de la persecución por la vía penal del abuso sexual de los niños (Artículo 18), el Convenio incluye disposiciones que tratan del intercambio de pornografía infantil (Artículo 20) y de la solicitación de niños para fines sexuales (Artículo 23).

Negociaciones relativas a otro Protocolo adicional

Ya en 2012 la Comisión del Convenio sobre la Ciberdelincuencia[1246] aprobó un informe relativo al acceso transfronterizo y la jurisdicción.[1247] Pese a la gran inquietud que suscita el acceso transfronterizo, el informe proponía la adopción de un Protocolo adicional especial.[1248] A diferencia de la negociación a puertas cerradas del Convenio sobre la Ciberdelincuencia, ese informe sugería un proceso de consultas más abierto.[1249] En junio de 2013, el Consejo de Europa organizó una serie de consultas públicas relativas al acceso transfronterizo. Basándose en los informes de los participantes, casi todos los expertos expresaron críticas, entre ellos organizaciones no gubernamentales, empresas, Estados Miembros del Consejo de Europa, la Comisión de la Unión Europea y expertos en protección de datos del Consejo de Europa.[1250]

En 2013 se publicó un informe del Grupo de Trabajo sobre acceso transfronterizo[1251], en el cual se enumeran posibles elementos de un Protocolo adicional, desde el acceso transfronterizo con consentimiento hasta diversas variantes de acceso sin consentimiento.[1252] En noviembre de 2013 se publicó una nota orientadora relativa al acceso transfronterizo.[1253]

5.2.2 Unión Europea [1254]

Durante la pasada década la Unión Europea (UE) ha elaborado varios instrumentos jurídicos que tratan aspectos del ciberdelito. Aunque estos instrumentos generalmente sólo son vinculantes para los 27 Estados Miembros, varios países y varias regiones están utilizando las normas europeas como referencia en sus debates nacionales y regionales sobre armonización de la legislación.[1255]

Situación hasta diciembre de 2009

Hasta 2009, el mandato de UE respecto de la legislación penal era limitado y controvertido.[1256] Además del reto planteado por las propias limitaciones del mandato, no estaba claro que el mandato para cualquier legislación penal, incluido el ciberdelito, se enmarca en el denominado "Primer Pilar" (Comunidad Europea) o en el "Tercer Pilar" (Unión Europea).[1257] Puesto que la opinión más extendida era que dependía del tercer pilar, la armonización sólo era posible mediante la cooperación internacional en el marco del tercer pilar que trata de la cooperación intergubernamental en materia de justicia y asuntos de interior.[1258] Cuando, en 2005, el Tribunal de Justicia declaró ilegal un instrumento del tercer pilar en el ámbito del derecho penal (la Decisión marco del Consejo relativa a la protección del medio ambiente mediante el derecho penal[1259] por primera vez se vio amenazada [1260]) la distribución de las competencias. El tribunal decidió que la Decisión marco, al ser indivisible, infringía el Artículo 47 ya que se arrogaba los poderes conferidos a la Comunidad en virtud del Artículo 175 de las Comunidades Europeas. Esta decisión tuvo una importante influencia en los debates sobre armonización del derecho penal en el seno de la Unión Europea. La Comisión Europea, que tiene la responsabilidad de hacer respetar los tratados de la Unión, indicó que, debido al juicio, algunas decisiones marco relativas al derecho penal eran en parte o en su totalidad incorrectas, puesto que todas o algunas de sus disposiciones se basaban en un texto jurídico incorrecto.[1261] A pesar del reconocimiento de las nuevas posibilidades para evaluar el mandato en el seno del primer pilar, las iniciativas de la CE fueron escasas debido a la falta de cobertura del asunto en el primer pilar. En 2007, el Tribunal de Justicia confirmó la sentencia jurídica en una segunda decisión.[1262]

Situación tras la ratificación del Tratado de Lisboa

El Tratado de Lisboa (el "tratado de la reforma"),[1263] que entró en vigor en diciembre de 2009, cambió las funciones de la Unión Europea de forma significativa. Además de rescindir la distinción entre "primer pilar" y "tercer pilar", por vez primera dotó a la Unión Europea de un mandato claro en el ámbito del delito informático. Los Artículos 82 a 86 del Tratado de Funcionamiento de la Unión Europea (TFUE) proporcionan a la UE competencias para armonizar la legislación penal (derecho penal sustantivo y derecho procesal). El Artículo 83[1264] del TFUE es el más importante en materia de ciberdelito. Autoriza a la Unión Europea a establecer reglas mínimas relativas a la definición de las infracciones y sanciones penales en ámbitos delictivos de especial gravedad y que tengan una dimensión transfronteriza. En el primer párrafo del Artículo 83 se menciona específicamente el delito informático como uno de los ámbitos delictivos. Puesto que el término delito informático es más amplio que el ciberdelito, autoriza a la Unión Europea a legislar ambos conceptos. Según el párrafo 2j del Artículo 4, la elaboración de legislación sobre delitos informáticos es una competencia compartida entre la Unión Europea y los Estados Miembros, lo que permite a la UE adoptar leyes vinculantes (Art. 2, párrafo 2) y limita la capacidad de los Estados Miembros a ejercer su competencia hasta donde la UE no haya ejercido la suya.

En el "Programa de Estocolmo", adoptado por el Consejo Europeo en 2009, la UE destacó que utilizaría sus nuevas competencias.[1265] El programa es una definición del interés de los trabajos de la UE en el ámbito de justicia e interior por un periodo de cinco años y es continuación del Programa de la Haya que finalizó en 2009.[1266] Subraya la intención de la UE de ejercer sus competencias al referirse a las cuestiones delictivas mencionadas en el párrafo 1 del Artículo 83 del TFUE, dando preferencia a las cuestiones relativas a la pornografía infantil y al delito informático.[1267]

Panorama de los instrumentos y directrices de la UE

A pesar de los cambios fundamentales realizados en la estructura de la UE, siguen vigentes los instrumentos adoptados en el pasado. Sobre la base del Artículo 9 del Protocolo sobre las decisiones transitorias, deben

preservarse los instrumentos adoptados con arreglo al Tratado en la Unión Europea antes de la entrada en vigor del Tratado de Lisboa hasta que sean revocados, anulados o enmendados. El Capítulo siguiente ofrece una visión general de todos los instrumentos pertinentes de la UE.

Política general

Desde el año 1996 la UE tuvo en cuenta los riesgos asociados con Internet en un comunicado que trataba del contenido ilegal y perjudicial de Internet.[1268] La UE destacaba la importancia de la cooperación entre los Estados Miembros para luchar contra el contenido ilegal en la red.[1269] En 1999 el Parlamento Europeo y el Consejo de Europa adoptaron un plan de acción para promover el uso seguro de Internet y combatir el contenido ilegal y perjudicial en las redes.[1270] El plan de acción se centraba en la auto regulación más que en la persecución del delito. También en 1999, la Unión Europea lanzó la iniciativa "eEurope", adoptando la Comunicación de la Comisión Europea "e-Europa – Una sociedad de la información para todos".[1271] La iniciativa define los objetivos clave pero no trata la persecución por la vía penal de los actos ilegales cometidos al utilizar las tecnologías de la información. En 2001 la Comisión Europea publicó una Comunicación que versaba sobre la creación de una sociedad de la información más segura, mejorando la seguridad de las estructuras de la información y luchando contra el ciberdelito.[1272] En dicha Comunicación la Comisión analizaba y abordaba el problema que constituía el delito cibernético e indicaba la necesidad de tomar medidas eficaces para enfrentarse a las amenazas que pesaban sobre la integridad, disponibilidad y fiabilidad de los sistemas y redes de información.

Las infraestructuras de información y comunicación se han convertido en un elemento fundamental de nuestras economías. Desgraciadamente, estas infraestructuras son vulnerables y brindan nuevas posibilidades de comportamiento delincuente. Estas actividades delictivas pueden ser muy variables y atravesar un gran número de fronteras. Pese a que, por varias razones, no hay estadísticas fiables en esta esfera, es prácticamente seguro que los delitos mencionados constituyen una amenaza para las inversiones y activos industriales, así como para la seguridad y confianza en la sociedad de la información. Se ha informado recientemente sobre casos de denegación de servicios y ataques de virus que han ocasionado grandes pérdidas financieras.

Puede hacerse mucho en lo que concierne a prevenir las actividades delictivas, fomentando la seguridad de las infraestructuras de la información y garantizando que las autoridades encargadas de hacer cumplir la ley cuenten con los medios de actuación adecuados en el marco de un respeto cabal de los derechos fundamentales del individuo.[1273]

Tras participar en el Consejo de Europa y en los debates del G8, la Comisión reconoce la complejidad y dificultad que plantean las cuestiones de procedimiento jurídico. Ahora bien, una cooperación eficaz con la Unión Europea para luchar contra el ciberdelito es un elemento fundamental de una sociedad de la información más segura, así como el establecimiento de un contexto de libertad, seguridad y justicia[1274].

[...] para fomentar un derecho penal sustantivo en la esfera del delito de alta tecnología. Esto incluye los delitos relacionados con el pirateo y los ataques que generan denegación del servicio. La Comisión examinará, por otra parte, el marco de acción contra el racismo y la xenofobia en Internet para que se adopte una Decisión marco en el contexto del Título VI del Tratado de la Unión Europea con la decisión que abarcaría las actividades racistas y xenofóbicas tanto en línea como fuera de línea. Por último, se examina también el problema que suscitan las drogas ilícitas.[1275]

La Comisión seguirá desempeñando un cometido cabal para garantizar la coordinación entre los Estados Miembros en otros foros internacionales en los que se discute el ciberdelito, por ejemplo el Consejo de Europa y el G8. Las iniciativas adoptadas por la Comisión en el plano de la Unión Europea tomarán plenamente en cuenta los progresos logrados en otros foros internacionales y se intentará lograr una convergencia en el marco de la Unión Europea.[1276]

Asimismo, en 2001, la Comisión publicó una Comunicación, que versaba sobre la seguridad de las redes y la información[1277] en la que se analizaron los problemas que suscitaba la seguridad de las redes y se presentaba un esbozo estratégico para la actuación sobre el particular.

En las dos Comunicaciones mencionadas de la Comisión se destacaba la necesidad de lograr una convergencia del derecho penal sustantivo de los países miembros de la Unión Europea, especialmente para ocuparse de los ataques lanzados contra los sistemas de información. Asimismo se reconocía que la armonización del derecho penal sustantivo de los países miembros de la Unión Europea en lo que respecta a la lucha del ciberdelito era un elemento indispensable de todas las iniciativas que se emprendan en el plano de la Unión Europea.[1278]

En 2007, la Comisión publicó una Comunicación relativa a una política general en cuanto a la lucha contra el ciberdelito.[1279] En la Comunicación se resume la situación actual y destaca la importancia del Convenio sobre la Ciberdelincuencia, ya que se trata del principal instrumento internacional para combatir el ciberdelito. Asimismo, en la Comunicación se indican las cuestiones sobre las que la Comisión centrará sus futuras actividades; por ejemplo:

- Fortalecer la cooperación internacional en la lucha contra el ciberdelito
- Coordinar más adecuadamente el apoyo financiero para realizar actividades de capacitación
- Organizar una reunión de expertos en obligada observancia de la ley
- Fortalecer el diálogo con la industria
- Supervisar las cambiantes amenazas del ciberdelito para evaluar la necesidad de legislar en mayor medida.

Directiva relativa al comercio electrónico (2000)

La Directiva sobre comercio electrónico[1280] de la UE versa, entre otras cuestiones, de la responsabilidad legal de los proveedores de servicios de Internet por actos cometidos por terceros (Artículo 12 *et seq.*). Confrontados a las dificultades derivadas de la dimensión internacional que ha adquirido Internet, los redactores de la Directiva decidieron elaborar normas que faciliten un marco jurídico para la construcción general de la sociedad de la información, y de esta forma respaldar el desarrollo económico global así como la labor de las autoridades competentes.[1281] Esto se argumenta en la consideración de que el desarrollo de los servicios de la sociedad de la información está dificultado por algunos obstáculos legales para el adecuado funcionamiento del mercado interno, que otorga su mandato a la Comunidad Europea.[1282] Las disposiciones relativas a la responsabilidad se inspiran en el principio de responsabilidad progresiva.[1283] Aunque la Directiva destaca que no pretende armonizar el ámbito propio del derecho penal, también regula la responsabilidad penal.[1284]

Decisión del Consejo para luchar contra la pornografía infantil en Internet (1999)

En 2000 el Consejo de la Unión Europea se comprometió con un planteamiento para abordar la pornografía infantil en Internet. La Decisión se adoptó como continuación de la comunicación de 1996 relativa al contenido ilegal y prejudicial en Internet[1285] y el plan de acción correspondiente de 1999 para promover un uso más seguro de Internet y luchar contra el contenido ilegal y prejudicial en las redes.[1286] Sin embargo, la Decisión no estipula obligaciones en lo que respecta a la adopción de disposiciones específicas de derecho penal.

Decisión marco relativa a la lucha contra el fraude (2001)

En 2001 la UE adoptó su primer marco legal directamente relacionado con aspectos del ciberdelito. La Decisión marco de la UE para combatir cualquier fraude que implique medios de pago distintos del efectivo[1287] incluye la obligación de armonizar la legislación penal en lo relativo a aspectos específicos del fraude informático y la concepción de instrumentos, tales como los programas informáticos, que estén especialmente adaptados para cometer un delito mencionado en la Decisión marco.[1288]

Artículo 3 *– Delitos relacionados con equipos informáticos*
Cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario que cause una pérdida no autorizada de propiedad a otra persona, con el ánimo de procurar un beneficio económico no autorizado a la persona que comete el delito o a terceros, mediante:
— la introducción, alteración, borrado o supresión indebido de datos informáticos, especialmente datos de identidad, o
— la interferencia indebida en el funcionamiento de un programa o sistema informáticos.

De acuerdo con la opinión prevalente en aquel momento y como consecuencia de la falta de mandato en el tercer pilar, el instrumento se elaboró en virtud del primer pilar, resaltando que, dada la dimensión internacional del fenómeno, estas cuestiones no las pueden abordar adecuadamente los propios Estados Miembros.

Decisión marco del Consejo de la Unión Europea relativa a los ataques contra los sistemas de información (2005)[1289]

Tras la publicación de su política general en 2001, la CE presentó una propuesta para una Decisión marco relativa a los ataques contra los sistemas de información.[1290] Fue modificada y adoptada por el Consejo en 2005.[1291] Entretanto, este instrumento fue sustituido por la Directiva de 2012 (véase *infra*). Aunque toma nota del Convenio del Consejo de Europa sobre la Ciberdelincuencia,[1292] se centra en la armonización de disposiciones penales sustantivas destinadas a la protección de las infraestructuras. No se integraron en la Decisión marco aspectos relativos a la ley de procedimiento penal (en particular la armonización de los instrumentos necesarios para investigar y perseguir el ciberdelito) ni instrumentos relativos a la cooperación internacional. Destaca las lagunas y diferencias en los marcos jurídicos de los Estados Miembros y la cooperación efectiva policial y judicial en materia de ataques contra los sistemas de información.[1293]

Artículo 2 *– Acceso ilegal a los sistemas de información*
1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.
2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad.
Artículo 3 *– Intromisión ilegal en los sistemas de información*
Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.
Artículo 4 *– Intromisión ilegal en los datos*
Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Directiva sobre la conservación de datos (2005)

En 2005 el consejo adoptó la Directiva sobre la conservación de datos.[1294] Incluye la obligación a los proveedores de servicio de Internet de almacenar ciertos datos de tráfico necesarios para la identificación de delincuentes en el ciberespacio. En 2014 el Tribunal de Justicia Europeo declaró nula la Directiva.[1295]

Artículo 3 *– Obligación de conservar datos*
1. Como excepción a los Artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el Artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.
2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el Artículo 5 en relación con las llamadas telefónicas infructuosas en las que los datos los generan o tratan, y conservan (en lo que a los datos telefónicos se refiere) o registran (en lo que a los datos de Internet se refiere), proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. La conservación de datos en relación con las llamadas no conectadas no será obligatoria con arreglo a la presente Directiva.

El hecho de que la Directiva trate de informaciones fundamentales sobre cualquier comunicación en Internet ha sido objeto de acerbas críticas por parte de organizaciones de derechos humanos, lo cual podría a su vez provocar una revisión de la Directiva y de su aplicación en tribunales constitucionales.[1296] En su conclusión en el caso *Productores de Música de* España (Promusicae) contra *Telefónica de España*,[1297] Juliane Kokott, Abogada General ante el Tribunal de Justicia Europeo, señaló que le parecía poco probable que se pudiera aplicar la obligación de conservación de datos sin violar derechos fundamentales.[1298] En 2001 el G8 ya señaló dificultades con respecto a la aplicación de ese tipo de reglamentaciones.[1299]

La Directiva se basó en el mandato de la Comunidad Europea para el mercado interno (Artículo 95).[1300] Los redactores destacaron que el aplazamiento de las normas jurídicas y técnicas relacionadas con la conservación de datos para fines de investigación del ciberdelito planteaba obstáculos al mercado interno de las comunicaciones electrónicas, ya que los proveedores de servicio se enfrentaban a diferentes requisitos que conllevan diferentes inversiones financieras.[1301] Irlanda con el apoyo de Eslovaquia, solicitó al Tribunal de Justicia Europeo que anulara la Directiva puesto que no había sido adoptada con la debida base legal. Ambos países argumentaron que el Artículo 95 no era suficiente, ya que ese instrumento no se centraba en el funcionamiento del mercado interior sino más bien en la investigación, detección y persecución del delito. El Tribunal de Justicia Europeo rechazó la propuesta por improcedente, resaltando que las diferencias en lo que respecta a la obligación de conservar los datos tendrían repercusiones directas sobre el funcionamiento del mercado interior.[1302] Destacó así mismo que esta situación justificaba el derecho comunitario al perseguir el objetivo de salvaguardar el adecuado funcionamiento del mercado interior mediante la adopción de reglas armonizadas.

En 2014, el Tribunal de Justicia Europeo declaró finalmente nula la Directiva[1303] que, en su opinión, supone una amplia y particularmente grave interferencia a derechos fundamentales del respeto a la vida privada y a la protección de datos personales, sin que se imponga a dicha interferencia los límites estrictamente necesarios. Por consiguiente, esa Directiva ya no tiene carácter vinculante para los Estados Miembros. Las leyes nacionales promulgadas en virtud de la Directiva no quedan automáticamente nulas. Por el momento, es incierta la presentación y adopción de una nueva directiva por parte de la Unión Europea.

Enmienda a la Decisión marco del Consejo de la Unión Europea sobre la lucha contra el terrorismo (2007)

En 2007 la Unión Europea inició un debate acerca de un proyecto de enmienda de la Decisión marco sobre la lucha contra el terrorismo.[1304] En la introducción de este proyecto de enmienda la Unión Europea subraya el hecho de que el marco jurídico vigente tipifica como delito ayudar o inducir o incitar al terrorismo, pero no así diseminar conocimientos técnicos de terrorismo a través de Internet.[1305] La idea que preside este proyecto de enmienda es que la Unión Europea adopte medidas para colmar esta laguna y hacer que la legislación de los Estados Miembros de la Unión Europea se aproxime al Convenio del Consejo de Europa para la Represión del Terrorismo.

Artículo 3 *– Delitos ligados a actividades terroristas*

1. A efectos de la presente Decisión marco, se entenderá por:

(a) "inducción pública a la comisión de delitos de terrorismo" la distribución o difusión pública, por cualquier medio, de mensajes destinados a inducir a la comisión de cualesquiera de los actos citados en el Artículo 1, (1)(a) a (h), cuando dicha conducta, independientemente de que promueva o no directamente la comisión de delitos de terrorismo, conlleva el riesgo de comisión de uno o más de tales delitos;

(b) "reclutamiento de terroristas", la petición a otra persona de que cometa cualesquiera de los actos citados en el Artículo 1(1), o en el Artículo 2(2);

(c) "adiestramiento de terroristas" impartir instrucciones sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre otros métodos o técnicas específicos, con el fin de cometer cualesquiera de los actos citados en el Artículo 1(1), a sabiendas de que las enseñanzas impartidas se utilizarán para dichos fines.

2. Los Estados Miembros adoptarán las medidas necesarias para garantizar que entre los delitos de terrorismo se incluyan los siguientes actos dolosos:

(a) inducción pública a la comisión de delitos de terrorismo;

(b) reclutamiento de terroristas;

(c) adiestramiento de terroristas;

(d) hurto o robo con agravantes cometido con el fin de llevar a cabo cualesquiera de los actos citados en el Artículo 1(1);

(e) chantaje con el fin de cometer cualesquiera de los actos citados en el Artículo 1(1);

(f) libramiento de documentos administrativos falsos con el fin de llevar a cabo cualesquiera de los actos citados en el Artículo 1(1)(a) a (h), y en el Artículo 2(2)(b).

3. Para que un acto sea punible según lo expuesto en el apartado 2, no será necesario que se cometa realmente un delito de terrorismo.

Basándose en el Artículo 3, (1)(c), [1306] de la Decisión marco, se obliga, entre otras cosas, a los Estados Miembros a tipificar como delito la publicación de instrucciones sobre la forma de utilizar explosivos, a sabiendas de que dicha información tenga por objeto ser utilizada con propósitos relacionados con el terrorismo. Es muy probable que la necesidad de disponer de pruebas en el sentido de que el objetivo sea utilizar la información mencionada con propósitos relacionados con el terrorismo limita la aplicación de la disposición en lo que concierne a la mayoría de las instrucciones sobre la forma de utilizar armas disponibles en línea, ya que la publicación de dichas instrucciones no supone que estén directamente vinculadas con los ataques terroristas. Como la mayoría de las armas y explosivos pueden utilizarse tanto para cometer delitos "ordinarios" como delitos relacionados con el terrorismo (doble utilización), es poco probable que pueda utilizarse la información precitada para demostrar que quienes la publiquen tengan conocimiento de la forma en que dicha información se utiliza ulteriormente. Por consiguiente, habrá que tener en cuenta el contexto de la publicación (por ejemplo, en un sitio web gestionado por una organización terrorista).

Directiva sobre pornografía infantil (2011)

El primer proyecto de marco jurídico relacionado con el ciberdelito presentado tras la ratificación del Tratado de Lisboa fue la propuesta para una Directiva relativa a la lucha contra la explotación y el abuso sexual de los niños y la pornografía infantil[1307] que se adoptó en 2011.[1308] Los redactores indicaron que las tecnologías de la información permiten a los delincuentes producir y distribuir pornografía infantil con mayor facilidad[1309] y destacaron la importancia de afrontar los desafíos resultantes con disposiciones específicas. La Directiva aplica normas internacionales, tales como el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual.[1310]

Artículo 5 – *Infracciones relacionadas con la pornografía infantil*
1. Los Estados miembros adoptarán las medidas necesarias para garantizar la punibilidad de las conductas dolosas mencionadas en los apartados 2 a 6 cuando se cometan de forma ilícita.
2. La adquisición o la posesión de pornografía infantil se castigará con penas privativas de libertad de una duración máxima de al menos un año.
3. El acceso a sabiendas a pornografía infantil por medio de las tecnologías de la información y la comunicación se castigará con penas privativas de libertad de una duración máxima de al menos un año.
4. La distribución, difusión o transmisión de pornografía infantil se castigará con penas privativas de libertad de una duración máxima de al menos dos años.
5. El ofrecimiento, suministro o puesta a disposición de pornografía infantil se castigará con penas privativas de libertad de una duración máxima de al menos dos años.
6. La producción de pornografía infantil se castigará con penas privativas de libertad de una duración máxima de al menos tres años.
7. Quedará a la discreción de los Estados miembros decidir si el presente artículo será aplicable a los casos relacionados con la pornografía infantil a que se refiere el Artículo 2, letra c), inciso iii), cuando la persona que parezca ser un menor resulte tener en realidad 18 años o más en el momento de obtenerse las imágenes.
8. Quedará a la discreción de los Estados miembros decidir si los apartados 2 y 6 del presente artículo serán aplicables a los casos en que se determine que el material pornográfico definido en el Artículo 2, c), inciso iv), ha sido producido y está en posesión de su productor estrictamente para su uso privado, siempre que para su producción no se haya empleado material pornográfico al que se refiere el Artículo 2, letra c), incisos i), ii) e iii), y que el acto no implique riesgo de difusión del material.

Al igual que el Convenio, la Directiva propone la persecución por la vía penal del acceso a la pornografía infantil mediante las tecnologías de la información y de la comunicación.[1311] Esto permite a los responsables del cumplimiento de la ley enjuiciar a los delincuentes en aquellos casos en que sean capaces de demostrar que el delincuente accedió a sitios web de pornografía infantil, aunque no puedan demostrar que el delincuente descargara material. Este tipo de dificultades para recabar pruebas surgen, por ejemplo, cuando el delincuente utiliza tecnología de cifrado para proteger los ficheros descargados en sus dispositivos de almacenamiento.[1312] La memoria explicativa del Convenio relativo a la protección de la infancia indica que la disposición debería también poderse aplicar en los casos en los que el delincuente sólo ve imágenes de pornografía infantil sin descargarlas.[1313] Generalmente cuando se accede a una página web se inicia automáticamente un proceso de descarga – a menudo sin el conocimiento del usuario.[1314] Por consiguiente, la disposición es sobre todo importante cuando se consume pornografía infantil sin descargar material. Por ejemplo, puede ser el caso cuando el sitio web permite vídeo de flujo continuo y, debido a la configuración técnica de este proceso de vídeo, no almacena la información recibida sino que la descarta inmediatamente después de finalizar la transmisión.[1315]

Artículo 25 – *Medidas contra los sitios web de Internet que contengan o difundan pornografía infantil*
1. Los Estados miembros adoptarán las medidas necesarias para garantizar la rápida retirada de las páginas web de Internet que contengan o difundan pornografía infantil que se encuentren en su territorio y procurarán obtener la retirada de las páginas de esa índole que se encuentren fuera de su territorio.
2. Los Estados miembros podrán adoptar medidas para bloquear el acceso a las páginas web de Internet que contengan o difundan pornografía infantil a los usuarios de Internet en su territorio. Dichas medidas se establecerán mediante unos procedimientos transparentes y ofrecerán garantías adecuadas, sobre todo con miras a garantizar que la restricción se limite a lo necesario y proporcionado, y que los usuarios estén informados del motivo de la restricción. Estas garantías también incluirán la posibilidad de recurso a los tribunales.

Además de la persecución por la vía penal de los actos relacionados con la pornografía infantil, el borrador inicial contenía una disposición que obligaba a los Estados Miembros a imponer el bloqueo de sitios web con contenidos de pornografía infantil.[1316] Varios países europeos,[1317] así como países no europeos como China,[1318] Irán[1319] y Tailandia[1320] utilizan este tipo de planteamiento. Suscita preocupación el que ninguno de

los conceptos técnicos haya demostrado su eficacia[1321] y que este planteamiento acarrea el riesgo asociado de un exceso de bloqueos.[1322] Por ello, se modificó el bloqueo obligatorio y se dejó a los Estados Miembros que decidieran si se debía incluir la obligación del bloqueo a escala nacional.

Directiva relativa a los ataques contra los sistemas de información (2013)

En septiembre de 2010 la Unión Europea presentó una propuesta para una Directiva relativa a los ataques contra los sistemas de información,[1323] que fue adoptada en 2013.[1324] Como se ha descrito anteriormente con mayor detalle, en 2005 la UE adoptó una Decisión marco del Consejo relativa a los ataques contra los sistemas de información.[1325] La memoria explicativa de la propuesta destacaba que la intención de los redactores era actualizar y reforzar el marco jurídico para combatir el ciberdelito en la Unión Europea, respondiente a los nuevos métodos en la comisión de los delitos.[1326] Además de la persecución por la vía penal del acceso (Artículo 3), la interferencia ilegal a sistemas (Artículo 4) y la interferencia ilegal a los datos (Artículo 5), ya introducidos en la Decisión marco de 2005, el proyecto de Directiva de 2010 incluye dos delitos adicionales.

Artículo 6 – Interceptación ilegal
Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.
Artículo 7 – Instrumentos utilizados para cometer las infracciones
Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción internacional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad:
(a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los Artículos 3 a 6;
(b) una contraseña de ordenador, un código de acceso, o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Ambas disposiciones son totalmente coherentes con las correspondientes disposiciones del Convenio sobre la Ciberdelincuencia.

Relación con el Convenio del Consejo de Europa sobre la Ciberdelincuencia

Como se ha indicado anteriormente, el Convenio del Consejo de Europa sobre la Ciberdelincuencia se negoció entre 1997 y 2000. En 1999 la Unión Europea expresó su visión sobre el Convenio sobre la Ciberdelincuencia mediante una postura común.[1327] Hacía un llamamiento a los Estados Miembros para que apoyaran la redacción del borrador de Convenio sobre la Ciberdelincuencia.[1328] En aquellas fechas la propia UE carecía de competencias para elaborar un marco jurídico semejante. La ratificación del Tratado de Lisboa cambió la situación. Sin embargo, hasta la fecha, la UE no ha decidido modificar su postura respecto del Convenio sobre la Ciberdelincuencia. En el Programa de Estocolmo se destaca que la UE no sólo pide a los Estados Miembros que ratifiquen el Convenio, sino que también establece que, en la opinión de UE, debería ser un marco jurídico de referencia para luchar contra el ciberdelito en todo el mundo.[1329] Esto no implica, sin embargo, que la UE no proponga un planteamiento acabado sobre el ciberdelito, puesto que los planteamientos de la UE presentan dos ventajas importantes. En primer lugar, las directivas de la UE se deben llevar a efecto en un plazo de tiempo especificado corto, mientras que el Consejo de Europa no tiene medios para obligar a la firma y ratificación de los convenios salvo la presión política.[1330] En segundo lugar, la UE tiene la costumbre de actualizar permanentemente sus instrumentos, mientras que el Convenio del Consejo de Europa sobre la Ciberdelincuencia no se ha actualizado en los últimos 13 años.

5.2.3 Organización de Cooperación y Desarrollo Económicos [1331]

En 1983 la Organización de Cooperación y Desarrollo Económicos (OCDE) inició un estudio sobre la posibilidad de emprender una armonización internacional del derecho penal vigente para abordar el problema que representaba el delito cibernético.[1332] La OCDE publicó en 1985 un Informe que analizaba la legislación vigente y formuló propuestas para combatir el ciberdelito.[1333] La OCDE recomendó establecer una lista mínima de delitos que los países podrían tipificar en su derecho penal, por ejemplo, el ciberfraude, la ciberfalsificación, la alteración de programas y datos informáticos y la intercepción de comunicaciones. En 1990 el Comité de Políticas de Información, Informática y Comunicación (ICCP) creó un Grupo de Expertos para preparar un conjunto de directrices de seguridad de la información, que se terminaron de redactar en 1992 y fueron adoptadas ese año por el Consejo de la OCDE.[1334] Las directrices versan, entre otros aspectos, sobre la cuestión de las sanciones:

> *Resulta importante imponer sanciones por la utilización abusiva de los sistemas de información para proteger los intereses de todos aquellos que dependen de los sistemas de información, atendiendo a los daños resultantes de los ataques contra la disponibilidad, confidencialidad e integridad de esos sistema y sus componentes. Entre dichos ataques cabe citar, por ejemplo, dañar o perturbar sistemas de información insertando virus y gusanos, alterar datos, acceder ilegalmente a datos, cometer fraudes y falsificaciones por computador, y reproducir programas informáticos no autorizados. Para oponerse a tales peligros, los países han optado por responder a los actos delictivos y describirlos de diferentes formas. Cunde el acuerdo internacional sobre la necesidad de aplicar el derecho penal de los diferentes países a los delitos informáticos, como demuestra la legislación sobre el ciberdelito y la protección de datos de los países miembros de la OCDE que se ha promulgado durante las dos últimas décadas y las actividades de la OCDE y otros organismos internacionales en materia de legislación encaminada a luchar contra el ciberdelito […]. La legislación nacional debería revisarse periódicamente para garantizar que responda adecuadamente a los peligros que plantea la utilización indebida de los sistemas de información.*

Tras revisar las directrices en 1997, el ICCP creó en 2001 un segundo Grupo de Expertos, que actualizó las directrices. En 2002 se adoptó una nueva versión de las directrices de seguridad de los sistemas y redes de información en el marco de una cultura de seguridad de la OCDE como Recomendación del Consejo de la OCDE.[1335] Las directrices contienen nueve principios complementarios:

> *1) Sensibilización*
> *Los participantes deben ser conscientes de la necesidad de garantizar la seguridad de los sistemas y redes de información y de lo que deben hacer para fomentar dicha seguridad.*
> *2) Responsabilidad*
> *Todos los participantes son responsables de la seguridad de los sistemas y redes de información.*
> *3) Respuesta*
> *Los participantes deberían actuar de manera oportuna y coordinada para prevenir y detectar los incidentes de seguridad y responder a los mismos.*
> *4) Ética*
> *Cada participante debería respetar los legítimos intereses de los demás.*
> *5) Democracia*
> *La seguridad de los sistemas y redes de la información debería ser compatible con los valores esenciales de una sociedad democrática.*
> *6) Evaluación de riesgos*
> *Los participantes deberían realizar evaluaciones del riesgo.*
> *7) Diseño e implementación en materia de seguridad*
> *Los participantes deberían incorporar la seguridad como el elemento esencial en los sistemas y redes de información.*
> *8) Gestión de la seguridad*
> *Los participantes deberían adoptar un enfoque cabal respecto de la gestión de la seguridad.*

9) Reevaluación
Los participantes deberían examinar y reevaluar la seguridad de los sistemas y redes de información e introducir los cambios oportunos en las políticas, prácticas, medidas y procedimientos de seguridad.

En 2005 la OCDE publicó un Informe en el que se analizaba el impacto del correo basura en los países en desarrollo[1336] y se indicaba, igualmente, que debido al hecho que los recursos son más limitados y onerosos en los países en desarrollo, el correo basura es un problema más grave para estos países que para las naciones desarrolladas como son los Estados Miembros de la OCDE.[1337] Tras recibir una petición de la Unidad de Planificación Estratégica de la Oficina Ejecutiva del Secretario General de las Naciones Unidas, en el sentido de preparar un esbozo comparativo de las diversas soluciones legislativas nacionales en lo que concierne a la utilización de Internet con propósitos terroristas, la OCDE publicó en 2007 un Informe sobre el tratamiento legislativo del "ciberterror" en las legislaciones de los diferentes Estados.[1338] En 2008 la OCDE publicó un documento de trabajo relativo al robo de identidad en Internet.[1339] El documento facilita una visión general de las características del robo de identidad, sus diferentes formas, asuntos relacionados con las víctimas y planes para hacer cumplir la ley. Destaca que la mayoría de los países de OCDE no abordan el propio asunto mediante disposiciones específicas y que es preciso considerar si el robo de identidad debería perseguirse por la vía penal como un delito en sí mismo.[1340] En 2009 la OCDE publicó un informe sobre programas informáticos dañinos.[1341] Aunque el informe trata brevemente aspectos relativos a la persecución penal, se centra en el ámbito de los programas informáticos dañinos y de sus repercusiones económicas.

5.2.4 Foro de Cooperación Económica Asia-Pacífico [1342]

El Foro de Cooperación Económica Asia-Pacífico (APEC) identificó al ciberdelito como un importante ámbito de actividad y los dirigentes del APEC hicieron un llamamiento para promover una cooperación más estrecha entre los funcionarios que participan en la lucha contra el ciberdelito.[1343] En la Declaración adoptada por los Ministros de Comunicaciones e Información del APEC reunidos en Bangkok, Tailandia, en 2008, se destacaba la importancia de proseguir la colaboración contra el ciberdelito.[1344] Hasta la fecha, el APEC no ha facilitado ningún marco jurídico sobre el ciberdelito, aunque se ha referido a normas internacionales tales como el Convenio sobre la Ciberdelincuencia de Budapest. Además, ha estudiado a fondo la legislación nacional sobre el ciberdelito de varios países,[1345] mediante la encuesta correspondiente, y ha elaborado una base de datos con los distintos enfoques con el fin de ayudar a los países a elaborar y revisar su legislación.[1346] El cuestionario utilizado para la encuesta se basó en el marco jurídico que figura en el Convenio sobre la Ciberdelincuencia de Budapest.

Declaración relativa a la lucha contra el terrorismo (2002)

En 2002 los dirigentes del APEC presentaron una declaración relativa a la lucha contra el terrorismo y al fomento del crecimiento para promulgar leyes integrales relacionadas con el ciberdelito y desarrollar capacidades nacionales para la investigación del ciberdelito.[1347] Se comprometieron a esforzarse en elaborar antes de octubre de 2003 un conjunto integral de leyes sobre ciberdelito y ciberseguridad que fuera coherente con las disposiciones de los instrumentos jurídicos internacionales, incluidos la Resolución 55/63 de la Asamblea General de las Naciones Unidas y el Convenio sobre la Ciberdelincuencia del Consejo Europeo. Además, se comprometieron a identificar unidades nacionales de ciberdelito, determinar puntos de contacto para la asistencia internacional de alta tecnología y crear, cuando no existieran, esas capacidades y poner en marcha instituciones que intercambiaran evaluaciones de amenazas y vulnerabilidades (tales como equipos de respuesta ante emergencias informáticas) antes del mes de octubre de 2003.

Conferencia sobre legislación en materia de ciberdelito (2005)

El APEC ha organizado diversas conferencias[1348] e hizo un llamamiento para promover una cooperación más estrecha entre los funcionarios que participan en la lucha contra el ciberdelito.[1349] En 2005 el APEC organizó la Conferencia sobre Legislación en materia de Ciberdelito.[1350] Los principales objetivos de dicha Conferencia eran promover la preparación de marcos jurídicos cabales para combatir el ciberdelito y

fomentar la ciberseguridad; ayudar a las autoridades encargadas de hacer cumplir la ley a responder a los urgentes desafíos y problemas que plantea el progreso de la tecnología y promover la cooperación entre los investigadores y el ciberdelito en la región.

Grupo de Trabajo sobre telecomunicaciones e información

El Grupo de Trabajo sobre telecomunicaciones e información del APEC [1351] participó activamente en la definición de enfoques del APEC para acrecentar la ciberseguridad.[1352] En 2002 el Grupo de Trabajo adoptó la estrategia de ciberseguridad del APEC.[1353] El Grupo de Trabajo expresó su posición en cuanto a la legislación sobre el ciberdelito, remitiéndose para ello a los enfoques internacionales adoptados por instituciones que van de las Naciones Unidas al Consejo de Europa.[1354] En el contexto del Grupo de Tareas Especiales sobre ciberseguridad del Grupo de Trabajo de Telecomunicaciones e Información reunidos en dos conferencias[1355] en Bangkok, Tailandia, en 2003[1356] se abordó la experiencia adquirida en materia de elaboración de legislación relativa al ciberdelito.

5.2.5 La Commonwealth

El ciberdelito se encuentra entre los temas abordados por la Commonwealth. Las actividades se centran en particular en la armonización de la legislación. Para definir este enfoque de armonización legislativa en el seno de la Commonwealth y fomentar la cooperación internacional se tuvo presente, entre otras cosas, el hecho de que dicho enfoque requeriría la adopción de no menos de 1 272 tratados bilaterales en el marco de la Commonwealth para abordar la cooperación internacional sobre el particular.[1357]

Habida cuenta de la creciente importancia del ciberdelito, los Ministros del Interior de la Commonwealth decidieron constituir un Grupo de Expertos para preparar un marco jurídico que permitiera luchar contra el ciberdelito, basándose en el Convenio del Consejo de Europa sobre la Ciberdelincuencia.[1358] El Grupo de Expertos presentó su Informe y recomendaciones en marzo de 2002.[1359] En la fecha ulterior de dicho año se presentó el proyecto de Ley modelo sobre el ciberdelito y los actos delictivos afines.[1360] Debido a las claras instrucciones dadas a este respecto, así como al reconocimiento de que el Convenio sobre la Ciberdelincuencia es una norma internacional del Grupo de Expertos, esta Ley modelo es conforme con las normas definidas por el Convenio. Existen, sin embargo, diferencias que se tratarán con mayor detalle en el Capítulo 6.

En la reunión de 2000 los Ministros de Justicia y los fiscales generales de pequeñas jurisdicciones de la Commonwealth decidieron formar un grupo de expertos para elaborar una Ley modelo sobre pruebas digitales. La Ley modelo se presentó en 2002.[1361]

Además de la promulgación de leyes, la Commonwealth ha organizado varias actividades de formación. La red de la Commonwealth para las TI y el desarrollo (COMNET-IT) coorganizó cursos de formación sobre el ciberdelito en abril de 2007.

En 2009 se celebró en Malta el tercer programa de formación de la Commonwealth sobre un marco jurídico para las TIC, con el apoyo del Fondo de la Commonwealth para la Cooperación Técnica (CFTC). En 2011 se organizó otro curso de formación.

En 2011 la Commonwealth presentó la "Iniciativa de la Commonwealth sobre el Ciberdelito". El principal objetivo de la iniciativa fue asistir a los países de la Commonwealth en la creación de capacidades institucionales, humanas y técnicas en relación con la política, la legislación, la reglamentación, la investigación y el cumplimiento de la ley.[1362] Pretende permitir a todos los países de la Commonwealth una cooperación efectiva en la lucha mundial contra el ciberdelito.

5.2.6 Unión Africana

Durante la conferencia extraordinaria de Ministros de la Unión Africana encargados de las tecnologías de la comunicación y la información, que se celebró en Johannesburgo en 2009, los participantes abordaron distintos temas relacionados con la utilización creciente de las TIC en los países africanos. Se decidió que la Comisión de la Unión Africana –junto a la Comisión Económica para África de las Naciones Unidas– debía

elaborar un marco legal para los países africanos en el que se abordaran cuestiones tales como las transacciones electrónicas, la ciberseguridad y la protección de los datos.[1363]

En 2011, la Unión Africana ha presentado el proyecto de Convenio de la Unión Africana sobre el Establecimiento de un Marco Legal Fiable para la Ciberseguridad en África.[1364] La intención de sus redactores es fortalecer la legislación en vigor en los Estados Miembros en lo que respecta a las tecnologías de la información y la comunicación. En lo que atañe al mandato, éste no se limita al ciberdelito, sino que incluye otras cuestiones de la sociedad de la información tales como la protección de los datos y las transacciones electrónicas. El Convenio tiene un alcance más global que la mayoría de los demás enfoques regionales. Se divide en cuatro partes. La primera parte se refiere al comercio electrónico, y aborda distintos aspectos tales como la responsabilidad contractual de un proveedor electrónico de bienes y servicios[1365], la presentación de las obligaciones del tratado en formato electrónico[1366] y la seguridad de las transacciones electrónicas.[1367] La segunda parte trata de cuestiones relativas a la protección de los datos.[1368] La tercera parte se refiere a la lucha contra el ciberdelito. La Sección 1 se divide en cinco capítulos. Incluye un conjunto de seis definiciones (comunicación electrónica, datos computarizados, racismo y xenofobia en las TIC, el menor, la pornografía infantil y los sistemas informáticos).[1369]

Artículo III – 1:
A los efectos de este Convenio:
1) se entiende por comunicación electrónica cualquier transmisión al público o a parte del mismo utilizando medios de comunicación electrónicos o magnéticos, signos, señales, imágenes, sonidos o mensajes de cualquier naturaleza;
2) se entiende por datos computarizados toda representación de hechos, información o conceptos en cualquier forma que se preste al procesamiento mediante computadora;
3) se entiende por racismo y xenofobia en las TIC cualquier escrito, imagen o cualquier otra representación de ideas o teorías que aboguen por o fomenten el odio, la discriminación o la violencia contra una persona o grupo de personas por razón de raza, color, linaje, origen nacional o étnico o religión, cuando se utilice como pretexto para el racismo y la xenofobia o una motivación conexa;
4) se entiende por menor toda persona de menos de dieciocho (18) años en términos de la Convención de las Naciones Unidas sobre los Derechos del Niño;
5) se entiende por pornografía infantil todo dato, cualquiera que sea su naturaleza o forma, que representa visualmente a un menor prestándose a un acto sexual explícito, o imágenes realistas que representen a un menor prestándose a un comportamiento sexual explícito;
6) se entiende por sistema informático todo aparato, aislado o no, y una serie de aparatos interconectados utilizados parcial o totalmente para el procesamiento automatizado de datos con el objeto de ejecutar un programa.

Además, en la tercera parte se aborda la necesidad de una política nacional de ciberseguridad y de una estrategia en esta materia.[1370] El segundo Capítulo trata de aspectos generales relacionados con las medidas legales. Se incluyen normas relacionadas con las autoridades reglamentarias, los principios democráticos, la protección de la infraestructura de información esencial, la armonización, la doble criminalidad y la cooperación internacional.[1371] El tercer Capítulo aborda cuestiones relacionadas con un sistema nacional de ciberseguridad. Trata, entre otros temas, una cultura de la seguridad, el papel del gobierno, las asociaciones público-privadas, la educación y la formación y la sensibilización del público.[1372] El Capítulo cuatro está dedicado a las estructuras nacionales de vigilancia de la ciberseguridad. El Capítulo cinco trata de la cooperación internacional. La diferencia principal respecto de otros marcos regionales comparables, tales como el Convenio del Consejo de Europa sobre la Ciberdelincuencia, radica en el hecho de que –de no existir otro instrumento de cooperación internacional en esta materia– el proyecto de Convenio de la Unión Africana no puede utilizarse con este fin. La diferencia de concepto se manifiesta expresamente en los Artículos 21 y 25.

Artículo III – 1 – 21: *Cooperación internacional*
Cada Estado Miembro adoptará las medidas que considere oportunas para fomentar sobre una base bilateral o multilateral el intercambio de información y compartir datos de manera rápida, expedita y recíproca entre las organizaciones de los Estados Miembros y organizaciones similares de otros Estados Miembros encargadas de velar por el cumplimiento de la legislación en el territorio.

Artículo III – 1 – 25: *Modelo de cooperación internacional*
Cada Estado Miembro adoptará las medidas y estrategias que considere oportunas para tomar parte en la cooperación regional e internacional en materia de ciberseguridad. Las Resoluciones encaminadas a promover la participación de los Estados Miembros dentro de este marco de relaciones han sido adoptadas por un gran número de organismos gubernamentales internacionales, entre los que se incluyen las Naciones Unidas, la Unión Africana, la Unión Europea, el G8, etc. Organizaciones como la Unión Internacional de Telecomunicaciones, el Consejo de Europa, la Commonwealth y otras, han creado Marcos Modelo para la cooperación internacional que los Estados Miembros pueden adoptar como guía.

En la Sección II de la tercera parte se trata de la legislación penal sustantiva. La Sección 1 incluye la calificación como delito del acceso ilegal a un sistema informático[1373], la permanencia ilegal en un sistema informático[1374], la interferencia ilegal de un sistema[1375], la introducción ilegal de datos[1376], la intercepción ilegal de datos[1377] y la interferencia ilegal de datos.[1378] Las disposiciones presentan muchas similitudes respecto de las prácticas óptimas seguidas en otras regiones –incluidas las normativas introducidas en África. Un ejemplo de ello es la consideración como delito de la permanencia ilegal en un sistema informático, que fue introducida por el proyecto de Directiva de la ECOWAS.[1379]

Artículo III – 3:
Cada Estado Miembro de la Unión Africana adoptará las medidas legislativas oportunas para que se considere como delito penal el hecho de permanecer o de tratar de mantenerse fraudulentamente en un sistema informático o parte de él.

Un concepto nuevo a este respecto -si bien no constituye una disposición penal sino una medida conexa- que no ha sido incorporado a otros marcos regionales, es la introducción de una obligación para las empresas de someter sus productos a pruebas de vulnerabilidad.

Artículo III–7:
[...]
2) Los Estados Miembros adoptarán normas para obligar a los vendedores de productos de TIC a someter los mismos a pruebas de vulnerabilidad y garantía, que serán llevadas a cabo por expertos independientes, y a dar a conocer al público toda forma de vulnerabilidad que se encuentre en dichos productos y las medidas recomendadas para solucionarla.

En la Sección 2 se incluye la persecución por la vía penal de aspectos ligados a la falsificación informática[1380], la utilización ilegal de datos[1381], la interferencia ilegal de sistemas con intención de obtener una ventaja[1382], las violaciones de la protección de datos [1383], los dispositivos ilegales [1384] y la participación en una organización criminal.[1385]

Artículo III – 9:
Cada Estado Miembro de la Unión Africana adoptará las medidas legislativas oportunas a fin de considerar como delito penal la utilización ilícita de los datos obtenidos con pleno conocimiento de un caso.

En especial la consideración penal de la utilización ilegal de datos informáticos va más allá de las normas definidas en la mayoría de los demás instrumentos regionales.

La sección 3 trata de la persecución por la vía penal de los contenidos ilegales. El proyecto de Convenio africano introduce una persecución penal de la producción y difusión de pornografía infantil[1386], la adquisición e importación de pornografía infantil[1387], la posesión de pornografía infantil[1388], facilitar el

acceso de menores a la pornografía[1389], la difusión de material racista o xenófobo[1390], los ataques racistas perpetrados a través de sistemas informáticos[1391] , el abuso racista a través de sistemas informáticos[1392] y la denegación o aprobación del genocidio o los crímenes contra la humanidad.[1393]

En la última sección del Capítulo uno se recogen disposiciones que tratan en sentido amplio de la legislación relacionada con el ciberdelito y la admisibilidad de las pruebas electrónicas ("material electrónico escrito").

Artículo III – 23 – 1: *Legislación contra el ciberdelito*
Cada Estado Miembro adoptará las medidas legislativas que considere efectivas para definir como delitos penales materiales los actos que afecten a la confidencialidad, integridad, disponibilidad y supervivencia de los sistemas de TIC y las redes de infraestructura conexas; y adoptará las medidas de procedimiento que considere efectivas para la detención y el procesamiento de los infractores. Se pedirá a los Estados Miembros que tomen en consideración, cuando sea necesario, las opciones de redacción aprobadas en los modelos internacionales de legislación contra el ciberdelito, como es el lenguaje utilizado por el Consejo de Europa y la Commonwealth.

Artículo III – 23 – 2*:*
Cada Estado Miembro de la Unión Africana adoptará las medidas legislativas necesarias para garantizar que el material escrito con medios electrónicos se considere admisible en lo que respecta a las cuestiones penales para establecer la existencia de delitos con arreglo a la legislación penal, siempre que dicho material escrito haya sido presentado durante la audiencia y discutido ante el juez, que la persona de la que emana el material escrito pueda ser debidamente identificada, y que dicho material haya sido preparado y conservado en condiciones que permitan garantizar su integridad.

En especial en lo que respecta al Artículo III-23-1, no es posible conocer plenamente la intención de sus redactores dado que los delitos recogidos en las partes anteriores del Capítulo 1 se definen como delitos contra la integridad y disponibilidad de los sistemas informáticos. En consecuencia, no queda claro hasta qué punto el Artículo III-23-1 –en lo que respecta a la persecución por la vía penal– exige a los países que incluyan delitos distintos de los que se definen de manera más detallada en el proyecto de Convenio africano.

El Capítulo 2 incluye disposiciones destinadas a actualizar otras disposiciones habituales a fin de garantizar la aplicabilidad de las mismas cuando estén implicados sistemas y datos informáticos. Requiere a los países que establezcan una agravación de la sanción en caso de que los delitos tradicionales se cometan utilizando tecnologías de la información y la comunicación[1394]; la persecución penal de la violación de la propiedad perpetrada a través de delitos tales como el robo, el abuso de confianza o el chantaje que impliquen datos informáticos[1395]; la actualización de las disposiciones existentes de modo que incluyan los mecanismos de difusión, a fin de asegurarse de que se abarca la utilización de los medios de comunicación electrónica digitales[1396], y velen por que pueden aplicarse a los datos informáticos las disposiciones que protegen el secreto en interés de la seguridad nacional.[1397] Estas disposiciones no se incluyen en otros marcos regionales. En lo que respecta al Artículo III-24 no está claro el motivo de que el mero hecho de utilizar un sistema informático en alguna fase durante la comisión de un delito tradicional (por ejemplo el hecho de que, antes de atracar un banco, los delincuentes envíen un correo electrónico en vez de hacer una llamada telefónica) dé lugar a un agravamiento de la sentencia.

Artículo III – 24:
Cada Estado Miembro de la Unión Africana adoptará las medidas legislativas necesarias para fijar como circunstancia agravante la utilización de TIC para la comisión de delitos comunes tales como el robo, el fraude, la posesión de bienes robados, el abuso de confianza, la extorsión de dinero, el terrorismo, el blanqueo de capitales, etc.

Los Artículos III-28 a III- 35 tratan de la responsabilidad y las sanciones.

La Sección III trata de la legislación procesal. Se requiere a los Estados Miembros que hagan posible la conservación de datos informáticos[1398], la incautación de datos informáticos[1399], la conservación expedita[1400] y la intercepción de la comunicación de datos.[1401] A julio de 2014, el Convenio no había sido adoptado.[1402]

5.2.7 La Liga Árabe y el Consejo de Cooperación del Golfo [1403]

Varios países de la Región Árabe ya han tomado medidas en el plano nacional y adoptado diferentes enfoques para luchar contra el ciberdelito, o se encuentran preparando legislación al respecto.[1404] Entre estos países, cabe citar: Pakistán,[1405] Egipto[1406] y los Emiratos Árabes Unidos (EAU).[1407] Con el fin de armonizar la legislación en la región, los EAU presentaron una legislación modelo a la Liga Árabe (Ley de Orientación para la Lucha contra el Crimen de IT).[1408] En 2003, el Consejo Árabe de Ministros del Interior y el Consejo Árabe de Ministros de Justicia adoptaron la legislación.[1409] En una Conferencia celebrada en 2007, el Consejo de Cooperación del Golfo[1410] recomendó que los países que lo integran intentasen definir un enfoque común en el que se tomaran en consideración diferentes normas internacionales.[1411]

5.2.8 Organización de los Estados Americanos[1412]

Desde 1999 la Organización de los Estados Americanos (OEA) ha venido ocupándose activamente de la cuestión del ciberdelito en la región. Entre otras cosas, la Organización ha celebrado una serie de reuniones en el marco del mandato y ámbito de actuación de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA).[1413]

Grupo de Expertos Intergubernamental sobre el Delito Cibernético

En 1999, la REMJA recomendó la creación de un Grupo de Expertos Intergubernamental sobre el Ciberdelito. Se dio mandato al Grupo de Expertos para que concretara un diagnóstico de la actividad criminal dirigida contra las computadoras y la información, o que utilice computadoras como instrumento para la comisión de un delito; que concretara un diagnóstico de la legislación, las políticas y las prácticas nacionales en relación con dicha actividad; que identificara organismos nacionales e internacionales que contaran con los conocimientos técnicos especializados pertinentes; y, por último, que definiera mecanismos de cooperación dentro del Sistema Interamericano para la Lucha contra el Ciberdelito.

Recomendaciones de los Ministros de Justicia

Hasta 2010, la REMJA había celebrado ocho reuniones.[1414] En la tercera reunión, celebrada en 2000, los Ministros de Justicia o Ministros o Procuradores Generales de las Américas abordaron la cuestión del ciberdelito y se pusieron de acuerdo sobre una serie de recomendaciones.[1415] Entre dichas recomendaciones figuraba el examen de las recomendaciones formuladas en su reunión inicial por el Grupo de Expertos Gubernamentales, como contribución de la REMJA a la elaboración de la Estrategia interamericana para combatir las amenazas a la seguridad cibernética, a la que se hace referencia en la Resolución AG/RES. 1939 (XXXIII-O/03) de la Asamblea General de la OEA, y solicitar al Grupo, a través de su Presidente, a que siguiera prestando su apoyo para la elaboración de la citada estrategia. La reunión recomendó además que los Estados Miembros revisaran los mecanismos para facilitar una amplia y eficaz cooperación entre los mismos en la lucha contra el ciberdelito, y que estudiaran, cuando fuera posible, el desarrollo de una capacidad técnica y jurídica para incorporarse a la Red 24/7 creada por el G8 para la prestación de asistencia en las investigaciones sobre ciberdelitos. Se pedía a los Estados Miembros que evaluaran la conveniencia de aplicar los principios del Convenio del Consejo de Europa sobre la Ciberdelincuencia y estudiaran la posibilidad de incorporarse a dicho Convenio. Desde entonces, además de los Estados Unidos y Canadá, que firmaron el Convenio sobre la Ciberdelincuencia en 2001, el Consejo de Europa ha invitado a Chile, Costa Rica, la República Dominicana y México a integrarse en el Convenio. Por último, las recomendaciones instaban a los Estados Miembros de la OEA a revisar y, en su caso, actualizar la estructura y la labor de los órganos nacionales o los organismos encargados de velar por el cumplimiento de la ley, a fin de que se adaptaran a la naturaleza cambiante del ciberdelito, incluida la revisión de las relaciones entre los organismos que combaten el ciberdelito y los organismos policiales o que facilitan una asistencia jurídica mutua.

En 2002, la Cuarta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas recomendó que, en el marco de las actividades del grupo de trabajo de la OEA encargado del seguimiento de las recomendaciones de la REMJA, se volviera a convocar al Grupo de Expertos Intergubernamental[1416] sobre el Delito Cibernético y se le diera mandato para que llevara a cabo el seguimiento de las recomendaciones elaboradas por dicho grupo y adoptadas por la REMJA-III, y que estudiara la elaboración de una legislación modelo e instrumentos jurídicos interamericanos destinados a fortalecer la cooperación hemisférica en la lucha contra la ciberdelincuencia y en el estudio de las normas relativas a la privacidad, la protección de la información, los aspectos de procedimiento y la prevención del delito.

Las recomendaciones de la sexta reunión de Ministros de Justicia[1417] incluían un llamamiento a seguir fortaleciendo la cooperación con el Consejo de Europa, de modo que los Estados Miembros de la OEA pudieran considerar la posibilidad de aplicar los principios del Convención sobre la cibercriminalidad[1418] y de adherirse a la misma, así como de adoptar las medidas legales y de otro tipo que se requieren para su aplicación. De manera similar, la reunión recomendó que prosiguieran los esfuerzos encaminados a fortalecer los mecanismos de intercambio de información y cooperación con otras organizaciones y agencias internacionales en el ámbito del ciberdelito, tales como las Naciones Unidas, la Unión Europea, la APEC, la OCDE, el G8, la Commonwealth e Interpol, a fin de que los Estados Miembros de la OEA pudieran sacar partido de los avances logrados en dichos foros. Por otra parte, se pedía a los Estados Miembros que crearan unidades especializadas en la investigación de los ciberdelitos, designaran a las autoridades que habrían de encargarse de la coordinación a este respecto, y que aceleraran los mecanismos de intercambio de información y obtención de pruebas y, además, que fomentaran la cooperación entre las autoridades gubernamentales y los proveedores de servicios de Internet y otras empresas del sector privado en los esfuerzos para luchar contra el ciberdelito, mediante la prestación de servicios de transmisión de datos.

Dichas recomendaciones fueron reiteradas en la reunión de 2008,[1419] que recomendó además que, teniendo presente la recomendaciones adoptadas por el Grupo de Expertos Intergubernamental y por anteriores reuniones de la REMJA, los Estados consideraran la posibilidad de aplicar los principios del Convenio del Consejo de Europa sobre la Ciberdelincuencia, de adherirse al mismo y de adoptar las medidas jurídicas y de otro tipo necesarias para su aplicación. De manera similar, la reunión recomendó que prosiguieran las actividades de cooperación técnica bajo los auspicios de la Secretaría General de la OEA, a través de la Secretaría de Asuntos Jurídicos, y del Consejo de Europa, y que continuaran los esfuerzos para fortalecer el intercambio de información y la cooperación con otras organizaciones y organismos internacionales en el área del ciberdelito, a fin de que los Estados Miembros de la OEA pudieran sacar partido de los avances logrados en dichos foros. Por último, se pedía a las secretarías del Comité Interamericano contra el Terrorismo (CICTE) y de la Comisión Interamericana de Telecomunicaciones (CITEL) y al Grupo de Trabajo sobre el Delito Cibernético que siguieran elaborando medidas de coordinación y cooperación permanentes para velar por la aplicación de la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, adoptada a través de la Resolución AG/RES. 2004 (XXXIV-O/04) de la Asamblea General de la OEA.

En 2010, la REMJA abordó en su octava reunión la cuestión del ciberdelito.[1420] Se discutió brevemente acerca de la importancia de seguir consolidando y actualizando el Portal Interamericano de Cooperación en materia de Delito Cibernético a través de la página de Internet de la OEA, y de desarrollar la capacidad de los Estados para elaborar legislación y medidas de procedimiento en relación con el ciberdelito y las pruebas electrónicas. Además, en las recomendaciones de la reunión se destacó el deseo de fortalecer los mecanismos que permiten el intercambio de información y cooperación con otras organizaciones y organismos internacionales en el área del ciberdelito, tales como el Consejo de Europa, la Unión Europea, la APEC, la OCDE, el G8, la Commonwealth e Interpol, a fin de que los Estados Miembros de la OEA pudieran sacar partido de los avances logrados en dichos foros.

Durante la reunión celebrada en 2012, los Ministros de Justicia volvieron a examinar diversos aspectos del ciberdelito.[1421] Los participantes comprendieron la importancia que revisten las unidades específicas de lucha contra el ciberdelito.[1422] Además, hicieron un llamamiento a los Estados Miembros para que examinaran su ordenamiento jurídico y adoptaran la legislación necesaria en relación con el derecho procesal, la evidencia electrónica y los juicios penales.[1423] La recomendación contempla también el pedido de formulación de una estrategia de ciberseguridad que contenga medidas contra el ciberdelito. Se

abordaron asimismo otras cuestiones, entre ellas la educación de los ciudadanos y el reconocimiento de los resultados del Congreso sobre el Delito organizado por las Naciones Unidas. A diferencia de años atrás, no se pide en la recomendación la ratificación del Convenio sobre la Ciberdelincuencia pero, recurriendo a un lenguaje más delicado, se exhorta a los Estados Miembros a "reconocer la consideración prestada por algunos Estados Miembros de la OEA a la aplicación de los principios del Convenio del Consejo de Europa sobre la Ciberdelincuencia, adhiriéndose a ...".[1424]

En la reunión que tuvo lugar en 2014[1425] se adoptaron recomendaciones plenamente conformes a las de reuniones anteriores. Uno de los nuevos elementos lo constituyó el anuncio de que se tuvo en cuenta la elaboración de una legislación modelo.[1426]

5.2.9 Caribe

En diciembre de 2008, la UIT y la Unión Europea presentaron el proyecto titulado "Mejora de la competitividad en el Caribe a través de la armonización de las políticas, la legislación y los procedimientos reglamentarios relativos a las TIC" (HIPCAR) destinado a promover el sector de las TIC en la región del Caribe.[1427] Este proyecto se inscribe en el programa "ACP-Tecnologías de la información y la comunicación" y el noveno Fondo Europeo de Desarrollo. Los beneficiarios son 15 países del Caribe.[1428] El objetivo del proyecto es prestar asistencia a los países del CARIFORUM[1429] para que armonicen sus políticas y marcos jurídicos en el ámbito de las TIC.

En el marco de este proyecto, se definieron nueve áreas de trabajo[1430] en las que se desarrollaron políticas modelo y textos legislativos modelo para facilitar la formulación y armonización de la legislación en la región. El ciberdelito era una de las nueve áreas de trabajo. La elaboración del modelo de texto legislativo se desarrolló en tres fases. En la primera fase, se recopiló y examinó la legislación existente en los países beneficiarios. En paralelo, se determinaron prácticas óptimas regionales e internacionales. Se dio prioridad a las normas que fueran directamente aplicables en al menos uno de los países beneficiarios (por ejemplo la Ley modelo de la Commonwealth de 2002). No obstante, el examen también incluyó las prácticas óptimas de otras regiones, tales como la UE y África. El informe de evaluación[1431] incluía una visión general de la legislación existente, así como un análisis jurídico comparativo entre la legislación existente y las prácticas óptimas regionales e internacionales. Con el fin de preparar un análisis sobre las carencias detectadas, el informe de evaluación definió además las necesidades específicas de la región (tales como la legislación sobre el spam) que no son abordadas necesariamente por las prácticas óptimas internacionales. En un taller celebrado en 2010, se discutió el citado informe de evaluación con las partes interesadas de los países beneficiarios.[1432] Sobre la base del informe de evaluación y del análisis de carencias, las partes interesadas elaboraron unas directrices políticas modelo.

En la segunda fase, se desarrolló un texto legislativo modelo que tenía en cuenta las directrices políticas. En un segundo taller, expertos en materia de políticas, redactores legislativos y otras partes interesadas de los países beneficiarios discutieron y enmendaron el proyecto de texto legislativo modelo que fue preparado para la reunión, y lo adoptaron. El texto legislativo modelo tiene tres objetivos clave: proporciona un modelo de lenguaje específico que se ajusta a las prácticas óptimas internacionales, responde a las demandas específicas de la región, y se desarrolla teniendo presentes las prácticas en materia de redacción legislativa de la región, a fin de velar por la facilidad de su aplicación. El texto legislativo modelo incluye un conjunto complejo de definiciones, así como disposiciones penales sustantivas, incluidas las que tratan de cuestiones como el SPAM, que tienen un carácter prioritario para la región pero que no estaban necesariamente recogidas en marco regionales tales como el Convenio del Consejo de Europa sobre la Ciberdelincuencia.

15. (1) Toda persona que, de manera intencional y sin justificación legal o excusa:
a) inicie de manera voluntaria la transmisión de mensajes de correo electrónico múltiples a partir o a través de este tipo de sistema informático; o
b) utilice un sistema informático protegido para transmitir o retransmitir mensajes de correo electrónico múltiples, con la intención de engañar o inducir a error a los usuarios o a cualquier proveedor de correo electrónico o servicios de Internet, en lo que respecta al origen de tales mensajes, o
c) falsifique materialmente la información de cabecera en mensajes de correo electrónico múltiples e inicie de manera intencional la transmisión de dichos mensajes,
comete un delito susceptible de sancionarse, caso de ser hallado culpable, con una pena de cárcel por un período no superior a [periodo], o una multa no superior a [importe], o ambas.
(2) Un país podrá restringir la persecución por la vía penal en lo que respecta a la transmisión de mensajes electrónicos múltiples en el marco de relaciones de clientela o empresariales. Un país podrá decidir no perseguir por la vía penal la conducta descrita en la sección 15 (1) (a) siempre que existan otros remedios eficaces a disposición.

Por otra parte, el texto incluye disposiciones de legislación procesal (incluidos instrumentos de investigación avanzados tales como la utilización de herramientas forenses a distancia) y disposiciones relativas a la responsabilidad de los proveedores de servicios de Internet (ISP).

5.2.10 Pacífico

La UIT y la UE, en paralelo con el proyecto cofinanciado por ellas en la región del Caribe, han presentado un proyecto en el Pacífico (ICB4PAC).[1433] El proyecto tiene como finalidad –sobre la base de una solicitud formulada por los países insulares del Pacífico– proporcionar capacitación en materia de políticas y reglamentos de TIC. A este respecto, se centra en el desarrollo de la capacidad humana e institucional en el ámbito de las TIC recurriendo para ello a medidas de formación y educativas y al intercambio de conocimientos. Los beneficiarios son 15 países insulares del Pacífico.[1434] En marzo de 2011 se celebró un taller que trataba de la actual legislación en materia de ciberdelito en la región del Pacífico, que tuvo lugar en Vanuatu.[1435] Durante el taller se presentó un análisis jurídico comparativo global que facilitó una visión general acerca de la legislación en vigor en la región, así como una comparación con las prácticas óptimas seguidas en otras regiones.[1436] En agosto de 2011, y como continuación de este taller, se organizó en Samoa una conferencia para tratar de las técnicas de elaboración de las políticas y la legislación en materia de ciberdelito.[1437] Durante la conferencia se presentaron prácticas óptimas de otras regiones y se desarrollaron estructuras para lograr una legislación y una política armonizadas. Se abordaron la legislación penal sustantiva, la legislación procesal, la cooperación internacional, la responsabilidad de los proveedores de servicios de Internet (ISP), las pruebas electrónicas y las medidas de prevención del delito.

En abril de 2011, la Secretaría de la Comunidad del Pacífico organizó una conferencia relacionada con la lucha contra la ciberdelincuencia en el Pacífico.[1438] El evento fue coorganizado por el Consejo de Europa. Durante la conferencia se trataron aspectos relacionados con la legislación penal sustantiva, la legislación procesal y la cooperación internacional.[1439]

5.2.11 Comunidad de Desarrollo del África Meridional (SADC)

La Comunidad de Desarrollo del África Meridional (SADC) aprobó una legislación modelo que aplica un enfoque similar al de la Unión Africana y se refiere a cuestiones que guardan relación con la protección de datos[1440], el comercio electrónico[1441] y el ciberdelito.[1442]

5.3 Enfoques científicos e independientes

5.3.1 Proyecto de Convenio Internacional de Stanford

Un ejemplo conocido de enfoque científico en relación con la elaboración de un marco legal para enfrentarse al ciberdelito a escala mundial es el Proyecto de Convenio Internacional de Stanford (el

"Proyecto Stanford").[1443] El proyecto Stanford se elaboró como seguimiento de una conferencia organizada en los Estados Unidos por la Universidad de Stanford en 1999.[1444] La comparación con el Convenio del Consejo de Europa sobre la Ciberdelincuencia [1445], que se redactó aproximadamente en la misma época, revela numerosas similitudes. Ambos abarcan aspectos sustantivos en materia de legislación penal, legislación procesal y cooperación internacional. La diferencia más importante radica en el hecho de que los delitos e instrumentos procesales desarrollados por el Proyecto de Stanford sólo pueden aplicarse en relación con ataques contra la infraestructura de información y ataques terroristas, mientras que los instrumentos relacionados con la legislación procesal y la cooperación internacional que se mencionan en el Convenio del Consejo de Europa sobre la Ciberdelincuencia pueden aplicarse también en relación con los delitos tradicionales.[1446]

5.3.2 Protocolo Mundial sobre Ciberseguridad y Ciberdelito

Durante el Foro para la Gobernanza de Internet celebrado en Egipto en 2009, *Scholberg* y *Ghernaouti-Helie* presentaron una propuesta de Protocolo Mundial sobre Ciberseguridad y Ciberdelito.[1447] El Artículo 1-5 se refiere al ciberdelito y recomienda la aplicación de disposiciones penales sustantivas, de medidas contra el uso indebido de Internet por los terroristas, de medidas para la cooperación mundial y el intercambio de información, y de medidas en materia de derecho a la intimidad y derechos humanos.[1448] La legislación modelo que se incluye en el apéndice al Protocolo se basa en gran medida (Artículos 1-25) en una repetición literal de las disposiciones del Convenio del Consejo de Europa sobre la Ciberdelincuencia.

En junio de 2014, Scholberg presentó la 9ª edición de un proyecto de Tratado de las Naciones Unidas sobre un Tribunal Penal Internacional o Tribunal del Ciberespacio.[1449] El enfoque científico, que no se funda en un mandato oficial de las Naciones Unidas, destaca las dificultades relativas a la jurisdicción en el ciberespacio y elabora el concepto de tribunal internacional con jurisdicción limitada que es comparable al de la Corte Internacional de Justicia permanente.

5.4 Relaciones entre los enfoques legislativos regionales e internacionales

La eficacia de las normas únicas en lo que concierne a los protocolos técnicos lleva a preguntarse acerca de la forma de evitar los conflictos entre los diferentes enfoques internacionales.[1450] El Convenio del Consejo de Europa sobre la Ciberdelincuencia y la Ley modelo de la Commonwealth sobre el Ciberdelito son los marcos que aplican el enfoque más integral, ya que abarcan de manera sustantiva la legislación penal, la legislación procesal y la cooperación internacional. Pero ninguno de estos instrumentos ha sido modificado hasta la fecha para adaptarse a la evolución de la situación a lo largo de los últimos años. Además, ambos instrumentos tienen un ámbito de aplicación limitado. En el transcurso del debate celebrado con ocasión del último Congreso sobre el Delito, organizado por las Naciones Unidas, quedó de manifiesto el interés de los países por instrumentos internacionales.[1451] Esto suscita preguntas respecto de la relación entre los enfoques nacionales existentes y una posible acción en el plano internacional. Se dibujan tres escenarios posibles.

En el caso de que el nuevo enfoque jurídico definiera normas que no se ajustan a los enfoques aplicados de manera coherente en el plano regional y nacional, dicho enfoque podría tener, al menos al principio, efectos negativos sobre el necesario proceso de armonización. En consecuencia, es probable que todo nuevo enfoque analice con cuidado las normas existentes a fin de velar por la coherencia. Un ejemplo de ello es la persecución por la vía penal del acceso ilegal, que figura definido de manera similar en la Sección 5 de la Ley modelo de la Commonwealth sobre el Ciberdelito y en el Artículo 2 del Convenio del Consejo de Europa sobre la Ciberdelincuencia.

Además, un nuevo enfoque permitirá evitar incluir disposiciones cuya ejecución ya ha planteado dificultades, o incluso disuadido, a ciertos países a la hora de adherirse a un instrumento. Un ejemplo de ello es la polémica disposición del Artículo 32b del Convenio del Consejo de Europa sobre la Ciberdelincuencia. Dicha disposición recibió las críticas de la delegación rusa en la reunión de 2007 de la Comisión sobre el Ciberdelito.[1452]

Por último, el nuevo enfoque internacional podría -además de incluir las normas básicas que sean similares en los distintos enfoques jurídicos- centrarse en un análisis de las carencias a fin de determinar cuáles son

los ámbitos que aún no han sido suficientemente abordados y, de esta manera, penalizar determinados actos relacionados con los ciberdelito y definir instrumentos procesales que aún no se recogen en los instrumentos existentes. Desde 2001, han tenido lugar diversos acontecimientos de importancia. Cuando se redactó el Convenio del Consejo de Europa sobre la Ciberdelincuencia, delitos como la "peska" (phishing),[1453] el "robo de identidad"[1454] y otros relacionados con los juegos en línea y las redes sociales no revestían la importancia que han adquirido desde entonces. Un nuevo enfoque internacional podría proseguir con el proceso de armonización incluyendo nuevos delitos dotados de una dimensión transnacional.[1455]

5.5 Relación entre los enfoques legislativos internacionales y los nacionales

Como se indicó anteriormente los ciberdelitos son acciones que tienen un verdadero carácter internacional.[1456] Habida cuenta que los delincuentes pueden atacar, en general, a usuarios en todo el mundo, la cooperación internacional de los organismos encargados de hacer cumplir la ley es un requisito indispensable a la hora de realizar investigaciones internacionales en materia del delito cibernético.[1457] Estas investigaciones exigen dotarse de los medios de cooperación necesarios, así como armonizar las leyes. Habida cuenta del principio común de doble delincuencia,[1458] una cooperación eficaz requiere ante todo la armonización de una serie de disposiciones del derecho penal sustantivo de los diferentes países para impedir la constitución de refugios seguros.[1459] Por otra parte, es preciso armonizar los instrumentos de investigación para garantizar que los países que participen en una investigación internacional cuenten con los instrumentos necesarios para llevar a cabo dicha investigación. Por último, si los organismos encargados de hacer cumplir la ley desean cooperar de manera eficiente han de contar con procedimientos que sean eficaces en la práctica.[1460] La importancia de impulsar la armonización y la necesidad de hacer participar a los interesados en el proceso de armonización mundial es, pues, una tendencia, sino una necesidad, en cualquier estrategia nacional que se emprenda contra el ciberdelito.

5.5.1 Motivos que explican la popularidad de los enfoques nacionales

A pesar de la reconocida importancia de la armonización, el proceso de implementar normas jurídicas internacionales no ha llegado en modo alguno a su término.[1461] Una de las razones que explican que los enfoques nacionales desempeñen un cometido crucial en la lucha contra el ciberdelito es el hecho de que las consecuencias de estos delitos no son en todas partes las mismas. Un ejemplo que cabe dar en este sentido, es el enfoque adoptado para combatir el correo basura.[1462] El envío de correos electrónicos no deseados afecta concretamente a los países en desarrollo y es un tema que ha sido analizado en un Informe de la OCDE.[1463] A la vista de que en los países en desarrollo los recursos son más escasos y onerosos, el correo basura constituye un problema de mucha mayor magnitud en ellos que en las naciones occidentales.[1464] La adopción de un considerable número de iniciativas legislativas nacionales que no tienen por objeto, o sólo parcialmente, llevar a la práctica normas internacionales obedece ante todo a los diferentes efectos del ciberdelito, así como a la existencia de distintas estructuras y tradiciones jurídicas.

5.5.2 Soluciones internacionales frente a soluciones nacionales

En un contexto de mundialización técnica hacer de la comparación de las soluciones internacionales y las nacionales un tema de debate puede antojarse algo sorprendente, si se tiene en cuenta que todos aquéllos que desean conectarse a Internet deben utilizar los protocolos normalizados (técnicos) establecidos.[1465] Aunque la existencia de normas únicas es un requisito esencial para el funcionamiento de las redes, sigue habiendo disparidad entre las normas jurídicas, a diferencia de lo que ocurre en el caso de las normas técnicas.[1466] Habrá que preguntarse si es posible seguir aplicando enfoques nacionales, dada la naturaleza internacional del ciberdelito.[1467] Ésta es una pregunta que debemos plantearnos a la hora de considerar los enfoques nacionales y regionales de implementación de legislación no conformes con las normas internacionales vigentes. La falta de armonización en este contexto puede obstaculizar en gran medida las investigaciones internacionales, mientras que la existencia de enfoques nacionales y regionales que vayan más allá de las normas internacionales permite evitar problemas y dificultades cuando se realizan investigaciones internacionales.[1468]

Dos factores son la causa principal del creciente número de enfoques regionales y nacionales. El primero de ellos, es la velocidad legislativa. El Consejo de Europa no puede obligar a sus Estados Miembros a firmar el Convenio sobre la Ciberdelincuencia, ni forzar a los signatarios del Convenio a ratificarlo, lo que explicaría que la normalización suele considerarse un proceso lento, en comparación con los procedimientos legislativos nacionales y regionales.[1469] A diferencia del Consejo de Europa, la Unión Europea dispone de medios para obligar a los Estados Miembros a implementar sus Decisiones y Directivas Marco. Ésta es la razón por la que los países que firmaron en 2001 el Convenio sobre la Ciberdelincuencia, pero que no lo han ratificado aún, hayan aplicado, sin embargo, la Decisión marco del Consejo de Europa relativa a los ataques contra los sistemas de información adoptada en 2005.

El segundo factor tiene que ver con las diferencias nacionales y regionales. Ciertos actos sólo se han tipificado como delitos en algunos países de la región, por ejemplo, los que atentan contra los símbolos religiosos.[1470] Pese a que es poco probable que se llegue a armonizar internacionalmente las disposiciones del derecho penal aplicables a los actos que lesionan los símbolos religiosos en un país dado, un enfoque nacional podría garantizar la aplicación de las correspondientes normas jurídicas.

5.5.3 Dificultades planteadas por los enfoques nacionales

Los enfoques nacionales hacen frente a varios problemas. Por lo que hace a los delitos tradicionales, la decisión de uno o unos cuantos países de tipificar como delito ciertas conductas, puede influir en la capacidad de los delincuentes para actuar en dichos países. Con todo, cuando se trata de delitos relacionados con Internet, la capacidad de influencia sobre los delincuentes de un solo país es mucho más reducida, ya que éstos actúan conectándose a la red a partir de cualquier lugar.[1471] El fracaso de las investigaciones internacionales y de las peticiones de extradición es un fenómeno muy frecuente cuando los delincuentes actúan a partir de países que no tipifican como delito sus conductas. Así pues, uno de los objetivos clave de los regímenes jurídicos internacionales debe ser impedir la creación de refugios seguros, estipulando y aplicando normas mundiales,[1472] motivo por el cual la viabilidad práctica de los enfoques nacionales exige en general la adopción de medidas auxiliares adicionales.[1473] Las medidas auxiliares más populares son la persecución por la vía penal del usuario, además del proveedor de contenidos ilegales, así como de los servicios utilizados en la comisión de un delito.

Persecución por la vía penal del usuario, además del proveedor de contenidos ilegales

Un enfoque consiste en tipificar como delito no sólo la oferta de servicios ilegales, sino también su utilización. La tipificación como delitos de las conductas de los usuarios situados dentro de una jurisdicción es un enfoque que compensa la falta de influencia sobre el proveedor de servicios que actúa a partir de otro país.

Persecución por la vía penal de los servicios utilizados en la comisión de un delito

Un segundo enfoque es la reglamentación e incluso la tipificación, dentro de una jurisdicción de la oferta de ciertos servicios utilizados con propósitos delictivos. Esta solución va más allá del primer enfoque antes mencionado, ya que resulta aplicable a empresas y organizaciones que ofrecen servicios neutrales que se utilizan tanto para realizar actividades legales como ilegales. Un ejemplo de esta manera de proceder fue la promulgación en 2006 de una Ley en Estados Unidos con el objetivo de sancionar los juegos ilegales en Internet.[1474]

El establecimiento de la obligación de filtrar ciertos contenidos disponibles en Internet es una medida estrechamente relacionada con la anterior.[1475] Este enfoque se discutió en el marco de la célebre decisión sobre Yahoo[1476] y es objeto actualmente de debate en Israel, país en que los proveedores de acceso vendrán obligados a restringir el acceso a ciertos sitios web especializados en contenido para adultos. El intento de controlar ciertos contenidos en Internet, no se limita al contenido de adultos, ya que algunos países utilizan tecnología de filtro para restringir el acceso a sitios web en los que se discuten temas políticos. La Iniciativa OpenNet[1477] ha informado que unos veinticuatro países practican la censura en este contexto.[1478]

[1047] This includes regional approaches.

[1048] The Group of Eight (G8) consisted of eight countries: Canada, France, Germany, Italy, Japan, United Kingdom, United States and the Russian Federation. The presidency of the group, which represents more than 60 per cent of the world economy (source: http://undp.org), rotates every year. In 2014 Russia was excluded and the group meets as G7.

[1049] The idea of the creation of five subgroups – among them, one on high-tech crimes – was to improve implementation of the 40 recommendations adopted by G8 Heads of State in 1996.

[1050] The establishment of the subgroup (also described as the subgroup to the "Lyon Group") continued the efforts of the G8 (at that time still G7) in the fight against organized crime, which started with the launch of the Senior Experts Group on Organized Crimes (the "Lyon Group") in 1995. At the Halifax summit in 1995, the G8 stated: "We recognize that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from drug trafficking and other serious crimes. To implement our commitments in the fight against transnational organized crime, we have established a group of senior experts with a temporary mandate to look at existing arrangements for cooperation both bilateral and multilateral, to identify significant gaps and options for improved coordination and to propose practical action to fill such gaps". See: Chairman's Statement, Halifax G7 Summit, June 17 1995. For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1051] Regarding the G8 activities in the fight against cybercrime, see also: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1052] "Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October 1999.

[1053] 14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance

of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes – including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions – so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.

[1054] The idea of a 24/7 network has been picked up by a number of international approaches in the fight against cybercrime. One example is Article 35 of the Convention on Cybercrime:

(1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) the preservation of data pursuant to Articles 29 and 30;

c) the collection of evidence, the provision of legal information, and locating of suspects. […]

[1055] *Jean-Pierre Chevenement*, the French Minister of the Interior, stated: "Now that the G8 has provided the impetus, it's vital that we formalize the new legal rules and procedures for cooperation in a legal instrument applying world-wide. For France, the negotiations under way in the Council of Europe on a Convention on Cyber-Crime are of fundamental importance for several reasons. The draft currently under discussion defines the offences which all States would have to recognize. It goes on to propose ways in which they could cooperate, taking up, for example, the idea of national contact points. It also proposes extradition procedures. In short, this agreement is an essential instrument, which France wants to see concluded within a reasonable period of time. The important thing about these negotiations is that the countries involved include some major countries outside the Council of Europe and that, once signed, this convention will be opened for signature by all States wishing to accede to it. The idea is in fact to get a convention which applies world-wide so that there can be no more "digital havens" or "Internet havens" in which anyone wanting to engage in shady activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must never lose sight of the fact that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate."

[1056] G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

[1057] The experts expressed their concerns regarding implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible"; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001.

[1058] G8 Justice and Home Affairs Communiqué, Washington DC, 11 May 2004.

[1059] G8 Justice and Home Affairs Communiqué Washington DC, 11 May 2004:10. "Continuing to Strengthen Domestic Laws: To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."

[1060] The participants expressed their intention to strengthen the instruments in the fight against cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors". See: www.g7.utoronto.ca/justice/justice2006.htm.

[1061] Regarding the topic of cyberterrorism, see above: § 2.9.1. In addition, see: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis,* Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeldt*, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

[1062] The summit declaration calls for measures in the fight against cyberterrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists". For more information, see: http://en.g8russia.ru/docs/17.html.

[1063] For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1064] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 6, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1065] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 7, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1066] G8 Summit 2010 Muskoka Declaration, 2010, available at: www.g7.utoronto.ca/summit/2010muskoka/communique.html.

[1067] See press release from 30.5.2011, available at: www.eg8forum.com/en/documents/news/Final_press_release_May_30th.pdf.

[1068] See G8 Declaration, Renewed Commitment for Freedom and Democracy, available at: www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html.

[1069] The United Nations (UN) is an international organization founded in 1945. It had 192 Member States in 2010.

[1070] A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.

[1071] A/RES/45/121, adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.

[1072] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at www.uncjin.org/Documents/EighthCongress.html.

[1073] See the preface to the Optional Protocol.

[1074] See Art. 2.

[1075] See especially the background paper: Crimes related to computer networks, A/CONF.187/10.

[1076] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1077] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 174, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1078] "The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks".

[1079] A/RES/55/63. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

[1080] A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

[1081] A/RES/57/239, on Creation of a global culture of cybersecurity; A/RES/58/199, on Creation of a global culture of cybersecurity and the protection of critical information infrastructure.

[1082] Measures to Combat Computer-related Crime, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, A/CONF.203/14.

[1083] Committee II Report, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19.

[1084] Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

[1085] 30(d): "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

[1086] Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

[1087] See in this context especially the background paper prepared by the secretariat.

[1088] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1089] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1090] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1091] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1092] *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

[1093] Regarding the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

[1094] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

[1095] Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[1096] Resolutions 55/63 and 56/121

[1097] Resolutions 57/239 and 58/199.

[1098] Draft topics for consideration in a comprehensive study on the impact o fand response to cybercrime, 2010, UNODC, UNODC/CCPCJ/EG.4/2011/2.

[1099] Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive studay of the problem of cybercrime held in Vienna from 17 to 21 January 2011, UNODC/CCPCJ/EG.4/2011/3.

[1100] www.unodc.org/cybercrime-study/

[1101] UNODC Press Release (26.01.2012) available at: www.unodc.org/unodc/en/frontpage/2012/January/unodc-chief-announces-a-comprehensive-study-on-cybercrime.html

[1102] United Nations Commission on Crime Prevention and Criminal Justice.

[1103] www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[1104] Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, page X.

[1105] Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, S. XIX.

[1106] UNODC/CCPCJ/EG.4/2013/3.

[1107] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1108] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1109] Commission on Crime Prevention and Criminal Justice, Report on the twenty-thrid session (13 December 2013 and 12 to 16 May 2014), Economic and Social Council, Official Records,2014, Supplement No. 10

[1110] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1111] Development in the Field of Information and Telecommunications in the Context of International Security, 2013, available at: www.un.org/disarmament/topics/informationsecurity/

[1112] See: Development in the Field of Information and Telecommunications in the Context of International Security, 2013, page 1.

[1113] The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf.

[1114] Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

[1115] The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council.

[1116] CCPCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process in the development of the resolution and for an overview of different existing legal instruments, see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, see: www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

[1117] The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

[1118] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

[1119] For more information on the development process and the work of the intergovernmental expert group, see: Results of the second meeting of the Intergovernmental Expert Group to Prepare a study on Fraud and the Criminal Misuse and Falsification of Identity, Commission on Crime Prevention and Criminal Justice, 16th session, 2007, E/CN.15/2007/8, page 2..

[1120] ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf..

[1121] Regarding Internet-related ID-theft, see above: § 2.8.3, and below: § 6.2.16.

[1122] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.

[1123] ECOSOC Resolution 2004/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

[1124] Reports related to the activities of the working group are published. See: First meeting of the Core Group of Experts on Identity-Related Crime, Courmayeur Mont Blanc, Italy, 29-30 November 2007, available at: www.unodc.org/documents/organized-crime/Courmayeur_report.pdf (last visited: October 2008); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, available at: www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf (last visited: October 2008).

[1125] See for example: Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, 2009, E/CN.15/2009/CRP.13.

[1126] ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

[1127] For further information see: www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html.

[1128] The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. For more information, see: www.itu.int.

[1129] WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

[1130] WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

[1131] For more information on Action Line C5, see: www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, available at: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

[1132] For more information, see www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1133] www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1134] The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building, international cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1135] See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

[1136] www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; See: *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2009, Issue 7, page 533.

[1137] See, in this context: *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1, page 7 *et seq.*

[1138] Global Strategic Report, Chapter 1.6.

[1139] Global Strategic Report, Chapter 1.7.

[1140] Global Strategic Report, Chapter 1.10.

[1141] Global Strategic Report, Chapter 1.11.

[1142] 23-25 November 2009 (Santo Domingo, Dominican Republic): www.itu.int/ITU-D/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa; 15-18 July 2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on

Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP); 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP).

[1143] Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/

[1144] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

[1145] Information about the project are available at: www.itu.int/ITU-D/treg/projects/itu-ec/index.html

[1146] The adoption took place during the 3rd Ordinary General Assembly of the West African Telecommunications Regulators Assembly.

[1147] www.itu.int/ITU-D/treg/projects/itu-ec/ECOWAS_MINISTERS_ADOPTS_GUIDELINES_FOR_TELECOMMUNICATION_MARKET_AT_ABUJA.pdf

[1148] http://news.ecowas.int/en/presseshow.php?nb=2&lang=en&annee=2007

[1149] Angla, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cap-Verde, Chad, Congo, Cote d'Ivoire, Eritrea, Gabon, Gambia, Ghana, Guinea, Guinea Equatorial, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Uganda, Central African Republic, Democratic Republic of Congo, Rwanda, Sao Tome-e-Principe, Senegal, Seychelles, Sierra Leone, South Africa, Swaziland, Tanzania, Togo, Zambia and Zimbabwe.

[1150] ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 5.

[1151] The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

[1152] CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

[1153] Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

[1154] Detailed information about requested support, activities and documents are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

[1155] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[1156] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

[1157] The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

[1158] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

[1159] The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD and UN. Source: *Nilsson* in *Sieber*, Information Technology Crime, page 577.

[1160] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1161] *Nilsson* in Sieber, Information Technology Crime, page 576.

[1162] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

[1163] Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

[1164] The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.

[1165] Decision CDPC/103/211196. CDPC explained its decision by pointing out the international dimension of computer crimes: "By connecting to communication and information services, users create a kind of common space, called "cyber-space", which is used for legitimate purposes, but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."

[1166] Explanatory Report of the Convention on Cybercrime (185), No. 10.

[1167] The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

[1168] For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*,
The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[1169] Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

[1170] Albania, Armenia, Australia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Malta, Mauritius, Moldova, Montenegro, Netherlands, Norway, Panama, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, United States.

[1171] The need for a ratification is laid down in Article 36 of the Convention on Cybercrime:

> *Article 36 – Signature and entry into force*
>
> *1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.*
>
> *2)This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.*

[1172] Australia, Dominican Republic, Mauritius and Philippines.

[1173] Argentina, Australia, Chile, Colombia, Costa Rica, Dominican Republic, Israel, Mauritius, Mecixo, Panama, Philippines, Senegal.

[1174] Argentina, Chile, Colombia, Costa Rica, Dominican Republic, Israel, Mexico, Morocco, Philippines and Senegal.

[1175] Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention on Cybercrime shall be distributed to all Interpol member countries in the four official languages", available at:
www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and

56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf; APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 19, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[1176] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[1177] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention on Cybercrime."

[1178] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1179] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1180] See Art. 3 of the Fourth Draft Convention, PC-CY (98) Draft No. 4, 17.04.1998.

[1181] Albania, Andorra, Armenia, Austria, Belgium, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Spain, Sweden, Switzerland, South Africa, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine.

[1182] Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Finland, France, Germany, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine.

[1183] Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp. The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf.

[1184] For more information on the achievements and shortcomings see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

[1185] Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

[1186] Draft Electronic Crime Act 2006.

[1187] Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

[1188] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1189] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

[1190] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

[1191] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, page 18

[1192] Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

[1193] Albania, Croatia,

[1194] Estonia, Hungary.

[1195] Lithuania, Romania, Slovenia, The former Yugoslav Republic of Macedonia.

[1196] Bulgaria, Cyprus, Denmark.

[1197] Armenia, Bosnia and Herzegovina, France, Netherlands, Norway, Ukraine, United States.

[1198] Finland, Iceland, Latvia.

[1199] Italy, Slovakia.

[1200] Germany, Moldova, Serbia.

[1201] Azerbaijan, Montenegro, Portugal, Spain.

[1202] United Kingdom, Switzerland

[1203] Austria, Belgium, Georgia, Malta, Australia and Japan.

[1204] Czech Republic, Dominican Republic and Mauritius.

[1205] See Sec. 202a of the German Penal Code.

[1206] Country profiles can be downloaded at www.coe.int/cybercrime.

[1207] For details on the requirements, see: *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025, available at: www.fas.org/sgp/crs/misc/97-1025.pdf.

[1208] *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1209] See in this context, for example: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4,

[1210] See Art. 44 Convention on Cybercrime.

[1211] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1212] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1213] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1214] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1215] *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

[1216] Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1217] See *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009, page 127-150.

[1218] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

[1219] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.8.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq*.

[1220] Criticism about the lack of coverage of such topics in the existing instruments: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07, page 7.

[1221] See: Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, COM(2010) 517, page 6.

[1222] *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1223] See Art. 44 Convention on Cybercrime.

[1224] See Art. 37 Convention on Cybercrime.

[1225] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1226] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1227] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7)..

[1228] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1229] See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[1230] See: Art. 41 Salvador Declaration on Comprehensive Strategies for Global Challenges, 2010. Available at: www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

[1231] See ITU Resolution 130 (Rev. Guadalajara, 2010).

[1232] San Marino did not even sign the Convention. Andorra, Monaco and Lichtenstein signed but never ratified the Convention.

[1233] See Explanatory Report to the Convention on Cybercrime, No. 298.

[1234] *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

[1235] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

[1236] ICB4PAC Workshop on Concepts and Techniques of Developing CyberCrime Policy and Legislation, Apia, Samoa 22-25 August 2011.

[1237] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, No. 47.

[1238] Model Law on Computer and Computer Related Crime, LMM(02)17. For more information about the Model Law see:

[1239] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1240] For further information and references on electronic evidence see blow: § 6.5.

[1241] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[1242] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1243] Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, Moldova,Monaco, Montegegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Sweden, The former Yugoslav Republic of Macedonia, Turkey, Ukraine and United Kingdom.

[1244] Albania, Andorra, Austria, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Greece, Ireland, Italy, Latvia, Luxemburg, Malta, Moldova, Montegegro, Netherlands, Portugal, Romania, Russia, San Marino, Serbia, Slovenia, Spain, Sweden, Sweden, The former Yugoslav Republic of Macedonia and Turkey.

[1245] For more details, see: *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

[1246] Cybercrime Convention Committee (T-CY)

[1247] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3.

[1248] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

[1249] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

[1250] EDRI, Transborder Data Access: Strong Criticsm on planst o extend CoE Cybercrime Treaty, 5.6.2013, available at: www.edri.org/edrigram/number11.11/transborder-data-access-cybercrime-treaty.

[1251] Report of the Transborder Group for 2013, Cybercrime Convention Committee, T-CY (2013) 30.

[1252] 1: transborder access with consent but without the limitation to data stored "in another Party"; 2: transborder access without consent but with lawfully obtained credentials; 3: transborder access without consent in good faith or in exigent or other circumstances; 4: extending a search from the original computer to connected systems without the limitation "in its territory"; 5: the power of disposal as connecting legal factor.

[1253] T-CY Guidance Note #3 Transborder Access to Data (Article 32), Cybercrime Convention Committee, T-CY (2013) 7E.

[1254] The European Union is a supranational and intergovernmental union with, as at today, 27 Member States from the European continent.

[1255] One example is the EU funded HIPCAR project on Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures. For more information, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1256] *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007, page 69 *et seq.*; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007, page 15 *et seq.*; *Ambos*, Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections, Maastricht Journal of European and Comparative Law, 2005, 173 *et seq.*

[1257] See: *Satzger*, International and European Criminal Law, 2005, page 84 for further reference.

[1258] Title VI, Treaty on European Union.

[1259] Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

[1260] Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03. See in this context: *Gercke.*

[1261] Communication from the Commission to the European Parliament and the Council on the implications of the Court's judgement of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583..

[1262] Decision of the Court of Justice of the European Communities, 23.10.2007, Case C-440/05; See in this context: *Eisele*, Anmerkung zum Urteil des EuGH C 440/05, JZ 2008, page 251 *et seq.*; *Fromm*, Anmerkung zum Urteil des EuGH C 440/05, ZIS 2008, page 168 *et seq.*

[1263] ABl. 2007 C 306, 1.

[1264] Regarding the impact of the reform on the harmonization of criminal law, see: *Peers*, EU criminal law and the Treaty of Lisbon, European law review 2008, page 507 *et seq.*; *Zeder*, EU-minimum rules in substantive penal law: What will be new with the Lisbon Treaty?, ERA Forum 2008, page 209 *et seq.*

[1265] Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009.

[1266] Regarding the Hague Programme, see: *Braum*, Das Haager-Programm der Europaeischen Union: falsche und richtige Schwerpunkte europaeischer Strafrechtsentwicklung in *Joerden/Szwarc*, Europaeisierung des Strafrechts in Deutschland und Polen, 2007, page 11 *et seq.*

[1267] See: Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009, No. 3.3.1.

[1268] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1269] See: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487, page 24.

[1270] Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1271] Communication of 8 December 1999 on a Commission initiative for The Lisbon Special European Council, 23 and 24 March 2000 – *e*Europe – An information society for all – COM 1999, 687. See in this regard also: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1272] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26.1.2001, COM(2000) 890

[1273] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1274] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1275] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 31.

[1276] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 32.

[1277] Network and Information Security – A European Policy approach – adopted 6 June 2001.

[1278] For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

[1279] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1280] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1281] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[1282] See Directive 2000/31/EC, recital 1 *et seq.*

[1283] For more details, see below: § 6.

[1284] *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 *et seq.*

[1285] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1286] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1287] Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA).

[1288] See Art. 4 of the Framework Decision.

[1289] This instrument was in the meantime substituted by the 2012 Directive (see below).

[1290] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

[1291] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1292] See the explanation of the Framework Decision in the Proposal For A Council Framework Decision on combating serious attacks against information systems, No. 1.6.

[1293] Council Framework Decision 2005/222/JHA of 24.02.2005 on attacks against information systems, recital 5.

[1294] Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

[1295] See below.

[1296] *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, page 286.

[1297] European Court of Justice, Case C-275/06.

[1298] See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

[1299] In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001..

[1300] Data Retention Directive, recital 6.

[1301] Data Retention Directive, recital 6.

[1302] Case C-301/06.

[1303] Judgement in Joined Cases C-293/12 and C-594/12.

[1304] Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[1305] "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

[1306] "Training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

[1307] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2010) 94.

[1308] Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[1309] See: Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, page 2.

[1310] ETS 201. For more information see: § 5.2.1

[1311] See Art. 5, No. 3, of the Draft Directive.

[1312] Regarding the challenges related to the use of encryption technology, see above: § 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1313] See Explanatory Report to the Convention on the Protection of Children, No. 140.

[1314] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180.

[1315] Regarding the underlying technology, see: *Austerberrry*, The Technology of Video & Audio Streaming, 2004, page 130 *et seq.*; *Wu/Hou/Zhu/Zhang/Peha*, Streaming Video over the Internet: Approaches and Directions, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 3, 2001, page 282 *et seq.*; *Garfia/Pau/Rico/Gerla*, P2P Streaming Systems: A Survey and Experiments, 2008.

[1316] Regarding filter obligations/approaches, see*: Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide.

[1317] See *Gercke*, The Role of Internet Service Providers in the Fight against Child Pornography, Computer Law Review International, 2009, page 69 *et seq.*

[1318] *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1319] *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1320] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55.

[1321] *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

[1322] *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009, page 131 *et seq.*; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page ix.

[1323] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

[1324] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Deciion 2005/222/JHA.

[1325] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1326] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, page 3.

[1327] 1999/364/JHA: Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the draft Convention on Cyber Crime held in the Council of Europe.

[1328] See Art. 1 of the Common Position.

[1329] See in this context: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1330] See *Gercke*, The Slow Awake of a Global Approach against Cybercrime, Computer Law Review International, page 145.

[1331] The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is based in Paris. For more information, see: www.oecd.org.

[1332] *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1333] OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

[1334] In 1992, the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information Systems. The 24 OECD member countries adopted the guidelines later.

[1335] Adopted by the OECD Council at its 1037th session on 25 July 2002. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

[1336] Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1337] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1338] The report is available at: www.legislationline.org/upload/lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

[1339] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1340] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, page 5, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1341] Computer Viruses and other malicious software: A threat to the internet economy, OECD, 2009.

[1342] The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties. It has 21 members.

[1343] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1344] The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

[1345] Australia, Brunei Darussalam, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Philippines, Singapore, Chinese Taipei, Thailand and United States.

[1346] See: Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

[1347] APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, on 26 October 2002. Regarding national legislation on cybercrime in the Asian-Pacific region, see: *Urbas*, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf. See also in this regard: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1348] APEC TEL-OECD Malware Workshop (2007); APEC TEL and ASEAN Workshop on Network Security (2007); Workshop on Cyber Security and Critical Information Infrastructure Protection (CIIP); APEC Symposium on Spam and Related Threats (2007); APEC Best Practices In International Investigations Training Sessions (2004); Conference on cybercrime for the APEC region (2005); Conference on cybercrime for the APEC region (2004); Conference on cybercrime for the APEC region (2003); Cybercrime legislation training workshops (several, 2003); Judge and Prosecutor Capacity Building Project.

[1349] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1350] Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar, APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

[1351] "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws."

[1352] The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1353] For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/som/mtg/2002/word.Par.0204.File.v1.1

[1354] See: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1355] Cybercrime Legislation & Enforcement Capacity Building Workshop, and Electronic Commerce Steering Group Meeting.

[1356] 2003/SOMIII/ECSG/O21.

[1357] *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.

[1358] See: Model Law on Computer and Computer Related Crime, LMM(02)17, Background information.

[1359] See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

[1360] Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1361] Draft Model Law on Electronic Evidence, LMM(02)12.

[1362] For more information see: www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf.

[1363] For more information see: African Union, Oliver Tambo Declaration, Johannesburg 2009, available at: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf.

[1364] The Draft Convention is available for download at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf.

[1365] See Part 1, Sec. II, Ch. II.

[1366] See Part 1, Sec. IV.

[1367] See Part 1, Sec. V.

[1368] See Part 2.

[1369] Art. III-1.

[1370] Part 3, Chaptr 1, Art. 1 and Art. 2.

[1371] Art. III-1-1 to Art. III-1-7

[1372] Art. III-1-8 to Art. III-1-12.

[1373] Art. III-2.

[1374] Art. III-3.

[1375] Art. III-4.

[1376] Art. III-5.

[1377] Art. III-6.

[1378] Art. III-7 1).

[1379] For more information see below: § 6.2.2.

[1380] Art. III-8.

[1381] Art. III-9.

[1382] Art. III-10.

[1383] Art. III-11.

[1384] Art. III-12.

[1385] Art. III-13.

[1386] Art. III-14.

[1387] Art. III-15.

[1388] Art. III-16.

[1389] Art. III-17.

[1390] Art. III-19.

[1391] Art. III-20.

[1392] Art. III-21.

[1393] Art. III-22.

[1394] Art. III-24.

[1395] Art. III-25.

[1396] Art. III-26.

[1397] Art. III-27.

[1398] Art. III-36.

[1399] Art. III-37.

[1400] Art. III-39.

[1401] Art. III-41.

[1402] Regarding reasons for this delay see for example: Gareth van Zyl, Adoption of flawed AU cybersecurity convention postponed, IT Web Africa, 21.01.2014, available at: www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed.

[1403] The League of Arab States is a regional organization, with currently 22 members.

[1404] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1405] Draft Electronic Crime Act 2006.

[1406] Draft Law on Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1407] Law No. 2 of 2006, enacted in February 2006.

[1408] Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1409] Decision of the Arab Justice Ministers Council, 19th session, 495-D19-8/10/2003.

[1410] Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE.

[1411] Non-official translation of the recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18 June 2007, Abu Dhabi:

1) Calling for the adoption of a treaty by the Gulf Cooperation Council (GCC) countries, inspired by the Council of Europe Cybercrime convention, to be expanded later to all Arab countries.

2) Calling all GCC countries to adopt laws combating cybercrime inspired by the model of the UAE cybercrime Law.

3) Calling for the adoption of laws in relation to procedural matters such as seizure, inspection and other investigation procedures for such special type of crimes.

5) Providing trainings to inspection and law enforcement officials on dealing with such crimes.

6) Providing sufficient number of experts highly qualified in new technologies and cybercrime particularly in regard to proof and collecting evidence.

7) Recourse to the Council of Europe's expertise in regard to combating cybercrime particularly in regard to studies and other services which would contribute in the elaboration and development of local countries legislation in GCC countries.

8) Harmonization of the legislations in Arab and particularly GCC countries in regard to basic principles in combating this type of crimes on both procedural and substantive level.

9) Increasing cooperation between public and private sectors in the intent of raising awareness and exchange of information in the cybercrime combating field.

[1412] The Organization of American States is an international organization with 34 active Member States. For more information, see: www.oas.org/documents/eng/memberstates.asp.

[1413] For more information, see: www.oas.org/juridico/english/cyber.htm, and the Final report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations, at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

[1414] The conclusions and recommendation of the meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas on Cyber Crime are available at: www.oas.org/juridico/english/cyber_meet.htm.

[1415] The full list of recommendations from the 2000 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber. The full list of recommendations from the 2003 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

[1416] The OAS General Secretariat, through the Office of Legal Cooperation of the Department of International Legal Affairs, serves as the technical secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: www.oas.org/dil/department_office_legal_cooperation.htm.

[1417] In addition, the Working Group of Governmental Experts on cybercrime recommended that training be provided in the management of electronic evidence and that a training programme be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G8 to help conduct cybercrime investigations. Pursuant to such recommendation, three OAS regional technical workshops were held during 2006 and 2007, the first being offered by Brazil and the United States, and the second and third by the United States. The list of technical workshops is available at: www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

[1418] In the meantime, OAS has established joint collaboration with the Council of Europe and attended and participated in the 2007 Octopus Interface Conference on Cooperation against cybercrime. See: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

[1419] Conclusions and Recommendations of REMJA-VII, 2008, are available at: www.oas.org/juridico/english/cybVII_CR.pdf.

[1420] Conclusions and Recommendations of REMJA-VIII, 2010, are available at: www.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf.

[1421] The seventh meeting of the working group on Cybercrime took place from 6-7 February 2012.

[1422] Recommendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VII/doc.6/12rev.1.

[1423] Recommendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VII/doc.6/12rev.1.

[1424] Recommendation of the Working Group: OEA/Ser.K/ XXXIV, CIBER-VII/doc.6/12rev.1.

[1425] The eighth meeting oft he Working Group on Cyber-Crime took place from 27-28 February 2014.

[1426] mendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VIII/doc.4/14rev.1.

[1427] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1428] The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

[1429] CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

[1430] Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

[1431] The assessment report is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html

[1432] The workshop was held in Saint Lucia on 8-12 March 2010. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1433] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[1434] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

[1435] More information about the event are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/port_vila/port_vila.html.

[1436] The assessment report will be made available through the project website.

[1437] www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/samoa/samoa.html.

[1438] More information about the event are available at: www.spc.int/en/component/content/article/704-responding-to-cybercrime-threats-in-the-pacific.html.

[1439] An overview about the output of the conference is available at: and www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_tonga_apr_11/AGREED_Cybercrime_Workshop_Outcomes.pdf.

[1440] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[1441] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

[1442] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_cybercrime.pdf

[1443] *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

[1444] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at:

www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf ; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. ABA International Guide to Combating Cybercrime, 2002, page 78.

[1445] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq*.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq*.

[1446] Regarding the application of Art. 23 *et seq.* with regard to traditional crimes, see: Explanatory Report to the Convention on Cybercrime, No. 243.

[1447] *Schjolberg*, A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, twelfth UN Crime Congress, 2010, A/CONF.213, page 3, available at: www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

[1448] *Schjolberg/Ghernaouti-Helie*, A Global Protocol on Cybersecurity and Cybercrime, 2009, available at: www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

[1449] Available online: www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf.

[1450] For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

[1451] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations, No. 41 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations, No. 47 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations, No. 29 (page 7); "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations, No. 40 (page 10).

[1452] Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/6_cybercrime/t%2Dcy/FINAL%20T-CY%20_2007_%2003%20-%20e%20-%20Report%20of%20the%20meeting1.pdf.

[1453] The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions, see *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon of phishing, see *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, available at: www.usdoj.gov/opa/report_on_phishing.pdf. and the Attorney General of the United States, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

[1454] For an overview of the different legal approaches, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm. Regarding the economic impact, see for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1455] There are two aspects that need to be taken into consideration in this context: To avoid redundancy, a new approach should focus on offences that are not intended to be covered within further amendments of the Convention on Cybercrime. The second aspect is related to the difficulties in finding a common position all countries can agree on. Based on the experiences with the negotiations of the Convention on cybercrime, it is likely that negotiations of criminalization that go beyond the standards of the Convention will run into difficulties.

[1456] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1457] Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cybercrime, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 35 *et seq*., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 1 *et seq*., available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1458] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties which the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and surrender procedures between Member States (2002/584/JHA).

[1459] Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1460] See Convention on Cybercrime, Articles 23-35.

[1461] See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq*.

[1462] See above: § 2.6.7.

[1463] See Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1464] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1465] Regarding the network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1466] See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper, No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[1467] Regarding the international dimension, see above: § 3.2.6.

[1468] With regard to the Convention on Cybercrime, see: Explanatory Report to the Convention on Cybercrime, No. 33.

[1469] Regarding concerns related to the speed of the ratification process, see *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 144.

[1470] See below: § 6.2.10.

[1471] See above: §§ 3.2.6 and 3.2.7.

[1472] The issue has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 stipulates: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 Ten-Point Action Plan highlights: "There must be no safe havens for those who abuse information technologies".

[1473] For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*

[1474] For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm. For more information, see below: § 6.2.11.

[1475] Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/*; Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches,
see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf; *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

[1476] See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *www.juriscom.net/en/uni/doc/yahoo/poullet.htm*; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

[1477] The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

[1478] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

6 Respuesta jurídica

En el presente Capítulo se ofrecerá una visión general de la respuesta jurídica dada al fenómeno de la ciberdelincuencia, mediante la explicación de los enfoques jurídicos para la persecución de ciertos actos por la vía penal.[1479] Siempre que sea posible, se expondrán enfoques internacionales y, cuando no se disponga de ellos, se presentarán ejemplos en el ámbito nacional o regional.

6.1 Definiciones

Bibliografía (seleccionada): *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.; *Macagno*, Definitions in Law, Bulletin Suisse de Linguistique Appliquée, Vol. 2, 2010, page 199 et seq, available at: http://ssrn.com/abstract=1742946.

6.1.1 El cometido de las definiciones

Las definiciones son un elemento habitual de los distintos marcos jurídicos nacionales y regionales. Sin embargo, es importante distinguir entre las diferentes funciones que desempeñan tales definiciones. En general, en el ámbito del Derecho, es posible dividir las definiciones en dos clases: las definiciones descriptivas y las definiciones jurídicas.[1480] Las definiciones descriptivas se utilizan para explicar el significado de palabras ambiguas, mientras que las definiciones jurídicas tienen como finalidad remitir al sujeto de derecho a una definición específica de una palabra.[1481] En la visión general que se ofrece a continuación, no se distingue entre ambos tipos de definición.

Los marcos jurídicos y modelos de legislación regionales abordan de maneras distintas no sólo el tipo sino también la cantidad de definiciones. El Convenio sobre la Ciberdelincuencia, por ejemplo, sólo incluye cinco definiciones,[1482] mientras que el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia contiene veinte.

6.1.2 Proveedor de acceso

Los proveedores de acceso desempeñan un importante papel, ya que hacen posible que los usuarios se conecten a Internet. En la legislación sobre cibercriminalidad, el término "proveedor de acceso" se utiliza tanto en lo que respecta a la regulación de la responsabilidad jurídica[1483] como en lo que atañe a la implicación del mismo en las investigaciones – en especial la interceptación legal de las comunicaciones.[1484] En el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia se ofrece una definición del término.

> ***Definiciones***
> ***3.*** *(1) Se entiende por proveedor de acceso toda persona física o jurídica que presta un servicio de transmisión electrónica de datos, mediante la transmisión de la información facilitada por o a un usuario del servicio de una red de comunicaciones, o que proporciona acceso a una red de comunicaciones.*
> *[…]*

Se trata de una disposición amplia, ya que abarca tanto a los proveedores comerciales como a las empresas que se limitan a proporcionar acceso a los empleados y operadores de las redes privadas. Aunque este criterio resulta útil para lograr una amplia aplicación de las normas en materia de responsabilidad jurídica, la definición podría cuestionarse en caso de que se aplicara también al procedimiento legal (algo que no pretendían los redactores del Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia).

6.1.3 Proveedor de recursos de almacenamiento

Los proveedores de recursos de almacenamiento prestan un importante servicio al incrementar la velocidad de acceso a los contenidos populares. En lo que respecta a la necesidad de regular la responsabilidad

jurídica[1485] de los proveedores de recursos de almacenamiento, los redactores del Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia decidieron incluir una definición.

> ***Definiciones***
> ***3.*** *[...]*
> *(2) Se entiende por proveedor de recursos de almacenamiento toda persona física o jurídica que presta un servicio electrónico de transmisión de datos mediante el almacenamiento automático, intermedio y temporal de información, con el único objeto de mejorar la eficacia de la transmisión hacia adelante de la información a otros usuarios del servicio a petición de los mismos;*
> *[…]*

Al igual que ocurre con su definición de proveedor de acceso, los redactores no limitan la aplicación de la disposición a las operaciones comerciales. En consecuencia, la disposición también abarca a las empresas y a los operadores de redes privados.

6.1.4 Menor de edad

El término "menor de edad" resulta especialmente pertinente en lo que respecta a la persecución de la pornografía infantil por la vía penal.[1486] También se utiliza en el contexto de las disposiciones que persiguen penalmente la realización de ciertos contenidos (por ejemplo la pornografía de adultos) que quedan al alcance de los menores de edad.[1487] Una de las definiciones utilizadas con más frecuencia es la que se da de "niño" en la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989.

> *Para los efectos de la presente Convención, se entiende por niño todo ser humano menor de dieciocho años de edad salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad.*

Diversos marcos legales y leyes modelo en materia de ciberdelincuencia, como son la Directiva de la UE sobre la lucha contra la pornografía infantil de 2011[1488], el Convenio del Consejo de Europa para la protección de los niños de 2007[1489] y el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia[1490], contienen definiciones similares. En el Convenio del Consejo de Europa sobre la Ciberdelincuencia, sólo se define la pornografía infantil, pero no el término "niño".

6.1.5 Pornografía infantil

La pornografía infantil es uno de los pocos delitos relacionados con la categoría de contenidos ilegales en que la mayoría de los países del mundo está de acuerdo en su persecución por la vía penal.[1491] Dado que puede resultar difícil la distinción entre las modalidades legales del material de contenido sexual y la pornografía infantil, algunos marcos jurídicos ofrecen una definición de la pornografía infantil.

Para los legisladores, uno de los principales desafíos a este respecto es huir de posibles conflictos entre distintas categorías de edad, a fin de evitar una posible persecución penal no deseada en casos en que difieran entre sí la edad para contraer matrimonio u otorgar el consentimiento sexual y la edad límite recogida en la definición de pornografía infantil.[1492] Si, por ejemplo, se define la pornografía infantil como la representación visual de actos sexuales de una persona menor de 18 años y, al mismo tiempo, la edad para dar el consentimiento sexual y contraer matrimonio es de 16 años, dos menores de 17 años podrían casarse o mantener relaciones sexuales legalmente, pero estarían cometiendo un grave delito (producción de pornografía infantil) si tomaran fotografías o películas del acto sexual.[1493]

En el Art. 2 *c)* del Protocolo opcional de la Convención de los derechos del niño, de la venta de niños, prostitución de niños y pornografía de niños, se facilita una definición.

Artículo 2
A los efectos del presente Protocolo:
[…]
(c) Por utilización de niños en la pornografía se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.

La definición que se facilita en el Protocolo Opcional no abarca explícitamente las modalidades de pornografía infantil ficticias tales como las imágenes realistas. Para asegurarse que este material también queda abarcado, algunos marcos jurídicos como el Convenio del Consejo de Europa sobre la ciberdelincuencia han modificado la definición de pornografía infantil.

Artículo 9 - Delitos relacionados con la pornografía infantil
[…]
2) A los efectos del anterior apartado 1, por pornografía infantil se entenderá todo material pornográfico que contenga la representación visual de:
a) un menor comportándose de una forma sexualmente explícita;
b) una persona que parezca un menor comportándose de una forma sexualmente explícita;
c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.
3) A los efectos del anterior apartado 2, por "menor" se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.
[…]

En el párrafo 2 del Artículo 9 se incluyen tres subsecciones dedicadas al material que representa visualmente la pornografía infantil: un menor comportándose de forma sexualmente explícita, una persona con aspecto de menor comportándose de una forma sexualmente explícita, y las imágenes realistas que representen a un menor comportándose de forma sexualmente explícita.

A este respecto, si bien el Convenio sobre la ciberdelincuencia amplía la definición recogida en el Protocolo opcional de la Convención de las Naciones Unidas, reduce por otra parte su aplicabilidad en dos aspectos importantes.

En primer lugar, aunque los redactores de la Convención sobre la cibercriminalidad hicieron hincapié en la importancia de disponer de una norma internacional uniforme en lo que respecta a la edad,[1494] este Convenio permite no obstante a las partes solicitar límites de edad distintos si bien nunca inferiores a los 16 años.

La segunda diferencia fundamental respecto de la definición recogida en el Protocolo Opcional es el hecho de que la definición del Convenio del Consejo de Europa sobre la ciberdelincuencia se centra en la representación visual. La pornografía infantil no se distribuye necesariamente en forma de fotografías o películas, sino también en forma de archivos de audio.[1495] Dado que la disposición del Artículo 9 se refiere al "material que contenga la representación visual" de un menor, la disposición no abarca los archivos de audio.

Como consecuencia de ello, enfoques más recientes tales como el texto legislativo sobre ciberdelincuencia[1496] de la HIPCAR[1497] siguen el concepto del Protocolo Opcional de las Naciones Unidas en vez del recogido en el Convenio del Consejo de Europa y evitan el término "visual".

Definiciones
3.
[...] (4) Se entiende por pornografía infantil el material pornográfico que presenta o representa:
a) un menor comportándose de una forma sexualmente explícita;
b) una persona que parezca un menor comportándose de una forma sexualmente explícita; o
c) imágenes que representen a un menor comportándose de una forma sexualmente explícita;
esto incluye, pero no se limita a, todo material pornográfico sonoro, visual o escrito. Un país puede limitar la consideración penal no aplicando los apartados b) y c).

También se incluyen definiciones de la pornografía infantil en la Directiva de 2011 de la UE sobre la lucha contra la pornografía infantil[1498], así como en el Convenio de 2007 del Consejo de Europa sobre la protección de la infancia.[1499]

6.1.6 Datos informáticos

La creciente utilización de la tecnología informática, así como la tendencia a la digitalización de los datos, han determinado la importancia creciente que revisten los datos informáticos. A consecuencia de ello, es cada vez más frecuente que los datos informáticos sean objeto de ataques que van desde la interferencia en la transmisión de datos[1500] hasta el espionaje de los datos.[1501] Son varios los marcos regionales que incluyen definiciones de los datos informáticos. Ejemplo de ello es la Sección 3 de la Ley modelo de la Commonwealth sobre el Ciberdelito y relacionado con la informática.

Definiciones
3*. En esta Ley, a menos que surja una intención contraria:*
se entiende por "datos informáticos" toda representación de hechos, información o conceptos de una forma que permita su procesamiento en un sistema de computadoras, incluido un programa capaz de provocar que un sistema informático realice una función;
[…]

Se recogen definiciones similares en el Convenio de 2001 del Consejo de Europa sobre la ciberdelincuencia[1502], la Decisión marco del Consejo de Unión Europea de 2005 relativa a los ataques contra los sistemas de información[1503], el proyecto de Directiva de 2008 de la ECOWAS sobre la lucha contra el ciberdelito[1504], y el Texto Legislativo Modelo de 2009 de la HIPCAR sobre Ciberdelincuencia[1505].

6.1.7 Dispositivo de almacenamiento de datos informáticos

Los dispositivos de almacenamiento desempeñan un importante papel en lo que respecta al ciberdelito – tanto en lo que se refiere a la posible interferencia de los datos como en lo que atañe a la incautación de pruebas. Un ejemplo de definición incluida en un marco regional es la de la Sección 3 de la Ley modelo de la Commonwealth sobre el Ciberdelito y relacionado con la informática.

Definiciones
3.
[…]
se entiende por "medio de almacenamiento de datos informáticos" todo artículo o material (por ejemplo un disco) a partir del cual es posible reproducir información, con o sin ayuda de cualquier otro artículo o dispositivo;
[…]

En el Texto Legislativo Modelo de 2009 de la HIPCAR sobre Ciberdelincuencia figura una definición similar.[1506]

6.1.8 Sistema informático

En la legislación sobre ciberdelito, el término "sistema informático" se utiliza tanto en relación con el derecho penal sustantivo como con el derecho procesal. Los sistemas informáticos pueden ser objeto de ataques; pueden utilizarse como herramienta para la comisión de un delito y, en último término ser incautados como prueba. En consecuencia, la mayoría de los marcos regionales y de las legislaciones modelo incluyen una definición al respecto. Ejemplo de ello es la Sección 3 de la Ley modelo de la Commonwealth sobre el Ciberdelito y relacionado con la informática:

> ***Definiciones***
> ***3.***
> *[…]*
> *se entiende por "sistema informático" un aparato o grupo de aparatos interconectados o relacionados, incluida Internet, en que uno o varios de ellos llevan a cabo, con arreglo a un programa, el procesamiento automático de datos o cualquier otra función;*
> *[…]*

Un aspecto insólito es el hecho de que la definición mencione "Internet". En general se define Internet como un sistema de redes interconectadas.[1507] Desde un punto de vista técnico la propia Internet no es en sí un sistema informático, sino una red y, por consiguiente, no debería incluirse en la definición de "sistemas informáticos" pero podría incluirse en la definición de redes informáticas. No obstante, varios redactores de marcos jurídicos siguieron el ejemplo de la Ley modelo de la Commonwealth e incluyeron Internet en la definición de sistema informático.

También se incluyen definiciones de término en el Convenio de 2001 del Consejo de Europa sobre la cibercriminalidad[1508], la Decisión marco del Consejo de la Unión Europea de 2005 relativa a los ataques contra los sistemas de información[1509], el proyecto de Directiva de 2008 de la ECOWAS sobre la lucha contra el ciberdelito [1510], y el Texto Legislativo Modelo de 2009 de la HIPCAR sobre Ciberdelincuencia.[1511]

6.1.9 Infraestructura esencial

A raíz de la utilización creciente de la tecnología informática y de red para el funcionamiento de la infraestructura esencial, dicha infraestructura se convierte en un posible objeto de ataques.[1512] Teniendo en cuenta las posibles repercusiones de un ataque de este tipo, algunos de los marcos más recientes incluyen una penalización/sanción agravada específica para determinados ataques contra la infraestructura esencial y, en consecuencia, también una definición. Puede citarse como ejemplo el Texto Legislativo Modelo de 2009 de la HIPCAR sobre Ciberdelincuencia.

> ***Definiciones***
> ***3.***
> *[…]*
> *(8) Se entiende por infraestructura esencial aquellos sistemas, aparatos y redes de información, programas y datos informáticos que resultan tan vitales para el país que la incapacitación, destrucción o interferencia de tales sistemas y activos supondría un menoscabo de la seguridad, la seguridad económica o nacional, la salud y protección públicas nacionales o cualquier combinación de estos factores*
> *[...]*

6.1.10 Criptología

La utilización de la tecnología de criptación por parte de delincuentes puede dificultar gravemente el acceso a los medios de prueba pertinentes.[1513] Como consecuencia, varios países han promulgado legislación para abordar la cuestión del uso de la tecnología de criptación y de los instrumentos de investigación conexos para velar por el respeto de la ley.[1514] Ello no obstante, de los distintos marcos regionales que tratan del

ciberdelito, sólo el Convenio de la Unión Africana sobre ciberseguridad[1515] ofrece una definición de criptología en su Artículo I-1.

> *8) Se entiende por criptología la ciencia que trata de proteger y asegurar la información, y más concretamente para garantizar la confidencialidad, la autenticación, la integridad y el no rechazo de los datos.*

6.1.11 Dispositivo

El término "dispositivo" se utiliza especialmente en relación con la persecución por la vía penal de los "dispositivos ilegales".[1516] En lo que respecta al riesgo potencial de que tales dispositivos puedan diseminarse ampliamente y utilizarse para cometer delitos, los redactores de varios marcos legislativos regionales decidieron incluir una disposición para la persecución por la vía penal de ciertas actividades relacionadas con los dispositivos ilegales. A diferencia del Convenio del Consejo de Europa sobre la ciberdelincuencia y de la Ley modelo de la Commonwealth, instrumentos ambos que utilizan el término "dispositivo", el Texto Legislativo Modelo de 2009 de la HIPCAR sobre Ciberdelincuencia incluye una definición del término en su Sección 3.

> ***Definiciones***
> ***3.***
> *[...]*
> *(9) El dispositivo incluye, entre otros*
> *a) componentes de sistemas informáticos tales como tarjetas gráficas, unidades de memoria, chips;*
> *b) elementos de almacenamiento tales como discos duros, tarjetas de memoria, discos compactos, cintas;*
> *c) instrumentos de entrada tales como teclados, ratones, tapetes de seguimiento (track pad), escáneres, cámaras digitales;*
> *d) instrumentos de salida como impresoras, pantallas.*
> *[…]*

Es una definición descriptiva típica, dado que la disposición indica explícitamente que la definición de dispositivo no se limitará a los componentes enumerados ("incluye, entre otros"). En referencia a la disposición subyacente[1517] por la que se persiguen por vía penal los dispositivos ilegales, el término incluye también los programas informáticos.

6.1.12 Perturbación

En las sociedades y economías de la información que incluyen el cibercomercio, el funcionamiento de los sistemas de computadoras resulta esencial. Los ataques contra un sistema de computadoras que impide a este último desarrollar operaciones puede suponer una grave interferencia para la sociedad y la economía. A consecuencia de ello, muchos marcos regionales persiguen por la vía penal la perturbación de un sistema de computadoras que impida su funcionamiento.[1518] El Texto Legislativo Modelo de 2009 de la HIPCAR sobre Ciberdelincuencia incluye en su Sección 3 una definición específica del término "perturbación" a efectos del ciberdelito.

Definiciones
3.
[...]
(10) Perturbar en relación con un sistema de computadoras incluye, entre otros:
a) cortar el suministro eléctrico a un sistema de computadoras;
b) causar interferencias electromagnéticas a un sistema de computadoras;
c) corromper por cualquier medio un sistema de computadoras; e
d) ingresar, transmitir, dañar, borrar, deteriorar, alterar o suprimir datos informáticos.
[…]

En la definición se subraya que las manipulaciones incluyen la interferencia física (como el corte del suministro eléctrico) y las manipulaciones en relación con los datos (como el ingreso de datos informáticos).

6.1.13 Proveedor de hospedaje

Los proveedores de hospedaje desempeñan un papel esencial en lo que respecta a la lucha contra la ciberdelincuencia, ya que sus servicios se utilizan, por ejemplo, para almacenar contenidos ilegales. En consecuencia, hay varios marcos regionales que tratan las cuestiones relacionadas con la responsabilidad jurídica de los ISP.[1519] No obstante, los principales marcos regionales no ofrecen una definición del proveedor de hospedaje. Sin embargo, en el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia se incluye una definición del término.

Definiciones
3.
[…]
(11) Se entiende por proveedor de hospedaje toda persona física o jurídica que presta un servicio de transmisión electrónica de datos mediante el almacenamiento de la información proporcionada por un usuario del servicio.
[…]

La definición no limita la aplicación de la disposición a los proveedores comerciales, sino que incluye también al proveedor privado. A consecuencia de ello, incluso el proveedor de un sitio web privado que permite almacenar información a terceros en el sitio web puede estar sometido a las normas conexas en materia de responsabilidad legal.

6.1.14 Hiperenlace

Aunque es muy frecuente que sólo se incluya a los proveedores de hospedaje, los proveedores de acceso y los proveedores de almacenamiento como subcategorías de proveedores de servicios de Internet (ISP), hay varios marcos legislativos que incluyen disposiciones específicas para otros servicios tales como los motores de búsqueda[1520] y los hiperenlaces. A este respecto, el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia incluye una definición de hiperenlace.

Definiciones
3.
[…]
(12) Se entiende por hiperenlace las características o propiedades principales de un elemento que puede ser un símbolo, una frase, una oración o una imagen que contiene información acerca de otra fuente y que, al ejecutarse, dirige hacia y hace que se presente un documento distinto.
[…]

La definición es amplia y abarca distintos tipos de hiperenlace tales como los enlaces profundos (deep links).

6.1.15 Interceptación

El término "interceptación" se utiliza con frecuencia en la legislación penal sustantiva en relación con la persecución por la vía penal de las interceptaciones ilegales[1521], así como en la ley de procedimiento penal en relación con la interceptación ilegal de las comunicaciones. Aunque marcos regionales como el Convenio del Consejo de Europa sobre la ciberdelincuencia y la Ley modelo de la Commonwealth incluyen disposiciones relacionadas con la interceptación tanto ilegal como legal, dichos marcos no ofrecen una definición de la interceptación. No obstante, en el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia sí se recoge una disposición de este tipo.

Definiciones
3.
[…]
(13) Se entiende por interceptación, entre otras cosas, la adquisición, visualización y captación de cualquier comunicación de datos informáticos, ya sea por medios alámbricos, inalámbricos, electrónicos, ópticos, magnéticos, verbales o de otro tipo, durante la transmisión a través de la utilización de cualquier dispositivo técnico.
[…]

6.1.16 Interferencia

El término "interferencia" es un término normalizado que se utiliza en varias disposiciones relacionadas con el ciberdelito. Cabe citar como ejemplos la interferencia de los datos[1522] así como la interferencia de los sistemas.[1523] No obstante, en varios instrumentos regionales el término se utiliza únicamente en los epígrafes de ciertas disposiciones, pero no se describe en sí mismo como un acto que sea objeto de persecución por la vía penal. En consecuencia, este término no se define en la mayoría de los modelos regionales y modelos legislativos.

6.1.17 Correos electrónicos múltiples

Una proporción importante de todos los correos electrónicos que se envían son correo basura (SPAM). A consecuencia de ello, numerosos países, así como recientes legislaciones modelo, han incluido disposiciones para la persecución por vía penal de actos relacionados con el SPAM.[1524] Un término clave utilizado en dicha disposición es "correo electrónico múltiple". El Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia incluye una definición de este término.

Definiciones
3.
[…]
(14) Se entiende por mensaje de correo electrónico múltiple un mensaje de correo que incluye el envío de correos electrónicos y mensajes instantáneos a más de un millar de destinatarios.
[…]

6.1.18 Programa informático forense a distancia

Algunos de los marcos jurídicos más recientes y avanzados incluyen instrumentos de procedimiento que, en ciertos casos, autorizan a los organismos encargados de velar por el cumplimiento de la ley a aplicar herramientas forenses modernas – caso del registro de pulsaciones de teclado o keylogger.[1525] En el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia se incluye una definición para el término "programa informático forense a distancia".

Definiciones
3.
[…]
(15) Se entiende por "programa informático forense a distancia" un programa informático de investigación instalado en un sistema de computadoras y utilizado para realizar tareas que incluyen, entre otras cosas, el registro de pulsaciones del teclado o la transmisión de una dirección IP.
[…]

En los debates acerca de la aplicación en la región del Pacífico de las normas de la HIPCAR, que se desarrollaron para el Caribe, se indicó que, a fin de abarcar toda la gama de soluciones forenses, era preferible utilizar el término "herramienta" (que también abarca las soluciones informáticas) en vez de "programa informático".

6.1.19 Incautar

La incautación sigue siendo uno de los instrumentos de investigación más importantes para recoger pruebas, no sólo en relación con los delitos tradicionales, sino también en el caso de la ciberdelincuencia.[1526] La Ley modelo de la Commonwealth sobre el Ciberdelito y relacionado con la informática incluye una definición del término "incautación" en la Sección 11 de la Parte III, Facultades procesales.

Definiciones para esta Parte
[…]
11. En esta Parte:
[…]
"incautar" incluye:
(a) crear y conservar una copia de datos informáticos, incluso utilizando los equipos in situ;
(b) suprimir o hacer que no pueda accederse a datos informáticos existentes en el sistema de computadoras al que se accede; e
(c) imprimir una copia de los datos informáticos salientes.

Esta definición, que contiene tres subapartados, se modificó en el proceso de elaboración del Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia. Se incluye una definición del término en la Sección 3 (16).

Definiciones
3.
(16) incautar incluye:
a. Activar in situ cualquier computadora y medio de almacenamiento de datos informáticos;
b. Crear y conservar una copia de datos informáticos, incluso utilizando equipos in situ;
c. Mantener la integridad de los datos informáticos pertinentes almacenados;
d. suprimir o hacer que no pueda accederse a datos informáticos existentes en el sistema de computadoras al que se accede;
e. imprimir una copia de los datos informáticos salientes; o
f. incautar o asegurar de manera similar un sistema de computadoras o parte del mismo, o un medio de almacenamiento de datos informáticos.
[…]

En el Convenio del Consejo de Europa sobre la ciberdelincuencia se aplicó un enfoque distinto y se incluyeron en la propia disposición los distintos elementos de la incautación.[1527]

6.1.20 Proveedor de servicio

La categoría de "proveedor de servicio" se utiliza para describir distintos tipos de proveedores que ofrecen servicios de Internet. Como se indicó anteriormente, varios marcos regionales incluyen disposiciones relativas al proveedor de servicio (por ejemplo las disposiciones relativas a la responsabilidad jurídica de los distintos tipos de proveedor de servicio o los instrumentos procesales que obligan a un proveedor de servicio a prestar apoyo a las actividades destinadas a imponer el respeto de la ley). No todos distinguen entre distintos tipos de proveedor de servicio. En consecuencia, y especialmente en aquellos marcos regionales que no establecen esta distinción, se incluye una definición del término "proveedor de servicio". Ejemplo de ello es el Convenio del Consejo de Europa sobre la Ciberdelincuencia.

Artículo 1 - Definiciones
[...]
c) Se entiende por "proveedor de servicio":
i. toda entidad pública o privada que ofrece a los usuarios de su servicio la capacidad de comunicar por medio de un sistema de computadoras, y
ii. cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicación o de los usuarios de dicho servicio.
[…]

La Ley modelo de la Commonwealth sobre el Ciberdelito y relacionado con la informática de 2002[1528], y el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia de 2009[1529] también incluyen definiciones similares.

6.1.21 Datos de tráfico

La categoría "datos de tráfico" es una categoría de datos para la que algunos marcos jurídicos y legislaciones modelo prevén instrumentos de investigación específicos.[1530] En consecuencia, dichos marcos jurídicos y legislaciones modelo también incluyen con frecuencia una definición. Así ocurre con la Sección 3 de la Ley modelo de la Commonwealth sobre el Ciberdelito y relacionado con la informática de 2002.

Definiciones
3.
[...]
Por "datos de tráfico" se entiende los datos informáticos:
(a) que se relacionan con una comunicación por medio de un sistema informático;
(b) que son generados por un sistema informático que forma parte de una cadena de comunicación; y
(c) que muestran cuáles son el origen, el destino, la ruta, la fecha y la hora, el volumen, la duración o el tipo de servicios subyacentes.

Se incluyen definiciones similares en el Convenio del Consejo de Europa sobre la ciberdelincuencia de 2001[1531], así como en el Texto Legislativo Modelo de la HIPCAR sobre Ciberdelincuencia de 2009.[1532]

6.2 Derecho penal sustantivo

Bibliografía (seleccionada): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002; *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime,

Southern California Law Review, 2008, Vol. 81; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke/Tropina*, from Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, Cybercrime Training for Judges, 2009; *Gercke*, How Terrorist Use the Internet in Pieth/Thelesklaf/Ivory, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf; Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.*, available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf; *Lavalle*, A Politicized and Poorly Conceived Notion Crying Out for Clarification: The Alleged Need for Universally Agreed Definition of Terrorism, Zeitschrift fuer auslaendisches oeffentliches Recht und Voelkerrecht, 2006, page 89 *et seq.*; *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999; *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11; *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact and Prevention, Youth & Society, Vol. 34, 2003; *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; *Parsonage*, Web Browser Session Restore Forensics, A valuable record of a user's internet activity for computer forensic examinations, 2010, available at: http://computerforensics.parsonage.co.uk/downloads/WebBrowserSessionRestoreForensics.pdf; Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement Act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII; *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, 2001; *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP/e-RIAPL, 2008, C-07; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33; *Walden*, Computer Crimes and Digital Investigations, 2006; *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2; *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729; *Wolak/ Finkelhor/Mitchell*, Child-

Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

6.2.1 Acceso ilícito (piratería)

Desde que se desarrollaron las redes informáticas, gracias a su capacidad para conectar a los ordenadores y ofrecer a los usuarios acceso a otros sistemas informáticos, los piratas han utilizado los ordenadores con fines delictivos[1533]. Las motivaciones que mueven a los piratas son muy diversas[1534]: no es necesario que estén presentes en la escena del delito[1535]; basta con que éstos eludan los sistemas de protección que aseguran a la red[1536]. En muchos casos de acceso ilícito, los sistemas de seguridad que protegen el emplazamiento físico de los equipos de red son más sofisticados que los sistemas de seguridad que protegen información delicada en las redes, incluso dentro del mismo edificio[1537].

El acceso ilícito a los sistemas informáticos dificulta a los operadores una gestión, explotación y control de sus sistemas sin perturbación o impedimento[1538]. La finalidad de la protección es mantener la integridad de los sistemas informáticos[1539]. Es esencial hacer una distinción entre el acceso ilícito y las subsiguientes infracciones (tales como el espionaje de datos[1540]), dado que las disposiciones jurídicas abordan de diferente manera la protección. En la mayoría de los casos, el acceso ilícito (cuando la ley trata de proteger la integridad del propio sistema informático) no es el objetivo final, sino más bien un primer paso en la consecución de otros delitos, tales como la modificación u obtención de datos almacenados (cuando la ley trata de proteger la integridad y la confidencialidad de los datos)[1541].

La cuestión consiste en determinar si se debe penalizar o no el acto de acceso ilícito, además de los subsiguientes delitos[1542]. De un análisis de los diversos enfoques aplicados para la penalización del acceso informático ilícito a escala nacional se desprende que las disposiciones vigentes al respecto a veces confunden el acceso ilícito con los delitos subsiguientes, o tratan de limitar la penalización del acceso ilícito únicamente a los casos de graves violaciones[1543]. En algunos países se penaliza el mero acceso, mientras que en otros se limita la penalización únicamente cuando el sistema al que se ingresó está protegido con medidas de seguridad, o cuando el perpetrador tiene intenciones perjudiciales, o cuando se obtuvieron, modificaron o dañaron datos[1544]. En otros países no se penaliza el acceso propiamente dicho, sino únicamente los delitos subsiguientes[1545]. Los detractores de la penalización del acceso ilícito aducen como argumento en contra situaciones en las cuales la mera intrusión no creó peligro alguno, o los casos en los cuales los actos de "piratería" condujeron a la detección de fallos o debilidades en los sistemas de seguridad de los ordenadores.[1546]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

El Convenio del Consejo de Europa sobre la Ciberdelincuencia contiene una disposición sobre el acceso ilegal que protege la integridad de los sistemas informáticos mediante la penalización del acceso no autorizado a un sistema. Habida cuenta de la adopción de enfoques incoherentes a escala nacional[1547], el Convenio ofrece la posibilidad de imponer limitaciones que -por lo menos en la mayoría de los casos- permiten a los países carentes de legislación mantener en vigor unas leyes más liberales en la esfera del acceso ilícito[1548]. La disposición pretende proteger la integridad de los sistemas informáticos.

Disposición

Artículo 2 – Acceso ilícito
Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Actos contemplados

El término "acceso" no especifica un medio concreto de comunicación, sino que admite diversas connotaciones y está abierto a nuevos adelantos técnicos[1549]. Este término se refiere a todos los medios de entrar en otro sistema informático, con inclusión de los ataques por Internet[1550], así como el acceso ilícito a las redes inalámbricas. En la disposición se contempla incluso el acceso no autorizado a los ordenadores que no están conectados a ninguna red (por ejemplo, esquivando la protección de una contraseña)[1551]. En aplicación de este amplio enfoque, el acceso ilícito no sólo abarca los futuros adelantos técnicos, sino también los datos secretos a los que tienen acceso las personas informadas y los empleados[1552]. La segunda frase del Artículo 2 ofrece la posibilidad de limitar la penalización del acceso ilícito al acceso a través de una red[1553].

Así pues, los actos ilícitos y los sistemas protegidos se definen de tal modo que su concepto queda abierto a la evolución futura. En el Informe Explicativo se enumeran los equipos, componentes, datos almacenados, directorios, los datos relacionados con el contenido y el tráfico como ejemplos de las partes de un sistema informático a las que es posible obtener acceso [1554] .

Predisposición

Al igual que todos los otros delitos definidos en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, en el Artículo 2 se exige que para penalizar un delito el delincuente lo haya efectuado de manera intencional[1555]. El Convenio no contiene una definición del término "intencionalmente". Los redactores del Informe Explicativo subrayaron que "intencionalmente" debe definirse a nivel nacional.[1556]

Sin derecho

A tenor del Artículo 2 del Convenio, el acceso a un ordenador sólo puede penalizarse si éste tiene lugar "sin derecho"[1557]. Se considera que el acceso a un sistema que permite al público su acceso libre y abierto o el acceso a un sistema con la autorización del propietario u otro titular de derechos no es un acceso "sin derecho"[1558]. Además del tema del acceso libre, también se aborda la legitimidad de los procedimientos de ensayo de seguridad[1559]. Los administradores de la red y las compañías encargadas de la seguridad que someten a prueba la protección de los sistemas informáticos con miras a detectar posibles deficiencias manifestaron su inquietud respecto de la posibilidad de penalización en el marco del acceso ilegal[1560]. Pese al hecho de que en general estos profesionales trabajan con el permiso del propietario y por consiguiente actúan legalmente, los redactores del Convenio hicieron hincapié en que "el ensayo o la protección del sistema de seguridad de un ordenador con autorización del propietario o del operador [...] se consideran actos con derecho"[1561].

El hecho de que la víctima del delito le haya transmitido al infractor una contraseña o un código de acceso similar no implica forzosamente que el delincuente haya actuado con derecho al penetrar al sistema informático de la víctima. Si el delincuente persuadió a la víctima de que le revelase una contraseña o un código de acceso mediante una astuta manipulación social[1562], es necesario verificar si la autorización concedida por la víctima incluye al acto efectuado por el delincuente[1563]. Por lo general éste no es el caso y por lo tanto el delincuente actúa sin derecho.

Restricciones y reservas

Como una alternativa al enfoque general, el Convenio sobre la Ciberdelincuencia ofrece la posibilidad de limitar la penalización con elementos adicionales, tal como se enumeran en la segunda frase[1564]. En el Artículo 42 del Convenio sobre la Ciberdelincuencia se describe el procedimiento adecuado para recurrir a esta reserva[1565]. Las posibles reservas guardan relación con las medidas de seguridad[1566], la intención especial de obtener datos informáticos[1567], otras intenciones deshonestas que justifican una culpabilidad penal, o la imposición del requisito de que el delito sea cometido en contra de un sistema informático a través de una red[1568]. La Decisión marco del Consejo de la Unión Europea[1569] relativa a los ataques contra los sistemas de información[1570] contiene una disposición similar.

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

Un enfoque similar se describe en la Sección 5 de la Ley modelo de la Commonwealth de 2002[1571]. Al igual que en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, la disposición protege la integridad de los sistemas informáticos.

> ***Acceso ilícito 5.***
> *Una persona que deliberadamente, sin excusa o justificación legal, penetre en la totalidad o en cualquier parte de un sistema informático, comete un delito punible, tras el fallo condenatorio, con una pena de prisión por un periodo no superior a [periodo] o una multa no superior a [cuantía], o ambas cosas.*

La Sección 5 sigue un planteamiento similar al Artículo 5 del Convenio del Consejo de Europa sobre la Ciberdelincuencia. La principal diferencia con el Convenio del Consejo de Europa sobre la Ciberdelincuencia es que en la Ley modelo de la Commonwealth no se ofrece ninguna opción para formular reservas.

Directiva de la Unión Europea relativa a los ataques contra los sistemas de información

La Directiva de la Unión Europea relativa a los ataques contra los sistemas de información[1572], en su Artículo 3, contiene una disposición que penaliza el acceso ilícito a los sistemas de información.

> ***Artículo 3*** *– Acceso ilegal a los sistemas de información*
> *1. Los Estados Miembros adoptarán las medidas necesarias para que, cuando se comete intencionalmente, el acceso sin autorización, al conjunto o a una parte de un sistema de información, sea sancionable como infracción penal, cuando se comete transgrediendo medidas de seguridad, al menos en los casos que no sean de menor gravedad.*

La disposición fue redactada de conformidad con las normas definidas por el Convenio del Consejo de Europa sobre la Ciberdelincuencia[1573]. Hay dos diferencias principales con el Convenio del Consejo de Europa sobre la Ciberdelincuencia. La primera es que los Estados Miembros pueden limitar la penalización a los casos que no sean de menor gravedad. En este contexto, la Directiva señala explícitamente que el instrumento no cubre los casos de menor gravedad.[1574] La segunda es que el Artículo 3 limita la aplicabilidad a casos para los que se habían previsto medidas de seguridad, que fueron transgredidas. En el Convenio sobre la Ciberdelincuencia se trata sólo de una restricción optativa.

Proyecto de Convenio Internacional de Stanford

En el Proyecto de Convenio Internacional de Stanford de 1999, de carácter oficioso[1575], se reconoce que el acceso ilícito es uno de los delitos que deben penalizar los Estados signatarios.

Disposición

> ***Art. 3 – Delitos***
> *1. En el marco del presente Convenio, una persona comete un delito toda vez que ilegal e intencionalmente realiza cualesquiera de los siguientes actos sin autoridad, permiso o consentimiento legalmente reconocidos:*
> *[...]*
> *(c) penetra en un cibersistema cuyo acceso se encuentra restringido de una manera conspicua e inequívoca;*
> *[...]*

Actos contemplados

El proyecto de disposición muestra algunas similitudes con el Artículo 2 del Convenio del Consejo de Europa sobre la Ciberdelincuencia, por cuanto ambos imponen el requisito de que un acto intencional sea aquel acto que se comete sin derecho/sin autoridad. En este contexto, el requisito que impone el proyecto de disposición (*"sin autoridad, permiso o consentimiento legalmente reconocidos"*) es más preciso que el

término "sin derecho"[1576] utilizado en el Convenio del Consejo de Europa sobre la Ciberdelincuencia y apunta explícitamente a incorporar el concepto de autodefensa[1577]. Otra diferencia con los enfoques tradicionales como el Convenio sobre la Ciberdelincuencia es que en este proyecto de disposición se utiliza el término "cibersistema", tal como está definido en el párrafo 3 del Artículo 1 de dicho Proyecto de Convenio. Este término abarca a cualquier ordenador o red de ordenadores utilizada para retransmitir, transmitir, coordinar o controlar las comunicaciones de datos o programas. Esta definición contiene numerosas similitudes con la definición del término "sistema informático" que figura en el Artículo 1 a) del Convenio del Consejo de Europa sobre la Ciberdelincuencia[1578]. Aunque el Proyecto de Stanford se refiere a actos relacionados con el intercambio de datos y por consiguiente apunta principalmente a los sistemas informáticos basados en redes, ambas definiciones abarcan a ordenadores interconectados así como a máquinas autónomas.[1579]

6.2.2 Permanencia ilegal

No sólo se viola la integridad de los sistemas informáticos cuando se entra ilegalmente en ellos, también cuando se siguen utilizando después de que el permiso haya caducado. Dado que en estos casos no se ha accedido ilegalmente, puede resultar difícil aplicar las disposiciones que penalizan el acceso ilegal a los sistemas informáticos.

Consejo de Europa

El Convenio del Consejo de Europa sobre la Ciberdelincuencia penaliza el acceso ilegal a un sistema informático, pero no la permanencia ilegal. Sin embargo, la permanencia ilegal se debatió durante la negociación del Convenio. En 1998, cuando se terminó la cuarta versión del proyecto del Convenio del Consejo de Europa sobre la Ciberdelincuencia, aún contenía este elemento.

> ***Art. 2** – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos*
> *Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente, la siguiente conducta:*
> *[…]*
> *1bis: El hecho intencionado de no salir de un sistema informático, al que, en parte o en su totalidad, una persona pueda haber accedido inadvertidamente sin derecho, tan pronto tome consciencia de su situación [indebida].*
> *[…]*

Sin embargo, la versión definitiva del Convenio del Consejo de Europa sobre la Ciberdelincuencia que quedó abierta a la firma en 2001 ya no contenía tal disposición.

Ejemplo

Algunos de los enfoques recientes incluyen disposiciones específicas para tratar esta cuestión, por ejemplo, el texto legislativo sobre la ciberdelincuencia[1580] de HIPCAR[1581]. En la Sección 5 se criminaliza la permanencia ilegal en un sistema informático. Como en el caso de la penalización del acceso ilegal, el bien jurídico protegido es la integridad de los sistemas informáticos.

> ***Permanencia ilegal***
> ***5.**(1) Una persona que intencionalmente, sin excusa o justificación legal, o excediéndose de una excusa o justificación legal, permanezca conectado en un sistema informático o en parte de un sistema informático o siga utilizando un sistema informático comete un delito punible, en caso de condena, con pena de prisión por un período no superior a [periodo], o una multa máxima de [cuantía], o con ambas.*
> *(2) Un país puede decidir no tipificar como delito la simple permanencia no autorizada, siempre que haya disponibles otros tratamientos efectivos. Alternativamente, podrá exigir que el delito sea cometido infringiendo medidas de seguridad o con la intención de obtener datos informáticos u otras intenciones deshonestas.*

La disposición, que no figura de forma similar en ninguno de los enfoques regionales, refleja el hecho de que no sólo se viola la integridad de un sistema informático cuando alguien se introduce en él sin tener derecho a ello, sino también cuando permanece cuando ha vencido la autorización. La permanencia requiere que el delincuente tenga todavía acceso al sistema informático. Se puede producir, por ejemplo, cuando permanece conectado o sigue realizando operaciones. El hecho de que tenga la posibilidad teórica de iniciar sesión en el sistema informático no es suficiente. En la Sección 54 se requiere que el delincuente esté llevando a cabo los delitos intencionalmente. No están cubiertos los actos imprudentes. Además, en la Sección 54 sólo se criminalizan los actos cuando se cometen "sin justificación o excusa legal".

6.2.3 Adquisición ilegal de datos informáticos

El Convenio del Consejo de Europa sobre la Ciberdelincuencia, así como la Ley modelo de la Commonwealth y el Proyecto de Convenio Internacional de Stanford, proporcionan soluciones jurídicas únicamente para la interceptación ilegal[1582]. Cabe poner en tela de juicio si el Artículo 3 del Convenio del Consejo de Europa sobre la Ciberdelincuencia se aplica a casos distintos de los casos en los cuales los delitos se cometen mediante interceptación de los procesos de transferencia de datos. Según se indica más abajo[1583], se examinó con gran interés la cuestión de determinar si el acceso ilegal a la información almacenada en un disco duro está incluido en el Convenio sobre la Ciberdelincuencia[1584]. Puesto que para la penalización es preciso que haya un proceso de transferencia, es probable que el Artículo 3 del Convenio sobre la Ciberdelincuencia no se aplique a otras formas de espionaje de datos distintas a la interceptación de los procesos de transferencia[1585]. Esta circunstancia es cuando menos curiosa puesto que el 9º Proyecto sobre el Convenio sobre la Ciberdelincuencia mencionaba la importancia de penalizar el espionaje de datos.

Una cuestión que se aborda con frecuencia en este contexto es la determinación de si la penalización del acceso ilícito hace que resulte innecesaria la penalización del espionaje de datos. En los casos en los cuales el delincuente tiene acceso legítimo a un sistema informático (por ejemplo, porque se le ha ordenado repararlo) y en ese momento (en violación de la legitimación limitada) copia ficheros del sistema, a dicho acto no se aplica en general las disposiciones que penalizan el acceso ilícito[1586].

Puesto que actualmente gran parte de los datos vitales se almacenan en sistemas informáticos, es indispensable evaluar si los mecanismos existentes para proteger dichos datos son o no adecuados o si es preciso formular otras disposiciones de derecho penal para proteger al usuario contra el espionaje de datos[1587]. Hoy en día los usuarios de ordenadores pueden recurrir a diversos dispositivos hardware y software con miras a proteger información secreta. Éstos pueden instalar cortafuegos, sistemas de control de acceso o encriptar la información almacenada y de ese modo reducir los riesgos de espionaje de datos[1588]. Aunque se dispone de dispositivos de fácil utilización por el usuario, para cuya operación sólo se requiere un conocimiento limitado, a menudo la protección verdaderamente eficaz de los datos en un sistema informático exige un nivel de conocimientos que muy pocos usuarios tienen[1589]. En particular los datos almacenados en sistemas informáticos privados con frecuencia no están adecuadamente protegidos contra el espionaje. Así pues, las disposiciones de derecho penal pueden ofrecer una protección adicional.

Algunos países han decidido ampliar el alcance de la protección que confieren las medidas técnicas, mediante la penalización del espionaje de datos. Existen dos enfoques fundamentales. Algunos países aplican un enfoque estrecho y penalizan el espionaje de datos únicamente cuando se obtiene información secreta; un ejemplo de ello es la disposición 18 USC § 1831 que penaliza el espionaje económico. Esta disposición no sólo abarca el espionaje de datos, sino también otros medios de obtener información secreta.

Código de Estados Unidos

§ 1831 – Espionaje económico

a) En general toda persona que, intencionalmente o a sabiendas de que la infracción beneficiará a cualesquiera gobiernos, agencias o agentes extranjeros

(1) robe o, sin autorización, se apropie de, tome, se lleve u oculte, o mediante fraude, artificio o engaño, obtenga un secreto comercial;

(2) sin autorización copie, duplique, esboce, dibuje, fotografíe, descargue, cargue, altere, destruya, fotocopie, replique, transmita, entregue, expida, envíe por correo electrónico, comunique o transporte un secreto comercial;
(3) reciba, compre o posea un secreto comercial, a sabiendas de que éste ha sido robado o ha sido objeto de apropiación, obtenido o convertido sin autorización;
(4) intente cometer cualesquiera de los delitos descritos en los anteriores párrafos 1) a 3); o
(5) conspire con una o más personas para cometer cualquiera de los delitos descritos en los anteriores párrafos 1) a 3) y una o más de esas personas actúe para llevar a la práctica el objeto de la conspiración, será multada, con la excepción consignada en el apartado b), con una multa no superior a 500 000 $ o condenada a una pena de prisión no superior a 15 años, o a ambas cosas.
b) Las organizaciones, es decir cualquier organización que cometa alguno de los delitos descritos en el apartado a) será castigada con una multa no superior a 10 000 000 $.

La Ley de Espionaje Económico de 1996 introdujo este § 1831.[1590] Hasta 1996, el espionaje económico era tipificado como delito únicamente por leyes estatales en gran medida inconsistentes.[1591] La Ley de Espionaje Económico criminaliza dos tipos de apropiación indebida de secretos comerciales en el Título 18: el robo de un secreto comercial en beneficio de un gobierno, agencia o agente extranjeros, y el robo con fines comerciales de secretos realizados para obtener beneficios económicos, independientemente de que beneficie, o no, a un gobierno, agencia o agente extranjeros.[1592] Aunque la disposición se centra en la protección de contenidos (secretos comerciales) y no requiere un formato específico (datos informáticos), no sólo es aplicable a la delincuencia tradicional, sino también a los delitos relacionados con la informática.[1593] En general, en estos casos también se aplica 18 USC § 1030 (a)(2). [1594] Con respecto a los casos informáticos, el § 1831(a)(2)-(5) contempla los actos.

Texto legislativo sobre la ciberdelincuencia de HIPCAR

En la Sección 8 del texto legislativo sobre la ciberdelincuencia[1595] de HIPCAR[1596] hay otro ejemplo.

Espionaje de datos
8. *(1) Una persona que, intencionalmente, sin excusa o justificación legal o en exceso de una excusa o justificación legal obtenga, para sí o para otro, datos informáticos que no estén destinados a él y que estén especialmente protegidos contra el acceso no autorizado, comete un delito punible, en caso de condena, con pena de prisión por un período no superior a [periodo], o con una multa que no exceda de [cuantía], o con ambas.*
(2) Cada país puede limitar la penalización a determinadas categorías de datos informáticos.

En la Sección 8 se protege la confidencialidad de los datos informáticos almacenados y protegidos. La protección especial requiere que el proveedor de alojamiento de la información haya puesto en marcha medidas de protección que dificulten significativamente la obtención de acceso a los datos sin autorización. Ejemplos de posibles medidas son la protección por contraseña y el cifrado. Las notas explicativas de los puntos del texto legislativo señalan que es necesario que las medidas de protección vayan más allá de las medidas de protección estándar que se aplican a los datos, así como otras propiedades, por ejemplo, restricciones de acceso a ciertas partes de los edificios del gobierno.[1597]

Código Penal alemán

En la Sección 202a de la versión en vigor hasta 2007 del Código Penal alemán se encuentra un enfoque parecido.[1598]

Sección 202a. – Espionaje de datos:
(1) Cualquier persona que obtenga sin autorización, para sí misma o para otra persona, datos que no le están destinados y se hallan especialmente protegidos contra un acceso no autorizado, podrá ser objeto de prisión por un periodo no superior a tres años o se le podrá imponer una multa.
(2) Los datos a los que se refiere el apartado 1) son únicamente aquellos datos almacenados o transmitidos por medios electrónicos o magnéticos o de cualquier otro modo no visible directamente.

Esta disposición no incluye únicamente a los secretos económicos, sino también a los datos informáticos almacenados en general[1599]. En lo que respecta a sus objetos de protección, este enfoque es más amplio que el consignado en el 18 USC § 1831 Espionaje económico, pero la aplicación de la disposición es limitada, ya que la obtención de datos sólo se penaliza cuando los datos se hallan especialmente protegidos contra un acceso no autorizado[1600]. Así pues, a tenor del derecho penal alemán la protección de los datos informáticos almacenados se limita a las personas o empresas que hayan tomado medidas para evitar ser víctimas de esos delitos.[1601]

Pertinencia de la disposición

La implementación de esta disposición resulta particularmente pertinente en los casos en los cuales el delincuente fue autorizado a penetrar en un sistema informático (por ejemplo, porque se le ordenó solucionar un problema informático) y luego éste abusó de la autorización para obtener ilegalmente información almacenada en el sistema informático[1602]. En lo tocante al hecho de que el permiso cubre el acceso al sistema informático, en general no es posible abarcar estos casos con las disposiciones que penalizan el acceso ilegal.

Sin derecho

Para aplicar las disposiciones sobre espionaje de datos es necesario generalmente que los datos hayan sido obtenidos sin el consentimiento de la víctima. El éxito de los ataques de usurpación de identidad[1603] demuestra claramente el éxito de las estafas basadas en la manipulación de los usuarios[1604]. Debido al consentimiento de la víctima, los delincuentes que lograron manipular con éxito a los usuarios para que éstos revelasen información secreta no pueden ser procesados a tenor de las disposiciones antes mencionadas.

6.2.4 Interceptación ilegal

La utilización de las TIC comporta varios riesgos relacionados con la seguridad de la transferencia de información[1605]. A diferencia de las operaciones por correo clásico dentro de un país, los procesos de transferencia de datos por Internet involucran a numerosos proveedores y diferentes puntos en los cuales el proceso de transferencia podría ser interceptado[1606]. El punto más vulnerable de interceptación sigue siendo el usuario, en particular los usuarios de computadores de vivienda privados, que a menudo están insuficientemente protegidos contra ataques externos. Dado que por lo general los delincuentes apuntan al blanco más débil, el riesgo de ataque contra usuarios privados es el mayor riesgo, tanto más habida cuenta de:

- el desarrollo de tecnologías vulnerables; y
- la pertinencia cada vez mayor de la información personal para los delincuentes.

Las nuevas tecnologías de red (tales como las LAN inalámbricas) ofrecen varias ventajas para el acceso a Internet[1607]. El establecimiento de una red inalámbrica en una vivienda privada, por ejemplo, permite a las familias conectarse a Internet desde cualquier sitio dentro de un radio dado, sin necesidad de conexiones por cable. Pero la propagación de esta tecnología y el bienestar que ésta aporta van acompañados de graves riesgos para la seguridad de la red. Si disponen de una red inalámbrica sin protección, los perpetradores pueden activar dicha red y utilizarla con fines delictivos sin necesidad de introducirse en un edificio. Lo único que éstos necesitan es estar dentro del radio de la red inalámbrica para lanzar un ataque. Las pruebas en el terreno indican que en algunas zonas nada menos que el 50 por ciento de las redes inalámbricas privadas no están protegidas contra interceptaciones o acceso no autorizado[1608]. En la mayoría de los casos la falta de protección es el resultado de una falta de conocimientos en cuanto a la manera de configurar las medidas de protección[1609].

En el pasado, los perpetradores concentraron sus interceptaciones ilegales principalmente en redes empresariales[1610], pues en éstas era más probable encontrar información útil que en las interceptaciones de los datos transferidos por redes privadas. No obstante, el creciente número de casos de usurpación de identidad para robar datos personales privados señala que tal vez los perpetradores hayan cambiado de objetivo[1611]; actualmente los delincuentes manifiestan gran interés por datos privados tales como los

números de tarjeta de crédito, los números de seguridad social[1612], las contraseñas y la información sobre cuentas bancarias.[1613]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

El Convenio del Consejo de Europa sobre la Ciberdelincuencia contiene una disposición que protege la integridad de las transmisiones no públicas mediante la penalización de su interceptación no autorizada. Esta disposición apunta a igualar la protección de las transferencias electrónicas con la protección de las conversaciones vocales contra la grabación y/o intervención ilícita que ya existe actualmente en la mayor parte de los sistemas jurídicos.[1614]

Disposición

> ***Artículo 3*** *– Interceptación ilegal*
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.*

Actos contemplados

La aplicabilidad del Artículo 3 se limita a la interceptación de las transmisiones realizadas mediante medidas técnicas[1615]. Las interceptaciones relacionadas con los datos electrónicos pueden definirse como cualquier acto de adquisición de datos durante un proceso de transferencia[1616]

Según se indicó anteriormente, la cuestión de si el acceso ilícito a la información almacenada en un disco duro está contemplada o no en la disposición es una cuestión polémica y muy debatida[1617]. En general la disposición se aplica únicamente a la interceptación de las transmisiones, pues el acceso a la información almacenada no se considera como una interceptación de transmisión[1618]. El hecho de que la aplicación de esta disposición se considere incluso en casos en los cuales el delincuente accede físicamente a un sistema informático autónomo surge en parte como resultado del hecho de que el Convenio no contiene ninguna disposición relacionada con el espionaje de datos[1619] y el Informe Explicativo del Convenio contiene dos explicaciones ligeramente imprecisas en lo que respecta a la aplicación del Artículo 3:

En el Informe Explicativo se indica ante todo que la disposición abarca los procesos de comunicación que tienen lugar en un sistema informático[1620]. Sin embargo, esto deja abierta la cuestión de si la disposición se debe aplicar únicamente a los casos en los cuales las víctimas envían datos que luego son interceptados por delincuentes o si ésta también debería aplicarse a la situación en la cual el delincuente opera el computador. El segundo punto se relaciona con la penalización de la adquisición ilegal de datos informáticos.

En la Guía se destaca que la interceptación puede cometerse indirectamente mediante el uso de dispositivos "de intervención" o "mediante el acceso al sistema informático y su utilización"[1621]. Si los delincuentes obtienen acceso a un sistema informático y lo utilizan para hacer copias no autorizadas de datos almacenados en un disco externo, aunque ese acto conduce a la transferencia de datos (envío de datos del disco duro interno al disco duro externo), este proceso no es *interceptado*, sino más bien *iniciado*, por los delincuentes. El elemento faltante de la interceptación técnica es un sólido argumento en contra de la aplicación de la disposición en casos de acceso ilícito a información almacenada[1622].

El término "transmisión" se aplica a todas las transferencias de datos, ya sean por teléfono, facsímil, correo electrónico o transferencia de ficheros[1623]. El delito consignado a tenor del Artículo 3 se aplica únicamente a las transmisiones no públicas[1624]. Una transmisión es "no pública" si el proceso de transmisión es confidencial[1625]. El elemento esencial para hacer una distinción entre las transmisiones públicas y no públicas no es la naturaleza de los datos transmitidos, sino la naturaleza del propio proceso de transmisión. Incluso la transferencia de información disponible públicamente puede considerarse un acto delictivo si las partes que participan en la transferencia tienen la intención de mantener en secreto el contenido de sus

comunicaciones. La utilización de redes públicas no excluye la posibilidad de que las comunicaciones sean "no públicas".

Predisposición

Como ocurre en el caso de todos los otros delitos definidos en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, en el Artículo 3 se impone el requisito de que para proceder a la penalización el delincuente debe llevar a cabo los delitos intencionalmente[1626]. El Convenio no contiene una definición del término "intencionalmente". Los redactores del Informe Explicativo destacaron que "intencionalmente" debe definirse a escala nacional.[1627]

Sin derecho

Sólo se puede entablar juicio por interceptación de comunicaciones a tenor del Artículo 3 del Convenio sobre la Ciberdelincuencia si ésta tiene lugar "sin derecho"[1628]. Los redactores del Convenio sobre la Ciberdelincuencia proporcionaron un conjunto de ejemplos de interceptación que no se efectúan sin derecho: acción sobre la base de instrucciones o por autorización de los participantes en la transmisión[1629], actividades de protección o ensayo autorizadas y convenidas por los participantes[1630]e interceptación legal sobre la base de las disposiciones de derecho penal o en favor del interés de la seguridad nacional[1631].

Otra cuestión planteada durante la negociación del Convenio sobre la Ciberdelincuencia consistía en determinar si la utilización de "galletitas" ("*cookies*") debía dar lugar a sanciones penales a tenor del Artículo 3[1632]. Los redactores subrayaron que las prácticas comerciales comunes (como los *cookies*) no se consideran interceptaciones sin derecho.[1633]

Restricciones y reservas

El Artículo 3 ofrece la opción de restringir la penalización al requerir los elementos adicionales enumerados en la segunda frase, con inclusión de una "intención delictiva" o la relación de un sistema informático conectado a otro sistema informático.

Directiva de la Unión Europea relativa a los ataques contra los sistemas de información

En su Artículo 6, la Directiva de la Unión Europea relativa a los ataques contra los sistemas de información[1634] contiene una disposición en virtud de la cual se penaliza la interceptación ilegal.

> ***Artículo 6*** *– Interceptación ilegal*
> *Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.*

La disposición fue redactada de conformidad con las normas definidas por el Convenio del Consejo de Europa sobre la Ciberdelincuencia.[1635] La principal diferencia reside en la posibilidad de limitar la penalización a los casos de menor gravedad.

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

En la Sección 8 de la Ley modelo de la Commonwealth de 2002[1636] se describe un enfoque similar:

Interceptación ilegal de datos, etc.
8. *Toda persona que, deliberadamente y sin excusa o justificación legal, intercepta por medios técnicos:*
(a) cualquier transmisión no pública hacia, desde o dentro de un sistema informático; o
(b) las emisiones electromagnéticas procedentes de un sistema informático que transportan datos informáticos; comete un delito punible, previo fallo condenatorio, con una pena de prisión por un periodo no superior a [periodo] o una multa no superior a [cuantía], o ambas cosas

En la Sección 8 se sigue un enfoque similar al Artículo 3 del Convenio del Consejo de Europa sobre la Ciberdelincuencia: se protegen los datos durante los procesos de transmisión no públicos.

Proyecto de Convenio Internacional de Stanford

En el Proyecto de Convenio Internacional de Stanford de 1999, de carácter oficioso[1637], no se penaliza explícitamente la interceptación de datos informáticos.

6.2.5 Interferencia en los datos

La protección de objetos tangibles o físicos contra daños intencionales es un elemento clásico de la legislación penal nacional. Como consecuencia de la digitalización continua, un volumen cada vez mayor de información comercial esencial se almacena en forma de datos digitales[1638]. Los ataques a esa información o la obtención de la misma pueden dar lugar a pérdidas financieras[1639]. Además del borrado, la alteración de esa información también puede tener importantes consecuencias[1640]. En algunos casos la legislación en vigor no protege los datos de igual modo que los objetos tangibles, lo que les ha permitido a los delincuentes concebir formas de estafa que no dieran lugar a sanciones penales.[1641]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

El Artículo 4 del Convenio del Consejo de Europa sobre la Ciberdelincuencia contiene una disposición que protege la integridad de los datos contra la interferencia no autorizada[1642]. La finalidad de esta disposición es colmar las lagunas existentes en algunas legislaciones penales nacionales y conferir a los datos informáticos y a los programas informáticos una protección contra el daño intencional similar a la que se otorga a los objetos tangibles.[1643]

Disposición

Artículo 4 – Ataques a la integridad de los datos
(1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
(2) Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Actos contemplados

En el Artículo 4 se penalizan cinco actos diferentes. Los términos "dañe" y "deteriore" definen a cualquier acto tendiente a la alteración negativa de la integridad del contenido informativo de datos y programas[1644]. "Borre" se refiere a actos mediante los cuales se elimina información de un medio de almacenamiento, y este acto se considera comparable a la destrucción de un objeto tangible. Aunque proporcionaron una definición, los redactores del Convenio sobre la Ciberdelincuencia no hicieron una distinción entre las diversas formas según las cuales se pueden borrar datos[1645]. Si se manda un fichero a la papelera virtual no se elimina este fichero del disco duro [1646]. Incluso el "vaciado" de la papelera virtual no elimina necesariamente el fichero[1647]. Por lo tanto, no está claro si la posibilidad de recuperar un fichero borrado impide la aplicación de la disposición[1648]. Con "suprima" datos informáticos se denota una acción que afecta negativamente a la disponibilidad de datos para la persona que tiene acceso al medio donde se almacena la información[1649]. Se considera particularmente la aplicación de esta disposición en el caso de ataques[1650] de denegación de servicio[1651]. Durante el ataque, los datos del sistema informático víctima dejan de estar

disponibles para los usuarios potenciales o para el propietario del sistema informático[1652]. El término "altere" indica la modificación de los datos existentes, sin reducir forzosamente su disponibilidad[1653]. Este acto abarca en particular la instalación de software dañino tales como programas espías, virus o programas publicitarios en el ordenador de la víctima.[1654]

Predisposición

Como ocurre con todos los otros delitos definidos en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, el Artículo 4 impone el requisito de que, para proceder a la penalización del delincuente, éste debe haber efectuado los delitos deliberadamente[1655]. El Convenio sobre la Ciberdelincuencia no contiene ninguna definición del término "intencionalmente". Los redactores del Informe Explicativo señalaron que "intencionalmente" debe definirse a escala nacional[1656]

Sin derechos

Como ocurre con las disposiciones antes examinadas, estos actos deben cometerse "sin derecho"[1657]. Se consideró el derecho a alterar datos, especialmente en la cuestión de los "repetidores de correo" ("*remailers*")[1658]. Los repetidores de correo se utilizan para modificar ciertos datos con el fin de facilitar las comunicaciones anónimas[1659]. En el Informe Explicativo se indica que, en principio, estos actos son considerados como una protección legítima de la privacidad y por consiguiente cabe considerar que se realizan con autorización.[1660]

Restricciones y reservas

El Artículo 4 ofrece la opción de restringir la penalización mediante su limitación a los casos en los cuales se producen daños graves, lo que supone adoptar un enfoque similar al de la Decisión marco del Consejo de la Unión Europea relativa a los ataques contra los sistemas de información[1661], que permite a los Estados Miembros limitar la aplicabilidad de la disposición de derecho penal sustantiva a "los casos que no sean menores".[1662]

Directiva de la Unión Europea relativa a los ataques contra los sistemas de información

En su Artículo 5, la Directiva de la Unión Europea relativa a los ataques contra los sistemas de información[1663] contiene una disposición en virtud de la cual se penaliza la interferencia ilegal en los datos.

> ***Artículo 5*** *– Interferencia ilegal en los datos*
> *Los Estados miembros adoptarán las medidas necesarias para que borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.*

La disposición fue redactada de conformidad con las normas definidas por el Convenio del Consejo de Europa sobre la Ciberdelincuencia.[1664] La principal diferencia reside en la posibilidad de limitar la penalización a los casos de menor gravedad.

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

En la Sección 8 de la Ley modelo de la Commonwealth de 2002[1665] se aplica un enfoque que está en consonancia con el Artículo 4 del Convenio del Consejo de Europa sobre la Ciberdelincuencia.

Disposición

> ***Interferencia con datos***
> ***6.*** *(1) Toda persona que, deliberada o imprudentemente, sin excusa o justificación legal, realice cualesquiera de los siguientes actos:*
> *(a) destruya o altere datos; o*
> *(b) haga que los datos resulten incompresibles, inútiles o ineficaces; o*

(c) obstruya, interrumpa o interfiera con la utilización legal de los datos; o
(d) obstruya, interrumpa o interfiera con cualquier persona en la utilización legal de los datos; o
(e) deniegue el acceso a los datos a cualquier persona con derecho a acceder a los mismos; cometerá una ofensa punible, previo fallo condenatorio, con una pena de prisión durante un periodo no superior a [periodo] o con una multa no superior a [cuantía], o ambas cosas.
(2) El apartado (1) se aplica independientemente del hecho de que el acto de la persona tenga un efecto temporal o permanente.

La primera diferencia principal entre la Sección 6 y la disposición correspondiente del Convenio sobre la Ciberdelincuencia es que esta disposición de la Ley modelo de la Commonwealth, además de los actos deliberados, penaliza incluso los actos imprudentes. A diferencia de la Sección 6, hay otras tres disposiciones de la Ley modelo[1666] que, como en el Convenio sobre la Ciberdelincuencia, se limitan a penalizar los actos deliberados. La cobertura de la imprudencia amplía significativamente el enfoque, ya que incluso la eliminación involuntaria de los archivos de un sistema informático o el daño a un dispositivo de almacenamiento conducirían a sanciones penales.

La segunda diferencia es que los actos cubiertos por la Sección 6 varían ligeramente de los cubiertos en la disposición correspondiente del Convenio sobre la Ciberdelincuencia. Finalmente, en el apartado 2 de la disposición se aclara que los actos no requieren que tengan un efecto permanente, que incluso los efectos temporales están cubiertos.

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford de 1999 ("Proyecto de Stanford"), de carácter oficioso[1667], contiene dos disposiciones a tenor de las cuales se penalizan los actos relacionados con la interferencia con los datos informáticos.

Disposición

Artículo 3
1. A tenor del presente Convenio, cometerá un delito cualquier persona que ilegal e intencionalmente realice cualesquiera de los siguientes actos sin autorización, permiso o consentimiento reconocidos legalmente:
(a) cree, almacene, altere, borre, transmita, desvíe, desencamine, manipule o interfiera con datos o programas de un cibersistema con la finalidad de causar, o sabiendo que esas actividades causarán a dicho cibersistema u otros cibersistemas una interrupción de su funcionamiento previsto, o que lo harán desempeñar funciones o realizar actividades no previstas por su propietario y consideradas ilegales a tenor del presente Convenio;
(b) cree, almacene, altere, borre, transmita, desvíe, desencamine, manipule o interfiera con los datos (de un cibersistema con la finalidad y el efecto de proporcionar información falsa para causar daños apreciables a una persona o a la propiedad.

Actos contemplados

La principal diferencia entre el Convenio del Consejo de Europa sobre la Ciberdelincuencia y la Ley modelo de la Commonwealth, por una parte, y el enfoque del Proyecto de Stanford, por otra, estriba en que este último penaliza únicamente la interferencia con los datos si ello interfiere con el funcionamiento de un sistema informático (párrafo 1 a) del Artículo 3) o si el acto se comete con la finalidad de proporcionar información falsa para causar daños a una persona o a la propiedad (párrafo 1 b) del Artículo 3). Por lo tanto, el proyecto de Stanford no penaliza el borrado de un texto de un dispositivo de almacenamiento de datos, puesto que esto no influye en el funcionamiento de un ordenador ni entraña el suministro de información falsa. Tanto el Convenio del Consejo de Europa sobre la Ciberdelincuencia como la Ley modelo de la Commonwealth aplican un enfoque más amplio, por cuanto protegen la integridad de los datos informáticos sin que se deba cumplir obligatoriamente el requisito de que ello tenga efectos adicionales.

6.2.6 Interferencia con el sistema

Las personas o las empresas que ofrecen servicios basados en las TIC dependen del funcionamiento de sus sistemas informáticos[1668]. La indisponibilidad de páginas web que son víctimas de ataques de denegación de servicio (*Denial-of-Service*, DOS)[1669] pone de relieve la gravedad del ataque[1670]. Este tipo de ataques puede provocar importantes pérdidas financieras y afectar incluso a los sistemas más poderosos[1671]. Las empresas no son las únicas víctimas. Actualmente los expertos de todo el mundo se encuentran considerando posibles hipótesis de "ciberterrorismo" en las que se tienen en cuenta los ataques contra infraestructuras esenciales tales como las fuentes de suministro de electricidad y los servicios de telecomunicaciones[1672]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

Con el fin de proteger el acceso de los operadores y los usuarios a las TIC, en su Artículo 5 el Convenio del Consejo de Europa sobre la Ciberdelincuencia contiene una disposición que penaliza la obstaculización deliberada del uso legal de los sistemas informáticos.[1673]

Disposición

Artículo 5 – Ataques a la integridad del sistema
Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Actos contemplados

Para aplicar esta disposición es necesario que se obstaculice el funcionamiento de un sistema informático[1674]. Por "obstaculización" se entiende cualquier acto que interfiera con el funcionamiento correcto de un sistema informático[1675]. La aplicación de esta disposición se limita a los casos en los cuales la obstaculización es el resultado de uno de los actos antes mencionados. Además, la aplicación de esta disposición requiere que la obstaculización sea "grave". Incumbe a las Partes determinar los criterios que se han de cumplir para que la obstaculización se considere grave.[1676] Entre las posibles restricciones a tenor de la ley nacional podrían figurar la exigencia de un volumen mínimo de daños, así como la posibilidad de limitar la penalización a los ataques contra importantes sistemas informáticos.[1677]

La lista de actos que influyen de manera negativa en el funcionamiento de un sistema informático es concluyente[1678].

El término "introducción" no se define en el mismo Convenio sobre la Ciberdelincuencia, ni tampoco lo hacen los redactores del mismo. Dado que en el Artículo 5 la transmisión se menciona como otro acto más, el término "introducción" podría definirse como cualquier acto relacionado con la utilización de interfaces de entrada físicas para transferir información a un sistema informático, mientras que el término "transmisión" se referiría a actos que suponen la introducción de datos a distancia[1679].

Los términos "daño" y "deterioro" tienen significados superpuestos y fueron definidos por los redactores del Convenio sobre la Ciberdelincuencia, en el Informe Explicativo en relación con el Artículo 4, como una alteración negativa de la integridad del contenido informativo de los datos y programas[1680].

Los redactores del Convenio también definieron en el Informe Explicativo en relación con el Artículo 4 el término "borrado", que cubre aquellos actos como consecuencia de los cuales se elimina información de los medios de almacenamiento[1681].

El término "alteración" se refiere a la modificación de los datos existentes, sin que disminuya forzosamente su disponibilidad[1682].

La "supresión" de datos informáticos denota una acción que afecta negativamente a la disponibilidad de los datos para la persona que tiene acceso al medio en el que la información se almacena.[1683]

Aplicación de la disposición en lo que respecta al correo basura

Se consideró si el problema del correo electrónico basura (*spam*)[1684] podía abordarse en el marco del Artículo 5, puesto que el correo basura puede sobrecargar los sistemas informáticos[1685]. Los redactores del Convenio indicaron claramente que el correo basura puede no conducir forzosamente a una obstaculización "grave" y que la "conducta sólo debe penalizarse cuando la comunicación se vea obstaculizada de manera deliberada y grave"[1686]. Los redactores señalaron asimismo que, en función de su propia legislación nacional[1687], las Partes podrían aplicar un enfoque diferente en lo tocante a la obstaculización, por ejemplo, tipificar como delitos administrativos o actos susceptibles de sanción a los actos de interferencia.[1688]

Predisposición

Como ocurre con el resto de los delitos definidos en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, en el Artículo 5 se impone el requisito de que, para proceder a la penalización, el delincuente cometa sus infracciones intencionalmente[1689]. Ello incluye la intención de llevar a cabo uno de los actos enumerados, así como la intención de obstaculizar gravemente el funcionamiento de un sistema informático.

El Convenio sobre la Ciberdelincuencia no contiene ninguna definición del término "intencionalmente". En el Informe Explicativo, los redactores subrayaron que el término "intencionalmente" debía definirse a escala nacional.[1690]

Sin derecho

Es preciso que el acto se efectúe "sin derecho"[1691]. Según se mencionó anteriormente, los administradores de la red y las empresas de seguridad que someten a prueba la protección de los sistemas informáticos temían la posible penalización de sus trabajos[1692]. Ahora bien, estos profesionales trabajan con el permiso del propietario y por lo tanto actúan legalmente. Además, los redactores del Convenio sobre la Ciberdelincuencia indicaron explícitamente que el someter a prueba la seguridad de un sistema informático con la autorización del propietario no constituye un acto sin derecho.[1693]

Restricciones y reservas

A diferencia de los Artículos 2 a 4, el Artículo 5 no ofrece una posibilidad explícita de limitar la aplicación de la disposición a la implementación en la ley nacional. No obstante, la responsabilidad de las Partes de definir la gravedad del delito les confiere la posibilidad de ajustar la penalización durante el proceso de aplicación. En la Decisión marco de la Unión Europea[1694] relativa a los ataques contra los sistemas de información[1695] se aplica un enfoque similar.

Ley modelo de la Commonwealth sobre delitos informáticos y delitos relacionados con la informática

En la Sección 7 de la Ley modelo de la Commonwealth de 2002 se aplica un enfoque que está en consonancia con el Artículo 5 del Convenio del Consejo de Europa sobre la Ciberdelincuencia.[1696]

Disposición

Sec Interferencia con sistemas informáticos

7. *(1) Toda persona que deliberada o imprudentemente y sin una excusa o justificación legal:*

(a) obstaculice o interfiera con el funcionamiento de un sistema informático; o

(b) obstaculice o interfiera con una persona que utiliza u opera legalmente un sistema informático; cometerá un delito punible, previo fallo condenatorio, con una pena de prisión por un periodo no superior a [periodo] o una multa no superior [cuantía], o ambas cosas.

En el apartado (1) la "obstaculización" relacionada con un sistema informático incluye, entre otros, los siguientes actos:

(a) cortar el suministro de electricidad a un sistema informático; y

(b) causar interferencia electromagnética a un sistema informático; y

(c) corromper un sistema informático por cualquier medio; y

(d) introducir, borrar o alterar datos informáticos;

La principal diferencia con respecto a la disposición correspondiente del Convenio del Consejo de Europa sobre la Ciberdelincuencia estriba en que, a tenor de lo dispuesto en la Sección 7 de la Ley modelo de la Commonwealth, se penalizan incluso los actos de imprudencia. Por tanto, incluso el corte involuntario del suministro de energía durante unas obras de construcción puede conllevar sanciones penales. Al aplicar este enfoque, la Ley modelo va más allá de los requisitos impuestos en el Convenio sobre la Ciberdelincuencia. Otra diferencia es que en la definición de "obstaculización" consignada en la Sección 7 de la Ley modelo de la Commonwealth se enumera un mayor número de actos que los indicados en el Artículo 5 del Convenio del Consejo de Europa sobre la Ciberdelincuencia.

Directiva de la Unión Europea relativa a los ataques contra los sistemas de información

En su Artículo 4, la Directiva de la Unión Europea relativa a los ataques contra los sistemas de información[1697] contiene una disposición en virtud de la cual se penaliza la interferencia ilegal en los sistemas de información.

> ***Artículo 4*** *– Interferencia ilegal en los sistemas de información*
> *Los Estados miembros adoptarán las medidas necesarias para que la obstaculización o la interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.*

La disposición fue redactada de conformidad con las normas definidas por el Convenio del Consejo de Europa sobre la Ciberdelincuencia.[1698] La principal diferencia reside en la posibilidad de limitar la penalización a los casos de menor gravedad.

El enfoque se basa en el Convenio del Consejo de Europa sobre la Ciberdelincuencia. La primera diferencia principal es que, además de los actos contemplados en el Convenio sobre la Ciberdelincuencia (introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo), el Artículo 4 penaliza también la obstaculización del funcionamiento de un sistema informático "haciendo inaccesibles datos informáticos". Los datos se quedan inaccesibles si, por cometer el acto, el delincuente impide a alguien tener acceso a ellos. Sin embargo, a pesar de la lista más compleja de actos del Artículo 4, no hay ninguna diferencia con el artículo correspondiente del Convenio del Consejo de Europa sobre la Ciberdelincuencia en la medida en que el acto de dejar inaccesibles datos informáticos está cubierto por el acto de la supresión de los datos. En la explicación al 19º proyecto de versión del Convenio sobre la Ciberdelincuencia se destaca que el grupo de expertos que lo redactó coincidían en que la supresión de datos tiene dos significados: la eliminación de datos de manera que físicamente dejan de existir y el hecho de dejar los datos inaccesibles.[1699]

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford de 1999, de carácter oficioso[1700], contiene una disposición que penaliza los actos relacionados con la interferencia a los sistemas informáticos.

Disposición

> ***Art. 3***
> *1. A tenor del presente Convenio, cometerá un delito toda persona que ilegal y deliberadamente realice cualesquiera de los siguientes actos sin autorización, permiso o consentimiento reconocidos legalmente:*
> *(a) cree, almacene, altere, borre, transmita, desvíe, desencamine, manipule o interfiera con datos o programas de un cibersistema con la finalidad de causar o sabiendo que esas actividades causarán a dicho cibersistema o a otros cibersistemas una interrupción del funcionamiento previsto, o que lo harán desempeñar funciones o realizar actividades no previstas por su propietario y consideradas ilícitas a tenor de este Convenio;*

Actos contemplados

La principal diferencia entre el Convenio del Consejo de Europa sobre la Ciberdelincuencia y la Ley modelo de la Commonwealth y el enfoque aplicado en el Proyecto de Stanford estriba en que en este último se abarca cualquier manipulación de los sistemas informáticos, mientras que el Convenio del Consejo de Europa sobre la Ciberdelincuencia y la Ley modelo de la Commonwealth limitan la penalización a la obstaculización del funcionamiento de un sistema informático.

6.2.7 Material erótico y pornográfico

La penalización del contenido ilícito y sexual explícito, así como la gravedad de la misma, varía según el país[1701]. Las Partes que negociaron el Convenio del Consejo de Europa sobre la Ciberdelincuencia se concentraron en la armonización de la legislación sobre pornografía infantil, dejando de lado la penalización en general del material erótico y pornográfico. En algunos países se ha abordado este asunto mediante la aplicación de disposiciones que penalizan el intercambio de material pornográfico a través de sistemas informáticos. Ahora bien, la falta de definiciones normativas dificulta a las fuerzas de seguridad la investigación de tales delitos cuando los infractores actúan desde países que no penalizan el intercambio de contenido sexual[1702]

Ejemplos

Como ejemplo de penalización del intercambio de material pornográfico puede citarse la Sección 184 del Código Penal alemán.

Sección 184 – Distribución de escritos pornográficos.
(1) Quien, en lo relativo a escritos pornográficos (Sección 11, subsección (3)):

1. los ofrezca, ceda o ponga a disposición de menores de dieciocho años de edad;
2. los muestre, publique, presente o ponga a disposición en lugares accesibles a menores de dieciocho años de edad o donde éstos puedan verlos;
3. los ofrezca o entregue a otra persona en una operación comercial al por menor fuera de locales comerciales, en quioscos u otros puntos de venta en los que normalmente el cliente no entra, en venta por correo o en bibliotecas de préstamo comercial o en círculos de lectura;
3a. los ofrezca o ceda a otra persona en alquiler u otra forma comparable de operación comercial, salvo en tiendas que no permitan la entrada a menores de dieciocho años ni éstos puedan ver su interior;
4. los trate de importar mediante un pedido por correo;
5. los ofrezca, anuncie o recomiende en un lugar accesible a menores de dieciocho años o donde éstos puedan verlos, o los distribuya por transacciones no comerciales en puntos de venta normales;
6. permita que otros los obtengan sin habérselo solicitado;
7. los muestre en una sala de cine pública con un precio de entrada que cubriese íntegra o parcialmente su proyección;
8. los produzca, obtenga, suministre, almacene o trate de importar para utilizarlos o hacer copias de los mismos según lo especificado en los apartados 1 a 7 o facilite que otros así lo utilicen; o
9. los trate de exportar con el fin de distribuir los originales o copias en el extranjero de manera que infrinja las disposiciones penales aplicables en el país del caso o los haga públicos o facilite que otros los hagan públicos, será sancionado con una pena de prisión no superior a un año o una multa.

Esta disposición se basa en el concepto de que las transacciones comerciales y de otro tipo de escritos pornográficos no se penalizan siempre y cuando no haya menores de por medio[1703]. Así pues, la ley tiene por objetivo proteger el desarrollo del menor sin trastornos[1704]. El que la pornografía tenga una incidencia negativa en el desarrollo del menor es un asunto polémico[1705]. La Sección 184 no penaliza el intercambio de escritos pornográficos entres adultos. Por "escritos" se entiende no sólo los escritos tradicionales, sino también los digitales[1706]. Análogamente, "ponerlos a disposición" no sólo se refiere a actos fuera de Internet, sino también a los casos en que los infractores lo publican en sitios web[1707].

Un ejemplo de enfoque más estricto, que penaliza todo contenido sexual es la Sección 4.C.1, del proyecto de Ley de la Cámara Legislativa de Filipinas Nº 3777 de 2007.[1708]

> ***Sección 4.C1.:*** *Delitos relacionados con el cibersexo – Sin perjuicio de la interposición de un acto judicial con arreglo a las Leyes de la República Nº 9208 y Nº 7610, toda persona que anuncie, promueva o facilite la realización de cibersexo a través de las tecnologías de la información y la comunicación por computador, redes informáticas, televisión, satélite, teléfono móvil, etc., […]*
> ***Sección 3i.:*** *Cibersexo o sexo virtual – Se refiere a cualquier forma de actividad o excitación sexual con la ayuda de computadores o redes de comunicaciones*

Esta disposición adopta un enfoque muy general, dado que penaliza cualquier tipo de anuncio o facilitación de actividad sexual por Internet. Debido al principio de doble criminalización[1709], las investigaciones de alcance internacional respecto a estos enfoques generales se topan con dificultades.[1710]

6.2.8 Pornografía infantil

Internet se está convirtiendo en el principal instrumento para el comercio e intercambio de material con pornografía infantil[1711]. Las principales razones de este desarrollo son la velocidad y eficacia de Internet para la transferencia de ficheros, los reducidos costes de producción y distribución y la sensación de anonimato[1712]. Las fotos que se publican en una página web son accesibles por millones de usuarios del mundo, que pueden descargarlas[1713]. Una de las razones más importantes del "éxito" de las páginas web que contienen pornografía, incluida la infantil, es que el usuario de Internet se siente menos observado desde su casa mientras descarga material de Internet. A no ser que los usuarios recurran a mecanismos para la comunicación anónima, la impresión de que no deja rastros es falsa[1714]. Lo que sucede es sencillamente que la mayoría de los usuarios desconocen las huellas electrónicas que dejan cuando navegan por Internet[1715].

Las disposiciones que penalizan la pornografía infantil en general se redactan para proteger intereses jurídicos diferentes. La penalización de la producción de pornografía infantil busca proteger a los niños de que sean víctimas de abuso sexual.[1716] Con respecto a la prohibición de actos relacionados con el intercambio de pornografía infantil (oferta, distribución) así como tenencia, la penalización pretende conseguir que desaparezca el mercado, en la medida en que la continua demanda de nuevos materiales podría motivar a delincuentes a continuar con el abuso de niños.[1717] Además, la prohibición del intercambio busca que a las personas les resulte más difícil acceder a dichos materiales y así prevenir que se desencadene más abuso sexual de niños. Por último, con la penalización de la tenencia se pretende impedir que los delincuentes utilicen material de pornografía infantil para seducir a los niños a involucrarse en relaciones sexuales.[1718]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

Para mejorar y armonizar la protección del menor contra la explotación sexual[1719], el Convenio sobre la Ciberdelincuencia incluye un artículo relativo a la pornografía infantil.

Disposición

Artículo 9 – Delitos relacionados con la pornografía infantil
(1) Cada Parte adoptará las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
b) la oferta o puesta a disposición de pornografía infantil a través de un sistema informático;
c) la difusión o transmisión de pornografía infantil a través de un sistema informático;
d) la adquisición para uno mismo o para otros de pornografía infantil a través de un sistema informático;
e) la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

(2) A los efectos del párrafo 1 anterior, se entenderá por "pornografía infantil" todo material pornográfico que contenga la representación visual de:

a) un menor adoptando un comportamiento sexualmente explícito;
b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

(3) A los efectos del párrafo 2 anterior, se entenderá por "menor" toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo 16 años.
(4) Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

La mayoría de los países penalizan el abuso de menores y los métodos tradicionales de distribución de pornografía infantil[1720]. Por tanto, la Convención sobre Ciberdelincuencia no se limita a colmar las lagunas del derecho penal nacional[1721], sino que trata de armonizar las reglamentaciones divergentes.[1722]

Actos contemplados

La "producción" describe cualquier proceso de creación de pornografía infantil. En la actualidad se debate sobre la interpretación del término. En el Reino Unido, la descarga de imágenes de pornografía infantil se considera como producción de pornografía infantil.[1723] El hecho de que en el Artículo 9 del Convenio del Consejo de Europa sobre la Ciberdelincuencia se distinga entre "adquisición" y "producción" indica que el redactor no consideraba la mera descarga de pornografía infantil como producción. A pesar de la distinción realizada en el Convenio sobre la Ciberdelincuencia, aún se necesita diferenciar más. Un delincuente que toma fotografías de niños que sufren abuso es producir pornografía infantil; pero es dudoso que una persona que utilice imágenes de pornografía infantil para ponerlas juntas en una animación esté produciendo también pornografía infantil. Aunque sin duda es el productor de la animación, existen dudas de que el término "producción" en el Convenio del Consejo de Europa sobre la Ciberdelincuencia sólo se pueda aplicar cuando se documentan abusos reales de niños. El hecho de que el Convenio sobre la Ciberdelincuencia pretenda penalizar la producción de pornografía infantil ficticia, que no requiere el abuso real de un niño, es un argumento a favor de una interpretación amplia del término "producción". Por otro lado, el informe explicativo del Convenio sobre la Ciberdelincuencia indica que se necesita penalizar la producción para combatir el peligro "en el origen".[1724] Aunque el Convenio del Consejo de Europa sobre la Ciberdelincuencia no especifica esa intención de los redactores, el informe explicativo del Convenio del Consejo de Europa sobre la protección de los niños[1725] proporciona una explicación más concreta de la motivación de los redactores con respecto a una disposición similar.[1726] Los redactores del Convenio sobre la protección de los niños destacan que la penalización de la producción de pornografía infantil es "necesaria para combatir los actos de abuso y explotación sexuales en su origen", lo que puede verse como un argumento en favor a un enfoque más estricto.

Es necesario que la producción de pornografía infantil se realice con la intención de difundirla a través de un sistema informático. Si el delincuente produce el material para su propio uso o tiene la intención de

distribuirlo en forma no electrónica, no se puede aplicar el Artículo 9 del Convenio del Consejo de Europa sobre la Ciberdelincuencia. Otro problema controvertido en relación con la producción es la cobertura de la autorrepresentación.[1727] Si el delincuente, a distancia, convence a un niño para que tome fotografías pornográficas de sí mismo este acto, dependiendo de la legislación nacional, podría llevar a la penalización de la víctima (el niño) y no a la del delincuente.

La "oferta" cubre el acto de solicitar a otros que consigan pornografía infantil. No es necesario que el material se ofrezca en una relación comercial, pero sí implica que el delincuente que ofrece el material sea capaz de proporcionarlo.[1728] La "puesta a disposición" se refiere al acto que permite a otros usuarios acceder a pornografía infantil. El acto puede cometerse colocando pornografía infantil en páginas Web o conectándose a sistemas de compartición de archivos y permitiendo a otros acceder a ese material en dispositivos o carpetas de almacenamiento desbloqueados.

La "difusión" cubre los actos activos de redistribuir pornografía infantil a otros. La "transmisión" cubre todas las comunicaciones realizadas por medio de transmisión de señales. La "adquisición" para uno mismo o para otros cubre cualquier acto de obtención activa de pornografía infantil.

El Artículo 9, por último, tipifica como delito la "posesión" de pornografía infantil. La penalización de la posesión de pornografía infantil también varía según cada sistema jurídico nacional[1729] La demanda de este tipo de materiales podría conducir a su producción de forma habitual.[1730] Su posesión podría alentar el abuso sexual de niños, por lo que los redactores sugieren que una forma eficaz de reducir la producción de pornografía infantil es legislar que la posesión sea ilegal.[1731] Sin embargo, en el párrafo 4 del Convenio se permite a las Partes no penalizar la mera posesión, es decir, que la responsabilidad penal se limite sólo a la producción, oferta y distribución de pornografía infantil.[1732] La posesión implica el control que una persona ejerce intencionalmente sobre materiales de pornografía infantil. Requiere que el delincuente tenga el control sobre ellos, que no sólo se tiene con los dispositivos de almacenamiento locales sino también con los dispositivos de almacenamiento remotos sobre los que tenga acceso y control. Además, la posesión, en general, requiere una predisposición como se indica en la definición anterior.

Pornografía infantil

En el párrafo 2 del Artículo 9 figuran tres subsecciones acerca de materiales que representan visualmente la pornografía infantil: un menor adoptando un comportamiento sexualmente explícito; una persona que parezca un menor adoptando un comportamiento sexualmente explícito e imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito. El hecho de que sea necesaria una representación visual excluye los archivos de audio.

Aunque el objetivo de los redactores es aumentar la protección del menor contra la explotación sexual, el párrafo 2 tiene un alcance jurídico más amplio. El párrafo 2(a) se centra directamente en la protección contra el abuso infantil. Sin embargo, los párrafos 2(b) y 2(c) cubren imágenes que se han producido sin violar los derechos del niño, por ejemplo, imágenes creadas mediante el uso de programas de modelado en 3D.[1733] La razón por la que se penaliza la pornografía infantil ficticia es que dichas imágenes, aunque se crean sin causar daño alguno a ningún "niño" real, pueden utilizarse para seducir a niños con el fin de que participen en tales actos.[1734]

Uno de los principales problemas relacionados con la definición es que se centra en la representación visual. La pornografía infantil no se distribuye necesariamente como imágenes o películas, sino también como archivos de audio.[1735] Debido a que la disposición proporcionada en el Artículo 9 se refiere a "material pornográfico que contenga la representación visual de" un niño, la disposición no cubre los archivos de audio. Como consecuencia, los enfoques más recientes como el texto [1736] legislativo sobre la ciberdelincuencia de HIPCAR[1737] adoptan un enfoque diferente y evitan el término "visualmente".

Definiciones
3.
[…]
(4) Se entenderá por "pornografía infantil" el material pornográfico que ilustra, presenta o representa a:
a) un niño adoptando un comportamiento sexualmente explícito;
b) una persona que parezca un niño adoptando un comportamiento sexualmente explícito; o
c) imágenes que representen a un niño adoptando un comportamiento sexualmente explícito;
esta definición incluye, pero no se limita a, cualquier material pornográfico sonoro, visual o textual.
Un país puede decidir restringir la penalización no aplicando los apartados (b) y (c).

Otra definición más amplia puede encontrarse en el Artículo 2 c) del Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.

Artículo 2
A los efectos del presente Protocolo:
[…]
(c) Por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.

Una de las diferencias más importantes entre diferentes legislaciones nacionales es la edad de la persona implicada. Algunos países definen en su legislación el término "menor", en relación con la pornografía infantil, con arreglo a la definición de "niño" que figura en el Artículo 1 de la Convención sobre los Derechos del Niño de las Naciones Unidas[1738], a saber, todo ser humano menor de 18 años de edad. Otros países consideran menor a las personas menores de 14 años[1739]. En la Decisión marco de 2003 del Consejo de Europa relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil[1740] se adopta un planteamiento similar y en el Convenio de 2007 del Consejo de Europa relativo a la protección a los niños contra la explotación y el abuso sexual[1741]. Subrayando la importancia de alcanzar la unanimidad internacional en lo que respecta a la edad, el Convenio sobre la Ciberdelincuencia define este término con arreglo al Convenio de las Naciones Unidas[1742]. Sin embargo, debido a las grandes diferencias en las legislaciones nacionales existentes, el Convenio sobre la Ciberdelincuencia permite a las Partes adoptar un límite de edad diferente pero no inferior a los 16 años. Un problema que se plantea cada vez más frecuentemente es la posible penalización no intencionada que se produce cuando no coinciden la edad de consentimiento sexual y la edad límite fijada por la definición.[1743] Por ejemplo, cuando la pornografía infantil se define como la representación visual de actos sexuales de personas menores de 18 años y, al mismo tiempo, la edad de consentimiento sexual, como 16, dos jóvenes de 17 años legalmente podrían tener relaciones sexuales pero cometerían un grave delito (producción de pornografía infantil) si tomaran fotos o películas de este acto.[1744]

Predisposición

Al igual que otros delitos definidos en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, en el Artículo 9 se exige que el infractor actúe de una manera deliberada[1745]. En el Informe Explicativo se subraya explícitamente que el Convenio sobre la Ciberdelincuencia no contempla la interacción no deliberada con la pornografía infantil. Este hecho es especialmente pertinente en los casos en que el infractor abre sin querer una página web que contiene pornografía infantil y, pese a que cierra inmediatamente la página, algunas de las imágenes quedan almacenadas en ficheros temporales o en la caché del navegador.

Sin derecho

De conformidad con el Artículo 9 del Convenio sobre la Ciberdelincuencia, sólo pueden penalizarse los actos relacionados con la pornografía infantil que se realizan "sin derecho"[1746]. En el Convenio sobre la Ciberdelincuencia no se especifica más concretamente los casos en que el usuario actúa con autorización.

En general siempre se actúa "sin derecho" salvo en el caso de los miembros de las fuerzas de seguridad en el marco de una investigación.

Convenio del Consejo de Europa sobre la Protección de los Niños

Otro ejemplo de penalización de la pornografía infantil es el Artículo 20 del Convenio del Consejo de Europa relativo a la protección del niño contra la explotación sexual y el abuso sexual.[1747]

Disposición

Artículo 20 *– Delitos relativos a la pornografía infantil*
(1) Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito las siguientes conductas intencionales, cuando se cometan de forma ilícita:
a) la producción de pornografía infantil;
b) la oferta o puesta a disposición de pornografía infantil;
c) la difusión o transmisión de pornografía infantil;
d) la adquisición para sí o para otro de pornografía infantil;
e) la posesión de pornografía infantil;
f) el acceso a pornografía infantil, con conocimiento de causa y por medio de las tecnologías de la información y la comunicación.
(2) A efectos del presente artículo, por «pornografía infantil» se entenderá todo material que represente de forma visual a un niño manteniendo una conducta sexualmente explícita, real o simulada, o toda representación de los órganos sexuales de un niño con fines principalmente sexuales.
(3) Cada Parte se reserva el derecho de no aplicar, en todo o en parte, los apartados 1.a) y 1.e) relativos a la producción y posesión de material pornográfico:
– que consista exclusivamente en representaciones simuladas o imágenes realistas de un niño no existente;
– en el que participen niños que hayan alcanzado la edad fijada en aplicación del apartado 2 del Artículo 18, cuando dichas imágenes hayan sido producidas por ellos y estén en su poder, con su consentimiento y únicamente para su uso particular.
(4) Cada Parte podrá reservarse el derecho de no aplicar, en todo o en parte, el apartado 1.f.

Actos contemplados

Esta disposición se basa en el Artículo 9 del Convenio del Consejo de Europa sobre la Ciberdelincuencia y, por tanto, es comparable en gran medida al mismo[1748]. La principal diferencia radica en que el Convenio del Consejo de Europa sobre la Ciberdelincuencia se concentra en la penalización de actos relativos a los servicios de información y comunicaciones ("producción de pornografía infantil con la intención de difundirla a través de un sistema informático") mientras que el Convenio sobre la Protección de los Niños adopta un enfoque más general ("producción de pornografía infantil") que contempla incluso los actos que guardan relación con las redes informáticas.

A pesar de las similitudes en cuanto a los actos contemplados, el Artículo 20 del Convenio sobre la Protección de los Niños integra un acto no contemplado en el relativo a la Ciberdelincuencia. De conformidad con el párrafo 1 del Artículo 20 del Convenio sobre la Protección de los Niños, el acceso a pornografía infantil a través de un computador está penalizado. El término "acceder" cubre cualquier acto que dé comienzo a procesos que muestren información facilitada *a través de las tecnologías de la información y la comunicación*. Como sería el caso, por ejemplo, cuando el delincuente entra el nombre de dominio de un sitio web conocido de pornografía e inicia el proceso de recepción de información de la primera página, que implica necesariamente un proceso de descarga automatizado. Esto permite a las fuerzas de seguridad incriminar a los infractores en los casos en que pueden probar que el infractor ha abierto un sitio web con pornografía infantil pero no pueden demostrar que el infractor haya descargado material. Surgen dificultades en la recopilación de pruebas cuando, por ejemplo, el infractor utiliza tecnologías de cifrado para proteger los ficheros descargados en su dispositivo de almacenamiento[1749]. En el Informe Explicativo del Convenio sobre la Protección de los Niños se indica que la disposición también

debe aplicarse en los casos en los que el infractor visualiza imágenes de pornografía infantil en línea aunque no las descargue[1750]. En general, al abrir un sitio web se inicia automáticamente un proceso de descarga, a menudo sin el conocimiento del usuario[1751]. El caso mencionado en el Informe Explicativo sólo atañe, por ende, a los casos en que no se produce la descarga de fondo.

Ley modelo de la Commonwealth sobre informática y delitos relacionados con la informática

En la Sección 10 de la Ley modelo de la Commonwealth de 2002 se adopta un enfoque similar al del Artículo 9 del Convenio del Consejo de Europa sobre la Ciberdelincuencia.[1752]

Pornografía infantil
10 *(1) Todo el que, deliberadamente, lleve a cabo uno de los actos siguientes:*
(a) publique pornografía infantil a través de un sistema informático; o
(b) produzca pornografía infantil con la intención de publicarla a través de un sistema informático; o
(c) posea pornografía infantil en un sistema informático o un dispositivo de almacenamiento de datos informáticos; comete un delito penado con encarcelamiento por un periodo no superior a [periodo], o una multa que no excederá de [importe], o ambos.[1753]
(2) Puede esgrimirse contra la acusación de un delito en virtud del párrafo (1) (a) o (1) (c) si la persona demuestra que la finalidad genuina de la pornografía infantil era la realización de estudios científicos, la investigación, la medicina o la aplicación de la ley.[1754]
(3) En esta sección:
se entenderá por "pornografía infantil" todo material pornográfico que contenga la representación visual de:
(a) un menor adoptando un comportamiento sexualmente explícito; o
(b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito; o
(c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.
Se entenderá por "menor" toda persona menor de [x] años.
Se entenderá por "publicar":
(a) distribuir, transmitir, divulgar, circular, enviar, mostrar, prestar con fines lucrativos, intercambiar, hacer trueques, vender o poner en venta, alquilar u ofrecer para alquilar, ofrecer de cualquier otro modo, o poner a disposición de cualquier otro modo; o
(b) tener en posesión o en custodia, o bajo control, a los efectos de realizar un acto de los mencionados en el párrafo (a); o
(c) imprimir, fotografiar, copiar o generar de cualquier otro modo (ya sea de la misma naturaleza o de una diferente) a los efectos de realizar un acto de los mencionados en el párrafo (a).

La principal diferencia respecto al Convenio del Consejo de Europa sobre la Ciberdelincuencia estriba en que la Ley modelo de la Commonwealth no define el término "menor" y permite a los Estados Miembros definir la edad límite. Al igual que ocurre en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, en la Ley modelo de la Commonwealth no se prevé la penalización de la obtención de acceso a la pornografía infantil a través de las tecnologías de la información.

Protocolo facultativo de la Convención sobre los Derechos del Niño de las Naciones Unidas

En el Artículo 3 del Protocolo facultativo relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía se encuentra un enfoque tecnológicamente neutro.

Artículo 3
1. Todo Estado Parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeran queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente:
[...]
c) La producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil, en el sentido en que se define en el Artículo 2.
[...]

Aunque el Protocolo facultativo se refiere explícitamente al papel de Internet en la distribución de dichos materiales,[1755] penaliza actos relacionados con la pornografía infantil en una forma neutral en cuanto a la tecnología. La pornografía infantil se define como toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.[1756] Los actos contemplados son comparables a los del Convenio sobre la Ciberdelincuencia, salvo que la disposición en el Artículo 3 se redactó para que fuera neutral con la tecnología.

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford[1757] de 1999 no prevé la penalización del intercambio de pornografía infantil a través de sistemas informáticos. En el Convenio se destaca que en general no debe considerarse delictivo en el marco del Proyecto de Stanford ningún discurso o publicación[1758]. El Convenio reconoce los distintos enfoques y deja a los Estados que decidan acerca de la penalización de estos aspectos.[1759]

6.2.9 Seducción de niños

Internet ofrece la posibilidad de comunicarse con otras personas sin revelar la edad o el género. Los delincuentes pueden abusar de esta posibilidad para seducir a niños.[1760] El fenómeno se denomina frecuentemente "grooming" (preparación o captación).[1761] Algunos marcos jurídicos regionales contienen disposiciones que penalizan dicho contacto.

Convenio sobre la protección de los niños del Consejo de Europa

Encontramos un ejemplo en el Artículo 23 del Convenio para la protección de los niños contra la explotación y el abuso sexual del Consejo de Europa.[1762]

Artículo 23 – Proposiciones a niños con fines sexuales
Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño que no haya alcanzado la edad fijada en aplicación del apartado 2 del Artículo 18 con el propósito de cometer contra él cualquiera de los delitos tipificados con arreglo al apartado 1.a del Artículo 18 o al apartado 1.a del Artículo 20, cuando a dicha proposición le hayan seguido actos materiales conducentes a dicho encuentro.

La seducción de un niño con el fin de abusar sexualmente de él, en general, no está cubierta por las disposiciones que penalizan el abuso sexual de niños, en la medida en que la seducción se considera un acto preparatorio. Teniendo en cuenta la creciente controversia sobre el grooming en línea, los redactores del Convenio decidieron incluir el Artículo 23 para penalizar ya los actos preparatorios.[1763] Para evitar la penalización excesiva, el redactor del Convenio destacó que la simple conversación sobre temas sexuales con un niño no debe considerarse suficiente para cometer el acto de seducción, aunque esto pueda formar parte de la preparación de un abuso sexual.[1764]

Hay dos problemas principales relacionados con este enfoque. En primer lugar, la disposición sólo cubre la seducción a través de las TIC. La disposición no cubre otras formas de seducción. Los redactores expresaron la opinión de que centrarse en estas tecnologías está justificado ya que son difíciles de controlar.[1765] Sin embargo, no se proporcionó ningún dato científicamente fiable que demostrara que la seducción de niños sólo es un problema en línea. Además, no sólo hay buenas razones para evitar situaciones donde algo que es ilegal cuando se comete fuera de línea sea legal cuando se hace en línea, también, al revés, para asegurarse de no penalizar comportamientos en línea que sean legales fuera de ella. La declaración conjunta de 2001 sobre los desafíos a la libertad de expresión en el nuevo siglo, por ejemplo, señala que los Estados no deben adoptar normas independientes que restrinjan el contenido de Internet; [1766]

Otro problema con la penalización de este acto preparatorio es que podría conducir a conflictos en el sistema de derecho penal, en la medida en que no se contempla la preparación de actos incluso más graves. Pondría en entredicho el sistema de valores de un país si estuviera penalizada la preparación del abuso sexual de un niño, mientras que la preparación de su asesinato no lo estuviera. Por lo tanto, cualquier enfoque de este tipo debería formularse dentro de un debate general sobre las ventajas y los riesgos de la penalización de los actos preparatorios.

6.2.10 Incitación al odio, racismo

El grado de penalización de la incitación al odio difiere significativamente.[1767] Especialmente en los países que tienen una protección constitucional alta de la libertad de expresión[1768] no se penaliza a menudo la incitación al odio. Las prohibiciones se encuentran sobre todo en África y Europa.[1769]

Convenio del Consejo de Europa sobre la Ciberdelincuencia (Protocolo Adicional)

El Consejo de Europa está desempeñando un papel activo en la lucha contra el racismo; adoptó, tras la Cumbre de Viena de 1993, una Declaración y un Plan de acción sobre la lucha contra el racismo, la xenofobia, el antisemitismo y la intolerancia,[1770] y, en 1995, unas recomendaciones sobre la lucha contra el racismo.[1771] La penalización de la incitación al odio y el racismo en línea se debatió durante la negociación del Convenio del Consejo de Europa sobre la Ciberdelincuencia. Dado que las partes que negociaron dicho Convenio no llegaron a un acuerdo[1772] acerca de una posición común sobre la penalización de la incitación al odio y los materiales xenófobos, las disposiciones relacionadas con esos delitos se integraron en un Primer Protocolo independiente al Convenio.[1773] Una de las principales dificultades de las disposiciones que penalizan los materiales xenófobos es mantener un equilibrio entre garantizar la libertad de expresión[1774] , por una parte, e impedir la violación de los derechos de las personas o grupos, por otra. Sin entrar en detalles, las dificultades en la negociación del Convenio del Consejo de Europa sobre la Ciberdelincuencia[1775] y el estado de las firmas y ratificaciones del Protocolo adicional[1776] demuestran que el diferente grado de protección de la libertad de expresión está obstaculizando un proceso de armonización.[1777] En lo que respecta especialmente al principio común de doble incriminación,[1778] la falta de armonización dificulta la aplicación de la ley en los casos de alcance internacional.[1779]

Disposición

Artículo 3 – Difusión de material racista y xenófobo mediante sistemas informáticos
1. Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta: difundir o poner a disposición del público de otro modo material racista y xenófobo por medio de un sistema informático.
2. Cualquiera de las Partes podrá reservarse el derecho de no imponer responsabilidad penal a la conducta prevista en el apartado 1 del presente artículo cuando el material definido en el apartado 1 del Artículo 2 propugne, promueva o incite a una discriminación que no esté asociada con el odio o la violencia, siempre que se disponga de otros recursos eficaces.
3. No obstante lo dispuesto en el apartado 2 del presente Artículo, cualquier Parte podrá reservarse el derecho de no aplicar el apartado 1 a aquellos casos de discriminación respecto de los cuales, a la luz de los principios establecidos en su ordenamiento jurídico interno en materia de libertad de expresión, no pueda prever los recursos eficaces a que se refiere en dicho apartado 2.

Artículo 4 – Amenazas con motivación racista y xenófoba
Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta:
amenazar, por medio de un sistema informático, con la comisión de un delito grave, tal como se define en su derecho interno, i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o ii) a un grupo de personas que se distinga por alguna de esas características
Artículo 5 – Insultos con motivación racista y xenófoba
1 . Cada parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta:
insultar en público, por medio de un sistema informático, i) a personas por razón de su pertenencia a un grupo que se caracterice por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o ii) a un grupo de personas que se distinga por alguna de esas características.
2. Cualquiera de las Partes podrá:
a. exigir que el delito a que se refiere el apartado 1 del presente Artículo tenga como efecto exponer a la persona o grupo de personas previstas en el apartado 1 al odio, al desprecio o al ridículo; o
b. reservarse el derecho de no aplicar, en todo o en parte, el apartado 1 del presente artículo.
Artículo 6 – Negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad
1. Cada Parte adoptará las medidas legislativas que sean necesarias para tipificar la siguiente conducta como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho:
difundir o poner a disposición del público de otro modo, por medio de un sistema informático, material que niegue, minimice burdamente, apruebe o justifique actos constitutivos de genocidio o crímenes contra la humanidad, tal como se definen en el derecho internacional y reconocidas como tales por una decisión definitiva y vinculante del Tribunal Militar Internacional, constituido en virtud del Acuerdo de Londres de 8 de agosto de 1945, o de cualquier otro tribunal internacional establecido por los instrumentos internacionales pertinentes y cuya jurisdicción haya sido reconocida por esa Parte.
2. Cualquiera de las Partes podrá
a. exigir que la negación o la minimización burda a que se refiere el apartado 1 del presente Artículo se cometa con la intención de incitar al odio, la discriminación o la violencia contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores, o bien
b. reservarse el derecho de no aplicar, en todo o en parte, el apartado 1 del presente artículo.

Actos contemplados

El Artículo 3 penaliza difundir o poner a disposición del público material xenófobo por medio de un sistema informático.[1780] En consecuencia, no están cubiertas las formas tradicionales de distribución que no implican sistemas informáticos (como libros y revistas). Según la definición proporcionada por el Artículo 2, el material racista y xenófobo es todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores Por «difusión» se entiende la distribución activa de material.[1781] "Poner a disposición" cubre el acto de colocar material en línea.[1782] Requiere que los usuarios puedan tener acceso al material. El acto puede cometerse colocando material en páginas Web o conectándose a sistemas de compartición de archivos y permitiendo a otros acceder a ese material en dispositivos o carpetas de almacenamiento desbloqueados. El informe explicativo señala que también se debería contemplar la creación o recopilación de hipervínculos.[1783] Puesto que los hipervínculos sólo facilitan el acceso al material, tal interpretación va más allá del texto de la disposición. La difusión cubre actos activos de reenvío de material racista o xenófobo a otros. La

penalización requiere además que la distribución y puesta a disposición incluya una interacción con el público y, por tanto, excluye la comunicación privada.[1784]

El Artículo 6 sigue un enfoque similar al Artículo 3, penaliza difundir o poner a disposición del público, por medio de un sistema informático,[1785] material que niegue, minimice burdamente, apruebe o justifique actos constitutivos de genocidio o crímenes contra la humanidad, tal como se definen en el derecho internacional y reconocidas como tales por una decisión definitiva y vinculante del Tribunal Militar Internacional, constituido en virtud del Acuerdo de Londres de 8 de agosto de 1945, o de cualquier otro tribunal internacional establecido por los instrumentos internacionales pertinentes y cuya jurisdicción haya sido reconocida por esa Parte.

El Artículo 4 penaliza amenazar personas, por medio de un sistema informático, con la comisión de un delito grave, tal como se define en su derecho interno, i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o ii) a un grupo de personas que se distinga por alguna de esas características. Se refiere a amenazas de ser objeto de la comisión de un delito que creen temor en las personas a quienes se dirigen.[1786] El término "amenazar", a diferencia del Artículo 3, no requiere ninguna interacción con el público y, por consiguiente, también contempla el envío de correos electrónicos a la víctima.

El Artículo 5 adopta un enfoque similar al Artículo 4, penaliza insultar a personas por razón de su pertenencia a un grupo que se caracterice por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o a un grupo de personas que se distinga por alguna de esas características. "Insultar" se refiere a cualquier expresión ofensiva o invectiva que perjudique la dignidad de una persona y esté directamente relacionada con la pertenencia de la persona insultada al grupo. Para evitar conflictos con el principio de la libertad de expresión,[1787] es necesario definir el acto de insultar de manera muy estricta. La principal diferencia del Artículo 5 con respecto al 4 es que la disposición requiere insultar públicamente y, por lo tanto, excluye la comunicación privada (como el correo electrónico).[1788]

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford[1789] de 1999 no prevé la penalización de la incitación al odio. En el Convenio se subraya que, en general, no debe considerarse delictivo en el marco del Proyecto de Stanford ningún discurso o publicación[1790]. El Convenio reconoce los distintos enfoques y deja a los Estados que decidan acerca de la penalización de estos aspectos.[1791]

6.2.11 Delitos contra la religión

Los países difieren entre sí en cuanto al grado de protección de las religiones y sus símbolos.[1792] Con respecto a la penalización se expresan varias preocupaciones. En la Declaración Conjunta de 2006 del Relator Especial de Naciones Unidas para la Libertad de Opinión y Expresión (ONU), el Representante de la Organización de Seguridad y Cooperación en Europa para la Libertad de los Medios de Comunicación (OSCE) y el Relator Especial para la Libertad de Expresión (OEA) se señala que en "muchos países, los poderosos abusan de la vigencia de normas excesivamente laxas en este ámbito para limitar las opiniones innovadoras, opositoras, críticas o minoritarias o la discusión de cuestiones sociales polémicas".[1793] La Declaración Conjunta de 2008 destaca que las organizaciones internacionales, en particular, la Asamblea General de las Naciones Unidas y el Consejo de Derechos Humanos, deben resistirse a adoptar más declaraciones que apoyen la idea de penalizar la difamación de religiones.

Convenio del Consejo de Europa sobre la Ciberdelincuencia (Protocolo Adicional)

Las negociaciones sobre este tema entre las Partes en el Convenio del Consejo de Europa sobre la Ciberdelincuencia experimentaron las mismas dificultades que en el caso del material xenófobo[1794]. Sin embargo, los países que negociaron las disposiciones del Primer Protocolo Adicional al Convenio sobre la Ciberdelincuencia incorporaron la protección de la religión en dos disposiciones.

Disposiciones

Artículo 4 – Amenazas con motivación racista y xenófoba
Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta:
amenazar, por medio de un sistema informático, con la comisión de un delito grave, tal como se define en su derecho interno, i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o ii) a un grupo de personas que se distinga por alguna de esas características.
Artículo 5 – Insultos con motivación racista y xenófoba
1. *Cada Parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno, cuando se cometa intencionadamente y sin derecho, la siguiente conducta: insultar en público, por medio de un sistema informático, i) a personas por razón de su pertenencia a un grupo que se caracterice por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores; o ii) a un grupo de personas que se distinga por alguna de esas características.*
   […]

Aunque estos Artículos consideran la religión como una característica, no protegen la religión ni sus símbolos mediante la penalización, sino que sólo penalizan las amenazas e insultos contra las personas por motivo de pertenencia a un grupo.

Ejemplos de legislación nacional

Algunos países adoptan un enfoque más estricto y penalizan los actos que atentan contra los aspectos religiosos. Como ejemplo cabe citar las Secciones 295 B a 295 C del Código Penal de Pakistán.

***295-B**. Profanación, etc., del Corán: Todo aquél que deliberadamente profane, dañe o deshonre una copia del Corán o de un extracto del mismo o blasfeme sobre el mismo o lo utilice con cualquier fin ilícito podrá ser condenado a cadena perpetua.*
***295-C**. Blasfemias, etc., sobre el Profeta: Todo aquél que profane el sagrado nombre de Mahoma (que la paz sea con él) oralmente, por escrito o mediante representación visual, o haga, directa o indirectamente, acusaciones, alusiones o insinuaciones acerca del mismo podrá ser condenado a muerte, a cadena perpetua y también multado.*

En cuanto a la incertidumbre que suscita la aplicación de esta disposición, el proyecto de ley sobre delitos electrónicos de Pakistán de 2006 contenía dos disposiciones que giraban en torno a los delitos relacionados con Internet[1795], que fueron eliminadas cuando se reintrodujo como la Ley de prevención de delitos electrónicos de 2007[1796], promulgada en diciembre de ese año.[1797]

***20. Profanación etc., de copias del Corán** – Todo aquél que mediante un sistema o dispositivo electrónico deliberadamente profane, dañe o deshonre una copia del Corán o de un extracto del mismo o blasfeme sobre el mismo o lo utilice con cualquier fin ilícito podrá ser condenado a cadena perpetua.*
***21. Blasfemias, etc., sobre el Profeta** – Todo aquél que, mediante un sistema o dispositivo electrónico, profane el sagrado nombre de Mahoma (que la paz sea con él) oralmente, por escrito o mediante representación visual, o haga, directa o indirectamente, acusaciones, alusiones o insinuaciones acerca del mismo podrá ser condenado a muerte, a cadena perpetua y también multado.*

Al igual que en las disposiciones relativas a la penalización del material xenófobo por Internet el principal problema que plantea la armonización mundial de la penalización de los delitos contra la religión es el relativo al principio de libertad de expresión[1798]. Como se indicó anteriormente, las diferencias en cuanto al grado de protección de la libertad de expresión dificultan el proceso de armonización[1799]. En lo que respecta

especialmente al principio común de doble incriminación[1800], la falta de armonización dificulta la aplicación de la ley en los casos de alcance internacional.[1801]

6.2.12 Juego ilegal

El creciente número de sitios web que ofrecen juego ilegal es motivo de preocupación[1802], dado que puede utilizarse para burlar la prohibición del juego que aplican algunos países[1803]. Si los servicios se ofrecen en lugares donde no está prohibido el juego en línea, resulta difícil para los países que penalizan el juego por Internet impedir que sus ciudadanos utilicen dichos servicios.[1804]

Ejemplo de legislación nacional

El Convenio del Consejo de Europa sobre la Ciberdelincuencia no prohíbe el juego en línea. Un ejemplo de enfoque nacional a este respecto es la Sección 284 del Código Penal Alemán:

Ejemplo

Sección 284 – Organización no autorizada de juegos de azar
(1) El que, sin el permiso de una autoridad pública, organice o dirija públicamente un juego de azar o facilite el equipo necesario, podrá ser condenado a cumplir una pena de hasta dos años de prisión o a una multa.
(2) Los juegos de azar en clubs o fiestas privadas donde se organicen juegos de azar con regularidad se considerarán juegos organizados públicamente.
(3) Quien, en los casos citados en el apartado (1), actúe:
1. de manera profesional; o
2. como miembros de una pandilla constituida para llevar a cabo constantemente estos actos, podrá ser condenado a penas de encarcelamiento de tres meses a cinco años.
(4) Quien contrate a terceros para llevar a cabo juegos de azar públicos (apartados (1) y (2)), podrá ser condenado a cumplir una pena de hasta un año de encarcelamiento o una multa.

La disposición tiene por objeto limitar el riesgo de adicción [1805] al juego, para lo cual define los procedimientos para la organización de estos juegos[1806]. Aunque no hace referencia explícita a los juegos de azar por Internet, éstos también quedan comprendidos[1807]. A este respecto, se penaliza la organización ilegal de juegos, sin la autorización de la autoridad pública competente. Además, penaliza a todo aquél que (deliberadamente) facilita el equipo necesario que luego se utiliza en el juego ilegal[1808]. Esta penalización transciende las consecuencias de la ayuda y la instigación, dado que los infractores pueden ser objeto de sentencias más graves[1809].

Para evitar la investigación penal el operador de sitios web de juego ilegal puede desplazar físicamente sus actividades[1810] a países que no penalizan el juego ilegal[1811]. Este desplazamiento supone un problema para las fuerzas de seguridad por cuanto el hecho de que el servidor se encuentre fuera del territorio nacional[1812] no impide, en general, que un usuario acceda al mismo desde dentro del país[1813]. Para que las fuerzas de seguridad luchen mejor contra el juego ilegal, el Gobierno alemán ha extendido la penalización al usuario[1814]. De conformidad con la Sección 285, las fuerzas de seguridad pueden enjuiciar a los usuarios que participan en juegos ilegales e iniciar investigaciones, aun cuando no pueda interponerse una acción judicial contra los operadores de tales juegos de azar por estar situados fuera del territorio de Alemania:

Sección 285 – Participación en juegos de azar no autorizados
El que participe en juegos de azar públicos (Sección 284) podrá ser condenado a una pena de hasta seis meses de prisión o una multa de hasta ciento ochenta veces la cantidad fijada como sanción diaria.

Si el infractor utiliza los sitios de juego en línea para lavar activos, la identificación del infractor suele resultar difícil[1815]. Un ejemplo de método[1816] para impedir el juego ilegal y el lavado de activos es la Ley sobre el juego ilegal por Internet de Estados Unidos de 2005.[1817]

§ 5363. Prohibición de aceptar cualquier instrumento financiero para el juego ilegal por Internet

Ninguna persona en el negocio de juegos o apuestas aceptará conscientemente, en relación con la participación de otra persona en juego ilegal por Internet

(1) crédito, o fondos procedentes de crédito, otorgado o en nombre de un tercero (comprendidas las tarjetas de crédito);

(2) una transferencia electrónica de fondos, o fondos transmitidos por empresas de envío de dinero o por conducto de las mismas, o los fondos procedentes de transferencias electrónicas o de servicios de envío de dinero, procedentes o en nombre de un tercero;

(3) cheques, talones u otros instrumentos similares a nombre o de parte de un tercero o a nombre o pagadero de cualquier institución financiera; o

(4) fondos procedentes de cualquier otra forma de transacción financiera, conforme lo prescriba el Secretario mediante la correspondiente reglamentación, en la que participen una institución financiera en calidad de pagador o intermediario financiero o en beneficio de un tercero.

§ 5364. Políticas y procedimientos para identificar e impedir las transacciones restringidas

Antes de concluir el periodo de 270 días contados a partir de la fecha de promulgación del presente subcapítulo, el Secretario, en consulta con la Junta Directiva del Sistema de Reserva Federal y del Fiscal General, prescribirán el reglamento mediante el cual se exige que todo sistema de pago designado, y todos los que intervienen en el mismo, determinen e impidan las transacciones restringidas mediante el establecimiento de políticas y procedimientos razonablemente concebidos para determinar e impedir las transacciones restringidas en cualquiera de los siguiente modos:

(1) El establecimiento de políticas y procedimientos que

(A) permitan al sistema de pago y a toda persona que participe en el mismo, identificar las transacciones restringidas mediante códigos en los mensajes de autorización u otros mecanismos; y

(B) bloqueen las transacciones restringidas que se hayan identificado utilizando las políticas y procedimientos creados de conformidad con el apartado (A).

(2) La creación de políticas y procedimientos que impidan aceptar los productos o servicios de los sistemas de pago derivados de transacciones restringidas.

(b) Al prescribir el reglamento de conformidad con el apartado (a) el Secretario deberá:

(1) identificar los tipos de políticas y procedimientos, con ejemplos no exclusivos, que se estimen, según proceda, razonablemente adecuados para identificar, bloquear o impedir la aceptación de productos o servicios para cada tipo de transacción restringidas;

(2) en la medida en que resulte práctico, permitir a todo participante en un sistema de pago que seleccione otros mecanismos alternativos para identificar y bloquear, o en su defecto impedir, la aceptación de productos o servicios de sistema de pago, o la participación conexa, basado en transacciones restringidas; y

(3) considerar la posibilidad de eximir las transacciones restringidas de cualquier requisito impuesto con arreglo a tal reglamento, si el Secretario llega a la conclusión de que no resulta razonablemente práctico identificar y bloquear, o en su defecto impedir, tales transacciones.

(c) Los proveedores de transacciones financieras se considerarán que cumplen el reglamento prescrito con arreglo al apartado (a), si

(1) la persona se basa y cumple las políticas y procedimientos de un sistema de pago concebido, del cual es miembro o participante, para

(A) identificar y bloquear transacciones restringidas; o

(B) en su defecto, impedir la aceptación de productos o servicios del sistema de pago, miembro, o participante en relación con las transacciones restringidas; y

(2) tales políticas y procedimientos del sistema de pago cumplen los requisitos de la reglamentación prescritos con arreglo al apartado (a).

(d) Toda persona sujeta a un reglamento prescrito u orden expedida con arreglo al presente subcapítulo, que bloquee, o en su defecto rehúse efectuar una transacción

(1) que es una transacción restringida;

(2) que la persona estima razonablemente que es una transacción restringida; o

(3) en su calidad de miembro de un sistema de pago designado que cumple las políticas y procedimientos del sistema de pago, con el fin de cumplir el reglamento prescrito con arreglo al apartado (a), no será responsable ante ninguna parte por actuar de tal forma.

(e) La aplicación de lo prescrito en esta sección corresponde exclusivamente a los organismos reguladores Federales y la Comisión Federal de Comercio, conforme a lo estipulado en la Sección 505(a) de la Ley Gramm-Leach-Bliley.

§ 5366. Sanciones penales

(a) Todo aquel que infrinja la Sección 5363 será condenado a una multa conforme al título 18, o a una pena de prisión de hasta 5 años, o ambas.

(b) Toda persona que haya sido condenada con arreglo a esta sección, el tribunal podrá solicitar un mandamiento judicial que le impida efectuar, recibir o hacer apuestas o jugar dinero, o enviar, recibir o anunciar información que ayude a hacer apuestas o jugar dinero.

La finalidad de la ley es resolver los problemas y amenazas que entraña el juego (transfronterizo) por Internet[1818]. Contiene dos reglas importantes. En primer lugar, prohibir a las personas que participan en el negocio de apuestas y juego de dinero que acepten cualquier instrumento financiero para el juego ilegal por Internet. Esta disposición no reglamenta las acciones emprendidas por el usuario de sitios de juego por Internet o por las instituciones financieras[1819]. El incumplimiento de esta prohibición puede ser objeto de sanciones penales[1820]. En segundo lugar, la ley exige al Secretario del Tesorero y de la Junta Directiva del Sistema de la Reserva Federal que prescriba reglamentos que exijan a los proveedores de transacciones financieras identificar y bloquear las transacciones confidenciales en relación con el juego ilegal por Internet mediante la aplicación de políticas y procedimientos razonables. Este segundo reglamento no se aplica solamente a la persona dedicada al negocio de apuestas y juego de dinero sino a toda institución financiera en general. A diferencia de las personas dedicadas al negocio de apuestas y juegos de dinero que aceptan instrumentos financieros para el juego ilegal por Internet, las instituciones financieras no tienen, en general, responsabilidad penal. Se está investigando[1821] actualmente la incidencia internacional de los posibles conflictos de este reglamento en relación al Acuerdo General sobre el Comercio de Servicios (AGCS).[1822]

6.2.13 Calumnias y difamación

La calumnia y la publicación de información falsa no se comenten exclusivamente por la redes. Ahora bien, como se subrayó más arriba, la posibilidad de comunicación anónima[1823] y los problemas logísticos que conlleva la inmensa cantidad de información disponible en Internet[1824] son parámetros favorables a este tipo de actos.

La cuestión de si debe penalizarse la difamación es un tema de debate polémico[1825]. La preocupación que suscita dicha penalización se debe especialmente a los posibles conflictos que puedan surgir con el principio de "libertad de expresión". Por consiguiente, varias organizaciones han pedido que se cambie la legislación en materia de difamación penal[1826]. El Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión y el Representante de la OSCE para la Libertad de los Medios de Comunicación expresaron: "La difamación penal no es una restricción justificable a la libertad de expresión; se deberán derogar todas las leyes de difamación penal y remplazarlas, donde proceda, por leyes adecuadas de difamación civil".

Pese a estas inquietudes, algunos países[1827] aplican disposiciones jurídicas que penalizan la calumnia y la publicación de información falsa. Es importante destacar que incluso en los países que penalizan la difamación el número de casos varía sobremanera. En el Reino Unido no se registró ningún caso en 2004 y sólo uno en 2005 fue acusado de calumnia[1828], mientras que en Alemania las estadísticas penales registran 187 527 delitos de difamación en 2006[1829]. El Convenio del Consejo de Europa sobre la Ciberdelincuencia, la Ley modelo de la Commonwealth y el Proyecto de Stanford no contienen disposición alguna que trate directamente de este tema.

Ejemplo de legislación nacional

Un ejemplo de legislación penal sobre este particular es la Sección 365 del Código Penal de Queensland (Australia). Queensland volvió a promulgar la responsabilidad penal por difamación en la Enmienda de Ley sobre la Difamación Penal de 2002.[1830]

Disposición

365 Difamación penal [1831]
(1) Toda persona que, sin justificación legítima, publique información difamatoria de otra persona con vida (la persona afectada)
(a) a sabiendas de que la información es falsa o sin preocuparse por la veracidad o falsedad de la misma; y
(b) trate de causar perjuicio grave a la persona afectada o a cualquier otra persona sin preocuparse de la gravedad del asunto; comete una falta. La pena máxima será de tres años de prisión.
(2) En un procedimiento jurídico por un delito definido en esta sección, el acusado tendrá justificación legítima para la publicación de la información difamatoria acerca de la persona afectada si, y sólo si, se aplica la sección (3). […]

Otro ejemplo de penalización de la calumnia es la Sección 185 del Código Penal de Alemania:

Disposición

Sección 185 – Injurias
La injuria se sancionará con una pena de encarcelamiento de hasta un año o una multa y, si ésta se causara recurriendo a la violencia, con una pena de hasta dos años o una multa.

Las dos disposiciones no se han concebido para contemplar exclusivamente los actos por Internet. La aplicación no se limita a determinados medios de comunicación, por lo que quedan comprendidos los actos que se comenten tanto por la red como fuera de ésta.

6.2.14 Correo basura

Dado que el 75 por ciento[1832] de todos los mensajes de correo electrónico son correo basura[1833], se ha debatido detenidamente acerca de la necesidad de penalizar el envío de este tipo de mensajes[1834]. Las medidas adoptadas en la legislación nacional sobre este particular varían de un país a otro[1835]. Una de las principales razones por las que el correo basura sigue siendo un problema es que las tecnologías de filtrado aún no permiten identificar y bloquear todos los mensajes de correo electrónico basura[1836]. Es decir, las medidas preventivas sólo ofrecen una protección limitada contra este tipo de mensajes.

En 2005 la OCDE publicó un Informe en el que se analiza la incidencia del correo basura en los países en desarrollo[1837]. En el Informe se indica que los representantes de los países en desarrollo consideran que los usuarios de Internet en sus países sufren mucho más los efectos del correo basura y los abusos cometidos en la red. Cuando se analizan los resultados del Informe se comprueba que la impresión de los representantes es acertada. Debido a sus recursos más limitados y onerosos, el correo basura es un asunto mucho más grave en los países en desarrollo que en los occidentales.[1838]

Ahora bien, la identificación del correo electrónico basura no es lo único que plantea problemas. No es fácil distinguir entre los correos electrónicos que el destinatario no desea recibir, pero que se enviaron de manera legítima, y los que se envían de manera ilícita. La tendencia hacia la transmisión por computador (con inclusión del correo electrónico y VoIP) hace que resulte cada vez más importante proteger las comunicaciones contra los ataques. Si el correo basura rebasa un determinado nivel, puede llegar a dificultar la utilización de las TIC y a reducir la productividad del usuario.

Convenio del Consejo de Europa sobre la Ciberdelincuencia

El Convenio del Consejo de Europa sobre la Ciberdelincuencia no penaliza de manera expresa el correo basura[1839]. Se propone que la penalización de estos actos debe limitarse a los casos en los que hay una clara intención de dificultar la comunicación de manera grave y deliberada[1840]. Este enfoque no se concentra en los mensajes de correo electrónico no solicitados, sino en los efectos de éstos sobre los sistemas informáticos y las redes. Así pues, de conformidad con el enfoque jurídico del Convenio del Consejo de Europa sobre la Ciberdelincuencia, la lucha contra el correo basura sólo pueden basarse en los ataques ilícitos contra las redes y sistemas informáticos:

> ***Artículo 5 – Ataques a la integridad del sistema***
> *Cada parte adoptará las medidas legislativas y de otro orden que sean necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.*

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford[1841] de 1999, de carácter oficioso, no prevé la penalización del correo basura. Al igual que el Convenio del Consejo de Europa sobre la Ciberdelincuencia, sólo penaliza el correo basura en el caso de que el correo electrónico no solicitado constituya un ataque deliberado contra la integridad del sistema.

Texto legislativo sobre la ciberdelincuencia de HIPCAR

La Sección 15 del texto legislativo sobre la ciberdelincuencia de HIPCAR[1842] constituye un ejemplo de un enfoque específico:[1843]

> ***SPAM***
> ***15. (1)*** *Una persona que, intencionalmente, sin excusa o justificación legal, o en exceso de excusa o justificación legal:*
> *(a) inicie la transmisión de mensajes de correo electrónico múltiples desde o por medio de dicho sistema informático, o*
> *(b) utilice un sistema informático protegido para transmitir o retransmitir mensajes de correo electrónico múltiples, con la intención de engañar o confundir a usuarios, o cualquier correo electrónico o proveedor de servicios de Internet, en cuanto al origen de estos mensajes, o*
> *(c) materialmente falsifique la información de encabezado de mensajes de correo electrónico múltiples y deliberadamente inicie la transmisión de estos mensajes,*
> *comete un delito punible, en caso de condena, con pena de prisión por un período no superior a [periodo], o una multa máxima de [cuantía], o con ambas cosas.*
> *(2) Los países tienen la opción de restringir la penalización con respecto a la transmisión de mensajes electrónicos múltiples a las relaciones con clientes o empresas. Pueden decidir no tipificar como delito la conducta en la Sección 15 (1) (a) siempre que haya disponibles otros tratamientos efectivos.*

En la disposición se incluyen tres actos diferentes. En la Sección 15 (1) (a) se contempla el proceso de iniciar la transmisión de correos electrónicos múltiples. En la Sección 3 (14) se definen los mensajes de correo electrónico múltiples como todo mensaje de correo, incluido el correo electrónico y la mensajería instantánea, que se envía a más de un millar de receptores. A este respecto, la nota explicativa señala que la limitación de la penalización a los actos llevados a cabo sin excusa o justificación legal cumple un papel importante en la distinción entre envíos masivos de correo legítimos (como boletines de noticias) y el correo basura ilegal.[1844] En la Sección 15 (1) (b) se penaliza la elusión de la tecnología de protección frente a los correos basura, abusando de sistemas informáticos protegidos para retransmitir o transmitir mensajes electrónicos. En la Sección 15 (1) (c) se contempla la elusión de la tecnología de protección frente a los correos basura mediante la falsificación de la información del encabezado. En la nota explicativa se señala

que en la Sección 15 se exige que el delincuente lleve a cabo los delitos intencionalmente y sin excusa o justificación legal. [1845]

Código de los Estados Unidos

La penalización del correo basura queda limitada a los casos en que el número de mensajes de correo electrónico basura afecta gravemente a la potencia de procesamiento de los sistemas informáticos. Sin embargo, no pueden enjuiciarse sus efectos sobre la actividad comercial, siempre que no afecten al sistema informático. En algunos países se adopta un enfoque distinto. Como ejemplo, puede citarse la legislación de Estados Unidos – 18 USC § 1037.[1846]

§ 1037. Fraude y actividades conexas en relación con el correo electrónico
(a) En general – Todo el que a sabiendas afecte el comercio en un Estado, entre Estados o el comercio exterior
(1) acceda si autorización a computadores protegidos, e inicie deliberadamente la transmisión de varios mensajes comerciales de correo electrónico desde o mediante dicho computador,
(2) utilice un computador protegido para enviar o retransmitir múltiples mensajes comerciales de correo electrónico, con el fin de engañar o inducir a error a los destinatarios, a cualquier servicio de acceso a Internet, en cuanto al origen de tales mensajes,
(3) falsifique la información del encabezamiento de los mensajes de correo electrónico e inicie deliberadamente la transmisión de tales mensajes,
(4) registre, utilizando información que falsifique la identidad real registrada, de cinco o más cuentas de correo electrónico o utilice cuentas de usuario en línea o dos o más nombres de dominio, y deliberadamente incite la transmisión de múltiples mensajes comerciales de correo electrónico desde cualquier combinación de tales cuentas o nombres de dominio, o
(5) se presente falsamente como la entidad de registro o el sucesor legítimo en nombre de la misma, de cinco o más direcciones de Protocolo Internet, e inicie deliberadamente la transmisión de múltiples mensajes comerciales de correo electrónico desde tales direcciones,
o conspire para hacerlo, será sancionado conforme a lo previsto en el apartado (b).
(b) Sanciones – La sanción en caso de un delito contemplado en el apartado (a) será:
(1) una multa conforme a este título, o una pena de prisión de hasta cinco años, o ambas, si:
(A) la infracción se comete para respaldar cualquier delito grave prescrito en la legislación de Estados Unidos o en alguno de sus Estados; o
(B) el acusado ya ha sido condenado previamente en virtud de esta sección o la Sección 1030, o conforme a la legislación de cualquier Estado por cualquier acto relacionado con la transmisión de múltiples mensajes comerciales de correo electrónico o por el acceso no autorizado a un sistema informático;

Esta disposición fue incorporada a la Ley sobre el correo basura de la CAN de 2003[1847]. La finalidad de esta ley era crear una única norma nacional destinada a controlar el envío de mensajes comerciales de correo electrónico[1848]. Esta disposición se aplica a los mensajes comerciales de correo electrónico pero no a los mensajes relacionados con las transacciones y las relaciones comerciales existentes. El enfoque reglamentario exige que los mensajes electrónicos comerciales incluyan una indicación de que se han solicitado, y las instrucciones para aquellos que decidan no seguir recibiéndoles, así como la dirección postal del remitente[1849]. En el 18 USC § 1037 se penaliza a los remitentes de correo basura, especialmente si han falsificado la información de los encabezamientos del correo electrónico para burlar la tecnología de filtrado[1850]. Además la disposición penaliza el acceso no autorizado a computadores protegidos y el inicio de transmisiones de múltiples mensajes comerciales de correo electrónico.

6.2.15 Abuso de los dispositivos

Otro problema grave es la disponibilidad de software y hardware diseñados para cometer delitos[1851]. Además de la proliferación de "dispositivos de piratería", el intercambio de contraseñas que permiten a usuarios no autorizados penetrar en sistemas informáticos constituye un serio problema[1852]. A causa de la

disponibilidad y la amenaza potencial de estos dispositivos, es difícil centrar la penalización en el uso de los mismos para cometer delitos únicamente. La mayoría de los sistemas de derecho penal nacional contienen alguna disposición que penaliza la preparación y producción de esos instrumentos, además del "intento de delito". Una forma de luchar contra la distribución de dichos dispositivos consiste en penalizar la producción de los mismos. Por lo general esa penalización -que normalmente va acompañada de un marcado desplazamiento de la responsabilidad penal- se limita a los delitos más graves. En la legislación de la Unión Europea, en particular, existe la tendencia de ampliar el alcance de la penalización de los actos preparatorios para incluir delitos menos graves. [1853]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

Tomando en consideración otras iniciativas del Consejo de Europa, los redactores del Convenio sobre la Ciberdelincuencia tipificaron un delito criminal independiente para determinados actos ilegales relacionados con ciertos dispositivos o con el acceso a datos que se utilicen abusivamente con el fin de atentar contra la confidencialidad, la integridad y la disponibilidad de sistemas o datos informáticos:[1854]

Disposición

Artículo 6 – Abuso de los dispositivos
(1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

(a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

(i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para comisión de cualquiera de los delitos previstos en los Artículos 2 a 5 del presente Convenio;

(ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los Artículos 2 a 5; y

(b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente Artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los Artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

(2) No se interpretará que el presente Artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente Artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los Artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

(3) Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente Artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente Artículo.

Objetos contemplados

En el párrafo 1 a) se identifican tanto los dispositivos[1855] diseñados para cometer y promover el ciberdelito como las contraseñas que permiten acceder a un sistema informático. El término "dispositivo" incluye tanto al hardware como al software concebido para cometer uno de los delitos mencionados. En el Informe Explicativo se mencionan por ejemplo software tales como programas de virus o programas diseñados o adaptados para obtener acceso a sistemas informáticos[1856]. "Una contraseña, un código de acceso o datos informáticos similares" a diferencia de los dispositivos no efectúan operaciones sino que constituyen códigos de acceso. En este contexto, se trató de determinar si la disposición incluía la publicación de las vulnerabilidades del sistema[1857]. A diferencia de los códigos de acceso clásicos, las vulnerabilidades no necesariamente permiten un acceso inmediato a un sistema informático, sino que le permiten al delincuente aprovechar esas vulnerabilidades para atacar con éxito a un sistema informático.

Actos contemplados

El Convenio sobre la Ciberdelincuencia penaliza una amplia gama de acciones. Además de la producción, también sanciona la venta, la adquisición para su uso, la importación, la distribución y otras formas de puesta a disposición de dispositivos y contraseñas. En la legislación de la Unión Europea sobre armonización de los derechos de autor[1858] se aplica un enfoque similar (limitado a los dispositivos diseñados para eludir disposiciones de orden técnico), y en el derecho penal de varios países se han adoptado disposiciones similares[1859]. Por "distribución" se entiende el acto deliberado de transmitir dispositivos o contraseñas a otros[1860]. En lo que se refiere al Artículo 6, "venta" incluye las actividades inherentes a la venta de dispositivos y contraseñas a cambio de dinero o alguna otra forma de compensación. "Obtención para su utilización" se refiere al acto de obtener activamente contraseñas y dispositivos[1861]. El hecho de que el acto de adquirir esté vinculado con la utilización de dichos dispositivos implica en general una intención por parte del delincuente de obtener los instrumentos para usarlos que va más allá de la intención "habitual", es decir, "*con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los Artículos 2 a 5*". La importación contempla el acto de obtener dispositivos y códigos de acceso procedentes de países extranjeros[1862]. Como resultado de ello, los delincuentes que importan esos elementos para venderlos pueden ser procesados incluso antes de que los ofrezcan. En lo que respecta al hecho de que la adquisición de dichos instrumentos sólo se penaliza si puede vincularse a la utilización de los mismos, cabe poner en tela de juicio si en el Artículo 6 del Convenio del Consejo de Europa sobre la Ciberdelincuencia se cubre la simple importación, sin la intención de vender o utilizar esos instrumentos. "Puesta a disposición" se refiere al acto que permite a otros usuarios acceder a esos elementos[1863]. En el Informe Explicativo se indica que el término "puesta a disposición" también abarca la creación o compilación de hiperenlaces con miras a facilitar el acceso a esos dispositivos. [1864]

Instrumentos de doble utilización

A diferencia del enfoque aplicado por la Unión Europea en lo que respecta a la armonización de los derechos de autor[1865], esta disposición no sólo se aplica a los dispositivos diseñados exclusivamente para facilitar la comisión de un ciberdelito, sino que el Convenio sobre la Ciberdelincuencia también contempla a los dispositivos que se utilizan normalmente con fines legales, pero a los que el delincuente tiene la intención manifiesta de utilizar para cometer un ciberdelito. Los redactores del Informe Explicativo señalan que si la aplicación se limitara exclusivamente a los dispositivos diseñados para cometer delitos, esa limitación sería demasiado estrecha y podría plantear dificultades insoslayables en lo tocante a la presentación de pruebas durante los procedimientos penales, como resultado de lo cual esa disposición resultaría prácticamente inaplicable o sólo podría aplicarse en raros casos[1866].

Con el fin de garantizar una protección adecuada de los sistemas informáticos, los expertos poseen y utilizan diversos instrumentos de software, a causa de los cuales podrían ser objeto de penalización en cumplimiento de la ley. Habida cuenta de ello, en el Convenio sobre la Ciberdelincuencia se abordan estos aspectos de tres maneras distintas[1867]: A tenor de lo dispuesto en el párrafo 1, subpárrafo b), del Artículo 6, cualquier Parte podrá exigir que se posea un número determinado de dichos elementos para que se pueda considerar que existe responsabilidad penal. Además, la penalización de la posesión de estos dispositivos está limitada por el requisito de intención de utilizar el dispositivo para cometer un delito, según se consigna en los Artículos 2 a 5 del Convenio sobre la Ciberdelincuencia[1868]. En el Informe Explicativo se destaca que esa intención manifiesta fue incluida con el fin de "evitar el peligro de una penalización excesiva cuando los dispositivos se producen y distribuyen en el mercado con fines legales, por ejemplo, para hacer frente a los ataques librados contra los sistemas informáticos"[1869]. Por último, los redactores del Convenio estipulan claramente en el párrafo 2 que la disposición no se aplica a los instrumentos creados para efectuar pruebas autorizadas o para la protección de un sistema informático, puesto que la disposición se aplica a actos no autorizados.

Penalización de la posesión

En el párrafo 1, subpárrafo b), se amplía aún más el alcance de la reglamentación consignada en el párrafo 1, subpárrafo a), al penalizar la posesión de dispositivos o contraseñas si es con intención de cometer un ciberdelito. La penalización de la posesión de instrumentos de ese tipo es polémica[1870]. El Artículo 6 no se

limita a los instrumentos diseñados exclusivamente para cometer delitos, y a los oponentes de la penalización les preocupa el hecho de que la penalización de la posesión de estos dispositivos pudiere suponer un riesgo inaceptable para los administradores de sistemas y los expertos en seguridad de redes[1871]. El Convenio sobre la Ciberdelincuencia le permite a las Partes imponer el requisito de que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

Predisposición

Como ocurre con todas las otras contravenciones definidas en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, en el Artículo 6 se exige que el delincuente cometa el delito deliberadamente[1872]. Además de la intención ordinaria con respecto a los actos de que se trata, en el Artículo 6 del Convenio se exige la intención especial adicional de que el dispositivo sea utilizado con la finalidad de cometer cualquiera de los delitos consignados en sus Artículos 2 a 5.[1873]

Sin derecho

De manera similar a las disposiciones antes examinadas, los actos deben cometerse "sin derecho"[1874]. Por lo que hace al temor de que la disposición pudiere utilizarse para penalizar la utilización legal de instrumentos informáticos en el marco de las medidas de autoprotección, los redactores del Convenio subrayaron que no se considera que dichos actos sean efectuados "sin derecho".[1875]

Restricciones y reservas

A causa del debate sobre la necesidad de penalizar la posesión de los dispositivos, en el Convenio se ofrece la opción de realizar una compleja reserva, según se indica en el párrafo 3 del Artículo 6 (además de la segunda frase del párrafo 1, subpárrafo b)). Si una de las Partes recurre a esta reserva, puede excluir la penalización de la posesión de instrumentos y cierto número de acciones ilegales conforme al párrafo 1, subpárrafo a); entre éstas figura por ejemplo la producción de dichos dispositivos.[1876]

Ley modelo de la Commonwealth sobre informática y delitos relacionados con la informática

En la Sección 9 de la Ley modelo de la Commonwealth de 2002[1877] se aplica un enfoque parecido al Artículo 6 del Convenio del Consejo de Europa sobre la Ciberdelincuencia:

> ***Dispositivos ilegales***
> ***9.***
> *(1) Una persona comete un delito si:*
> *a) deliberada o imprudentemente, sin una excusa o justificación legítima, produce, vende, adquiere para su utilización, importa, exporta, distribuye o pone a disposición:*
> *(i) un dispositivo, con inclusión de un programa informático, que ha sido diseñado o adaptado con el fin de cometer un delito en contra de lo dispuesto en los puntos 5, 6, 7 u 8; o*
> *(ii) una contraseña informática, un código de acceso o datos similares gracias a los cuales se puede acceder a un sistema informático en su totalidad o en parte;*
> *con la intención de que éste sea utilizado por cualquier persona con la finalidad de cometer un delito en contra de lo dispuesto en los puntos 5, 6, 7 u 8; o*
> *b) tiene en su poder un artículo de los mencionados en los subpárrafos i) o ii) con la intención de que éste sea utilizado por cualquier persona con la finalidad de cometer un delito en contra de lo dispuesto en los puntos 5, 6, 7 u 8.*
> *(2) Una persona sentenciada culpable de un delito contra lo dispuesto en este punto puede ser objeto de una pena de prisión por un periodo no superior a [periodo] o una multa no superior a [cuantía], o a ambas cosas.*

Aunque los dispositivos que contempla la disposición y los actos mencionados son los mismos, la principal diferencia con el Convenio del Consejo de Europa sobre la Ciberdelincuencia estriba en que la Ley modelo de la Commonwealth penaliza los actos de imprudencia además de los deliberados, mientras que el Convenio sobre la Ciberdelincuencia requiere una intención en todos los casos. Durante las negociaciones

entabladas en torno a la Ley modelo de la Commonwealth, se consideraron nuevas enmiendas a la disposición que penalizan la posesión de dichos dispositivos. El Grupo de Expertos propuso que se penalizara a los delincuentes que estuvieran en posesión de más de un artículo[1878]. Canadá propuso que se aplicase un enfoque similar, sin definir previamente el número de artículos que justificarían la penalización.[1879]

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford de 1999[1880] ("Proyecto de Stanford"), de carácter oficioso, contiene una disposición a tenor de la cual se penalizan los actos relacionados con ciertos dispositivos ilegales.

> ***Artículo 3 – Delitos***
> *1. Una persona comete un delito en el marco de este Convenio si participa de manera ilegal e intencional en cualquiera de las siguientes actividades sin autorización, permiso o consentimiento jurídicamente reconocidos:*
> *[...]*
> *(e) fabrica, vende, utiliza, envía por correo o de cualquier otro modo cualquier dispositivo o programa diseñado con el fin de cometer cualesquiera de los actos prohibidos a tenor de los Artículos 3 y 4 del presente Convenio;*

Los redactores del Convenio subrayaron que en general el Proyecto de Stanford no exige que se trate como acto delictivo ningún tipo de discurso o publicación[1881]. La única excepción está relacionada con los dispositivos ilegales[1882]. En este contexto, los redactores pusieron de relieve que la penalización debería limitarse a los actos mencionados y no incluir por ejemplo el examen de las vulnerabilidades del sistema.[1883]

Texto sobre la ciberdelincuencia de HIPCAR

Puede encontrarse un enfoque interesante en el texto legislativo que elaboraron los Estados beneficiarios de la iniciativa HIPCAR. [1884]

> ***Dispositivos ilegales***
> ***10.***
> *[...]*
> *(3) Los países pueden decidir no tipificar como delito el simple acceso no autorizado, siempre que haya disponibles otros tratamientos efectivos. Por otra parte, pueden decidir limitar la penalización a los dispositivos que figuren en una lista.*

Con el fin de evitar el exceso de penalización, el redactor decidió incluir la posibilidad de limitar la penalización mediante la introducción de una lista negra. En este caso, la disposición sólo contempla los dispositivos que figuran en la lista. Este enfoque limita los riesgos de penalizar actos que son deseables desde el punto de vista de la seguridad cibernética. Sin embargo, es muy probable que el mantenimiento de dicha lista requiriera importantes recursos.

6.2.16 Falsificación informática

Por lo general en el pasado los procedimientos penales de casos de falsificación informática han sido poco frecuentes, puesto que la mayor parte de los documentos jurídicos eran documentos tangibles. Actualmente, debido a la digitalización, la situación está cambiando[1885]. La tendencia hacia el uso de documentos digitales se ve respaldada por la creación de un marco jurídico que rige su utilización, por ejemplo mediante el reconocimiento de la legalidad de las firmas digitales. Por otro lado, las disposiciones contra la falsificación informática desempeñan una importante función en la lucha contra la usurpación de identidades ("*peska*" o "phishing").[1886]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

En la mayoría de los sistemas de derecho penal se penaliza la falsificación de documentos tangibles[1887]. Los redactores del Convenio sobre la Ciberdelincuencia señalaron que la estructura dogmática de los enfoques jurídicos varía según el país[1888]. Mientras un concepto se basa en la autenticidad del autor de los documentos, otro se basa en la autenticidad de la declaración. Los redactores decidieron aplicar normas mínimas y proteger la seguridad y la fiabilidad de los datos electrónicos mediante la tipificación de un delito paralelo a la falsificación tradicional de documentos tangibles para colmar las lagunas del derecho penal que pudiere no aplicarse a los datos almacenados electrónicamente.[1889]

Disposición

Artículo 7 – Falsificación informática
Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Objeto contemplado

El objetivo de una falsificación informática son los datos, independientemente del hecho de que éstos sean legibles y/o inteligibles directamente. En el Convenio sobre la Ciberdelincuencia se definen los datos informáticos[1890] como "toda representación de hechos, información o conceptos de una manera adecuada para su procesamiento en un sistema informático, con inclusión de un programa diseñado para hacer que un computador desempeñe una función". La disposición no se refiere únicamente a los datos informáticos como objeto de uno de los actos mencionados. Es necesario además que esos actos den lugar a datos fraudulentos.

En el Artículo 7 se exige -al menos en lo que se refiere a la predisposición- que los datos sean equivalentes a un documento público o privado. Ello significa que los datos deben ser jurídicamente pertinentes[1891]: en la disposición no se contempla la falsificación de datos que no puedan utilizarse con fines jurídicos.

Actos contemplados

La "introducción" de datos[1892] debe corresponderse con la producción de un documento falso tangible[1893]. El término "alteración" se refiere a la modificación de los datos existentes. [1894] En el Informe Explicativo se especifican particularmente las variaciones y los cambios parciales[1895]. El término "supresión" de datos informáticos describe una acción que afecta la disponibilidad de datos[1896]. En el Informe Explicativo los redactores se refieren en particular a la retención o el ocultamiento de datos[1897]. Este acto se puede realizar por ejemplo bloqueando cierta información de una base de datos durante la creación automática de un documento electrónico. El término "borrado" está en consonancia con la definición que figura en el Artículo 4 con referencia a actos mediante los cuales se elimina información[1898]. El Informe Explicativo se refiere únicamente a la eliminación de datos de un medio de datos[1899], pero el alcance de la disposición admite perfectamente una definición más amplia del término "borrado". Sobre la base de esa definición más amplia, el acto se puede efectuar mediante la eliminación de un fichero entero o borrando parcialmente cierto volumen de información en un fichero.[1900]

Predisposición

Al igual que todos los otros delitos definidos en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, en el Artículo 3 se exige para penalizar que el delincuente lleve a cabo los actos delictivos intencionalmente[1901]. El Convenio sobre la Ciberdelincuencia no contiene una definición del término "intencionalmente". Los redactores del Informe Explicativo señalaron que el término "intencionalmente" debía definirse a nivel nacional.[1902]

Sin derecho

Los actos de falsificación sólo pueden penalizarse a tenor del Artículo 7 del Convenio sobre la Ciberdelincuencia siempre que éstos se realicen "sin derecho". [1903]

Restricciones y reservas

El Artículo 7 también ofrece la posibilidad de hacer una reserva con miras a limitar la penalización, exigiendo elementos adicionales, tales como la intención de engañar, para que se considere que existe responsabilidad penal.[1904]

Ley modelo de la Commonwealth sobre informática y delitos relacionados con la informática

La Ley modelo de la Commonwealth de 2002 no contiene ninguna disposición que penalice la falsificación informática.[1905]

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford de 1999, de carácter oficioso [1906], contiene una disposición que penaliza los actos relacionados con la falsificación de datos informáticos.

> ***Artículo 3 – Delitos***
> *1. En el marco del presente Convenio, una persona comete un delito si perpetúa ilegal e intencionalmente cualquiera de los siguientes actos, sin autorización, permiso o consentimiento legalmente reconocidos:*
> *[...]*
> *(b) crea, almacena, altera, borra, transmite, desvía, desencamina, manipula o interfiere con los datos de un cibersistema con la finalidad y el efecto de proporcionar información falsa para causar un daño apreciable a las personas o la propiedad;*
> *[...]*

La principal diferencia con el Artículo 7 del Convenio del Consejo de Europa sobre la Ciberdelincuencia estriba en que el anterior Artículo 3 1b) no se centra en la mera manipulación de los datos, sino que impone el requisito de interferencia con un sistema informático, mientras que en el Artículo 7 del Convenio del Consejo de Europa sobre la Ciberdelincuencia no se requiere ese acto, sino que basta con que el delincuente actúe con la intención de que los datos se consideren o utilicen con fines legales como si fuesen auténticos.

6.2.17 Usurpación de identidad

Tomando en consideración la cobertura media [1907], los resultados de los estudios efectuados recientemente [1908], así como las numerosas publicaciones jurídicas y técnicas [1909] en este ámbito, es apropiado considerar la usurpación de identidades como un fenómeno de masas [1910]. Pese al alcance mundial de este fenómeno, no todos los países han incorporado en su sistema nacional de derecho penal disposiciones tendientes a penalizar todos los actos relacionados con el robo de identidad. Recientemente la Comisión de la Unión Europea señaló que no todos sus Estados Miembros han penalizado aún este fenómeno[1911]. La Comisión manifestó la opinión de que "si todos los Estados Miembros penalizaran la usurpación de identidades, se reforzaría la cooperación en lo tocante al cumplimiento de la ley en la Unión Europea" y anunció que entablaría a la brevedad consultas para evaluar si dicha legislación es adecuada[1912].

Uno de los problemas con los que se tropieza para comparar los instrumentos jurídicos en vigor para la lucha contra la usurpación de identidades es el hecho de que éstos difieren radicalmente[1913]. El único elemento consistente de los enfoques en vigor estriba en que el comportamiento censurado está relacionado con una o más de las siguientes fases[1914] .

- Fase 1: Acto de obtención de información relacionada con la identidad.
- Fase 2: Acto de posesión o transferencia de la información relacionada con la identidad.
- Fase 3: Acto de utilización de la información relacionada con la identidad con fines delictivos.

Sobre la base de esta observación, existen en general dos enfoques sistemáticos para penalizar la usurpación de identidad:

- El establecimiento de una única disposición que penalice el acto de obtener, poseer o utilizar información relacionada con la identidad (con fines delictivos).
- La penalización individual de actos típicos relacionados con la obtención de información relacionada con la identidad (como el acceso ilegal, la producción y divulgación de programas informáticos dañinos, la falsificación informática, el espionaje de datos y la interferencia de datos), así como actos relacionados con la posesión y el uso de dicha información (como el fraude informático).

Ejemplos de enfoques con una disposición única

Los ejemplos más conocidos de métodos con una disposición única son los consignados en 18 USC § 1028(a)(7) y 18 USC 1028A(a)(1). Las disposiciones abarcan una amplia gama de delitos relacionados con la usurpación de identidad. Estos enfoques no penalizan únicamente cierta fase sino que abarcan las tres fases antes mencionadas. No obstante, es importante destacar que la disposición no contempla todas las actividades relacionadas con la usurpación de identidad; no contempla, en particular, aquellas actividades en las cuales la persona que actúa es la víctima y no el delincuente.

§ 1028. Fraude y actividades relacionadas con la identificación de documentos, las características de autenticación y la información

(a) Toda persona que, en una circunstancia como la descrita en el apartado c) de esta sección

(1) produzca a sabiendas y sin autoridad legal un documento de identificación, una característica de autenticación o un documento falso de identificación;

(2) transfiera intencionalmente un documento de identificación, una característica de autenticación o un documento de identificación falsa, a sabiendas de que ese documento o característica ha sido robado o producido sin autoridad legal;

(3) posea con conocimiento con intención de utilizar ilegalmente o transferir ilegalmente cinco o más documentos de identificación (distintos de aquellos que han sido expedidos legalmente para su utilización por el poseedor), características de autenticación o documentos de identificación falsa;

(4) posea con conocimiento un documento de identificación (distinto del expedido legalmente para su utilización por el poseedor), una característica de autenticación o un documento de identificación falsa, con la intención de que dicho documento o característica sea utilizado con fines de fraude en los Estados Unidos;

(5) intencionalmente produzca, transfiera o posea una característica de autenticación o implementación de documentos con la intención de utilizar dicha característica para la producción de un documento de identificación falsa u otra característica de autenticación o implementación de documentos que se utilizará de ese modo;

(6) posea con conocimiento un documento de identificación o una característica de autenticación de los Estados Unidos que haya sido o parezca haber sido robado o producido sin autoridad legal, a sabiendas de que dicho documento o característica fue robado o producido sin la autorización pertinente;

(7) transfiera, posea o utilice, intencionalmente y sin autorización legal, un medio de identificación de otra persona con la intención de cometer, ayudar a cometer o instigar la comisión, o en conexión con, cualquier actividad ilegal que constituya una violación de la legislación federal, o que constituya una felonía a tenor de cualquier ley local o estatal aplicable; u

(8) trafique intencionalmente con características de autenticación real o falsa para su utilización en documentos de identificación falsa, implementaciones de documentos falsas o medios de identificación falsa; será castigada según lo dispuesto en el apartado b) de esta sección.

[…]

§ 1028A. Usurpación de identidad con circunstancias agravantes

(a) Delitos.

(1) En general – Toda persona que, durante y en relación con cualquier felonía de las enumeradas en el apartado c) transfiera, posea o utilice, intencionalmente y sin autoridad legal, un medio de identificación de otra persona, será condenada, además del castigo previsto para esa felonía, con una pena de prisión de 2 años.

[…]

Fase 1

Con miras a cometer delitos relacionados con la usurpación de identidad, el delincuente debe entrar en posesión de datos relacionados con la identidad [1915]. Al penalizar la "transferencia" de medios de identificación con la intención de cometer un delito, las disposiciones penalizan los actos relacionados con la Fase 1 de una manera muy amplia[1916]. Puesto que las disposiciones se centran en el acto de transferencia, éstas no abarcan actos realizados por el delincuente antes de la iniciación del proceso de transferencia[1917]. En otras palabras, las disposiciones 8 USC § 1028(a)(7) y 18 USC 1028A(a)(1) no contemplan actos tales como el envío de correos "de *peska*" y la concepción de programas informáticos dañinos que pueden utilizarse para obtener identidad informática relacionada con los datos de las víctimas.

Fase 2

Al penalizar la posesión con la intención de cometer un delito, estas disposiciones adoptan una vez más un enfoque muy amplio en lo tocante a la penalización de actos relacionados con la segunda fase. Ello incluye en particular la posesión de información relacionada con la identidad, con la intención de utilizarla posteriormente para la comisión de uno de los delitos clásicos relacionados con la usurpación de identidad[1918]. No se tipifica como delito la posesión de datos relacionados con la identidad sin intención de utilizarlos.[1919]

Fase 3

Mediante la penalización de la "utilización" con la intención de cometer un delito, las disposiciones abarcan los actos relacionados con la Fase 3. Según se indicó anteriormente, la disposición 18 USC § 1028(a)(7) no está relacionada con un delito específico (como el fraude).

Otro ejemplo es la Sección 14 del texto legislativo sobre la ciberdelincuencia que desarrollaron los países beneficiarios de la iniciativa de HIPCAR.[1920]

Delitos de robo de identidad

14.

Una persona que, intencionalmente, sin excusa o justificación legal, o en exceso de una excusa o justificación legal, mediante el uso de un sistema informático en cualquier etapa de la infracción, de forma deliberada transfiera, posea o utilice, sin excusa o justificación legal, un medio de identificación de otra persona con la intención de cometer, o ayudar o instigar, o en conexión con, cualquier actividad ilegal que constituya un delito, comete una infracción punible, en caso de condena, con pena de reclusión por un período no superior a [período], o una multa que no exceda de [cuantía], o ambas cosas.

En la disposición se contemplan las fases más importantes de los delitos típicos relacionados con la identidad, descritas anteriormente. Sólo la primera fase, en la que el delincuente obtiene la información relacionada con la identidad, no está cubierta. Con la "transferencia" de los medios de identificación se cubren los procesos de transmisión de datos desde un sistema informático a otro. Este acto es especialmente relevante para cubrir la venta (y consiguiente transferencia) de la información relacionada con la identidad[1921]. La "posesión" refleja el control que una persona intencionalmente ejerce sobre la información relacionada con la identidad. El "uso" cubre una amplia gama de prácticas, como la presentación de dicha información para su compra online. Con respecto a la predisposición, la disposición requiere que el delincuente actúe intencionalmente con respecto a todos los elementos objetivos y,

además, tenga la intención específica de realizar la actividad para cometer, ayudar o instigar cualquier actividad ilegal que no sea simplemente la transferencia, posesión o uso de información relacionada con la identidad.

Ejemplo de un enfoque con múltiples disposiciones

La principal diferencia entre el Convenio del Consejo de Europa sobre la Ciberdelincuencia y un enfoque con una disposición única (éste es por ejemplo el enfoque aplicado en los Estados Unidos) es el hecho de que en el Convenio sobre la Ciberdelincuencia no se define un ciberdelito separado de la utilización ilegal de información relacionada con la identidad[1922]. Análogamente a lo que ocurre con respecto a la penalización de la obtención de información relacionada con la identidad, el Convenio sobre la Ciberdelincuencia no contempla todos los actos posibles relacionados con la utilización ilegal de información personal.

Fase 1

El Convenio del Consejo de Europa sobre la Ciberdelincuencia[1923] contiene cierto número de disposiciones que penalizan los actos de usurpación de identidad por Internet en la Fase 1. Se trata concretamente de los siguientes actos:

- Acceso ilícito (Artículo 2)[1924]
- Interceptación ilegal (Artículo 3)[1925]
- Interferencia de los datos (Artículo 4)[1926]

Tomando en consideración las diversas modalidades según las cuales un delincuente puede obtener acceso a los datos, es necesario señalar que en la Fase 1 no se contemplan todos los actos posibles. Un ejemplo de un delito que a menudo está relacionado con la Fase 1 de la usurpación de identidad pero que no está contemplado en el Convenio del Consejo de Europa sobre la Ciberdelincuencia es el espionaje de datos.

Fase 2

El Convenio del Consejo de Europa sobre la Ciberdelincuencia no puede contemplar los actos que tienen lugar entre la obtención de la información y la utilización de los mismos con fines delictivos. No es posible, en particular, evitar la existencia de un mercado negro cada vez mayor de información relacionada con la identidad mediante la penalización de la venta de dicha información sobre la base de las disposiciones consignadas en el Convenio sobre la Ciberdelincuencia.

Fase 3

En el Convenio del Consejo de Europa sobre la Ciberdelincuencia del Consejo de Europa se define cierto número de infracciones relacionadas con el ciberdelito. Algunas de esas infracciones pueden ser cometidas por el perpetrador utilizando información relacionada con la identidad. Un ejemplo es el fraude informático, que a menudo se menciona en el contexto de la usurpación de identidad[1927]. De los estudios realizados sobre la usurpación de identidad se desprende que la mayoría de los datos obtenidos se utilizaron para falsificar cartas de crédito[1928]. Si el fraude con cartas de crédito se comete en línea, es probable que el perpetrador pueda ser procesado a tenor del Artículo 8 del Convenio del Consejo de Europa sobre la Ciberdelincuencia. El marco jurídico no contempla otros delitos que pueden realizarse utilizando información relacionada con la identidad que se obtuvo previamente pero que no están mencionados en el Convenio sobre la Ciberdelincuencia. No es posible, en particular, entablar un juicio por utilización de información relacionada con la identidad con la intención de mantener en secreto la identidad.

6.2.18 Fraude informático

El fraude es un delito muy propagado en el ciberespacio[1929]. Se trata asimismo de un problema común más allá de Internet, por lo cual la mayoría de las leyes nacionales contienen disposiciones que penalizan los delitos de fraude[1930]. No obstante, puede resultar difícil aplicar las disposiciones en vigor a los casos relacionados con Internet, cuando las disposiciones nacionales tradicionales del derecho penal están

basadas en la falsedad de una persona[1931]. En muchos casos de fraude cometidos por Internet, en realidad el que responde a un acto del delincuente es un sistema informático. Cuando las disposiciones criminales tradicionales en las que se aborda el fraude no incluyan a los sistemas informáticos, será necesario actualizar la legislación nacional.[1932]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia trata de penalizar cualquier manipulación indebida en el curso del procesamiento de datos con la intención de efectuar una transferencia ilegal de la propiedad, al establecer un Artículo sobre el fraude informático, a saber:[1933]

Disposición

Artículo 8 – Fraude informático
Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a) la introducción, alteración, borrado o supresión de datos informáticos;

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Actos contemplados

El apartado a) del Artículo 8 contiene una lista de los actos más importantes de fraude informático[1934]. Por "introducción" de datos informáticos se entiende todo tipo de manipulación de entradas como, por ejemplo, alimentar al computador con datos incorrectos, así como manipulaciones de programas informáticos y otros actos de interferencia con el procesamiento de datos[1935]. El término "alteración" se refiere a la modificación de los datos existentes[1936]. El término "supresión" de datos informáticos indica una acción que afecta la disponibilidad de datos[1937]. El término "borrado" se corresponde con la definición que figura en el Artículo 4 y abarca actos en los que se elimina información[1938].

Además de la lista de actos, en su apartado b) el Artículo 8 contiene la cláusula general que penaliza "cualquier interferencia en el funcionamiento de un sistema informático", la cual fue añadida a la lista con el fin de dejar la disposición abierta para nuevas adiciones[1939].

En el Informe Explicativo se indica que la "interferencia con el funcionamiento de un sistema informático" incluye actos tales como manipulaciones de hardware, actos de supresión de impresiones y actos que afectan el registro o el flujo de datos, o bien la secuencia según la cual funcionan los programas.[1940]

Pérdida económica

A tenor de la mayoría de los regímenes de derecho penal nacional, el acto delictivo debe tener como consecuencia una pérdida económica. En el Convenio sobre la Ciberdelincuencia se sigue una pauta similar y se limita la penalización a aquellos actos en los cuales la manipulación produce una pérdida económica o de propiedad directa a otra persona, con inclusión de dinero, bienes tangibles e intangibles con un valor económico.[1941]

Predisposición

Como ocurre con los otros delitos enumerados, en el Artículo 8 del Convenio del Consejo de Europa sobre la Ciberdelincuencia se impone el requisito de que el delincuente actúe intencionalmente, tanto en lo que respecta a la manipulación como a la pérdida financiera.

Por otro lado, para proceder a la penalización el Convenio exige que el delincuente actúe con intención fraudulenta o deshonesta con el fin de obtener beneficios económicos o de otra índole para sí mismo u otra persona[1942]. Entre ejemplos de actos que quedan excluidos de responsabilidad penal debido a la ausencia de una intención concreta, en el Informe Explicativo se mencionan las prácticas comerciales resultantes de

la competencia mercantil que pueden causar pérdidas económicas a una persona y beneficiar a otra, pero que no se realizan con una intención fraudulenta o deshonesta.[1943]

Sin derecho

El fraude informático sólo puede penalizarse a tenor del Artículo 8 del Convenio sobre la Ciberdelincuencia si tiene lugar "sin derecho"[1944]. Esto incluye el requisito de que el beneficio económico debe ser obtenido sin derecho. Los redactores del Convenio sobre la Ciberdelincuencia subrayaron que los actos efectuados en el marco de un contrato válido entre las personas afectadas no son considerados actos sin derecho.[1945]

Ley modelo de la Commonwealth sobre informática y delitos relacionados con la informática

La Ley modelo de la Commonwealth de 2002 no contiene disposición alguna que penalice el fraude informático.[1946]

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford de 1999, de carácter oficioso[1947], no contiene disposición alguna que penalice el fraude informático.

6.2.19 Delitos relacionados con infracciones de la propiedad intelectual

La transición de la distribución analógica de los contenidos protegidos por derechos de autor a su distribución digital marca un hito en lo que se refiere a las infracciones de la propiedad intelectual[1948]. Históricamente la reproducción de obras de música y vídeos se ha visto limitada por el hecho de que la reproducción de una fuente analógica a menudo entraña una pérdida de calidad en la copia, lo que a su vez limita la posibilidad de utilizar esa copia como una fuente para nuevas reproducciones. Ahora bien, después de la transición hacia fuentes digitales, ahora es posible obtener copias con la misma calidad que la fuente.[1949]

El sector de las actividades recreativas ha reaccionado mediante la adopción de medidas técnicas (gestión de derechos digitales – *digital rights management*, DRM) para evitar la reproducción[1950], pero hasta la fecha se ha esquivado el efecto de estas medidas muy poco tiempo después de su introducción[1951]. En Internet se dispone de diversos instrumentos de software que permiten a los usuarios copiar música (CD) y películas (DVD) que se encuentran protegidas por sistemas DRM. Además, Internet ofrece ilimitadas oportunidades de distribución. Como resultado de ello, los delitos relacionados con infracciones de la propiedad intelectual se cometen de manera generalizada por Internet.[1952]

Convenio del Consejo de Europa sobre la Ciberdelincuencia

En el Convenio sobre la Ciberdelincuencia se ha incluido una disposición que cubre estas infracciones de la propiedad intelectual, con la cual se intenta armonizar las diversas reglamentaciones consignadas en las leyes nacionales y que ha resultado ser uno de los principales obstáculos para utilizar dicho Convenio fuera de Europa.

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente Artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente Artículo.

Las infracciones de la propiedad intelectual están penalizadas en la mayoría de los países[1953] y se abordan en cierto número de tratados internacionales[1954]. En el Convenio sobre la Ciberdelincuencia se estipulan los principios fundamentales que rigen la penalización de las violaciones de la propiedad intelectual con miras a armonizar las legislaciones nacionales en vigor. En la disposición no se contempla los delitos relacionados con las patentes o la marca de fábrica.[1955]

Referencia a acuerdos internacionales

A diferencia de lo que ocurre con otros instrumentos jurídicos, en el Convenio sobre la Ciberdelincuencia no se designan explícitamente los actos que se han de penalizar, sino que se hace referencia a cierto número de acuerdos internacionales[1956]. Éste es uno de los aspectos que ha sido objeto de crítica en lo que respecta al Artículo 10. Además de que eso dificulta la determinación del alcance de la penalización y que dichos acuerdos podrían ser modificados posteriormente, se planteó la cuestión de saber si el Convenio sobre la Ciberdelincuencia obliga o no a los Estados signatarios a firmar los acuerdos mencionados en el Artículo 10. Los redactores del Convenio sobre la Ciberdelincuencia señalaron que en el Convenio del Consejo de Europa sobre la Ciberdelincuencia no se incluiría ninguna obligación de ese tipo. [1957]. Así pues, los Estados que no hayan firmado los acuerdos internacionales mencionados ni están obligados a hacerlo ni a penalizar actos relacionados con acuerdos que no hayan firmado. Por lo tanto, el Artículo 10 sólo impone obligaciones a aquellas Partes que hayan firmado uno de los acuerdos mencionados.

Predisposición

Debido a su carácter general, el Convenio sobre la Ciberdelincuencia limita la penalización a aquellos actos que hayan sido cometidos por conducto de un sistema informático[1958]. Además de los actos cometidos por un sistema informático, la responsabilidad penal se limita a actos que hayan sido cometidos voluntariamente y a escala comercial. El término "voluntariamente" se corresponde con el término "intencionalmente" que se utiliza en otras disposiciones jurídicas fundamentales del Convenio, y tiene en cuenta la terminología utilizada en el Artículo 61 del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio (ADPIC)[1959], que gobierna la obligación de penalizar las infracciones relacionadas con la propiedad intelectual.[1960]

Escala comercial

La limitación de la penalización a actos que se cometen a escala comercial también tiene en cuenta el Acuerdo sobre los ADPIC, en el cual se estipula que se han de imponer sanciones penales únicamente por "piratería a escala comercial". Dado que la mayor parte de las infracciones relacionadas con la propiedad intelectual en sistemas con compartición de ficheros no tienen escala comercial, a éstas no se les aplica el Artículo 10. El Convenio sobre la Ciberdelincuencia trata de establecer normas mínimas para delitos relacionados con Internet. Así pues, las Partes pueden ir más allá del umbral de la "escala comercial" para penalizar las infracciones relacionadas con la propiedad intelectual.[1961]

Sin derecho

Por lo general, en las disposiciones fundamentales de derecho penal definidas en el Convenio del Consejo de Europa sobre la Ciberdelincuencia se impone el requisito de que el acto sea realizado "sin derecho"[1962]. Los redactores del Convenio sobre la Ciberdelincuencia subrayaron que el término "infracción" ya implica la realización de un acto sin autorización.[1963]

Restricciones y reservas

El párrafo 3 autoriza a las Partes signatarias a formular una reserva, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumben a las Partes.

Proyecto de Convenio Internacional de Stanford

El Proyecto de Convenio Internacional de Stanford de 1999, de carácter oficioso[1964], no contiene disposición alguna que penalice las infracciones relacionadas con la propiedad intelectual. Los redactores del Convenio destacaron que en éste no se incluyeron los delitos relacionados con infracciones de la propiedad intelectual puesto que ello hubiera resultado difícil[1965]. En su lugar éstos hacen referencia directamente a los acuerdos internacionales en vigor.[1966]

6.2.20 Uso de Internet con fines terroristas

Como se señaló anteriormente, el término "uso de Internet con fines terroristas" se utiliza para describir un conjunto de actividades que van desde la difusión de propaganda hasta los ataques selectivos. Desde el punto de vista de la respuesta legal se pueden distinguir tres enfoques sistemáticos diferentes.

Enfoques sistemáticos

Uso de legislación existente sobre ciberdelincuencia

El primer enfoque estriba en utilizar la legislación existente sobre ciberdelincuencia (desarrollada para cubrir actos no relacionados con el terrorismo) para penalizar el uso de Internet con fines terroristas. En este contexto se deben tener en consideración tres aspectos. En primer lugar, las disposiciones de derecho penal sustantivo que se crearon para cubrir actos no relacionados con el terrorismo, como las relativos a la interferencia con el sistema[1967], podrían aplicarse en casos que sí estuvieran relacionados, pero muy a menudo la escala de penas de las sentencias diferirá de la correspondiente a la legislación específica para el terrorismo. Esta aplicación podría influir en la capacidad de utilizar instrumentos sofisticados de investigación que están restringidos a la investigación de delitos de terrorismo o del crimen organizado. En segundo lugar, la aplicación de instrumentos de investigación específicos sobre ciberdelincuencia en los casos de uso de Internet con fines terroristas se enfrenta a un menor número de problemas, en la medida en que la mayoría de los países no limitan la aplicación de instrumentos de investigación sofisticados para delitos cibernéticos tradicionales, siempre que incluya cualquier delito que afecte a los datos informáticos. Por último, los instrumentos jurídicos regionales que se desarrollan para afrontar el problema de la ciberdelincuencia pero no específicamente el uso de Internet con fines terroristas incluyen a menudo exenciones para la cooperación internacional con respecto a los delitos políticos. En el apartado 4 a) del Artículo 27 del Convenio del Consejo de Europa sobre la Ciberdelincuencia se encuentra un ejemplo.[1968]

> ***Artículo 27 - Procedimientos relativos a los pedidos de asistencia mutua en ausencia de acuerdos internacionales aplicables***
> *[…]*
> *4. Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del Artículo 25, la Parte requerida podrá denegar la asistencia si:*
> *a) la solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político;*
> *b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.*
> *[…]*

La disposición autoriza a las partes del Convenio a denegar las solicitudes de asistencia mutua si se refieren a un delito que la Parte requerida considera un delito político o delito vinculado a un delito político, lo que puede dificultar gravemente las investigaciones. Como consecuencia, marcos jurídicos específicos sobre el terrorismo como el Convenio del Consejo de Europa para la prevención del terrorismo de 2005[1969] contienen una exclusión de la cláusula de excepción política.

Artículo 20 – Exclusión de la cláusula de excepción política
1 Ninguno de los delitos mencionados en los Artículos 5 a 7 y 9 del presente Convenio se considerará, a efectos de los requisitos necesarios para la extradición o la asistencia judicial, como delito político o como delito conexo a un delito político, o como un delito inspirado por móviles políticos. Por consiguiente, una solicitud de extradición o de asistencia judicial basada en uno de esos delitos no podrá ser denegada por el solo hecho de que se refiera a un delito político, o a un delito conexo a un delito político o a un delito inspirado por móviles políticos.
[…]

Utilización de legislación existente contra el terrorismo

El segundo enfoque es el empleo de la legislación existente contra el terrorismo para criminalizar y perseguir el uso de Internet con fines terroristas. Este instrumento tradicional es, por ejemplo, el Convenio del Consejo de Europa para la prevención del terrorismo de 2005.[1970]

Artículo 5 – Provocación pública para cometer delitos terroristas
1. A los efectos del presente Convenio, se entenderá por "provocación pública para cometer delitos terroristas" la difusión o cualquier otra forma de puesta a disposición del público de mensajes con la intención de incitar a cometer delitos terroristas, cuando ese comportamiento, ya preconice directamente o no la comisión de delitos terroristas, cree peligro de que se puedan cometer uno o varios delitos.
2. Cada Parte adoptará las medidas necesarias para tipificar como delito, de conformidad con su derecho interno, la provocación pública para cometer delitos terroristas tal como se define en el apartado 1, cuando se cometa ilegal e intencionadamente.

Artículo 6 – Reclutamiento con fines terroristas
1. A los efectos del presente Convenio, se entenderá por "reclutamiento con fines terroristas" el hecho de incitar a otra persona a cometer o participar en la comisión de delitos terroristas, o a unirse a una asociación o a un grupo para contribuir a que éstos cometan uno o varios delitos terroristas.
2. Cada Parte adoptará las medidas necesarias para tipificar como delito, de conformidad con su derecho interno, el reclutamiento con fines terroristas, tal como se define en el apartado 1 del presente artículo, cuando se cometa ilegal e intencionadamente.

El Convenio para la Prevención del Terrorismo contiene varios delitos como la provocación pública para cometer delitos terroristas y el reclutamiento con fines terroristas pero no, por ejemplo, disposiciones que penalicen ataques relacionados con el terrorismo contra sistemas informáticos. Por otra parte, el Convenio no incluye instrumentos procesales. Especialmente con respecto a la investigación de delitos relacionados con Internet a menudo se requieren instrumentos procesales específicos. Para la identificación de un delincuente que ha incitado al terrorismo utilizando páginas web se necesitan instrumentos sofisticados como la inmediata conservación de los datos de tráfico.

Legislación específica

El tercer enfoque es el desarrollo de una legislación específica sobre el uso de Internet con fines terroristas.

Algunos ejemplos de legislación específica

Como se señaló anteriormente, el término "uso de Internet con fines terroristas" se utiliza para describir un conjunto de actividades que van desde la difusión de propaganda hasta los ataques selectivos. En cuanto a la respuesta legal, existen principalmente dos áreas de reglamentación: los ataques relacionados con la informática y los contenidos ilícitos.

Ataques relacionados con la informática

En la Sección 66F de la Ley sobre Tecnologías de la Información de la India de 2000, modificada en 2008, se encuentra un enfoque de una disposición que trata específicamente los ataques informáticos relacionados con el terrorismo:

Sanción 66F para el ciberterrorismo – Ley sobre Tecnologías de la Información, 2000. [Conforme a la enmienda de 2008 de la ley sobre tecnologías de la información]
(1) Toda persona que, -
(A) con la intención de poner en peligro la unidad, integridad, seguridad o soberanía de la India o para sembrar el terror en la población, o una parte de la misma, -
(i) niegue el acceso o provoque la denegación de acceso a cualquier persona autorizada a acceder a recursos informáticos; o
(ii) intente penetrar o tener acceso a un recurso informático sin autorización o excediendo el acceso autorizado; o
(iii) introduzca o cause la introducción de cualquier contaminante informático.
y que por medio de tal conducta cause, o pueda causar, la muerte, o lesiones, a personas, o daños a, o destrucción de, la propiedad; o interrumpa, o sepa que es probable que cause daño, o interrupción de, suministros, o servicios esenciales, para la vida de la comunidad; o afecte negativamente a las infraestructuras de información críticas que se especifican en la Sección 70, o
(B) a sabiendas, o intencionalmente, penetre, o acceda, a un recurso informático sin autorización, o excediendo el acceso autorizado, y por medio de tal conducta obtenga acceso a información, datos o base de datos informatizada que estén restringidos por razones de la seguridad del Estado o de las relaciones extranjeras; o cualquier información restringida, datos o base de datos informatizada, con razones para creer que dicha información, datos o base de datos informática así obtenidos puedan ser utilizados para causar, o puedan causar, perjuicio a los intereses de la soberanía y la integridad de la India, la seguridad del Estado, las relaciones amistosas con Estados extranjeros, el orden público, la decencia o la moralidad, o en relación con el desacato a los tribunales, la difamación o la incitación a un delito, o en beneficio de una nación extranjera, grupo de personas o no, comete el delito de ciberterrorismo.
(2) Todo aquel que cometa o conspire para cometer actos de ciberterrorismo será sancionado con pena de prisión que puede llegar hasta la cadena perpetua".

En la Sección 66F de la Ley de Tecnologías de la Información de la India no sólo se requiere que el delincuente actúe con intención relacionada con el terrorismo ("con la intención de poner en peligro la unidad, integridad, seguridad o soberanía de la India o para sembrar el terror en la población, o una parte de la misma"), sino también que el delito lleve a daños graves, como la muerte, lesiones o la interrupción de servicios que afecten a infraestructuras de información críticas.

Contenido ilegal

El contenido ilegal, como es el caso de la propaganda terrorista, es un área donde los Estados están particularmente adheridos a enfoques independientes de la tecnología. Un ejemplo de un enfoque de neutralidad tecnológica es el Artículo 10 de la Ley Federal de Rusia 149-FZ, de 27.07.2006, sobre la información, tecnologías de la información y protección de datos.

Artículo 10 – Difusión de información o suministro de información
[…]
6. Está prohibido difundir información destinada a la propaganda de guerra, a la discriminación y hostilidad por cuestiones nacionales, raciales o religiosas, además de otras informaciones cuya difusión está sujeta a responsabilidad penal o administrativa.

Esta disposición no se refiere específicamente a la distribución de contenidos ilegales por medio de redes informáticas, o a la puesta a disposición de contenido en estas redes, sino que se elaboró con el fin de no depender de la tecnología utilizada.

Otro ejemplo de un enfoque de neutralidad tecnológica es el Artículo 3 de la enmienda de 2008 de la Decisión marco de la UE[1971] sobre la lucha contra el terrorismo.[1972]

Artículo 3 – Delitos ligados a actividades terroristas
1. A efectos de la presente Decisión marco, se entenderá por:
a) "provocación a la comisión de un delito de terrorismo". la distribución o difusión pública, por cualquier medio, de mensajes destinados a inducir a la comisión de cualesquiera de los delitos enumerados en el Artículo 1, apartado 1, letras a) a h), cuando dicha conducta, independientemente de que promueva o no directamente la comisión de delitos de terrorismo, conlleve el riesgo de comisión de uno o algunos de dichos delitos;
b) "captación de terroristas": la petición a otra persona de que cometa cualesquiera de los delitos enumerados en el Artículo 1, apartado 1, letras a) a h), o en el Artículo 2, apartado 2;
c) "adiestramiento de terroristas": impartir instrucciones sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre otros métodos o técnicas específicos, con el fin de cometer cualesquiera de los delitos enumerados en el Artículo 1, apartado 1, letras a) a h), a sabiendas de que las enseñanzas impartidas se utilizarán para dichos fines.
2. Los Estados miembros adoptarán las medidas necesarias para garantizar que entre los delitos ligados a actividades terroristas se incluyan los siguientes actos dolosos:
a) provocación a la comisión de un delito de terrorismo;
b) captación de terroristas;
c) adiestramiento de terroristas;
d) hurto o robo con agravantes cometido con el fin de cometer cualesquiera de los delitos enumerados en el Artículo 1, apartado 1;
e) chantaje con el fin de cometer cualesquiera de los delitos enumerados en el Artículo 1, apartado 1;
f) libramiento de documentos administrativos falsos con el fin de cometer cualesquiera de los delitos enumerados en el Artículo 1, apartado 1, letras a) a h), y en el Artículo 2, apartado 2, letra b).
3. Para que un acto contemplado en el apartado 2 sea punible no será necesaria la comisión efectiva de un delito de terrorismo.".

Los redactores resaltaron en la introducción que el marco jurídico vigente penaliza la inducción, la complicidad y la incitación al terrorismo, pero no penaliza la difusión a través de Internet de conocimientos específicos en materia de terrorismo. A este respecto, los autores señalaron que "Internet se utiliza para inspirar y movilizar a redes terroristas locales e individuos en Europa y también sirve de fuente de información sobre medios y métodos terroristas, funcionando por lo tanto como un "campo de entrenamiento virtual".[1973] A pesar de que en la introducción se menciona explícitamente el uso de Internet con fines terroristas, la disposición proporcionada está redactada de una manera tecnológicamente neutra y, por lo tanto, comprende todos los actos de adiestramiento de terroristas, independientemente de sean en línea o no.[1974]Uno de los retos relacionados con la aplicación de la disposición en los casos relacionados con Internet es la dificultad de probar que el delincuente actuó a sabiendas de que las enseñanzas impartidas irían destinadas a ser utilizadas para este propósito. Es muy probable que la necesidad de tales pruebas limite las posibilidades de que la disposición se pueda aplicar a las guías en línea sobre armamento. Como la mayoría de las armas y los explosivos pueden utilizarse tanto para cometer delitos ordinarios como delitos relacionados con el terrorismo, la mera publicación de este tipo de información no prueba que el editor supiera cómo iba a ser utilizada. Por lo tanto, tendrá que considerarse el contexto de la publicación

(por ejemplo, que aparezca en un sitio web controlado por una organización terrorista). Esto puede presentar problemas si la información se publica fuera del contexto de otros contenidos relacionados con el terrorismo, como ocurre cuando se difunde por medio de sistemas de intercambio o servicios de alojamiento de archivos.

Un ejemplo de un enfoque específico sobre Internet es el Artículo 5 del Reglamento chino sobre la red informática y la seguridad, la protección y gestión de Internet:

*"**Artículo 5** – Ninguna unidad o individuo puede utilizar Internet para crear, reproducir, recuperar o transmitir información en la que se:*

(1) incite a resistir o quebrantar la Constitución, las leyes o la aplicación de los reglamentos administrativos;
(2) incite a derrocar al gobierno del sistema socialista;
(3) incite a la división del país, perjudicando la unidad nacional;
(4) incite al odio o a la discriminación entre las nacionalidades o se perjudique la unidad de estas;
(5) falte a la verdad o la distorsione, propagando rumores, destruyendo el orden de la sociedad;
(6) promueva supersticiones feudales, material sexualmente sugerente, juegos de azar, violencia, asesinato;
(7) incluya contenido terrorista, o se incite a otros a la actividad criminal; insulte abiertamente a otras personas o se distorsione la verdad para calumniar a personas;
(8) lesione la reputación de los órganos del Estado;
(9) incluyan otras actividades en contra de la Constitución, la ley o los reglamentos administrativos".

Guerra cibernética

A pesar de que desde hace varias décadas se viene debatiendo sobre las amenazas relacionadas con la guerra cibernética, el debate sobre la respuesta jurídica no ha hecho más que comenzar. Aún en mayor grado que la ciberdelincuencia, la guerra cibernética se rige por el derecho internacional. Los Convenios de La Haya, los Convenios de Ginebra y la Carta de las Naciones Unidas son instrumentos de derecho internacional importantes que contienen normas que rigen las leyes de la guerra. Si bien es una práctica habitual la aplicación de dichos instrumentos para regular los conflictos armados, su aplicación a los ataques informáticos y basados en red tropieza con dificultades. Esto se puede comprobar analizando la aplicabilidad del Artículo 2(4) de la Carta de las Naciones Unidas, que prohíbe el uso de la fuerza.

Artículo 2 de la Carta de las Naciones Unidas
Para la realización de los Propósitos consignados en el Artículo 1, la Organización y sus Miembros procederán de acuerdo con los siguientes Principios:
[...]
(4) Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas.
[...]

La prohibición del uso de la fuerza tiene la intención de imponer una prohibición completa de todos los tipos de fuerza, excepto los que están en consonancia con la Carta de las Naciones Unidas.[1975] En las últimas décadas, se ha cuestionado en varias ocasiones la prohibición del uso de la fuerza que figura en el Artículo 2 (4). Uno de los retos principales ha sido el cambio experimentado de las guerras a gran escala, que constituían el centro de atención cuando fue redactada la Carta de las Naciones Unidas después de la Segunda Guerra Mundial, a las guerras a pequeña escala, que son mucho más frecuentes actualmente.[1976] La cobertura de los ataques relacionados con la informática añade otra dimensión al desafío, en la medida en que no sólo es la escala lo que cambia, sino también los métodos y herramientas utilizados en el conflicto.[1977] En consecuencia, la principal dificultad relacionada con la aplicación del Artículo 2 es la interpretación del término "uso de la fuerza". Ni la Carta de las Naciones Unidas ni los instrumentos

internacionales relacionados definen con claridad el término "uso de la fuerza". Existe un amplio consenso en relación con que la Carta de la Naciones Unidas no prohíbe todos los tipos de actos hostiles. Prohíbe los ataques con armas convencionales, por ejemplo, pero no la amenaza de la fuerza y la coerción económica.[1978]

Los dos elementos constitutivos del uso de la fuerza son el uso de las armas y la participación de agentes estatales. A pesar de que la importancia de esto último, en particular, fue cuestionado por las resoluciones del Consejo de Seguridad después de los ataques del 9/11, ambos elementos siguen siendo esenciales con respecto a la prohibición del uso de la fuerza.

Uso de las armas/destrucción de vidas y bienes

El primer elemento constitutivo es el uso de las armas. Difícilmente puede llamarse a la tecnología informática utilizada para llevar a cabo los ataques relacionados con Internet un arma tradicional, en la medida en que este tipo de armas, en general, implican un impacto cinético.[1979] Sin embargo, la necesidad de incluir las armas químicas y biológicas ya ha exigido cambiar desde una definición orientada a la acción a un enfoque orientado a las repercusiones. Bajo este enfoque más amplio, las armas podrían definirse como una herramienta para destruir vidas o bienes.[1980]

Aun basándose en una interpretación amplia de este tipo, sin embargo, es problemático contemplar los ataques informáticos y los basados en red como uso de la fuerza y la tecnología informática como armas, ya que las repercusiones de los ataques son diferentes.[1981] No sólo los métodos utilizados, sino también los efectos difieren en relación a los conflictos armados tradicionales.[1982] Las estrategias militares tradicionales que implican el uso de las armas se centran en la eliminación física de las capacidades militares del enemigo. Los ataques informáticos y los basados en red pueden llevarse a cabo con el mínimo daño físico y pérdidas de vidas.[1983] A diferencia de un ataque con misiles, un ataque de denegación de servicio que temporalmente cierre un sitio web del gobierno no causa ningún daño físico real. Sin embargo, sería erróneo afirmar que los ataques informáticos no puedan acarrear daños graves. Un ataque de denegación de servicio contra el sistema informático de un hospital o banco de sangre puede representar una amenaza grave para la salud y poner en peligro las vidas de un gran número de personas. El descubrimiento de la posible repercusión física de Stuxnet es otro ejemplo que demuestra que los ataques informáticos no necesariamente tienen consecuencias inmateriales. Si los ataques informáticos y basados en red tienen un impacto físico de este tipo, pueden considerarse similares a las armas tradicionales.[1984]

Conflicto entre Estados

Como se señaló anteriormente, el segundo requisito para la aplicación del Artículo 2 de la Carta de las Naciones Unidas es que el uso de la fuerza se lleve a cabo por un Estado contra otro Estado. A pesar de las tendencias recientes para ampliar la aplicación de la Carta de las Naciones Unidas, el Artículo 2 de la Carta de las Naciones Unidas no contempla los actos cometidos por agentes no estatales. Esta circunstancia es muy importante para la cobertura de la guerra cibernética, en la medida que aquí, a diferencia de las guerras tradicionales, los agentes no estatales desempeñan un papel más importante. Existen serias preocupaciones con respecto a su proliferación, ya que los agentes no estatales pueden conseguir grandes medios que incluso podrían superar a los controlados por los Estados.[1985]Los redes robot más grandes incluyen varios millones de sistemas informáticos. Este número es probablemente mayor que el número de sistemas informáticos que controlen y dispongan para intervenciones militares la mayoría de los Estados. La capacidad de los agentes no estatales tiene gran relevancia, ya que actúan principalmente fuera del marco jurídico internacional que obliga a los Estados. Esto plantea preocupaciones con respecto a la atribución. La aplicación del Artículo 2 de la Carta de las Naciones Unidas requiere por el momento que un ataque informático se atribuya a un Estado. Las experiencias con los incidentes en Estonia en 2007 y Georgia en 2008 subrayan que, en la mayoría de los casos, la identificación o verificación del origen de un ataque puede resultar un desafío insuperable.

6.3 Evidencia digital

Bibliografía (seleccionada): *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf; *Gercke*, Impact of Cloud Computing on the work of law enforcement agencies, published in *Taeger/Wiebe*, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4; *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No.3; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002; *Hayes*, Forensic Handwriting Examination, 2006; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2; *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010; *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No.1; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No.

5; *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1; *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

Debido en particular a las crecientes capacidades de disco duro[1986] y la disminución de los costes de almacenamiento[1987] de los documentos digitales, en comparación con el almacenamiento de documentos físicos, el número de documentos digitales va en aumento.[1988] Hoy en día, un volumen considerable de datos se almacena en forma digital únicamente.[1989] Además, en los países desarrollados, y cada vez más en los países en desarrollo, las tecnologías informáticas y de red han pasado a formar parte de la vida diaria. Como consecuencia de ello los documentos electrónicos tales como documentos de texto, videos digitales e imágenes digitales[1990] se están utilizando en las investigaciones sobre ciberdelito y en las correspondientes actuaciones judiciales.[1991]

Ahora bien, los efectos de la digitalización y la importancia de la evidencia digital se están dilatando más allá de las investigaciones sobre el ciberdelito: incluso al cometer un delito tradicional, los delincuentes pueden dejar huellas digitales, tales como información sobre la ubicación de su teléfono celular[1992], o realizar búsquedas electrónicas sospechosas.[1993] Así pues, se considera que la capacidad para aprovechar determinadas herramientas de investigación relacionadas con los datos y presentar evidencias digitales ante el tribunal es esencial, tanto para las investigaciones de delitos tradicionales como para los relacionados con el ciberdelito.[1994]

Las "evidencias digitales" plantean algunas dificultades,[1995] pero también abren nuevas posibilidades para las investigaciones y para los trabajos de los tribunales y los expertos forenses. Ya desde la primera etapa –la compilación de evidencias–, la necesidad de estar en condiciones de manejar evidencias digitales ha cambiado la forma de trabajar de los investigadores. Éstos precisan instrumentos de investigación específicos para llevar a cabo sus investigaciones. Contar con esos instrumentos es particularmente importante cuando no se dispone de evidencias tradicionales como huellas digitales o testigos. En esos casos, la capacidad para identificar satisfactoriamente a un delincuente y enjuiciarlo puede depender de la compilación y evaluación correctas de la evidencia.[1996] Sin embargo, más allá de la compilación de evidencias, la digitalización también influye en la manera según la cual tratan la evidencia los tribunales y los organismos encargados de hacer cumplir la ley.[1997] Aunque los documentos tradicionales originales se presentan manualmente en el tribunal, en algunos casos la evidencia digital exige procedimientos específicos que no permiten su conversión en evidencia tradicional, como por ejemplo la presentación de una impresión de ficheros y otros datos.[1998]

En el Capítulo que figura a continuación se proporciona un panorama general de los aspectos prácticos y jurídicos de la evidencia digital y las investigaciones sobre ciberdelito.

6.3.1 Definición de evidencia digital

La digitalización y el uso cada vez mayor de las TIC tienen enormes repercusiones en los procedimientos para la compilación de evidencias y su utilización en los tribunales.[1999] Como consecuencia del desarrollo se ha introducido la evidencia digital como una nueva fuente de evidencia.[2000] No existe una definición única de evidencia electrónica o digital.[2001] En el Código Penal y Policial del Reino Unido se define evidencia digital como "toda información contenida en un ordenador".[2002] Con un enfoque más amplio, se podría definir la evidencia digital como cualquier dato almacenado o transmitido utilizando tecnología informática que sirve para fundamentar la teoría de cómo se ha cometido un delito.[2003]

6.3.2 Importancia de la evidencia digital en las investigaciones sobre ciberdelito

La evidencia digital desempeña una importante función en varias fases de las investigaciones del ciberdelito. En general caben considerar dos grandes fases[2004]: la fase de investigación (identificación de la

evidencia pertinente[2005], compilación y preservación de la evidencia[2006], análisis de la tecnología informática y evidencia digital), y la presentación y el uso de la evidencia en los procedimientos judiciales.

La primera fase está vinculada a la técnica forense aplicada a la informática, que se examinará más detalladamente infra. La expresión "técnica forense aplicada a la informática" se refiere al análisis sistemático de equipos TI para tratar de encontrar evidencia digital.[2007] El crecimiento constante del volumen de datos almacenados en formato digital pone de relieve las dificultades logísticas que entrañan las investigaciones.[2008] Por lo tanto, además de las investigaciones manuales[2009], también es importante aplicar procedimientos forenses automatizados, por ejemplo realizando búsquedas basadas en el valor de control ("hash-value") de imágenes conocidas de pornografía infantil[2010] o búsquedas por palabras clave.[2011] Las técnicas forenses en la esfera informática incluyen investigaciones tales como análisis de los hardware y software utilizados por un sospechoso,[2012] la recuperación de ficheros suprimidos,[2013] la decriptación de ficheros[2014] o la identificación de los usuarios de Internet mediante el análisis de los datos de tráfico.[2015]

La segunda fase guarda relación con la presentación de la evidencia digital ante el tribunal, y está estrechamente vinculada a ciertos procedimientos que es necesario aplicar porque la información digital sólo es visible cuando se imprime o visualiza recurriendo a tecnologías informáticas.

6.3.3 Importancia creciente de la evidencia digital en las investigaciones penales tradicionales

La aptitud de los investigadores para buscar datos y encontrar evidencias, así como la de los tribunales para tratar la evidencia digital, no se limita a las investigaciones sobre ciberdelitos. Debido a la integración cada vez mayor de la tecnología informática en la vida diaria de las personas, la evidencia digital se está transformando en una importante fuente de evidencia, incluso en el marco de las investigaciones tradicionales. Un ejemplo de ello es un juicio por asesinato que tuvo lugar en los Estados Unidos, durante el cual se utilizaron grabaciones de solicitudes de búsqueda almacenadas en el ordenador del sospechoso para probar que, antes del asesinato, éste utilizó intensamente los motores de búsqueda para encontrar información sobre venenos imposibles de detectar.

6.3.4 Nuevas oportunidades para la investigación

Dependiendo de los servicios TIC e Internet utilizados por un sospechoso, cabe rastrear toda una serie de huellas digitales.[2016] Si el sospechoso utiliza, por ejemplo, motores de búsqueda para buscar pornografía infantil en línea, se registran sus solicitudes de búsqueda, y por consiguiente sus direcciones IP y, en ciertos casos, incluso otros datos relacionados con la identidad (como el ID de Google).[2017] A veces las cámaras digitales utilizadas para producir imágenes de pornografía infantil contienen información geográfica en el fichero que permite a los investigadores determinar el lugar en que se tomó la fotografía, si esas imágenes se recogen en un servidor.[2018] En ocasiones se puede rastrear a las personas sospechosas que descargan contenidos ilegales de las redes con compartición de ficheros a partir del ID único que se genera al instalar el software de compartición de ficheros.[2019] Y la falsificación de un documento electrónico podría generar metadatos que permiten al autor original del documento probar la manipulación.[2020]

Otro aspecto que con frecuencia se menciona como una ventaja es la neutralidad y fiabilidad de la evidencia digital.[2021] En comparación con otras categorías de evidencia tales como las declaraciones de testigos, sin duda la evidencia digital es menos vulnerable a influencias que puedan afectar su preservación.[2022]

6.3.5 Dificultades

En los albores de la tecnología informática, la capacidad de las autoridades encargadas de hacer cumplir la ley para llevar a cabo investigaciones con datos digitales se veía limitada por la falta de competencia forense y equipos forenses aplicados a la informática.[2023] La importancia cada vez mayor de la evidencia digital ha dado lugar a un número creciente de laboratorios de informática forense. Sin embargo, aunque los aspectos logísticos de la cuestión pueden resolverse fácilmente, se sigue tropezando con dificultades.

La razón subyacente de estas dificultades es el hecho de que, pese a las numerosas similitudes entre la evidencia digital y otras categorías de evidencia, también existen grandes diferencias. Algunos de los

principios generales[2024], como el requisito de que la evidencia sea auténtica, completa, fiable[2025] y exacta, y que los procedimientos para obtener la evidencia estén en consonancia con los requisitos jurídicos, siguen estando vigentes.[2026] No obstante, junto con las similitudes, hay cierto número de aspectos que pueden conferirle a la evidencia digital un carácter único y por lo tanto merecen que se les preste especial atención a la hora de considerar la evidencia digital en una investigación penal.

Necesidad de formación e investigaciones científicas

La evidencia digital es una categoría de evidencia relativamente nueva y una esfera en rápido desarrollo. Y pese al marco temporal limitado de que se dispone para investigaciones científicas básicas, actualmente es preciso basar los procedimientos de búsqueda, obtención y análisis de evidencia digital en principios fiables desde el punto de vista científico.[2027] Pese a las abundantes investigaciones ya realizadas, existen varios ámbitos a los que los científicos deberían prestar atención. Por consiguiente, es importante proseguir las investigaciones científicas en ámbitos polémicos tales como la fiabilidad de la evidencia en general[2028] o la cuantificación de las posibles tasas de error[2029]. Los efectos de la evolución constante no se limitan a la necesidad de proseguir las investigaciones científicas; puesto que los progresos pueden plantear nuevas dificultades para el examen forense,[2030] es preciso impartir formación a expertos de manera constante.

Necesidad de normas jurídicas vinculantes

Aunque la informática y las tecnologías de red se utilizan a escala mundial, y las dificultades que plantea la admisibilidad de la evidencia digital en los tribunales son –a pesar de los diferentes sistemas jurídicos- similares, aún no se han establecido de manera generalizada unas normas jurídicas vinculantes sobre la evidencia digital.[2031] Hasta la fecha sólo algunos países han comenzado a actualizar su legislación pertinente para permitir que los tribunales consideren directamente evidencias digitales.[2032] En lo que respecta al derecho penal sustantivo y los instrumentos de procedimiento en la lucha contra el ciberdelito, la esfera de la evidencia digital también adolece de falta de armonización de las normas jurídicas a escala mundial.

Aspectos cuantitativos

Según se indicó anteriormente, los bajos costes[2033] en comparación con el almacenamiento físico de documentos está generando un número cada vez mayor de documentos digitales.[2034] Pese a la disponibilidad de herramientas para automatizar los procesos de búsqueda[2035], la identificación de la evidencia digital pertinente en un dispositivo de almacenamiento que puede transportar millones de documentos constituye un desafío logístico para los investigadores.[2036]

Dependencia de las declaraciones de expertos

Para analizar y evaluar la evidencia digital se necesitan aptitudes especiales y el conocimiento de técnicas que no están forzosamente incluidas en los programas educativos de los jueces, fiscales y abogados. Por consiguiente, éstos dependen cada vez más del apoyo de expertos para la recuperación de evidencias digitales.[2037] Esta situación aunque no es muy distinta de la de otras técnicas de investigación sofisticadas, tales como la del establecimiento de secuencias de ADN, pone de relieve la necesidad de examinar las consecuencias de esa dependencia. Para evitar una influencia negativa, se alienta a los tribunales a poner en tela de juicio la fiabilidad de la evidencia y exigir que se califique el grado de incertidumbre.[2038]

Fragilidad de la evidencia digital

Los datos digitales son muy frágiles y se pueden borrar[2039] o modificar[2040] tan fácilmente, que los expertos consideran este hecho un motivo de alarma.[2041] Al igual que otras categorías de evidencia, los datos digitales presentan cierto grado de incertidumbre.[2042] Para evitar un efecto negativo en la fiabilidad, a menudo la compilación de evidencia digital está sujeta a ciertos requisitos técnicos. Al apagar un sistema informático, por ejemplo, se perderá toda la memoria almacenada en el sistema RAM[2043], a menos que se tomen medidas técnicas especiales para evitarlo.[2044] En caso de que los datos estén almacenados en una memoria temporal, la técnica para compilar la evidencia puede ser diferente de la que se utiliza para compilar la evidencia digital tradicional.[2045] Este método sofisticado puede ser necesario, por ejemplo, si el sospechoso

utiliza tecnología de encripción y los investigadores desean examinar si la información almacenada en la memoria RAM puede facilitarles el acceso a la información encriptada.[2046]

El delincuente puede introducir modificaciones intencionalmente, o bien éstas pueden ser introducidas por los investigadores accidentalmente. En el peor de los casos, una pérdida o modificación de los datos puede dar lugar a una condena equivocada.[2047]

Como consecuencia de esa fragilidad, uno de los principios más fundamentales de la técnica forense aplicada a la informática es la necesidad de mantener la integridad de la evidencia digital.[2048] En este contexto puede definirse como integridad la propiedad por la cual los datos digitales no han sido alterados de forma no autorizada durante el tiempo en el que fueron creados, transmitidos o almacenados por una fuente autorizada.[2049] La protección de la integridad es necesaria para garantizar la fiabilidad y la exactitud.[2050] La manipulación de evidencias de este tipo exige normas y procedimientos con miras a mantener un sistema de calidad efectivo. Esto incluye aspectos generales tales como registros de casos, el empleo de tecnologías y procedimientos aceptados de forma generalizada y la intervención de expertos calificados únicamente[2051], así como la aplicación de métodos específicos tales como la suma de comprobación, el algoritmo de control ("hash algorithm") y las firmas digitales.[2052] Los métodos requeridos son costosos y no pueden excluir completamente los riesgos de alteración.[2053]

Volumen limitado de datos registrados

A muchos usuarios de Internet les sorprendería saber la cantidad de información sobre sus actividades que se almacena. El usuario medio podría no ser consciente de que, cuando accede a Internet o realiza ciertas acciones específicas como utilizar un motor de búsqueda[2054], está dejando huellas. Esas huellas pueden ser una valiosa fuente de evidencia digital en las investigaciones de ciberdelitos. Sin embargo, no toda la información digital generada mientras se utiliza un ordenador queda almacenada. Muchas acciones y un gran volumen de información como las pulsaciones con ratón y los tecleados no se registran a menos que se instalen software de vigilancia especiales.[2055]

Capa de abstracción

Incluso si las actividades de un sospechoso crean evidencias digitales, dicha evidencia se separa en el tiempo de los eventos que registra y por lo tanto se trata más de un registro histórico que de una observación en directo.[2056] Por otro lado, la evidencia no está forzosamente personalizada. Por ejemplo, si un sospechoso se sirve de un café Internet público para acceder a pornografía infantil, las huellas que deja no contienen necesariamente información relacionada con su identidad. A menos que el sospechoso descargue al mismo tiempo su correo electrónico o utilice servicios que exijan registrarse, en cuyo caso se crea un enlace. Pero puesto que este no es forzosamente el caso, los expertos señalan que ello podría llevar a una capa de abstracción que podría inducir a errores.[2057]

Requisitos relacionados con la infraestructura

En el diseño de las salas de los tribunales se siguen las mismas pautas desde hace décadas, y en algunos países incluso siglos. Dejando de lado los aspectos relacionados con la seguridad (por ejemplo, instalación de detectores de metal y máquinas de rayos X) y la comodidad (por ejemplo, acondicionamiento de aire), para los procedimientos penales se pueden utilizar salas de tribunal que tal vez han sido diseñadas y equipadas hace cientos de años.[2058] La necesidad de considerar evidencias digitales plantea dificultades relacionadas con la capa de abstracción y el hecho de que esa evidencia no pueda presentarse sin instrumentos tales como pantallas e impresoras tiene repercusiones en el diseño de los tribunales.[2059] Es preciso instalar pantallas para garantizar que el juez, el fiscal, el abogado defensor, el acusado y por supuesto el jurado puedan seguir la presentación de evidencias. La instalación y el mantenimiento de esos equipos representa un coste apreciable para los sistemas judiciales.

Entorno técnico cambiante

Según se indicó anteriormente, la tecnología cambia sin cesar. Ello exige la revisión constante de los procedimientos y los equipos, así como de la formación conexa, para garantizar la adecuación y la eficacia

de las investigaciones.[2060] Puesto que se van renovando continuamente las versiones de los software y los sistemas operativos, también pueden cambiar las modalidades de almacenamiento de los datos pertinentes para las investigaciones. Algo similar ocurre en lo tocante a los hardware.[2061] En el pasado, los datos se almacenaban en disquetes; hoy en día los investigadores saben que la información puede almacenarse en un reproductor MP3 o en relojes dotados de un dispositivo de almacenamiento USB. El desafío no se limita únicamente a mantenerse al corriente de las últimas tendencias de la tecnología informática,[2062] sino que los expertos forenses también necesitan equipos para tener en cuenta tecnologías anticuadas, tales como los disquetes de 5,25 pulgadas. Además de los cambios del hardware, se debe tener acceso a ciertos software que ya no se fabrican: a menudo los ficheros producidos con software en desuso no pueden abrirse si no se dispone del software original.

También es necesario contemplar detenidamente los cambios fundamentales del comportamiento del usuario. La disponibilidad de acceso en banda ancha y de servidores de almacenamiento a distancia, por ejemplo, ha influido en la forma según la cual se almacena la información. Mientras que en el pasado los investigadores podían centrarse en los locales del sospechoso para buscar evidencias digitales, hoy deben tener en cuenta el hecho de que los ficheros podrían estar almacenados físicamente en el extranjero y que el sospechoso podría tener acceso a los mismos a distancia cuando lo estime conveniente.[2063] El uso cada vez más frecuente de almacenamiento en nube supone nuevas dificultades para los investigadores.[2064]

6.3.6 Equivalencias entre la evidencia digital y la evidencia tradicional

Las investigaciones realizadas en Europa en 2005/2006 pusieron de relieve varios campos de equivalencia entre la evidencia digital y la tradicional en los 16 países objeto del análisis.[2065] La equivalencia más común es entre los documentos electrónicos y los documentos en papel. Otras equivalencias frecuentes se encuentran entre el correo electrónico y el convencional, entre las firmas electrónicas y las escritas a mano, y entre las actas notariales electrónicas y las tradicionales.[2066]

6.3.7 Relaciones entre la evidencia digital y la evidencia tradicional

Por lo que se refiere a las relaciones entre la evidencia digital y la tradicional, se puede hacer una distinción entre dos procesos: la sustitución de la evidencia tradicional por la evidencia digital, y la introducción de evidencia digital como una fuente adicional que complementa a las formas tradicionales de evidencia tales como los documentos y los testigos.

Un ejemplo de evidencia digital como sustitución de la tradicional es el uso cada vez más frecuente de correo electrónico en vez de cartas.[2067] En los casos en los cuales no se envían cartas físicas, las investigaciones deben centrarse en la evidencia digital. Esto tiene consecuencias en los métodos disponibles para analizar y presentar la evidencia. En el pasado, cuando las cartas escritas a mano eran la forma dominante de comunicación no verbal, los análisis forenses se centraban en las investigaciones de la escritura manual.[2068] Ya en la época en la que se generalizaron las máquinas de escribir, los métodos empleados por los expertos forenses cambiaron, para pasar de la técnica forense aplicada a la escritura a mano al análisis de la máquina de escribir.[2069] Debido al uso cada vez más frecuente del correo electrónico a expensas del correo convencional, los investigadores se ven ahora obligados a aplicar técnicas forenses al correo electrónico[2070] en vez de al convencional.[2071] Aunque por un lado la consiguiente incapacidad para utilizar documentos físicos limita la posibilidad de investigaciones conexas, por otro lado los investigadores actualmente pueden utilizar herramientas para automatizar las investigaciones sobre correo electrónico.[2072]

Aunque es probable que en la mayoría de los casos en los que intervienen comunicaciones electrónicas se ponga énfasis en la evidencia digital[2073], otras categorías de evidencia pueden seguir desempeñando una importante función para identificar al delincuente. Esto es especialmente pertinente por cuanto no todas las operaciones informáticas dejan huellas digitales y no siempre puede establecerse un vínculo entre las huellas dejadas y el sospechoso.[2074] Si se utilizan terminales Internet públicos para descargar imágenes de pornografía infantil es posible que no se establezca un nexo entre el proceso de descarga y una persona identificable, si esta última no se registró[2075] o dejó alguna información personal; pero de estar disponibles, la grabación en una cámara de vigilancia vídeo o las huellas dactilares en el teclado pueden resultar útiles. Inversamente, en los delitos tradicionales en los cuales las huellas dactilares, las trazas de ADN y las

declaraciones de testigos desempeñan un papel dominante, la evidencia digital puede ser una fuente de evidencia adicional muy útil. La información sobre la ubicación del teléfono celular del sospechoso puede permitir a las autoridades de policía determinar su emplazamiento[2076], y unas consultas sospechosas en el motor de búsqueda pueden conducir a la localización de una víctima perdida.[2077] En lo que respecta a los delitos que incluyen transacciones financieras (como el intercambio comercial de pornografía infantil[2078]), las investigaciones también pueden incluir registros mantenidos por organizaciones financieras con miras a identificar al delincuente. En 2007, durante una investigación mundial sobre pornografía infantil, se identificaron sospechosos sobre la base de registros de transacciones financieras relacionadas con la compra de materiales de pornografía infantil.[2079]

6.3.8 Admisibilidad de la evidencia digital

En la esfera de la evidencia digital hay dos grandes temas de debate: el proceso de compilación de la evidencia, y su admisibilidad en los tribunales. Los requisitos específicos inherentes a la compilación de la evidencia digital se examinarán más detenidamente en el Capítulo que versa sobre el derecho procesal. En lo que hace a la admisibilidad de la evidencia digital, a pesar de sus diferencias en comparación con la evidencia tradicional, los principios fundamentales son los mismos. No obstante, hacer una reseña de esos principios es muy complicado, puesto que no sólo hay una carencia de acuerdos internacionales jurídicamente vinculantes, sino que también existen diferencias sustanciales en el enfoque dogmático con el que se aborda la evidencia digital. Algunos países le confieren a los jueces amplia discreción para admitir o rechazar dicha evidencia, mientras que otros han comenzado a establecer un marco jurídico para contemplar la admisibilidad de la evidencia en los tribunales.[2080]

Legitimidad

Uno de los requisitos más fundamentales para la admisibilidad tanto de la evidencia tradicional[2081] como de la digital es su legitimidad.[2082] Este principio exige que la evidencia digital haya sido compilada, analizada, preservada y, finalmente, presentada ante el tribunal, en conformidad con los procedimientos vigentes y sin violar los derechos fundamentales del sospechoso.[2083] Tanto los requisitos relativos a la compilación, el análisis, la preservación y por último la presentación de la evidencia en los tribunales, como las consecuencias de una violación de los derechos del sospechoso, varían de un país a otro. Los principios y normas que podrían violarse van desde los derechos fundamentales de un sospechoso, tales como el derecho a la privacidad[2084], hasta la falta de respeto de los requisitos de procedimiento. Puesto que a menudo la legislación es insuficiente, a menudo se aplican a la evidencia digital los principios generales de la evidencia.[2085]

Normalmente los principios en los que debe basarse la compilación de la evidencia digital están consignados en el derecho procesal penal. En la mayoría de los países, para interceptar datos, por ejemplo, se requiere una orden del tribunal, y para ampliar el alcance de una búsqueda con el fin de incluir los dispositivos de almacenamiento a distancia es necesario que éstos estén situados en el mismo país. Si se procede a una intercepción sin una orden de tribunal, se estarán infringiendo los procedimientos adecuados y por consiguiente la investigación podría estar violando los derechos del sospechoso. Los requisitos para la preservación de la evidencia están definidos con menor frecuencia en la legislación.[2086] Sin embargo, el principio fundamental de que es necesario proteger la integridad de la evidencia digital es sin duda una directriz.[2087] Los investigadores deben asegurarse de que la evidencia no se altera de ninguna manera no autorizada a partir del momento en el que una fuente autorizada la crea, transmite o almacena.[2088] La protección de la integridad es necesaria para garantizar la fiabilidad y la exactitud, así como para observar el principio de legitimidad.[2089] En la legislación rara vez se definen los procedimientos para la presentación de evidencias ante el tribunal.

Según se indicó anteriormente, no sólo los requisitos, sino también las consecuencias de una violación de los procedimientos y de los derechos del sospechoso, varían considerablemente.[2090] Algunos países consideran que la evidencia es inadmisible únicamente si ésta ha sido compilada de una manera que viola gravemente los derechos del sospechoso (y no si se violan solamente los procedimientos oficiales), mientras que otros –en particular los partidarios de la doctrina del fruto del árbol envenenado– aplican otras normas para determinar la admisibilidad.[2091]

Regla de la mejor evidencia

En las jurisdicciones de derecho común la regla de la mejor evidencia es muy importante.[2092] Hay algunas referencias, sobre todo en casos antiguos, a una "regla de la mejor evidencia" que, en el marco del derecho común, estipula que sólo se considera admisible la mejor evidencia disponible de un hecho en cuestión. Sin embargo, aunque en una época esta regla pudo haber gozado de cierta categoría, actualmente tiene muy poca autoridad y hay quienes se han manifestado abiertamente a favor de su supresión.[2093]

Al parecer en la actualidad la regla general es considerar que el hecho de que una pieza de evidencia sea o no la mejor evidencia disponible sólo incide en el peso de la misma, no en su admisibilidad. [2094] Estrechamente relacionada con la regla de la mejor evidencia, la "regla de la evidencia primaria" anteriormente disponía que, cuando se trataba de evidencia documental, para probar el contenido y la autenticidad sólo podía admitirse el documento original o una copia "registrada" de ese documento. Ahora bien, los tribunales finalmente han desechado esta antigua regla, y cualquier posible vestigio remanente de la misma está limitado por ley en los procedimientos penales (que actualmente en general permiten utilizar copias autentificadas).[2095]

No caben dudas sobre la lógica de exigir que se presente un documento original, cuando se dispone del mismo, en vez de fiarse de copias posiblemente insatisfactorias, o en declaraciones de testigos[2096], aunque gracias a las técnicas modernas las objeciones a la primera alternativa resultan banales. A falta de la mejor evidencia o de la evidencia primaria de un documento, el tribunal aceptará la evidencia secundaria. Ello indica que existe otra evidencia mejor. Actualmente la autenticidad de los documentos públicos y jurídicos se demuestra con copias, sin tener en cuenta la ausencia de los originales, y una declaración contenida en un documento puede demostrarse presentando una copia autentificada del mismo. [2097] El principio subyacente es que se reducen los riesgos de transcripciones erróneas, declaraciones testimoniales equívocas del contenido del documento y manipulaciones no detectadas. [2098] La observancia de una interpretación estricta permite recurrir a la evidencia secundaria (en forma de una copia) cuando se ha perdido el original.

En lo que respecta a la evidencia digital, esto plantea algunas interrogantes, en la medida en la cual es necesario determinar qué es el original.[2099] Puesto que en general los datos digitales pueden copiarse sin pérdida de calidad, y dado que no siempre es posible presentar los datos originales ante el tribunal, la regla de la mejor evidencia parece ser incompatible con la evidencia digital. Pero los tribunales han comenzado a ampliar el alcance de la regla para contemplar nuevos adelantos, al aceptar una copia electrónica de igual modo que el documento original. [2100] Conforme a esta interpretación más amplia, la regla de la mejor evidencia no requiere en todos los casos un testimonio escrito u oral, sino que se utilice la mejor evidencia obtenible de su contenido.[2101] Por otro lado, la regla de la mejor evidencia ha sido consagrada en la mayor parte de los regímenes estatutarios en el campo del derecho común.[2102]

Regla contra los rumores

La regla contra los rumores es otro principio particularmente importante para los países regidos por el derecho común.[2103] La evidencia de oídas es la evidencia aportada por un testigo en el tribunal de una declaración hecha por otra persona fuera de la corte, cuando dicha evidencia tiende a demostrar la veracidad de la declaración. [2104] Con arreglo al derecho común en general la evidencia de oídas era inadmisible, hasta que la regla fue abolida en los procedimientos civiles en el Reino Unido a tenor de la Ley de Evidencia Civil de 1995, que prescribe la admisibilidad de la evidencia de oídas con sujeción a salvaguardias estatutarias, y mantiene algunas excepciones a la regla contra los rumores en el marco del derecho común.[2105]

De conformidad con la regla de derecho común contra los rumores, una afirmación distinta de la hecha por una persona al presentar evidencia oral en las actuaciones y presentada como una evidencia de los hechos afirmados es inadmisible[2106]. A los efectos de la regla, se entiende por declaración ajena al tribunal cualquier declaración distinta de la formulada por un testigo en el curso de su presentación de evidencias, y puede incluir, por ejemplo, una declaración formulada en anteriores actuaciones judiciales. Así, la declaración puede haber sido hecha sin o bajo juramento, oralmente o por escrito, o incluso por medio de gestos o señas, por una persona llamada o no como testigo en los procedimientos en cuestión.[2107] Además, la regla

apunta a permitir que se realice un examen cruzado de los testigos reales y a poner de relieve los puntos débiles de una declaración.[2108] En cambio, es necesario que un testigo con conocimiento personal lo demuestre directamente. No sólo el testimonio de un testigo, sino también las exposiciones, pueden contener rumores inadmisibles.[2109] Se han aducido algunas razones para justificar la regla de derecho común contra los rumores, como por ejemplo el peligro de una evidencia fabricada, en relación con la posible falta de credibilidad de la evidencia de oídas. Actualmente las reglas que gobiernan la admisibilidad de la evidencia de oídas se aplican si (y únicamente si) el tribunal estima que la finalidad, o una de las finalidades, de la persona que hace la declaración es lograr que otra persona crea el asunto, o que otra persona actúe o que una máquina funcione sobre la base del asunto tal como ha sido declarado.[2110]

Habida cuenta del hecho de que la finalidad de los datos compilados durante una investigación (como los ficheros de registro) es probar la veracidad del asunto afirmado en la propia evidencia digital, la aplicación estricta de la regla resulta problemática en una época en la cual con mucha frecuencia la evidencia digital es la categoría de evidencia más pertinente en las actuaciones judiciales, y algunos países regidos por el derecho común han comenzado a hacer excepciones estatutarias a la regla de los rumores.[2111] La evidencia producida por computadoras, cámaras u otras máquinas sin incorporación de ninguna declaración humana no puede ser evidencia de oídas. [2112] En el marco del derecho común o consuetudinario, se solía mantener que las imágenes visuales, aunque fueran producidas por manos humanas, no eran "declaraciones" de ningún hecho que representasen y por consiguiente no podían considerarse evidencia de oídas; hoy en día se han adoptado disposiciones para estipular expresamente lo contrario.[2113]

Cuando no existen excepciones estatutarias, la aplicación de la regla de la evidencia digital se pone en tela de juicio señalando que ésta se aplica únicamente a las declaraciones que contienen afirmaciones hechas por seres humanos. Sobre esta base, la información generada mecánicamente sin intervención humana no se consideraría evidencia de oídas[2114], a menos que el proceso de creación del software se utilice como un argumento para aplicar la regla incluso en esos casos.[2115]

Pertinencia/efectividad

La pertinencia y la efectividad son otros requisitos comunes para la admisibilidad de la evidencia digital.[2116] Si se tiene en cuenta la enorme cantidad de datos que se almacenan en un computador, incluso en uno privado, una minúscula proporción de la cual podría resultar pertinente para el caso, se advierte la importancia práctica de este criterio en las investigaciones sobre ciberdelitos. Su aplicación es importante tanto para restringir la compilación de evidencias, como las presentaciones ante el tribunal. A diferencia de la evidencia tradicional, que en el proceso de compilación permite sencillamente pasar por alto las piezas de evidencia irrelevantes, cuando se trata de evidencia digital el proceso de selección es más exigente[2117], dado que en el momento en el que se incauta el hardware informático, es prácticamente imposible determinar si los dispositivos de almacenamiento contienen o no información pertinente.

Transparencia

A diferencia de las operaciones tradicionales de búsqueda y captura, que se realizan abiertamente y por lo tanto se sabe que el sospechoso es consciente de que se está llevando a cabo una investigación, los mecanismos de investigación sofisticados tales como la intercepción de las comunicaciones en tiempo real no dan lugar a ese tipo de revelaciones. Independientemente de las capacidades técnicas, no todos los países permiten a las autoridades policiales llevar a cabo operaciones encubiertas, o por lo menos exigen que después se le informe al sospechoso. La transparencia durante todo el proceso de compilación, procesamiento y utilización de evidencias en el tribunal le brinda al sospechoso la posibilidad de poner en tela de juicio la legitimidad y la pertinencia de las evidencias recogidas.

6.3.9 Marco jurídico

Aunque hoy en día un gran número de países ha promulgado disposiciones de derecho penal sustantivo sobre las formas más comunes de delitos informáticos, la situación en lo que respecta a la evidencia digital es diferente. Hasta la fecha sólo unos pocos países han abordado aspectos concretos de la evidencia digital y, además, hacen falta normas jurídicamente vinculantes a escala internacional.[2118]

Ley modelo de la Commonwealth sobre evidencia electrónica (2002)

A tenor de la Law Ministers of Small Commonwealth Jurisdictions promulgada en 2000, se decidió crear un grupo de trabajo con el cometido de elaborar una legislación modelo sobre evidencia electrónica. La principal conclusión del análisis legislativo comparativo realizado por el grupo fue que, en lo tocante a la admisibilidad de la evidencia digital, reviste mayor importancia la fiabilidad del sistema por el cual se crea esa evidencia digital que el documento propiamente dicho. En la Ley modelo de 2002[2119], que estaba basada en la legislación de Singapur[2120] y Canadá[2121], se deja constancia de esa conclusión y se abarcan los aspectos más pertinentes de la evidencia digital en relación con los países regidos por el derecho común, tales como la aplicación de la regla de la mejor evidencia[2122] y la integridad de la evidencia digital.

> ***Admisibilidad general***
>
> *3. Las reglas de evidencia no contienen ninguna disposición que niegue la admisibilidad de un registro electrónico como evidencia únicamente porque se trata de un registro electrónico.*

La Sección 3 contiene un elemento común de los marcos jurídicos que apuntan a reglamentar los aspectos de la evidencia digital que pueden encontrarse en forma similar, por ejemplo en el Artículo 5 de la Directiva de la UE sobre firmas digitales de 1999.[2123] La disposición está destinada a velar por que la evidencia digital no sea inadmisible *per se*. A este respecto, la Sección 3 proporciona las bases para la utilización de la evidencia digital en las actuaciones de los tribunales. Sin embargo, la admisibilidad de la evidencia no está garantizada sólo porque es evidencia digital; antes bien, es necesario que esta evidencia satisfaga las normas de evidencia ordinarias. Si la evidencia está formada por materiales de oídas, no se convierte en admisible a causa de la Sección 3.

> ***Alcance de la Ley***
>
> *4. (1) Esta ley no modifica ninguna norma estatutaria de derecho común relativa a la admisibilidad de los registros, con excepción de las reglas relativas a la autentificación y la mejor evidencia.*
> *(2) Un tribunal puede tener en cuenta la evidencia alegada en el marco de esta Ley en aplicación de cualquier norma estatutaria o de derecho común relativa a la admisibilidad de los registros.*

> ***Aplicación de la Regla de la mejor evidencia***
>
> *6. (1) En cualquier procedimiento judicial, con sujeción al apartado (b), cuando la regla de la mejor evidencia es aplicable con respecto a un registro electrónico, la regla se cumple en prueba de la integridad del sistema de registros electrónicos en o mediante el cual se registraron o almacenaron los datos.*
> *(2) En cualquier procedimiento judicial, cuando se ha utilizado manifiesta o firmemente un registro electrónico en forma impresa o se ha actuado o confiado en éste como el registro de la información registrada o almacenada en la impresión, a los efectos de la regla de la mejor evidencia dicha impresión es el registro.*

Según se indicó anteriormente, algunos de los criterios para la admisibilidad de evidencia digital podrían estar en pugna con los principios tradicionales relacionados con la admisibilidad de la evidencia. Esto es particularmente pertinente respecto de la regla de la mejor evidencia, que reviste gran importancia para los países regidos por el derecho consuetudinario.[2124] La finalidad de la regla de la mejor evidencia es reducir al mínimo los riesgos de transcripciones erróneas, testimonios equívocos sobre el contenido del documento y manipulaciones no detectadas.[2125] La admisibilidad de la evidencia exige que la evidencia documental sea la mejor evidencia disponible para la parte. La cuestión de si eso excluye o no a la evidencia digital *per se* es un motivo de controversia.[2126] Las Secciones 4 y 6 de la Ley modelo de la Commonwealth sobre evidencia electrónica son ejemplos de una exención estatutaria. En este contexto, la Sección 4 aclara ante todo que la Ley modelo modifica exclusivamente los principios de autentificación y de mejor evidencia. Tras esta aclaración de carácter general, la Sección 6 modifica la regla de la mejor evidencia para garantizar que la evidencia digital no sea inadmisible *per se*. Sobre la base de la Sección 6, la evidencia digital no es

inadmisible debido a la regla de la mejor evidencia, a condición de que pueda demostrarse la integridad del sistema que creó los datos.

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática (2002)

En 2002 se presentó el proyecto de Ley modelo de la Commonwealth.[2127] Además de las disposiciones de derecho penal sustantivo y los instrumentos de procedimiento, esta ley contiene una disposición específica sobre la evidencia digital.

> ***Evidencia***
> *20 En los procedimientos penales por un delito cometido contra una ley de (país que la promulgó), el hecho de que:*
> *(a) se alegue que se ha cometido un delito de interferencia con un sistema informático, y*
> *(b) se haya generado evidencia a partir de ese sistema informático; no impide por sí mismo que la evidencia sea admitida.*

El enfoque es similar al del Artículo 3 de la Ley modelo de la Commonwealth sobre evidencia electrónica de 2002, de naturaleza más específica.

6.4 Jurisdicción

Bibliografía (seleccionada): *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004. *Hirst,* Jurisdiction and the Ambit of the Criminal Law, 2003; *Inazumi,* Universal Jurisdiction in Modern International Law, 2005; *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf; *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 69 et seq; *Sachdeva*, International Jurisdiction in Cyberspace: A Comparative Perspective, Computer and Telecommunications Law Review, 2007,, page 245 et seq; *Scassa/Currie*, New First Principles? Assessing the Internet's Challenges to Jurisdiction, Georgetown Journal of International Law, Vol. 42, 2001, page 117 et seq, available at: http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF; United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm; *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf; *Van Dervort*, International Law and Organizations: An Introduction, 1998; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

6.4.1 Introducción

La ciberdelincuencia suele ser un fenómeno transnacional que afecta a diferentes jurisdicciones. No es raro que varios países se vean afectados. Es posible que el delincuente actúe desde el país A, utilice los servicios de Internet del país B y que la víctima se encuentre en el país C. Esto supone un problema para la aplicación del derecho penal[2128] y plantea dudas acerca de qué países tienen la jurisdicción, qué país ha de realizar la investigación y cómo resolver las controversias. Si el caso expuesto ya parece bastante complicado, cabe tener en cuenta que si en el delito participan, por ejemplo, los servicios de computación en nube, hay todavía más jurisdicciones que pueden entrar en juego.[2129]

El término "jurisdicción" se emplea para diversos aspectos jurídicos.[2130] De acuerdo con los principios del derecho público internacional, "jurisdicción" es la autoridad de un Estado soberano para regular determinadas conductas.[2131] Es, por ende, uno de los elementos de la soberanía nacional.[2132] Sin embargo, en el contexto de la investigación sobre ciberdelincuencia, "jurisdicción" se refiere a la autoridad de un

Estado para aplicar su legislación nacional.[2133] En general, fuerzas del orden sólo podrán realizar una investigación, si el país tiene la jurisdicción.

6.4.2 Distintos principios de jurisdicción

Es posible establecer una diferencia entre los diversos principios de jurisdicción.

6.4.3 Principio de territorialidad/Principio de territorialidad objetiva

El principio más fundamental y más común de la jurisdicción es el principio de territorialidad.[2134] Se aplica cuando un delito – independientemente de la nacionalidad del delincuente o de la víctima – se comete en el territorio de un Estado soberano.[2135] La importancia de este principio reside en que esa jurisdicción en general sólo tiene sentido si puede aplicarse y la aplicación de la ley exige un control (generalmente limitado al territorio). En el Artículo 22(1)(a) del Convenio del Consejo de Europa sobre Ciberdelincuencia se codifican los principios de territorialidad aplicados a la informática.

Artículo 22** – **Jurisdicción
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los Artículos 2 a 11 del presente Convenio, siempre que se haya cometido:
a. en su territorio; o
b. a bordo de un buque que enarbole pabellón de dicha Parte; o
c. a bordo de una aeronave matriculada según las leyes de dicha Parte; o
d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.
[…]

Esta disposición se aplica a la informática pues sólo se refiere a los delitos enumerados en los Artículos 2 a 11 del Convenio sobre la Ciberdelincuencia.

Sin embargo, su aplicación a los ciberdelitos se está realizando con dificultades. Es seguro que se ha cometido un delito si el delincuente y la víctima estaban físicamente presentes en el país cuando el delincuente accedió ilegalmente al sistema informático de la víctima, pero ¿se puede considerar que el delito se cometió en el territorio de un Estado, si el delincuente actuó desde el extranjero al acceder al sistema informático de la víctima, que sí se encontraba en el país en cuestión?

Tales casos tienen un componente extraterritorial. No obstante, el Tribunal Internacional de Justicia determinó en el caso "·Lotus" que, aun cuando los países sólo aplican la jurisdicción en función de la territorialidad, se sigue pudiendo considerar que una conducta extraterritorial se ha cometido dentro del territorio, si uno de los elementos constituyentes del delito (en particular su consecuencia) tiene lugar en dicho país.[2136] Esta doctrina, también denominada "principio de territorialidad objetiva"[2137] es muy pertinente para la ciberdelincuencia.[2138] Si tenemos en cuenta que un software maligno enviado por un delincuente puede afectar a los sistemas informáticos de diversos países, queda patente que una definición tan amplia de la territorialidad puede fácilmente causar conflictos de jurisdicción.[2139] El riesgo de que surjan conflictos de este tipo aumenta aún más si el principio de territorialidad se aplica a los casos en que ni el delincuente ni la víctima se encuentran en el país, sino que sólo la infraestructura de ese país se empleó para cometer el delito – por ejemplo, si se envía un correo-e con contenido ilegal utilizando un proveedor de correo-e de un país o si se almacena en el servidor de un proveedor de servicio del país un sitio web con contenido ilegal.

Podemos encontrar una codificación de tan amplio enfoque en la Sección 11(3)(b) de la Ley de Utilización Indebida de la Informática de 2007 de Singapur.

Alcance territorial de los delitos contemplados por esta Ley
[...]
11. —(1) De acuerdo con la subsección (2), las disposiciones de la presente Ley se aplicarán a cualquier persona, cualquiera que sea su nacionalidad o ciudadanía, dentro o fuera de Singapur.
(2) Cuando una persona fuera de Singapur cometa un delito contemplado por la presente Ley, podrá considerarse que el delito se ha cometido dentro de Singapur.
(3) A los efectos de esta sección, la presente Ley se aplicará cuando, en el contexto del delito —
(a) el acusado se encontraba en Singapur en el momento de la comisión; o
(b) el computador, el programa o los datos se encontraban en Singapur en el momento de la comisión.

Este amplio enfoque muy probablemente también permite la aplicabilidad de la legislación de Singapur a los datos que simplemente transitan por los sistemas informáticos de Singapur.[2140]

6.4.4 Principio del pabellón

El principio del pabellón está estrechamente relacionado al principio de territorialidad, pero amplia la aplicación de las leyes nacionales a las aeronaves y los buques. La disponibilidad de acceso a Internet en los transportes marinos y aéreos,[2141] plantea problemas para la aplicación del derecho penal cuando el delincuente, o la víctima o el sistema informático afectado no está ubicado en el territorio, sino fuera de los límites territoriales del país a bordo de un buque o una aeronave.

Un ejemplo de regulación de estos casos se encuentra en los párrafos 1b y 1c del Artículo 22 del Convenio del Consejo de Europa sobre Ciberdelincuencia.

Artículo 22 – Jurisdicción
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los Artículos 2 a 11 del presente Convenio, siempre que se haya cometido:
a. en su territorio; o
b. a bordo de un buque que enarbole pabellón de dicha Parte; o
c. a bordo de una aeronave matriculada según las leyes de dicha Parte; o
d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.
[…]

6.4.5 Doctrina de los efectos/Principio de protección

La doctrina de los efectos atañe a la determinación de la jurisdicción para un delito cometido por una persona extranjera fuera del territorio nacional sin que haya elementos de conducta en el territorio, pero que causa un efecto sustancial en el territorio.[2142] Estrechamente relacionado está el principio de protección, que establece la jurisdicción en casos semejantes, cuando hay implicado un interés nacional fundamental. Dada la ausencia del delincuente, de la víctima y de la infraestructura utilizada, los vínculos con el país son débiles, por lo que la aplicación de este principio es objeto de controversia.[2143]

6.4.6 Principio de nacionalidad activa

El principio de nacionalidad se refiere a la jurisdicción que se ejerce sobre las actividades de las personas con la nacionalidad del país de que se trate en el extranjero.[2144] Está relacionado con la autoridad del Estado para regular el comportamiento de sus ciudadanos no sólo dentro de su territorio, sino también en el extranjero. Este principio es más común en los países que utilizan el derecho que en los que prevalece el derecho consuetudinario (common law).[2145] Por consiguiente, los países que se rigen por el derecho consuetudinario tienden a compensar la falta de jurisdicción basada en el principio de nacionalidad con una interpretación más amplia del principio de territorialidad.

Dado que los delitos relacionados con Internet pueden cometerse sin salir del país, el principio es menos pertinente para la ciberdelincuencia. Sin embargo, puede revestir una gran importancia en el contexto de la producción de pornografía infantil con fines de distribución por redes informáticas.[2146]

El principio de nacionalidad se regula, por ejemplo, en el párrafo 1.d del Artículo 22 del Convenio del Consejo de Europa sobre Ciberdelincuencia.

Artículo 22 – Jurisdicción
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los Artículos 2 a 11 del presente Convenio, siempre que se haya cometido:
a. en su territorio; o
b. a bordo de un buque que enarbole pabellón de dicha Parte; o
c. a bordo de una aeronave matriculada según las leyes de dicha Parte; o
d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.
[…]

6.4.7 Principio de nacionalidad pasiva

El principio de nacionalidad pasiva se refiere a la jurisdicción basada en la nacionalidad de la víctima. Dado que se solapa con el principio de territorialidad, sólo es pertinente si la persona se convierte en víctima fuera de su propio país. La aplicación de este principio es objeto de controversia[2147], en particular porque implica que el derecho de otro país no protege suficientemente a los extranjeros, pero ha ido ganando aceptación en las últimas décadas.[2148]

Podemos encontrar una codificación del principio de nacionalidad pasiva, aunque no aplicado específicamente a Internet, en la Sección 7 del Código Penal de Alemania.

Sección 7
Delitos cometidos en el extranjero – otros casos
(1) el Derecho penal alemán se aplicará a los delitos cometidos en el extranjero contra un ciudadano alemán, si al acto se considera delito penal en el lugar donde se ha cometido o si dicho lugar no está sujeto a ninguna jurisdicción penal.

6.4.8 Principio de universalidad

El principio de universalidad establece la jurisdicción en relación con delitos específicos en interés de la comunidad internacional.[2149] Este principio es particularmente importante en el caso de delitos graves, como los crímenes contra la humanidad y los crímenes de guerra.[2150] Sin embargo, en varios países que lo reconocen, este principio se ha desarrollado.[2151] Por consiguiente, en determinadas circunstancias este principio puede incluso aplicarse a la ciberdelincuencia.

Un ejemplo de disposición que puede aplicarse a los ciberdelitos se encuentra en la Sección 6(6) del Código Penal de Alemania.

Sección 6
Delitos cometidos en el extranjero contra intereses jurídicos bajo protección internacional
El derecho penal alemán se aplicará además, independientemente de cuál sea el lugar en que se han cometido, a los siguientes delitos cometidos en el extranjero:
1. (abolido) ;
2. delitos en que se haya utilizado la energía nuclear, los explosivos y la radiación, en virtud de la sección 307 y la sección 308(1) a (4), la sección 309(2) y la sección 310;
3. ataques al tráfico aéreo y marítimo (sección 316c);

> *4. tráfico de personas para su explotación sexual, su explotación laboral y complicidad en el tráfico de personas (secciones 232 a 233a);*
> *5. tráfico ilegal de drogas;*
> *6. distribución de pornografía, en virtud de las secciones 184a, 184b (1) a (3) y la sección 184c (1) a (3), además de la 1ª oración de la sección 184d;*
> *[...]*

De acuerdo con la Sección 6 (6), Alemania puede ejercer su jurisdicción en relación con los sitios web que ofrecen pornografía infantil para su descarga, incluso cuando el operador del sitio web no se encuentra en Alemania, los servidores no se encuentran en Alemania y ningún usuario de Internet alemán ha accedido al sitio web.

6.5 Derecho procesal

Bibliografía (seleccionada): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1; *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801; *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*; *Gercke/Tropina*, From Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf; *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal

of Law & Technology, Vol. 10, Nr. 3, 1997; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1.

6.5.1 Introducción

Según se explica en los puntos anteriores, la lucha contra la ciberdelincuencia exige que el derecho procesal contenga disposiciones fundamentales apropiadas[2152]. Al menos en los países en los que se aplica el derecho civil, las autoridades no pueden investigar delitos si no existen esas leyes, pero en su lucha contra la ciberdelincuencia, las autoridades no se limitan a las disposiciones fundamentales del derecho penal[2153]. Para llevar a cabo sus investigaciones necesitan instrumentos procesales, además de la capacitación y los equipos correspondientes, que les permitan adoptar las medidas necesarias para identificar al infractor y reunir las pruebas necesarias para el juicio[2154]. Estas medidas pueden ser las mismas que las adoptadas en otras investigaciones que no están relacionadas con la ciberdelincuencia, pero habida cuenta de que no es necesario que el infractor esté presente en el lugar del delito, o incluso cerca de él, es muy probable que las investigaciones se hayan de llevar a cabo de manera diferente a las tradicionales[2155].

La diversidad de las técnicas de investigación no sólo se debe al hecho de que el delincuente no se encuentra necesariamente en el lugar del delito. En la mayoría de los casos, la particularidad de las investigaciones de ciberdelitos es que las autoridades competentes deben afrontar simultáneamente varias de las dificultades mencionadas[2156]. Si el infractor se encuentra en otro país[2157], utiliza servicios que garantizan su anonimato y, además, utiliza varios terminales Internet públicos para cometer sus delitos el registro e incautación con medios tradicionales resultan harto difíciles. Para evitar malentendidos, se ha de señalar que esas investigaciones pueden ser tradicionales, pero también plantean dificultades que no se pueden resolver solamente de esa manera[2158].

Las autoridades de varios países ya disponen de instrumentos que les permiten investigar ciberdelitos y otros delitos tradicionales analizando datos informáticos[2159]. Al igual que el derecho penal sustantivo, el Convención sobre la Ciberdelincuencia del Consejo de Europa contiene varias disposiciones que reflejan normas mínimas generales aceptadas en lo que respecta a los instrumentos procesales necesarios para las investigaciones sobre los ciberdelitos[2160]. A continuación se estudiarán pues los instrumentos de este Convenio internacional y, además, se destacarán sistemas nacionales que van más allá de lo estipulado en el Convenio.

6.5.2 Investigaciones sobre equipos informáticos e Internet (Criminología informática)

El término criminología informática se emplea para describir la recopilación sistemática de datos y el análisis de tecnologías informáticas a fin de buscar pruebas digitales.[2161] Estos análisis suelen realizarse tras la comisión del delito.[2162] Es, por tanto, una parte fundamental de la delincuencia informática y de la investigación sobre ciberdelitos. Los investigadores de este tipo se enfrentan a diversos problemas que se describen más detalladamente en el Capítulo 3.

El grado de participación de los expertos en la criminología informática demuestra su importancia en el proceso de investigación. Además, el hecho de que el éxito de las investigaciones en Internet dependa de la disponibilidad de recursos criminológicos pone de relieve la necesidad de formación en este ámbito. Las investigaciones y acciones judiciales en materia de ciberdelincuencia sólo se pueden llevar a cabo de manera eficaz si los investigadores han recibido una formación en criminología informática o pueden consultar a expertos en la materia.

Definición

Existen varias definiciones de la "criminología informática"[2163]. Puede definirse como "examen de equipos y sistemas informáticos para obtener información en investigaciones penales o civiles"[2164]. Los delincuentes, tanto tradicionales como informáticos, suelen dejar rastros[2165]. La principal diferencia entre una investigación tradicional y la investigación de un ciberdelito es que para esta última se suele recurrir a

técnicas de investigación específicas para los datos, que pueden verse facilitadas por herramientas informáticas especializadas [2166]. Para realizar esos análisis, las autoridades necesitan instrumentos procesales apropiados y deben poder gestionar y analizar los datos pertinentes. Según cual sea la infracción y la tecnología informática empleada, los requisitos en lo que respecta a los instrumentos de investigación procesal y a los análisis criminológicos son diferentes[2167] y plantean dificultades particulares.[2168]

Fases de la investigación forense

En general es posible distinguir dos fases principales:[2169] la fase de investigación (identificación de las pruebas pertinentes,[2170] obtención y conservación de las pruebas,[2171] análisis de la tecnología informática y las pruebas digitales) y la presentación y utilización de las pruebas en el juicio. A fin de explicar las distintas actividades, a continuación se divide el modelo en cuatro fases.

Procedimientos de identificación de pruebas

El aumento de la capacidad de los discos duros [2172] y el coste cada vez menor [2173] que supone el almacenamiento de documentos digitales, en comparación con el almacenamiento de documentos físicos, está haciendo que el número de documentos digitales crezca constantemente.[2174] Habida cuenta de la necesidad de centrar las investigaciones en las pruebas pertinentes, para evitar la inadmisibilidad, se ha de prestar una atención particular a la identificación de las pruebas.[2175] Por consiguiente, los expertos forenses desempeñan un papel fundamental a la hora de elaborar estrategias de investigación y de selección de las pruebas pertinentes. Por ejemplo, pueden determinar la ubicación de las pruebas necesarias en grandes sistemas de almacenamiento, lo que permite a los investigadores limitar el ámbito de la investigación a las partes de la infraestructura informática que sean pertinentes y evitar la confiscación impropia y a gran escala de material informático. [2176] Este proceso de selección es importante, pues existen tipos de dispositivos de almacenamiento que pueden dificultar la identificación del emplazamiento donde se almacenan las pruebas pertinentes. [2177] Esto es aún más importante si el sospechoso no almacena la información localmente, sino que utiliza medios de almacenamiento a distancia. El acceso en banda ancha y los servidores de almacenamiento a distancia han influido en la manera de almacenar la información. Si el sospechoso almacena información en un servidor que se encuentra en otro país, ese simple hecho puede dificultar la obtención de las pruebas. En este caso, el análisis forense puede servir para determinar si se han utilizado servicios de almacenamiento a distancia. [2178] La identificación de la información digital pertinente no se limita a los archivos, también las bases de datos del software que utilizan los sistemas operativos para identificar rápidamente los ficheros pueden contener información interesante.[2179] Incluso los ficheros temporales generados por el sistema pueden contener pruebas procedentes para un juicio.[2180]

Otro ejemplo de identificación de pruebas es la participación de expertos forenses a la hora de definir los instrumentos procesales adecuados. En algunos países se permite a las fuerzas del orden llevar a cabo dos tipos de observación en tiempo real – la obtención de datos del tráfico en tiempo real y la intercepción de contenidos en tiempo real. En general, la intercepción de contenidos es más intrusiva que la obtención de datos de tráfico. Los expertos forenses pueden determinar si basta con la obtención de datos de tráfico para demostrar que se ha cometido un delito, ayudando así a los investigadores a equilibrar la necesidad de obtener las pruebas necesarias y la obligación de proteger los derechos del sospechoso escogiendo el instrumento menos intrusivo del abanico de opciones disponibles. Ambos ejemplos muestran que el trabajo de los investigadores forenses no se limita a los aspectos técnicos de la investigación, sino que comprende la responsabilidad de proteger los derechos fundamentales del sospechoso y al mismo tiempo evitar la obtención de pruebas inadmisibles.[2181]

Obtención y conservación de las pruebas

La obtención de pruebas digitales necesita conocimientos complejos, pues las técnicas utilizadas para obtener pruebas almacenadas en el disco duro de un computador doméstico y las que se emplean para interceptar un proceso de transmisión de datos son notablemente diferentes. En concreto, cuando se trata de delincuentes de alto nivel, los investigadores se ven a menudo confrontados con situaciones que pide una toma rápida de decisiones: por ejemplo si es necesario apagar o no un sistema informático activo y cómo aplicar tal procedimiento. Para no interferir con la integridad de las pruebas digitales pertinentes, un

medio habitual el sacar el enchufe, pues se detiene cualquier alteración de los ficheros.[2182] Sin embargo, una interrupción brutal de la alimentación puede activar un proceso de encriptación[2183] que impida acceder a los datos almacenados.[2184] Los equipos de intervención que se enfrentan los primeros a la obtención de pruebas digitales asumen una importante responsabilidad sobre todo el proceso de investigación, pues cualquier decisión errónea puede afectar en gran medida la capacidad para conservar las pruebas pertinentes.[2185] Si toman una decisión errónea sobre la conservación, puede que se pierdan rastros importantes.

Los expertos forenses han de asegurarse de que se identifican todas las pruebas necesarias[2186], lo que puede resultar difícil si los infractores ocultan ficheros en un dispositivo de almacén para evitar que las fuerzas del orden analicen el contenido del fichero. La investigación forense puede identificar los ficheros ocultos y hacer que sean accesibles.[2187] Los mismos procesos de recuperación se necesitan cuando la información digital se ha suprimido.[2188] Los ficheros que se suprimen simplemente mandándolos a una papelera virtual no necesariamente evitan que las fuerzas del orden puedan acceder a ellos, pues se pueden recuperar gracias a herramientas de software forense especiales.[2189] Sin embargo, si los infractores utilizan herramientas para garantizar que los ficheros se han suprimido con seguridad sobrescribiendo información, la recuperación suele ser imposible.[2190] La obtención de pruebas también puede resultar problemática si los delincuentes intentan impedir el acceso a la información pertinente utilizando tecnologías de encriptación, que cada vez son más frecuentes.[2191] Dado que así se impide que las fuerzas del orden puedan acceder y examinar la información encriptada, la utilización de tecnologías de encriptación supone un importante desafío para las fuerzas del orden.[2192] Los expertos forenses pueden intentar decriptar los ficheros encriptados[2193], pero, de no ser posible, pueden ayudar a las fuerzas del orden elaborando estrategias para acceder a los ficheros encriptados, por ejemplo, utilizando un *keylogger*.[2194]

Dentro de la obtención de pruebas también se evalúan y utilizan nuevos instrumentos, como por ejemplo las nuevas herramientas forenses a distancia[2195], que permiten a los investigadores obtener a distancia pruebas en tiempo real[2196] o vigilar a distancia las actividades del sospechoso[2197] sin que éste sepa que se está investigando su sistema. Estas herramientas pueden participar en la elaboración de una estrategia para obtener pruebas digitales.

Comunicación con los proveedores de servicio

Los proveedores de servicios Internet (PSI) desempeñan un importante papel en muchas investigaciones sobre ciberdelincuencia, pues la mayoría de los usuarios recurren a sus servicios para acceder a Internet o a los sitios web de venta. El hecho de que algunos PSI dispongan de las capacidades técnicas para detector e impedir delitos y respaldar a las fuerzas del orden en sus investigaciones ha suscitado un intense debate sobre el papel de los PSI en las investigaciones sobre ciberdelitos. Las opiniones oscilan entre imponer obligatoriamente la utilización de tecnologías de prevención a solicitar la contribución voluntaria a las investigaciones.[2198] Los expertos forenses también pueden participar en la investigación preparando las solicitudes que se presentarán a los proveedores de servicio[2199] y ayudando a los investigadores a preparar los informes[2200] necesarios para demostrar la fiabilidad de las pruebas obtenidas. La cooperación entre fuerzas del orden y PSI en el marco de tales investigaciones exige que se respeten determinados procedimientos.[2201] Las Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet[2202] contienen una serie de procedimientos fundamentales, que abarcan aspectos tales como la facilitación de explicaciones y asistencia en cuanto a técnicas de investigación[2203] y establecimiento de prioridades,[2204] ámbitos en los que la ayuda de los expertos forenses puede resultar útil para mejorar la eficacia de los dichos procedimientos.

Una estrecha cooperación con los PSI es especialmente importante en la fase de identificación del sospechoso. Los sospechosos que cometen ciberdelitos dejan rastros.[2205] El análisis de los datos de tráfico, como el examen de los ficheros cronológicos que mantienen los PSI, puede llevar a los investigadores a la conexión empleada por el infractor para conectarse a Internet.[2206] Los infractores pueden intentar dificultar la investigación utilizando tecnologías de comunicación anónima[2207], pero incluso en ese caso no es imposible realizar la investigación si los investigadores y los PSI trabajan de consuno.[2208] Por ejemplo, se puede utilizar la herramienta forense CIPAV (Verificador informático y de dirección de protocolo Internet), como se hizo en Estados Unidos para identificar a un sospechoso que había estado utilizando servicios de

comunicación anónima.[2209] Otro campo en que los PSI y los investigadores pueden colaborar son los correos-e, que se han convertido en un medio muy popular de comunicación.[2210] Para evitar ser identificados, en ocasiones los infractores utilizan direcciones de correo electrónico gratuitas, donde pueden inscribirse con información personal falsa. Sin embargo, también en ese caso el examen de la información del encabezamiento[2211] y de los ficheros cronológicos del proveedor de correo-e puede en ocasiones dar pistas que lleven a la identificación del sospechoso.

La necesidad de cooperar y comunicar con los proveedores no se limita a los PSI. Dado que algunos delitos, como la *peska*[2212] y la distribución comercial de pornografía infantil conllevan transacciones financieras, una de las estrategias utilizadas para ofender a los delincuentes es obtener datos de las instituciones financieras participantes en las transacciones.[2213] Puede citarse, por ejemplo, una investigación realizada en Alemania, donde los delincuentes descargaron pornografía infantil a partir de un sitio web comercial y fueron identificados gracias a los registros de las tarjetas de crédito. A petición de los investigadores, las empresas de tarjetas de crédito analizaron sus registros de clientes para identificar a los que utilizaron su tarjeta para adquirir pornografía infantil en ese sitio web concreto.[2214] Las investigaciones resultan más difíciles cuando se emplean métodos de pago anónimo.[2215]

Examen de las TIC

El primer paso en muchas investigaciones consiste en demostrar que el sospechoso tenía la capacidad de cometer el delito. Una de las principales tareas de los expertos forenses es el examen del hardware y el software confiscados.[2216] Los examines pueden realizarse *in situ* durante el registro de los locales del cliente[2217] o después de confiscar los equipos. Para poder llevar a cabo tal investigación, los equipos de intervención suelen requisar todos los dispositivos de almacén pertinentes, que pueden albergar cada uno de ellos millones de ficheros, lo que suele causar problemas logísticos.[2218] Como ya se ha dicho anteriormente, los principios de pertinencia y eficacia son fundamentales para la admisibilidad de las pruebas digitales.[2219] Por consiguiente, la identificación y selección del hardware pertinente es una de las tareas más importantes de la investigación.[2220]

El análisis del hardware disponible puede, por ejemplo, demostrar que el computador del sospechoso tenía capacidad para realizar un ataque de denegación de servicio[2221] o está equipado con un chip que impide manipular el sistema operativo. El análisis del hardware puede ser también necesario a la hora de identificar a un sospechoso. Algunos sistemas operativos analizan la configuración del hardware de un sistema informático durante el proceso de instalación y los comunica al fabricante del software. Si puede encontrarse el perfil del hardware del sospechoso a partir de la información facilitada por la empresa de software, el análisis del hardware puede resultar de utilidad para verificar que se trata realmente del sistema informático confiscado. El análisis del hardware no necesariamente se centra en los componentes físicos de un sistema informático. La mayoría de sistemas operativos conservan registros del hardware conectado a un sistema informático en cada operación.[2222] A partir de las entradas de esos ficheros cronológicos, como el Windows Registry, los expertos forenses pueden incluso identificar el hardware utilizado en el pasado, pero que no se encontró durante el registro y la confiscación de equipos.

Además del análisis de hardware, el análisis de software es una tarea habitual de las investigaciones sobre ciberdelitos. Los sistemas informáticos necesitan software para funcionar. Además de los sistemas operativos, es posible instalar otras herramientas de software para dirigir el funcionamiento de los sistemas informáticos en función de las necesidades del usuario. Los expertos forenses pueden analizar el funcionamiento de las herramientas de software a fin de demostrar que el sospechoso tuvo la capacidad de cometer un delito específico. Pueden, por ejemplo, indagar si el sistema informático del sospechoso contiene un software que permite encriptar datos en imágenes (esteganografía[2223]). El inventario de las herramientas de software instaladas en el computador del sospechoso puede también contribuir a orientar las investigaciones. Si, por ejemplo, los investigadores encuentran software de encriptación o herramientas para suprimir ficheros de manera definitiva, pueden buscar específicamente las pruebas encriptadas o suprimidas.[2224] Los investigadores pueden también determinar las funciones de los virus informáticos y otro tipo de software maligno y reconstruir los procesos operativos del software.[2225] En algunos casos, cuando se encuentra contenido ilegal en los computadores de los sospechosos, éstos afirman que ellos no han descargado los ficheros y que debe ser obra de un virus informático. En esos casos, la investigación forense

puede intentar identificar el software maligno instalado en el sistema informático y determinar su funcionamiento. Investigaciones de este tipo pueden efectuarse si se sospecha que un sistema informático puede haber sido infectado y transformado en parte de una red robot.[2226] Además, el análisis del software puede ser importante para determinar si éste se utiliza únicamente para cometer delitos o si, además de actividades ilegales, también se puede hacer de él un uso legítimo (doble uso). Este punto es importante, pues algunos países sólo penalizan la fabricación de dispositivos ilegales, si están diseñados principal o únicamente para cometer delitos.[2227]

Las investigaciones sobre datos no se limitan a las funciones de software, sino que pueden incluir también el análisis de ficheros no ejecutables, como los documentos en formato pdf y los ficheros de video. Estas investigaciones van del análisis del contenido de ficheros específicos a la búsqueda automática por palabras clave[2228] en ficheros de texto y la búsqueda de imágenes conocidas en el computador del sospechoso.[2229] El análisis de ficheros comprende también el examen de documentos digitales que pueden haberse falsificado[2230] así como de los metadatos.[2231] Con este tipo de análisis se puede determinar en qué momento[2232] se abrió o modificó por última vez un documento.[2233] Además, el análisis de los metadatos puede servir para identificar al autor de un fichero que contenga una amenaza, o el número de serie de la cámara empleada para crear una imagen de pornografía infantil. También se puede identificar a los autores a partir de un análisis lingüístico, que puede ayudar a determinar si el sospechoso ha escrito artículos con anterioridad y dejado información que pueda ayudar a identificarlo en este contexto.[2234]

Rastreo e información

Uno de los mayores problemas de las pruebas digitales es que son extremadamente frágiles y se pueden borrar[2235] o modificar[2236] con relativa facilidad. Como ya se ha señalado una de las consecuencias de esta fragilidad es que es necesario mantener su integridad.[2237] Por consiguiente, es necesario mantener un registro. Una de las posibilidades para mantener la integridad de las pruebas examinadas por los expertos forenses[2238] es contar con expertos cualificados[2239] para la elaboración de registros y copias. Pero los expertos forenses también tienen un papel que desempeñar cuando no es posible o no procede confiscar el hardware. En tal caso, en algunos países se les permite copiar los ficheros. Ha de prestar una atención especial a la protección de la integridad de los ficheros copiados a fin de que no sufran alteración alguna durante el proceso de copia.[2240]

Presentación de pruebas en ante un tribunal

La fase final de la investigación suele ser la presentación de pruebas ante el tribunal. Si bien la presentación de las pruebas ante el tribunal suelen hacerla el fiscal y los abogados de la defensa, los expertos forenses pueden desempeñar un papel muy importante en el juicio en tanto que testigos expertos que pueden ayudar a comprender los procesos mediante los cuales se obtuvieron las pruebas, los procedimientos utilizados para ello y la evaluación de dichas pruebas.[2241] Habida cuenta de la complejidad de las pruebas digitales, la participación de los expertos forenses es aún más necesaria y hace que los jueces, los jurados, los fiscales y los abogados confíen *de facto* en las afirmaciones de los expertos.[2242]

Examen forense

Aunque la informática forense se ocupa en gran medida del hardware y los datos informáticos, no necesariamente se trata siempre de un proceso automatizado y en numerosas ocasiones conlleva un trabajo manual[2243], en particular cuando se trata de elaborar estrategias y buscar posibles pruebas en la fase de registro e incautación. La cantidad de tiempo necesaria para efectuar dichas operaciones manuales, junto con la capacidad de los infractores para automatizar sus ataques, pone de manifiesto los desafíos a que se enfrentan las fuerzas del orden, en particular en el marco de investigaciones sobre un amplio número de sospechosos y grandes volúmenes de datos.[2244] Sin embargo, procesos como la búsqueda por palabras clave sospechosas o la recuperación de ficheros suprimidos pueden automatizarse con herramientas de análisis forense especiales.[2245]

6.5.3 Salvaguardias

Durante los últimos años, las autoridades competentes de todo el mundo han destacado la urgente necesidad de instrumentos de investigación apropiados [2246] y, habida cuenta de ello, es un poco sorprendente que el Convenio sobre la Ciberdelincuencia haya sido objeto de críticas en lo que respecta a los instrumentos procesales[2247], críticas que se refieren sobre todo al hecho de que el Convenio contenga varias disposiciones que tratan de instrumentos de investigación (Artículo 16-Artículo 21), pero sólo una (Artículo 15) que trata de salvaguardias[2248]. Además, cabe señalar que, a diferencia de las disposiciones sustantivas de derecho penal que figuran en el Convenio, sólo se dejan escasísimas posibilidades de ajustes nacionales en la aplicación del Convenio [2249]. Las críticas se refieren principalmente a los aspectos cuantitativos. Es apropiado que el Convenio siga el concepto de una reglamentación centralizada de las salvaguardias, en lugar de vincularlas individualmente a cada instrumento, pero ello no significa necesariamente que los derechos de los sospechosos estén menos protegidos.

El Convenio sobre la Ciberdelincuencia estaba concebido desde el principio como marco internacional e instrumento de lucha contra la ciberdelincuencia que no se limita exclusivamente a los países miembros del Consejo de Europa[2250]. Al negociar los instrumentos procesales necesarios, los redactores del Convenio, que comprendían representantes de países no europeos tales como Estados Unidos y Japón, cayeron en la cuenta de que los actuales planteamientos nacionales en lo que respecta a las salvaguardias y, en particular, la protección de los sospechosos en los diversos sistemas de derecho penal, eran tan diferentes que sería imposible definir una solución específica para cada Estado Miembro[2251]. Por consiguiente, los redactores decidieron no incorporar reglas específicas en el Convenio y pedir en cambio a los Estados Miembros que velasen por la aplicación de normas de salvaguardia nacionales e internacionales fundamentales.[2252]

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

El Artículo 15 se fundamenta en el principio de que los Estados signatarios aplicarán las condiciones y salvaguardias vigentes en la legislación nacional. Si la ley contempla normas centralizadas que se aplican a todos los instrumentos de investigación, esos principios se aplicarán también a los instrumentos relacionados con Internet[2253]. Si la legislación nacional no está basada en una reglamentación centralizada de salvaguardias y condiciones, se han de analizar las salvaguardias y condiciones que se aplican en lo que respecta a los instrumentos nacionales comparables con los instrumentos relacionados con Internet.

Ahora bien, el Convenio no se refiere únicamente a las salvaguardias existentes plasmadas en la legislación nacional, ya que tendría el inconveniente de que las diferencias entre las exigencias de aplicación anularían los aspectos positivos de la armonización. A fin de asegurar que los Estados signatarios que tienen tradiciones y salvaguardias legislativas diferentes apliquen ciertas normas[2254], en el Convenio sobre la Ciberdelincuencia se definen las normas mínimas haciendo referencia a marcos fundamentales tales como el Convenio de 1950 del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades

Fundamentales; el Pacto Internacional de Derechos Civiles y Políticos adoptado por las Naciones Unidas en 1996; y otros instrumentos internacionales aplicables sobre derechos humanos.

Como el Convenio también puede ser firmado y ratificado por países que no son miembros del Consejo de Europa[2255], es importante destacar el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas y el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales que se tendrán en cuenta al evaluar los sistemas de salvaguardias vigentes en los Estados signatarios que no son miembros del Convenio sobre la ciberdelincuencia.

En lo que respecta a la investigación de los ciberdelitos, una de las disposiciones más pertinentes del Artículo 15 del Convenio sobre la Ciberdelincuencia es la referencia al Artículo 8, párrafo 2 del Convenio Europeo para la Protección de los Derechos Humanos.

Artículo 8
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

El Tribunal Europeo de Derechos Humanos ha tratado de definir con más precisión las normas que rigen las investigaciones electrónicas y, en particular, la intervención de las comunicaciones. Actualmente, la jurisprudencia se ha convertido en una de las fuentes más importantes de normas internacionales en lo que respecta a las investigaciones relativas a las comunicaciones[2256]. La jurisprudencia tiene particularmente en cuenta la gravedad de la injerencia de la investigación[2257], su objeto[2258] y su proporcionalidad[2259]. Los principios fundamentales que se pueden extraer de la jurisprudencia son los siguientes: los instrumentos de investigación necesitan una base jurídica suficiente[2260]; la base jurídica debe ser clara con respecto al objeto[2261]; las competencias de las autoridades competentes deben ser previsibles[2262]; la intervención de las comunicaciones sólo puede justificarse cuando se trata de delitos graves[2263].

Por otra parte, en el Artículo 15 del Convenio sobre la Ciberdelincuencia se tiene en cuenta el principio de proporcionalidad[2264]. Esta disposición es particularmente pertinente para los Estados signatarios que no son miembros del Consejo de Europa. Cuando el sistema de salvaguardias nacional vigente no protege de manera adecuada a los sospechosos, los Estados Miembros están obligados a definir las salvaguardias necesarias en el proceso de ratificación y aplicación.

Por último, en el punto 2 del Artículo 15 del Convenio sobre la Ciberdelincuencia se hace referencia explícitamente a algunas de las salvaguardias más pertinentes[2265], y en particular la supervisión; los motivos que justifican la aplicación; la limitación del ámbito de aplicación y de la duración del procedimiento.

A diferencia de los principios fundamentales descritos *supra*, las salvaguardias mencionadas en este caso no se han de aplicar necesariamente a cualquier instrumento, pero sólo si procede habida cuenta del carácter de procedimiento en cuestión. El poder legislativo nacional es el que debe pronunciarse al respecto[2266].

Otro aspecto importante del sistema de salvaguardias contemplado en el Convenio sobre la Ciberdelincuencia es que la capacidad de las autoridades competentes de utilizar los instrumentos con flexibilidad, por una parte, y la garantía de salvaguardias efectivas, por otra, dependen de la aplicación de un sistema de salvaguardias escalonado. El Convenio no impide explícitamente a las Partes que apliquen las mismas salvaguardias (por ejemplo, la obligación de disponer de una orden judicial) para todos los instrumentos, pero ese planteamiento afectaría a la flexibilidad de las autoridades competentes. La capacidad de garantizar una protección adecuada de los derechos del sospechoso en un sistema de salvaguardas escalonado depende en gran medida de la posibilidad de equilibrar las posibles consecuencias de un instrumento de investigación con las salvaguardias correspondientes. Para ello se ha de distinguir

entre instrumentos más o menos coercitivos. En el Convenio sobre la Ciberdelincuencia se observan varias de esas distinciones que permiten que las Partes elaboren un sistema de salvaguardas escalonadas, como por ejemplo, lo siguiente. La distinción entre la interceptación de datos relativos al contenido (Artículo 21)[2267] y la obtención de datos relativos al tráfico (Artículo 20)[2268]. A diferencia de la obtención de datos relativos al tráfico, la interceptación de datos relativos al contenido se limita a los delitos graves[2269]. La distinción entre la orden de conservación rápida de datos informáticos almacenados (Artículo 16)[2270] y la de presentación de datos informáticos almacenados en cumplimiento de una orden de presentación (Artículo 18)[2271]. El Artículo 16 sólo permite que las autoridades competentes ordenen la conservación de los datos, pero no su revelación[2272]. La distinción en el Artículo 18[2273] entre la obligación de comunicar "datos relativos a los abonados"[2274] y "datos informáticos"[2275].

Si el carácter coercitivo de un instrumento de investigación y sus posibles consecuencias para el sospechoso se evalúan correctamente y las salvaguardias están concebidas con arreglo a los resultados del análisis, el sistema de salvaguardias escalonado no desequilibra el sistema de instrumentos procesales.

6.5.4 Conservación y revelación rápidas de datos informáticos almacenados (procedimiento de congelación rápida)

Para identificar al infractor que ha cometido un ciberdelito suele ser necesario analizar los datos relativos al tráfico[2276]. En particular, la dirección IP puede ayudar a las autoridades competentes a seguir el rastro del infractor. Siempre y cuando esas autoridades competentes tengan acceso a los datos de tráfico pertinentes, en algunos casos incluso pueden identificar al infractor que utiliza terminales Internet públicos en los cuales no necesita identificarse[2277].

Una de las principales dificultades para los investigadores es que los datos de tráfico que permitirían obtener la información en cuestión se suprimen a menudo automáticamente al poco tiempo. Esta supresión automática se debe a que al final de un proceso (por ejemplo, envío de un correo electrónico, acceso a Internet o telecarga de una película) los datos de tráfico generados durante el proceso y que permiten llevar a cabo el mismo ya no son necesarios. En lo que respecta a los aspectos económicos de esta actividad, la mayoría de los proveedores Internet tienen interés en suprimir la información lo antes posible, ya que almacenar los datos durante más tiempo exigiría una capacidad de almacenamiento aún más grande (y onerosa)[2278].

Los aspectos económicos no son sin embargo el único motivo de que las autoridades competentes deban llevar a cabo rápidamente sus investigaciones. Algunos países tienen leyes muy estrictas que prohíben almacenar determinados datos de tráfico cuando ha terminado un proceso. Ese tipo de restricción figura, por ejemplo, en el Artículo 6 de la Directiva de la Unión Europea sobre privacidad y comunicaciones electrónicas.[2279]

Artículo 6 – Datos de tráfico
1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente Artículo y en el apartado 1 del Artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.
2. Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

El tiempo es, por consiguiente, un parámetro fundamental de las investigaciones en Internet. Por lo general, dada la probabilidad de que transcurra algo de tiempo entre la perpetración del delito, su descubrimiento y la notificación de las autoridades competentes, es importante aplicar mecanismos que impidan la supresión de los datos pertinentes durante el proceso de investigación, que puede ser bastante largo. A este respecto, se estudian actualmente dos planteamientos diferentes[2280]: conservación de datos y preservación de datos ("Procedimiento de congelación rápida").

La obligación de conservar los datos fuerza al proveedor de servicios Internet a conservar los datos de tráfico durante cierto tiempo[2281]. En los sistemas legislativos más recientes se han de conservar los registros durante 6 a 24 meses[2282]. De este modo, las autoridades competentes pueden consultar los datos necesarios para identificar a los infractores incluso varios meses después del delito[2283]. El Parlamento de la Unión Europea adoptó recientemente una obligación de conservación de datos[2284], obligación que también se está examinando actualmente en Estados Unidos[2285]. En lo que respecta a los principios de conservación de datos, a continuación se facilita información adicional.

Convenio sobre la Ciberdelincuencia

La conservación de datos es un planteamiento diferente destinado a garantizar que la prolongada investigación de un ciberdelito no fracase simplemente porque se han suprimido datos de tráfico.[2286] Fundamentándose en la legislación sobre la conservación de los datos, las autoridades competentes pueden obligar a un proveedor de servicio a impedir la supresión de ciertos datos. La conservación rápida de datos informáticos es un instrumento que debería ayudar a las autoridades competentes a reaccionar inmediatamente y evitar que se puedan suprimir antes de que termine un juicio largo.[2287] Los redactores del Convenio sobre la Ciberdelincuencia prefirieron centrarse en la "conservación de los datos" en lugar de la "retención de datos".[2288] Véase la regla correspondiente en el Artículo 16 del Convenio sobre la Ciberdelincuencia.

Artículo 16 – Conservación rápida de datos informáticos almacenados
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.
2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.
4. Los poderes y procedimientos mencionados en el presente Artículo estarán sujetos a lo dispuesto en los Artículos 14 y 15.

Desde el punto de vista de los proveedores de servicios Internet, la conservación de datos es un instrumento menos coercitivo que la retención de datos.[2289] No es necesario que los PSI almacenen todos los datos de todos los usuarios, pero, tan pronto como reciben una orden de la autoridad competente, deben asegurarse de que datos específicos no se suprimen. La conservación de datos ofrece ventajas, ya que no se trata simplemente de conservarlos, sino también de protegerlos. No es necesario conservar los datos de millones de usuarios de Internet, sino únicamente los datos que puedan estar relacionados con posibles sospechosos en investigaciones judiciales. No obstante, es importante señalar que la retención de datos tiene ventajas cuando los datos se suprimen justo después del final de la perpetración, en cuyo caso la orden de conservación de datos, a diferencia de la obligación de retención de datos, no podría impedir la supresión de los datos pertinentes.

La orden conforme al Artículo 16 no obliga al proveedor a salvaguardar los datos que han sido procesados por el proveedor y no se han suprimido cuando éste recibe la orden.[2290] No se limita a los datos de tráfico, que en este caso son un simple ejemplo. El Artículo 16 no obliga al infractor a reunir información que normalmente no almacenaría,[2291] ni obliga al proveedor a transferir los datos pertinentes a las autoridades. Esta disposición sólo autoriza a las autoridades competentes a impedir la supresión de los datos

pertinentes, pero no obliga a los proveedores a transferir los datos. La obligación de transferir se contempla en los Artículos 17 y 18 del Convenio sobre la Ciberdelincuencia. La separación entre la obligación de conservar los datos y la de revelarlos tiene la ventaja de que se pueden exigir condiciones de aplicación diferentes.[2292] En lo que respecta a la importancia que reviste una reacción inmediata, quizá conviniera hacer caso omiso de la obligación de que un juez dicte una orden judicial y permitir que la acusación o la policía puedan ordenar la conservación.[2293] De este modo, esas autoridades competentes podrían reaccionar más rápidamente. La protección de los derechos del sospechoso se puede lograr exigiendo una orden para revelar los datos.[2294]

La revelación de los datos conservados es uno de los otros aspectos contemplados en el Artículo 18 del Convenio sobre la Ciberdelincuencia:

Artículo 18 – Orden de presentación
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:
a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y
b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.
2. Los poderes y procedimientos mencionados en el presente Artículo estarán sujetos a lo dispuesto en los Artículos 14 y 15.
3. A los efectos del presente Artículo, se entenderá por "datos relativos a los abonados" cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:
a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;
c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Con arreglo al apartado 1 a) del Artículo 18 del Convenio sobre la Ciberdelincuencia, se puede obligar a los proveedores que han conservado los datos a comunicarlos.

El Artículo 18 del Convenio sobre la Ciberdelincuencia no se aplica solamente después del envío de una orden de conservación conforme al Artículo 16 del Convenio.[2295] La disposición es un instrumento de carácter general al que pueden recurrir las autoridades competentes. Si el que recibe una orden de presentación transfiere voluntariamente los datos solicitados a las autoridades competentes, éstas pueden utilizar una orden de comunicación menos coercitiva en lugar de limitarse a incautar los equipos. En comparación con la incautación de equipos, la orden de someter la información pertinente suele ser menos coercitiva. Su aplicación es, por lo tanto, especialmente pertinente cuando el acceso al equipo no es necesario en las investigaciones judiciales.

Además de la obligación de someter datos informáticos, el Artículo 18 del Convenio sobre la Ciberdelincuencia permite que las autoridades competentes ordenen la comunicación de información sobre el abonado. Este instrumento de investigación reviste una gran importancia en las investigaciones sobre redes IP. Si las autoridades competentes pueden identificar una dirección IP utilizada por el infractor en el momento de la infracción, necesitarán identificar a la persona[2296] que utilizó la dirección IP en el momento de la infracción. Con arreglo al apartado 1.b del Artículo 18 del Convenio sobre la Ciberdelincuencia, un proveedor está obligado a someter la información sobre el abonado indicada en el punto 3 del Artículo 18.[2297]

Cuando las autoridades competentes siguen el rastro de un infractor y necesitan un acceso inmediato para identificar el trayecto por el que se transmitió la comunicación, el Artículo 17 les permite ordenar la revelación parcial rápida de los datos relativos al tráfico.

Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico
1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del Artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para:

a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y

b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente Artículo estarán sujetos a lo dispuesto en los Artículos 14 y 15.

Como ya se ha dicho, en el Convenio se distingue estrictamente la obligación de conservar datos previa petición y la de comunicarlos a las autoridades competentes.[2298] En el Artículo 17 la distinción es clara, ya que se combina la obligación de garantizar la conservación de datos de tráfico cuando varios proveedores participan en la transmisión, con la obligación de revelar la información necesaria para identificar la vía por la que se ha transmitido la comunicación. Sin esa revelación parcial, en algunos casos las autoridades competentes no podrían seguir el rastro del infractor si más de un proveedor participara en la comunicación.[2299] Habida cuenta de que la combinación de ambas obligaciones afectan de distintas maneras los derechos de los sospechosos, se ha de estudiar el tenor de las salvaguardias relativas a este instrumento.

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

Se pueden encontrar planteamientos similares en la Ley modelo de 2002 de la Commonwealth.[2300]

Disposición

Producción de datos
15 *Si, tras examinar la solicitud de un funcionario de policía, un magistrado queda convencido de que existen motivos fundados para pedir los datos informáticos especificados, o una versión impresa o información de otro tipo, a efectos de una investigación o un juicio penal, puede ordenar lo siguiente:*

(a) que una persona presente en el territorio del [país promulgador] y que controla un sistema informático extraiga del sistema datos informáticos específicos, o una versión impresa de los mismos, o una versión inteligible de los mismos;

(b) que un proveedor de servicio Internet en el [país promulgador] comunica información sobre las personas que están abonadas al servicio, o lo utilizan de algún otro modo; y

(c)[2301] *que una persona presente en el territorio del [país promulgador], que tiene acceso a un sistema informático especificado, tramite y compile datos informáticos especificados del sistema y los entregue a una persona determinada.*

Divulgación de los datos de tráfico almacenados
16[2302] *Si un agente de policía está convencido de que existen motivos fundados para necesitar datos almacenados en un sistema informático a efectos de una investigación penal, puede solicitar por escrito a la persona responsable del sistema informático que comunique datos de tráfico suficientes sobre una comunicación determinada para identificar:*

(a) los proveedores de servicio; y

(b) el trayecto por el cual se ha transmitido la comunicación.

Conservación de datos
17. *(1) Si un agente de policía está convencido de que:*

(a) existen motivos fundados para necesitar datos almacenados en un sistema informático a efectos de una investigación penal; y

(b) que existe el riesgo de que los datos sean destruidos o de que sea imposible acceder a los mismos; el funcionario de policía puede solicitar por escrito a la persona responsable del sistema informático, que se asegure de que los datos especificados en la notificación se conserven durante un periodo de hasta 7 días, especificado en la notificación.

(2) El periodo se puede prolongar después de los 7 días si, en una solicitud ex parte, un [juez] [magistrado] autoriza la prolongación durante un determinado periodo de tiempo e.

6.5.5 Conservación de datos

La obligación de conservación de datos fuerza al proveedor de servicios Internet a salvaguardar datos de tráfico durante cierto tiempo.[2303] La obligación de conservación de datos tiene por objeto evitar la mencionada dificultad de obtener acceso a datos de tráfico antes de que sean suprimidos. Ejemplo de ese tipo de planteamiento fue la Directiva de la Unión Europea sobre la conservación de datos[2304], que se declaró nula en 2014.[2305]

Artículo 3 – Obligación de conservar datos

1. Como excepción a los Artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados Miembros adoptarán medidas para garantizar que los datos especificados en el Artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.

2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el Artículo 5 en relación con las llamadas telefónicas infructuosas en las que los datos los generan o tratan, y conservan (en lo que a los datos telefónicos se refiere) o registran (en lo que a los datos de Internet se refiere), proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. La conservación de datos en relación con las llamadas no conectadas no será obligatoria con arreglo a la presente Directiva.

Artículo 4 – Acceso a los datos

Los Estados Miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional. Cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del Derecho de la Unión o del Derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos.

Artículo 5 – Categorías de datos que deben conservarse

1. Los Estados Miembros garantizarán que las siguientes categorías de datos se conserven de conformidad con la presente Directiva:

(a) datos necesarios para rastrear e identificar el origen de una comunicación:

(1) con respecto a la telefonía de red fija y a la telefonía móvil:

(i) el número de teléfono de llamada,

(ii) el nombre y la dirección del abonado o usuario registrado;

(2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

(i) la identificación de usuario asignada,

(ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía,

(iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono;

(b) datos necesarios para identificar el destino de una comunicación:

(1) con respecto a la telefonía de red fija y a la telefonía móvil:

(i) el número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas,

(ii) los nombres y las direcciones de los abonados o usuarios registrados;

(2) con respecto al correo electrónico por Internet y a la telefonía por Internet:

(i) la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet,

(ii) los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación;

(c) datos necesarios para identificar la fecha, hora y duración de una comunicación:

(1) con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la comunicación,

(2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

(i) la fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado,

(ii) la fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario;

(d) datos necesarios para identificar el tipo de comunicación:

(1) con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado,

(2) con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado;

(e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

(1) con respecto a la telefonía de red fija: los números de teléfono de origen y destino,

(2) con respecto a la telefonía móvil:

(i) los números de teléfono de origen y destino,

(ii) la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada,

(iii) la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada,

(iv) la IMSI de la parte que recibe la llamada,

(v) la IMEI de la parte que recibe la llamada,

(vi) en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio;

(3) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

(i) el número de teléfono de origen en caso de acceso mediante marcado de números,

(ii) la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación;

(f) datos necesarios para identificar la localización del equipo de comunicación móvil:

(1) la etiqueta de localización (identificador de celda) al comienzo de la comunicación,

(2) los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación.

Artículo 6** – **Períodos de conservación

Los Estados Miembros garantizarán que las categorías de datos mencionadas en el Artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación.

Artículo 7 – Protección y seguridad de los datos
Sin perjuicio de lo dispuesto en las disposiciones adoptadas de conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados Miembros velarán por que los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones cumplan, en lo que respecta a los datos conservados de conformidad con la presente Directiva, como mínimo los siguientes principios de seguridad de los datos:

(a) los datos conservados serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red;

(b) los datos estarán sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;

(c) los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas, y

(d) los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación.

Artículo 8 – Requisitos de almacenamiento para los datos conservados
Los Estados Miembros garantizarán que los datos especificados en el Artículo 5 se conservan de conformidad con la presente Directiva de manera que los datos conservados y cualquier otra información necesaria con ellos relacionada puedan transmitirse sin demora cuando las autoridades competentes así lo soliciten.

El hecho de que la Directiva trate de informaciones fundamentales sobre cualquier comunicación en Internet ha sido objeto de acerbas críticas por parte de organizaciones de derechos humanos[2306] , lo cual podría a su vez provocar una revisión de la Directiva y de su aplicación en tribunales constitucionales.[2307] Además, en su conclusión en el caso Productores de Música de España (Promusicae) contra Telefónica de España,[2308] Juliane Kokott, Abogada General ante el Tribunal de Justicia Europeo, señaló que le parecía poco probable que se pudiera aplicar la obligación de conservación de datos sin violar derechos fundamentales.[2309] En 2001 el G8 ya señaló dificultades con respecto a la aplicación de ese tipo de reglamentaciones.[2310]

Ahora bien, las críticas no se limitan a esta consideración. La conservación de los datos también ha resultado menos eficaz en la lucha contra la ciberdelincuencia porque las obligaciones se pueden eludir. Las maneras más fáciles de sortear la obligación de conservación de datos son, entre otras, la utilización de terminales Internet públicos diferentes o de servicios de datos por teléfonos móviles de pago previo que no están registrados [2311] y la utilización de servicios de comunicación anónimos explotados (al menos parcialmente) en países en los cuales no es obligatorio conservar los datos.[2312]

Si los infractores utilizan terminales públicos diferentes o servicios de datos por teléfonos móviles de pago previo para los cuales no están obligados a registrar los datos almacenados por los proveedores, la obligación de conservación de datos conducirá a los organismos legislativos al proveedor de servicio, pero no al delincuente en cuestión.[2313]

Los infractores pueden eludir además la obligación de conservación de datos utilizando servidores de comunicación anónimos.[2314] En este caso, las autoridades competentes quizá puedan demostrar que el infractor ha utilizado un servidor de comunicación anónimo, pero al no poder acceder a los datos de tráfico en el país en el cual está situado el servidor de comunicación anónimo, no podrán demostrar la participación del infractor en la perpetración del delito.[2315]

Dado que es muy fácil hacer caso omiso de esta disposición, la aplicación de la legislación sobre la conservación de datos en la Unión Europea se suma al temor de que el proceso exija la adopción de medidas adicionales para garantizar la eficacia del instrumento. Estas medidas podrían consistir, entre otras cosas, en la obligación de registrarse antes de utilizar servicios en línea[2316] o la prohibición de la utilización de tecnologías de comunicación anónimas.[2317]

En 2014, el Tribunal de Justicia Europeo declaró finalmente nula la Directiva[2318] que, en su opinión, entraña injerencias numerosas y particularmente graves a los derechos fundamentales de respeto a la vida privada y a la protección de los datos personales, sin que dicha injerencia se limite a la estrictamente necesaria. Por

ese motivo, la Directiva ya no es vinculante para los Estados Miembros. Las leyes nacionales, que fueron aplicadas en virtud de la Directiva, no quedan automáticamente derogadas. No se sabe a ciencia cierta por el momento si la Unión Europea presentará y aprobará una nueva directiva.

6.5.6 Registro y confiscación

Si bien algunos países ya estudian e incluso utilizan nuevos instrumentos de investigación tales como la compilación de datos de contenido en tiempo real o programas informáticos de investigación para identificar a los delincuentes, el registro y confiscación sigue siendo uno de los instrumentos de investigación más importantes.[2319] Tan pronto como las autoridades competentes identifican al delincuente y confiscan su equipo informático, los expertos judiciales especializados en informática pueden analizarlo a fin de reunir las pruebas necesarias para el juicio.[2320]

Algunos países europeos y Estados Unidos están contemplando la posibilidad de sustituir o enmendar el procedimiento de registro y confiscación.[2321] Para no tener que penetrar en la casa del sospechoso para confiscar el equipo informático, cabría la posibilidad de llevar a cabo una búsqueda en línea. En ese instrumento, que se explica con más detalle a continuación, se describe un procedimiento en el cual las autoridades competentes acceden al ordenador del sospechoso a través de Internet para llevar a cabo subrepticiamente su investigación.[2322] Si bien las autoridades competentes podrían aprovechar obviamente el hecho de que el sospechoso no fuera consciente de que se estaba llevando a cabo la investigación, el acceso físico al equipo permite utilizar técnicas de investigación más eficaces.[2323] Esto subraya la importancia de los procedimientos de registro y confiscación en la investigación en Internet.

Convenio del Consejo de Europa sobre la Ciberdelincuencia

La mayoría de las legislaciones procesales penales nacionales contienen disposiciones que autorizan a los organismos competentes a registrar y confiscar objetos.[2324] Los redactores del Convenio sobre la Ciberdelincuencia incluyeron no obstante una disposición que trata del registro y confiscación porque las legislaciones nacionales a menudo no abarcan procedimientos de registro y confiscación relativos a los datos.[2325] Algunos países, por ejemplo, limitan la aplicación de los procedimientos de confiscación a los objetos físicos.[2326] Según esas disposiciones, los investigadores judiciales pueden confiscar un servidor entero pero no los datos pertinentes que contiene copiándolos del servidor, lo cual puede plantear dificultades cuando la información pertinente está almacenada en un servidor junto con los datos de centenares de usuarios, datos que ya no estarían disponibles después de la confiscación del servidor por las autoridades. El registro y la confiscación tradicionales de bienes tangibles tampoco es suficiente cuando las autoridades competentes desconocen la ubicación física del servidor pero pueden acceder a él a través de Internet.[2327] El Artículo 19, al igual que otros instrumentos procesales previstos en el Convenio sobre la Ciberdelincuencia, no especifica las condiciones y requisitos que deben cumplir los investigadores para llevar a cabo dichas investigaciones. En la disposición no se afirma que sea necesaria una orden de un tribunal ni define las circunstancias en que puede hacerse una excepción a la obligación de obtener una orden del tribunal. Teniendo en cuenta la intrusión en las libertades y derechos civiles del sospechoso que suponen los procedimientos de registro y confiscación[2328], la mayoría de los países limitan la aplicabilidad del instrumento.[2329]

El punto 1 del Artículo 19 del Convenio del Consejo de Europa sobre la Ciberdelincuencia tiene por objeto establecer un instrumento que permita registrar sistemas informáticos y que sea tan eficaz como los procedimientos de registros tradicionales.[2330]

> ***Artículo 19 – Registro y confiscación de datos informáticos almacenados***
> *1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o tener acceso de un modo similar:*
> *a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados, y*
> *b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.*
> *[…]*

Si bien los investigadores recurren con frecuencia al procedimiento de registro y confiscación, su utilización en investigaciones de ciberdelitos plantea diversas dificultades.[2331] Una de las principales es que los mandatos judiciales suelen estar limitados a determinados lugares (por ejemplo, el hogar del sospechoso).[2332] En lo que respecta al registro de datos informáticos, la investigación puede revelar que el sospechoso no los almacenó en discos duros locales, sino en un servidor externo al cual accedió por Internet.[2333] La utilización de servidores Internet para almacenar y procesar datos se está generalizando entre los usuarios ("Informática en nubes"). Ese tipo de almacenamiento tiene, entre otras ventajas, la de poder acceder fácilmente a la información desde cualquier lugar con una conexión Internet. Para garantizar la eficacia de las investigaciones, es importante que éstas tengan cierta flexibilidad. Si los investigadores descubren que la información pertinente está almacenada en otro sistema informático, deben poder extender el registro a ese sistema.[2334] El Convenio del Consejo de Europa sobre la Ciberdelincuencia trata de este asunto en el punto 2 del Artículo 19.

Artículo 19 – Registro y confiscación de datos informáticos almacenados
[…]
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, pueden extender rápidamente el registro o el acceso de un modo similar al otro sistema.
[…]

La confiscación de datos informáticos también plantea otra dificultad. Si los investigadores llegan a la conclusión de que no es necesario o que es improcedente confiscar el equipo utilizado para almacenar la información, quizá necesiten a pesar de ello otros instrumentos que les permitan continuar el procedimiento de registro y confiscación de los datos informáticos almacenados.[2335] Los instrumentos necesarios no se limitan a copiar los datos pertinentes.[2336] Además, se requieren diversas medidas adicionales que resulten tan eficaces como la confiscación del equipo informático propiamente dicho. La consideración más importante es mantener la integridad de los datos copiados.[2337] Si los investigadores no están autorizados a tomar las medidas necesarias para garantizar la integridad de esos datos, éstos podrían no ser aceptados como prueba en un juicio penal.[2338] Una vez que los investigadores han copiado los datos y adoptado medidas para mantener su integridad, deberán tomar una decisión sobre cómo tratar los datos originales. Si los investigadores no desplazan el equipo durante el procedimiento de registro, por lo general la información permanecerá ahí. En las investigaciones sobre contenidos ilegales[2339] (por ejemplo, pornografía infantil) en particular, los investigadores no podrán dejar los datos en el servidor y, por lo tanto, necesitarán un instrumento que les permita suprimirlos o, al menos, garantizar que ya no sean accesibles.[2340] El Convenio sobre la Ciberdelincuencia trata de estas cuestiones en el punto 3 del Artículo 19.

Artículo 19 – Registro y confiscación de datos informáticos almacenados
[…]
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 ó 2. Estas medidas incluirán las siguientes prerrogativas:
a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
b. realizar y conservar una copia de esos datos informáticos;
c. preservar la integridad de los datos informáticos almacenados pertinentes; y
d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado
[…]

Otro inconveniente de los mandatos judiciales relativos a datos informáticos es que las autoridades competentes pueden tener dificultades para ubicar datos que, a menudo, están almacenados en sistemas informáticos en el extranjero. Aun cuando se conoce su ubicación exacta, el volumen de los datos almacenados suele obstaculizar notablemente las investigaciones[2341] , que entonces plantean dificultades particulares porque adquieren una dimensión internacional que exige, a su vez, una cooperación internacional en las investigaciones.[2342] Aun cuando se investigan sistemas informáticos ubicados dentro de las fronteras nacionales y los investigadores han identificado al proveedor que explota los servidores en los cuales el delincuente ha almacenado los datos pertinentes, los investigadores pueden tener dificultades para identificar la ubicación exacta de los datos. Es muy probable que incluso los proveedores de pequeñas y medianas dimensiones tengan centenares de servidores y miles de discos duros. Con frecuencia, los investigadores no podrán identificar la ubicación exacta con ayuda del administrador de sistema responsable de la infraestructura del servidor[2343] , pero aun cuando puedan identificar el disco duro que buscan, es posible que éste disponga de medidas de protección que les impida encontrar los datos pertinentes. Los redactores del Convenio decidieron tenerlo en cuenta introduciendo una medida coercitiva para facilitar el registro y confiscación de datos informáticos. El punto 4 del Artículo 19 permite que los investigadores obliguen al administrador de un sistema a ayudar a las autoridades competentes. Si bien la obligación de cumplir las órdenes del investigador se limita a la información y a la ayuda necesarias para el caso, este instrumento cambia el carácter de los procedimientos de registro y confiscación. En muchos países, los mandatos de registro y confiscación sólo obligan a las personas afectadas por la investigación a tolerar los procedimientos, pero no a facilitar activamente la investigación. En lo que respecta a las personas con conocimientos especiales a las que pueden tener que recurrir los investigadores, la aplicación del Convenio sobre la Ciberdelincuencia cambiará la situación de dos maneras. Primero, deberán facilitar la información necesaria a los investigadores. El segundo cambio está relacionado con esa obligación. La obligación de ayudar, de manera razonable, a los investigadores, eximirá a las personas con conocimientos especiales de sus obligaciones contractuales o de las órdenes recibidas de sus supervisores.[2344] En el Convenio no se define el término "*razonable*", pero en el Informe Explicativo se señala que razonable "*puede comprender la divulgación de una contraseña o de otras medidas de seguridad a las autoridades investigadoras*", pero en general no abarca "*la revelación de la contraseña o de otras medidas de seguridad*" cuando ello entrañe una "*amenaza improcedente contra la privacidad de otros usuarios u otros datos cuyo registro no esté autorizado*".[2345]

Artículo 19 – Registro y confiscación de datos informáticos almacenados
[…]
4. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.
[…]

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

Un planteamiento similar puede encontrarse en la Ley modelo de la Commonwealth de 2002.[2346]

Definiciones para esta Parte
11. *En esta parte:*
[…]
"confiscar" significa, entre otras cosas:
(a) efectuar y conservar una copia de datos informáticos, incluso utilizando equipos disponibles in situ;
(b) volver inaccesible, o suprimir, datos informáticos en el sistema informático en cuestión;
(c) tomar un ejemplar impreso de los datos informáticos.
[…]

Órdenes de búsqueda y confiscación

12[2347] *(1) Si, sobre la base de [una información sometida bajo juramento] [una declaración jurada por escrito], está convencido de que existen motivos fundados para [sospechar] [creer] que en un lugar determinado puede encontrarse un objeto o datos informáticos:*

(a) que pueden constituir una prueba material de un delito;

(b) que ha sido adquirido por una persona a raíz de un delito;

el magistrado [puede dictar] [dictará] una orden judicial en la cual autorice a un [funcionario judicial] [agente de policía], con la asistencia necesaria, a penetrar en el lugar para registrar y confiscar el objeto o los datos informáticos.

[…]

Asistencia a la labor policial

13[2348] *(1) Una persona que posee o controla un medio de almacenamiento de datos informáticos o un sistema informático que es objeto de un registro con arreglo a la Sección 12 debe autorizar y, en su caso, ayudar a la persona que efectúa el registro a:*

(a) acceder al sistema informático o medio de almacenamiento de datos informáticos, o a utilizarlo, para registrar cualesquiera datos informáticos a los que se pueda acceder a través del sistema o estén disponibles en el sistema;

(b) obtener y copiar esos datos informáticos;

(c) utilizar equipos para efectuar copias;

(d) obtener una salida inteligible de un sistema informático en formato de texto normal legible por una persona.

(2) Una persona que, sin excusa o justificación legítimas, no da permiso o ayuda a una persona, comete un delito punible con el encarcelamiento por un periodo no superior a [periodo] o una multa no superior a [importe], o ambas.

6.5.7 Orden de presentación

Aun cuando la legislación nacional no contempla una obligación como la del punto 4 del Artículo 19 del Convenio sobre la Ciberdelincuencia, los proveedores cooperan a menudo con las autoridades competentes a fin de evitar consecuencias negativas para su negocio. Si por falta de cooperación del proveedor, los investigadores no pueden encontrar los datos o los dispositivos de almacenamiento que necesitan registrar y confiscar, es probable que tengan que confiscar más equipos de lo que suele ser necesario. Por lo tanto, los proveedores ayudarán generalmente en las investigaciones y facilitarán los datos pertinentes que les pidan las autoridades competentes. El Convenio sobre la Ciberdelincuencia contiene instrumentos que autorizan a los investigadores a prescindir de mandato judicial si la persona que posee los datos pertinentes los somete a los investigadores.[2349]

Si bien los esfuerzos conjuntos de las autoridades competentes y los proveedores de servicios, aun cuando se carece de fundamentos jurídicos, parece ser un caso positivo de colaboración entre los sectores público y privado, una cooperación no reglamentada puede plantear diversas dificultades. Además de las consideraciones de protección de los datos, lo más inquietante es que los proveedores de servicio podrían violar sus obligaciones contractuales con sus clientes si someten ciertos datos y la solicitud correspondiente no está suficientemente fundamentada desde el punto de vista jurídico.[2350]

Artículo 18 – Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento; y

b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

El Artículo 18 contiene dos obligaciones: con arreglo al apartado 1a), cualquier persona (o incluso proveedor de servicio) está obligada a someter datos informáticos específicos que obren en su poder o estén bajo su control. A diferencia del apartado 1b), la aplicación de la disposición no se limita a datos específicos. La expresión "obrar en su poder" significa que esta persona tiene un acceso físico a los dispositivos de almacenamiento de datos en los que se encuentra la información especificada.[2351] El término "control" amplía el alcance de la disposición. Los datos están bajo control de una persona aunque no tenga acceso físico a los mismos, si gestiona la información. Tal caso se da, por ejemplo, cuando el sospechoso almacena los datos en un sistema de almacén en línea distante. En el citado Informe, los redactores del Convenio sobre la Ciberdelincuencia señalan no obstante que la mera capacidad técnica de acceder a distancia a datos almacenados no implica necesariamente que se tenga control sobre los mismos. [2352] La aplicación del Artículo 18 del Convenio sobre la Ciberdelincuencia está, pues, limitada a los casos en los cuales el grado de control por parte del sospechoso es superior a la simple posibilidad de acceder a los mismos.

El apartado 1b) contiene una orden de presentación que se limita a ciertos datos. Con arreglo a ese apartado, los investigadores pueden ordenar a un proveedor de servicio que someta información sobre un abonado, información que puede ser necesaria para identificar a un delincuente. Si los investigadores pueden descubrir la dirección IP utilizada por el delincuente, necesitan relacionar ese número con una persona.[2353] En la mayoría de los casos, la dirección IP sólo conduce al proveedor Internet que proporciona la dirección IP al usuario. Antes de autorizar la utilización de un servicio, el proveedor Internet suele pedir al usuario que se inscriba con su información de abonado.[2354] El apartado 1b) permite que los investigadores ordenen al proveedor que someta esta información. A este respecto, es importante subrayar que el Artículo 18 del Convenio sobre la Ciberdelincuencia no contempla una obligación de conservación de datos [2355] ni una obligación de que los proveedores de servicio registren información sobre los abonados.[2356]

La distinción entre "datos informáticos" del apartado 1a) y "datos relativos a los abonados" en el apartado 1b) no parece necesaria a primera vista, ya que la información sobre el abonado almacenada en formato digital también se aborda en el apartado 1a). Esta distinción se debe en primer lugar a la diferencia entre las definiciones de "datos informáticos" y de "datos relativos a los abonados". A diferencia de "datos informáticos", la expresión "datos relativos a los abonados" no significa que la información esté almacenada como datos informáticos. El apartado 1b) del Artículo 18 del Convenio sobre la Ciberdelincuencia autoriza a las autoridades competentes a someter información que no está en formato digital.[2357]

Artículo 1** – **Definiciones
A los efectos del presente Convenio:
[...]
b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

Artículo 18** – **Orden de presentación
[...]
3. A los efectos del presente Artículo, se entenderá por "datos relativos a los abonados" cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:
a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;
c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

La distinción entre "datos informáticos" e "información sobre el abonado" se debe, en segundo lugar, a que de este modo los legisladores pueden estipular diversas condiciones de aplicación de los instrumentos.[2358] Se pueden, por ejemplo, aplicar exigencias más estrictas[2359] para la orden de presentación relacionada con el apartado 1b), ya que este instrumento autoriza a las autoridades competentes a acceder a cualquier tipo de datos informáticos, incluidos datos sobre el contenido.[2360] La distinción entre la obtención en tiempo real de datos relativos al tráfico (Artículo 20)[2361] y la obtención en tiempo real de datos relativos al contenido (Artículo 21)[2362] muestra que los redactores del Convenio cayeron en la cuenta de que, dependiendo del tipo de datos de que se trate, las autoridades competentes deben tener en cuenta diversas salvaguardias.[2363] Con la distinción entre "datos informáticos" y "datos relativos a los abonados", el Artículo 18 del Convenio sobre la Ciberdelincuencia permite que los Estados signatarios elaboren un sistema similar de salvaguardias escalonadas en lo que respecta a la orden de presentación.[2364]

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

Se pueden encontrar planteamientos similares en la Ley modelo de 2002 de la Commonwealth.[2365]

Producción de datos
15. *Si, tras examinar la solicitud de un funcionario de policía, un magistrado queda convencido de que existen motivos fundados para pedir los datos informáticos especificados, o una versión impresa o información de otro tipo, a efectos de una investigación o un juicio penal, puede ordenar lo siguiente:*

(a) que una persona presente en el territorio del [país promulgador] y que controla un sistema informático extraiga del sistema datos informáticos específicos, o una versión impresa de los mismos, o una versión inteligible de los mismos;

(b) que un proveedor de servicio Internet en el [país promulgador] comunique información sobre las personas que están abonadas al servicio, o lo utilizan de algún otro modo;

(c)[2366] que una persona presente en el territorio del [país promulgador] y que tiene acceso a un sistema informático especificado, tramite y compile datos informáticos especificados del sistema y los entregue a una persona determinada.

6.5.8 Obtención de datos en tiempo real

Las escuchas telefónicas se utilizan en muchos países en investigaciones de delitos de sangre.[2367] En muchos delitos se utilizan teléfonos, especialmente móviles, ya sea en su preparación o ejecución. En el tráfico de drogas especialmente, el éxito de la investigación depende fundamentalmente de la intervención de conversaciones entre los perpetradores. El instrumento ayuda a los investigadores a obtener valiosísimas informaciones, aunque se limita a la información intercambiada por las líneas o los teléfonos intervenidos. Si el delincuente utiliza otros medios de comunicación (por ejemplo, cartas) o líneas que no están intervenidas, los investigadores no podrán registrar la conversación. Por lo general, las conversaciones cara a cara plantean las mismas dificultades.[2368]

El intercambio de datos ha sustituido hoy a las clásicas conversaciones telefónicas y no se limita a los correos electrónicos y a las transferencias de ficheros, ya que un número creciente de comunicaciones telefónicas se cursan con tecnologías de protocolo Internet (voz por IP).[2369] Desde un punto de vista técnico, las llamadas telefónicas de voz por IP son mucho más parecidas a un intercambio de correo electrónico que a una llamada telefónica clásica por línea fija, y la intervención de este tipo de llamadas plantea dificultades muy particulares.[2370]

Habida cuenta de que muchos delitos informáticos entrañan un intercambio de datos, el éxito de las investigaciones depende fundamentalmente de la capacidad de interceptar estos procesos o los datos relacionados con los mismos. En algunos países es difícil ahora aplicar las disposiciones vigentes en materia de intervención telefónica y las disposiciones relacionadas con la utilización de datos de tráfico de telecomunicaciones en las investigaciones de ciberdelitos. Las dificultades son tanto técnicas[2371] como jurídicas. Desde el punto de vista jurídico, la autorización de grabar una conversación telefónica no significa necesariamente la de interceptar los procesos de transferencia de datos.

El Convenio sobre la Ciberdelincuencia tiene por objeto subsanar las lagunas actuales que impiden a las autoridades competentes vigilar los procesos de transferencia de datos.[2372] Habida cuenta de ello, el

Convenio sobre la Ciberdelincuencia distingue entre dos tipos de observación de transferencia de datos. En el Artículo 20 se autoriza a los investigadores a obtener datos relativos al tráfico. La expresión "datos relativos al tráfico" se define en el apartado d) del Artículo 1 del Convenio sobre la Ciberdelincuencia.

Artículo 1 – Definiciones
[...]
d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de información, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño, y la duración de la comunicación o el tipo de servicio subyacente.

La distinción entre "datos relativos al contenido" y "datos relativos al tráfico" es la misma que en la mayoría de las legislaciones nacionales conexas.[2373]

6.5.9 Obtención de datos relativos al tráfico

Convenio del Consejo de Europa sobre la Ciberdelincuencia

En lo que respecta al hecho de que la definición de los datos relativos al tráfico no es la misma en todos los países,[2374] los redactores del Convenio sobre la Ciberdelincuencia decidieron definir esa expresión para mejorar la aplicación de la disposición conexa en las investigaciones internacionales. La expresión "datos relativos al tráfico" se utiliza para describir datos generados por ordenadores durante el proceso de comunicación a fin de encaminar la comunicación del origen al destino. Cuando el usuario se conecta a Internet, telecarga correos electrónicos o abre un sitio web, se generan datos de tráfico. En lo que respecta a las investigaciones de ciberdelitos, los datos de tráfico más importantes para determinar el origen y el destino son las direcciones IP que identifican a los participantes en comunicaciones por Internet.[2375]

A diferencia de "datos relativos al contenido", la expresión "datos relativos al tráfico" se refieren únicamente a los datos generados en procesos de transferencia de datos y no a los datos transferidos propiamente dichos. Si bien en algunos casos puede ser necesario acceder a los datos relativos al contenido, porque de este modo las autoridades competentes pueden analizar la comunicación mucho más eficazmente, los datos relativos al tráfico son muy importantes en las investigaciones de ciberdelitos.[2376] Si bien el acceso a los datos relativos al contenido ayuda a las autoridades competentes a analizar el tipo de mensajes o ficheros intercambiados, los datos relativos al tráfico pueden ser necesarios para identificar al infractor. En los casos de pornografía infantil, los datos relativos al tráfico pueden ayudar, por ejemplo, a los investigadores a identificar una página web en la cual el infractor telecarga imágenes de pornografía infantil. Al analizar los datos de tráfico generados durante la utilización de servicios Internet, las autoridades competentes pueden identificar las direcciones IP del servidor y tratar de determinar así su ubicación física.

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes:
- *a. a obtener o grabar con medios técnicos existentes en su territorio, y*
- *b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:*
  - *i. a obtener o a grabar con medios técnicos existentes en su territorio, o*
  - *ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.*

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente Artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente Artículo estarán sujetos a lo dispuesto en los Artículos 14 y 15.

El Artículo 20 contiene dos planteamientos diferentes de la obtención de datos relativos al tráfico, ambos aplicables.[2377]

El primer planteamiento consiste en estipular la obligación de que los proveedores de servicios Internet permitan que las autoridades competentes puedan obtener directamente los datos pertinentes. Para ello suele ser necesario instalar una interfaz que las autoridades competentes pueden utilizar para acceder a la infraestructura de los proveedores de servicio Internet.[2378]

El segundo planteamiento consiste en que las autoridades competentes obliguen al proveedor de servicio Internet a compilar datos a petición de las autoridades competentes. De este modo, los investigadores pueden utilizar las capacidades técnicas existentes y los conocimientos de que suelen disponer los proveedores. Uno de los motivos para combinar ambos planteamientos es garantizar que si los proveedores no disponen de la tecnología necesaria para registrar los datos, las autoridades competentes deben poder llevar a cabo la investigación (sobre la base del apartado 1b) del Artículo 20) sin ayuda del proveedor.[2379]

En el Convenio del Consejo de Europa sobre la Ciberdelincuencia no se da preferencia a ninguna tecnología en particular ni se definen normas que obliguen a realizar grandes inversiones financieras en el sector de que se trata.[2380] Desde este punto de vista, el apartado 1a) del Artículo 20 del Convenio sobre la Ciberdelincuencia parece ser la solución preferible. Ahora bien, lo estipulado en el punto 2 del Artículo 20 demuestra que los redactores del Convenio eran conscientes de que algunos países pueden tener dificultades para aplicar legislaciones que permitan que las autoridades competentes lleven a cabo directamente las investigaciones.

Una de las principales dificultades que se plantean en las investigaciones realizadas con arreglo al Artículo 20 es la utilización de medios de comunicación anónimos. Como ya se ha explicado anteriormente,[2381] los delincuentes pueden utilizar servicios de comunicación anónima por Internet. Si el infractor utiliza un servicio de comunicación anónima como el software TOR,[2382] en la mayoría de los casos los investigadores son incapaces de analizar satisfactoriamente los datos de tráfico e identificar a los participantes en la comunicación. El infractor puede obtener un resultado similar utilizando terminales Internet públicos.[2383]

En comparación con los procedimientos tradicionales de registro y confiscación, una de las ventajas de la obtención de datos de tráfico es que el sospechoso no cae necesariamente en la cuenta de que es objeto de una investigación[2384] , lo cual limita sus posibilidades de manipular o suprimir pruebas. A fin de garantizar que el proveedor de servicio no informe a los infractores sobre la investigación en curso, el punto 3 del Artículo 20 trata de esta situación y obliga a los Estados signatarios a adoptar legislaciones que garanticen que los proveedores de servicio garanticen a su vez la confidencialidad de la investigación. Para el proveedor de servicio tiene además la ventaja de que queda eximido de la obligación [2385] de informar a los usuarios.[2386]

El Convenio sobre la Ciberdelincuencia se concibió para mejorar y armonizar las legislaciones sobre todo lo relacionado con la ciberdelincuencia.[2387] A este respecto, es importante subrayar que el texto del Artículo 21 del Convenio no se aplica solamente a los delitos relacionados con la ciberdelincuencia, sino a todos los delitos. En lo que respecta al hecho de que la utilización de comunicaciones electrónicas puede no servir solamente para ciberdelitos, la aplicación de esta disposición en casos diferentes de los ciberdelitos puede ser útil para las investigaciones ya que, de este modo, las autoridades competentes podrían utilizar datos de tráfico generados durante intercambios de correos electrónicos entre delincuentes que preparan un delito tradicional. En el punto 3 del Artículo 14 se permite que las Partes añadan reservas y limiten la aplicación de la disposición a ciertos delitos.[2388]

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

Se puede encontrar un planteamiento similar en la Ley modelo de 2002 de la Commonwealth.[2389]

Interceptación de datos de tráfico
19. (1) Si un agente de policía está convencido de que existen motivos fundados para necesitar datos relativos al tráfico asociados con una comunicación determinada a efectos de una investigación penal, puede solicitar por escrito a la persona que controla esos datos, que:
(a) reúna o registre los datos relativos al tráfico asociados con una comunicación específica durante un periodo determinado;
(b) permita y ayude a un agente de policía determinado a reunir o registrar esos datos.
(2) Si, sobre la base de [información sometida bajo juramento] [una declaración jurada por escrito], un magistrado está convencido de que existen motivos fundados para [sospechar] de que datos relativos al tráfico son necesarios a efectos de una investigación penal, el magistrado [puede autorizar] [autorizará] a un agente de policía a reunir o registrar datos relativos al tráfico asociados con una comunicación específica durante un periodo determinado por medio de la utilización de medios técnicos.

6.5.10 Interceptación de datos relativos al contenido

Convenio del Consejo de Europa sobre la Ciberdelincuencia

Aparte de que el Artículo 21 trata de los datos relativos al contenido, su estructura es similar a la del Artículo 20. La posibilidad de interceptar procesos de intercambio de datos puede tener importancia cuando las autoridades competentes ya saben quiénes son los participantes en una comunicación pero no disponen de información sobre el tipo de información intercambiada. El Artículo 21 les ofrece la posibilidad de registrar comunicaciones de datos y analizar su contenido,[2390] ya sean ficheros telecargados de sitios web o sistemas de compartición de ficheros, correos electrónicos enviados o recibidos por el infractor o conversaciones en salas de charla.

Artículo 21 – Interceptación de datos relativos al contenido
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a:
a. obtener o grabar con medios técnicos existentes en su territorio, y
b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:
i. obtener o grabar con medios técnicos existentes en su territorio, o
ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los Artículos 14 y 15.

A diferencia de los datos relativos al tráfico, el Convenio sobre la Ciberdelincuencia no contiene una definición de los datos relativos al contenido. Como su nombre indica, "datos relativos al contenido" se refiere al contenido de la comunicación.

Los datos relativos al contenido en las investigaciones de ciberdelitos son, entre otros:

- el asunto de un correo electrónico;
- el contenido de un sitio web visitado por el sospechoso;
- el contenido de una conversación por VoIP.

Una de las mayores dificultades que plantean las investigaciones sobre la base del Artículo 21 es la utilización de tecnologías de cifrado.[2391] Como ya se ha explicado detalladamente en este documento, la utilización de tecnologías de cifrado puede ayudar a los infractores a proteger el contenido intercambiado de tal manera que a las autoridades competentes les resulte imposible acceder al mismo. Si la víctima potencial cifra el contenido que transfiere, los infractores sólo pueden interceptar la comunicación cifrada, pero no analizar su contenido. Si no disponen de acceso a la clave utilizada para cifrar los ficheros, el descifrado tomara muchísimo tiempo.[2392]

Ley modelo de la Commonwealth sobre delitos informáticos y relacionados con la informática

Se puede encontrar un planteamiento similar en la Ley modelo de 2002 de la Commonwealth.[2393]

Interceptación de comunicaciones electrónicas
18. (1) Si, sobre la base de [información sometida bajo juramento] [una declaración jurada por escrito], un [magistrado] [juez] está convencido de que existen motivos fundados para [sospechar] [creer] que el contenido de comunicaciones electrónicas es necesario a efectos de una investigación penal, [podrá ordenar] [ordenará]:

(a) a un proveedor de servicio Internet cuyo servicio esté disponible en el [país promulgador] que, utilizando medios técnicos, reúna o registre, o permita o autorice que las autoridades competentes compilen o registren los datos relativos al contenido asociados con comunicaciones específicas transmitidas por medio de un sistema informático; o

(b) [podrá autorizar] [autorizará] que un agente de policía reúna o registre esos datos utilizando medios técnicos.

6.5.11 Reglamentación de la tecnología de cifrado

Como se describe anteriormente, los infractores también pueden dificultar el análisis de datos relativos al contenido utilizando tecnologías de cifrado. Existen diversos productos informáticos que permiten proteger eficazmente ficheros y procesos de transferencia de datos contra accesos no autorizados.[2394] Si los sospechosos utilizan ese tipo de producto y los investigadores no disponen de la clave utilizada para cifrar los ficheros, el descifrado puede tomar mucho tiempo.[2395]

La utilización de tecnologías de cifrado por los infractores plantea dificultades a las autoridades competentes.[2396] Existen varios planteamientos nacionales e internacionales[2397] para abordar el problema.[2398] Dado que las estimaciones de la amenaza que representan las tecnologías de cifrado no son las mismas en todas partes, todavía no se ha aceptado de manera generalizada un sistema internacional para tratar este tema. Las soluciones más comunes son las siguientes.

Según uno de los enfoques, en las investigaciones judiciales las autoridades competentes deben poder romper las claves en caso necesario.[2399] Sin ese tipo de autorización, o sin la posibilidad de expedir una orden de presentación, los investigadores no podrían reunir las pruebas necesarias. Además, cabría la posibilidad de que los investigadores pudieran utilizar programas de registro de claves para interceptar la contraseña de un fichero cifrado y romper la clave.[2400]

Otro enfoque consiste en limitar el rendimiento de los programas de cifrado limitando la longitud de las contraseñas.[2401] Dependiendo del grado de limitación, los investigadores podrían romper la clave en un plazo razonable. Los detractores de esa solución temen que esas limitaciones ayuden a los investigadores a romper la clave, pero también a los espías económicos que tratan de acceder a información comercial cifrada.[2402] Además, esa limitación sólo impediría que los infractores utilizaran programas de cifrado más potentes si no existieran esas herramientas informáticas. Para ello, se necesitarían en primer lugar normas

internacionales que impidieran que los fabricantes de programas de cifrado potentes ofrecieran sus programas en países que no limitan de manera adecuada la longitud de las claves. En cualquier caso, los infractores podrían elaborar relativamente fácilmente sus propios programas de cifrado que no limitan la longitud de las claves.

La obligación de crear un sistema de custodia de claves o un procedimiento de recuperación de clave para los productos de cifrado avanzados.[2403] . La aplicación de ese tipo de reglamentación permitiría que los usuarios siguieran utilizando tecnologías de cifrado potentes pero también que los investigadores pudieran acceder a los datos pertinentes obligando al usuario a someter la clave a la autoridad especial que la detiene y que la facilita, en su caso, a los investigadores.[2404] Los detractores de esa solución temen que los infractores puedan acceder a las claves sometidas y utilizarlas para descifrar información confidencial. Además, los infractores podrían eludir la reglamentación relativamente fácilmente elaborando sus propios programas de cifrado sin tener que someter la clave a las autoridades.

Por último, hay países que tratan de resolver esta dificultad mediante la ejecución de una orden de presentación.[2405] Este término describe la obligación de revelar la clave utilizada para cifrar datos. La aplicación de ese tipo de instrumento se examinó en la reunión de 1997 del G8 en Denver.[2406] Varios países han llevado a efecto esas obligaciones.[2407] La Sección 69 de la Ley de 2000 sobre Tecnologías de la Información de la India es un ejemplo de aplicación nacional:[2408]. La Sección 49 de la Ley del Reino Unido de 2000 sobre la Reglamentación de los Derechos de los Investigadores [2409] es otro ejemplo de esa obligación:

Notificaciones que requieren la revelación de la información

49 *(1) Se aplicarán las disposiciones del presente Artículo siempre que una información protegida:*

(a) obre en poder de una persona como consecuencia del ejercicio de una autoridad legal para obtener, retener, inspeccionar, indagar o averiguar de otro modo a través de documentos u otros medios, o de la posibilidad de ejercerla;

(b) obre en poder de una persona como consecuencia del ejercicio de una autoridad legal para interceptar comunicaciones, o de la posibilidad de ejercerla;

(c) obre en poder de una persona como consecuencia del ejercicio de una autoridad conferida a través de una autorización en virtud del Artículo 22 (3) o de la Parte II o de una notificación en aplicación del Artículo 22(4), o de la posibilidad de ejercerla;

(d) obre en poder de una persona por haberse facilitado o revelado en aplicación de una obligación legal (resulte o no de una solicitud de información) o de la posibilidad de ejercerla; u

(e) obre, como consecuencia de cualquier otro medio lícito que no implique el ejercicio de facultades legales, en poder de cualquiera de los servicios de inteligencia, policía o de aduanas, o que pueda llegar a poder de dichos servicios de inteligencia, policía o de aduanas.

(2) Si una persona debidamente autorizada en aplicación de los supuestos de la Lista 2 considera razonablemente:

(a) que la clave para acceder a la información protegida obra en poder de una persona,

(b) que se impone emitir una orden de revelación respecto de la información protegida i) con arreglo a los motivos recogidos en el párrafo 3, o ii) a efectos de garantizar el ejercicio efectivo o la aplicación apropiada de una facultad u obligación legal por parte de cualquier autoridad pública,

(c) que el hecho de imponer el cumplimiento de la citada orden es proporcional al resultado que se espera obtener de ella, y

(d) que no cabe racionalmente esperar que la persona debidamente facultada para entrar en posesión de la información protegida pueda obtenerla en un formato inteligible sin remitir una notificación en virtud del presente Artículo, en cuyo caso la persona debidamente facultada puede, mediante notificación a la persona que considera detenta la clave, emitir una orden de revelación respecto de la información protegida.

(3) Deberá emitirse una orden de revelación respecto de cualquier información protegida por los motivos recogidos en el presente apartado siempre que:

(a) se considere necesario en interés de la seguridad nacional;

(b) tenga como finalidad impedir o descubrir un delito; o

(c) sea en defensa del bienestar económico del Reino Unido.

(4) Toda notificación de una orden de revelación respecto de cualquier información protegida:

(a) deberá comunicarse por escrito o (de no hacerse por escrito) proporcionarse de manera que su entrega quede registrada;

(b) deberá describir la información protegida a la que se refiere la notificación;

(c) deberá especificar las cuestiones abarcadas por las disposiciones del apartado (2)(b)(i) o (ii) en las que se basa la entrega de la notificación;

(d) deberá especificar la función, el rango o la posición de la persona que la emite;

(e) deberá especificar la función, el rango o la posición de la persona que, a los efectos previstos en la Lista 2, autorizó la emisión de la notificación o (en caso de que la persona que emite la notificación esté habilitada para hacerlo sin la autorización de un tercero) describir las circunstancias que dieron lugar al ejercicio de ese derecho;

(f) deberá especificar el plazo para cumplir con lo dispuesto en la notificación, y

(g) deberá explicar la revelación que se requiere en virtud de la notificación, y la forma y la manera en que habrá de procederse a dicha revelación; el plazo especificado a efectos del párrafo f) deberá prever en todo caso un plazo de cumplimiento de la notificación que sea razonable.

A fin de garantizar que la persona obligada a proceder a la revelación cumple con la orden y de hecho presenta la clave, la Ley de Poderes de Investigación del Reino Unido de 2000 incluye una disposición que califica como delito el incumplimiento de dicha orden.

Incumplimiento de una notificación

53 *(1) Se considerará culpable de un delito a toda persona a la que se haya entregado una notificación en aplicación del Artículo 49 y a sabiendas, no proceda a la revelación exigida en virtud de la entrega de la notificación.*

(2) En el proceso judicial entablado contra cualquier persona por un delito previsto en el presente Artículo, si se demuestra que una clave para acceder a una información protegida obraba en poder de dicha persona en cualquier momento anterior a la entrega de la notificación del Artículo 49, se entenderá, a efectos de dicho proceso, que dicha clave siguió ulteriormente en su poder, salvo que se demuestre que la clave citada no obraba en su poder después de la entrega de la notificación ni antes del momento en que se le exigió su revelación.

(3) A los efectos del presente Artículo, se entenderá que una persona habrá demostrado no estar en posesión de una clave para acceder a una información protegida en un momento determinado si:

(a) se aportan pruebas suficientes de ello para que pueda cuestionarse, y

(b) no se demuestre lo contrario más allá de toda duda razonable.

(4) En el proceso judicial seguido contra cualquier persona acusada de un delito previsto en el presente Artículo, la persona podrá alegar en su defensa:

(a) que no podía razonablemente proceder a la revelación exigida en virtud de la entrega de la notificación del Artículo 49 antes del momento en que se le exigió en virtud de dicha notificación, pero

(b) que procedió a dicha revelación tan pronto le resultó posible razonablemente proceder a la misma.

(5) Toda persona culpable de un delito previsto en este Artículo podrá verse infligir:

(a) en caso de condena a raíz de un proceso con jurado, una pena de cárcel de hasta dos años, o una multa, o ambas;

(b) en caso de una condena por un juez, una pena de cárcel no superior a seis meses o una multa por un importe no superior al máximo legal, o ambos.

[...]

La Ley de 2000 sobre la Reglamentación de los Derechos de los Investigadores obliga al sospechoso de un delito a facilitar la labor de las autoridades competentes.[2410]

Una inquietud de carácter general es que la obligación puede conducir a un posible conflicto con los derechos fundamentales del sospechoso contra la autoincriminación.[2411] En lugar de dejar la investigación en manos de las autoridades competentes, el sospechoso debe facilitar activamente las investigaciones. La fuerte protección contra la autoincriminación en muchos países impulsa a preguntarse en qué medida esa

reglamentación puede convertirse en una solución modelo para las dificultades que plantea la tecnología de cifrado.[2412]

Otra inquietud es que perder la clave podría dar lugar a una investigación judicial. Si bien la tipificación penal exige que el infractor se niegue intencionalmente a revelar la clave, perder la misma podría entrañar la utilización de la clave de cifrado en investigaciones judiciales no deseadas y, especialmente el apartado 2 del Artículo 53 podría interferir con la carga de la prueba.[2413]

Varias soluciones técnicas ayudan a los infractores a eludir la obligación de revelar la clave utilizada para cifrar datos. Se trata, por ejemplo, del infractor que utiliza un programa de cifrado basado en el principio de "capacidad de denegación verosímil"[2414].[2415]

6.5.12 Software forense a distancia

Como ya se ha explicado, para buscar pruebas en el ordenador de un sospechoso se necesita acceder físicamente al equipo en cuestión (sistema informático y medios de almacenamiento externos), lo cual obliga a su vez a visitar el apartamento, la casa o la oficina del sospechoso. En este caso, el sospechoso estará enterado de la investigación en curso tan pronto como los investigadores la inicien,[2416] lo cual podría incitarlo a cambiar de comportamiento.[2417] Si, por ejemplo, el infractor ataca varios sistemas informáticos para probar sus capacidades y participar posteriormente en la preparación de una serie de ataques mucho más amplios junto con otros infractores, el registro podría impedir que los investigadores identificaran a los demás sospechosos, ya que es muy probable que el infractor dejara de comunicar con ellos.

Para impedir que se puedan detectar las investigaciones en curso, las autoridades competentes piden un instrumento que les permita acceder a datos informáticos almacenados en el ordenador del sospechoso y que puedan utilizar discretamente, de modo similar a las escuchas telefónicas.[2418] Ese instrumento les permitiría acceder a distancia al ordenador del sospechoso y buscar la información. La cuestión de determinar si esos instrumentos son necesarios o no es actualmente objeto de acalorados debates.[2419] En 2001 se señalaba ya en varios Informes que el FBI de Estados Unidos estaba desarrollando un registrador de teclas llamado "lámpara mágica" para las investigaciones relacionadas con Internet.[2420] En 2007 se publicaron Informes según los cuales las autoridades competentes de Estados Unidos utilizaban programas informáticos para seguir el rastro de sospechosos que utilizaban medios de comunicación anónimos.[2421] Los Informes se referían a una orden de allanamiento cuando era preciso utilizar[2422] una herramienta llamada CIPAV [2423]. Después de que el Tribunal Federal de Alemania dictaminara que las disposiciones de la Ley Procesal Penal vigente no permitían que los investigadores utilizaran software judicial a distancia para analizar en secreto el ordenador de un sospechoso, comenzó un debate sobre la necesidad de enmendar la legislación vigente en esta materia.[2424] En el curso del debate se divulgó que las autoridades de investigación habían utilizado ilegalmente software forense a distancia en un par de investigaciones.[2425]

Se han estudiado varios conceptos de "software forense a distancia" y, especialmente, sus posibles funciones,[2426] que, teóricamente, podrían ser las siguientes: la función de registro – Esta función permitiría que los organismos competentes registraran contenidos ilegales y compilaran información sobre los ficheros almacenados en el ordenador;[2427] la función de grabación – los investigadores podrían grabar datos tratados en el sistema informático del sospechoso pero no almacenados permanentemente; si, por ejemplo, el sospechoso utiliza servicios de voz por IP para comunicar con otros sospechosos, normalmente no se almacena el contenido de las conversaciones.[2428] El software forense a distancia podría grabar los datos procesados y conservarlos para que los pudieran consultar los investigadores. Si el software forense a distancia contiene un módulo que registra los golpes de tecla, se podría utilizar para registrar las contraseñas que utiliza el sospechoso para cifrar sus archivos.[2429] Además, una herramienta de este tipo podría incluir funciones de identificación que permitirían a los investigadores demostrar la participación del sospechoso en un delito, aun si utiliza servicios de comunicación anónimos que impiden que los investigadores identifiquen al infractor siguiendo el rastro de la dirección IP utilizada.[2430] Por último, el software se podría utilizar a distancia para activar una webcam o el micrófono para observar el recinto.[2431]

Si bien las posibles funciones del software parecen muy útiles para los investigadores, se ha de señalar que la utilización de ese software plantea diversas dificultades jurídicas y técnicas. Desde el punto de vista técnico, se ha de tener en cuenta lo siguiente:

Dificultades de instalación

El software se ha de instalar en el sistema informático del sospechoso. La gran difusión de software maliciosos demuestra que se puede instalar software en el ordenador de un usuario de Internet sin que éste dé su permiso, pero la diferencia principal entre un virus y un software judicial a distancia es que este último debe instalarse en un sistema informático determinado (el ordenador del sospechoso), mientras que un virus informático trata de infectar tantos ordenadores como pueda sin concentrarse en un sistema en particular. Existen diversas técnicas para transmitir el software al ordenador del sospechoso. Por ejemplo, entre otras muchas, instalación con acceso físico al sistema informático, colocación del software en un sitio web para que se pueda telecargar, acceso en línea al sistema informático burlando las medidas de seguridad, y ocultación del software en el flujo de datos generado durante actividades Internet.[2432] Habida cuenta de las medidas de protección de que disponen la mayoría de los ordenadores, tales como buscadores de virus y cortafuegos, todos los métodos de instalación a distancia plantean dificultades a los investigadores.[2433]

Ventaja del acceso físico

Varios de los análisis realizados (por ejemplo, la inspección física de medios de tratamiento de datos) exigen un acceso al equipo. Además, el software judicial a distancia sólo permitiría analizar sistemas informáticos que están conectados a Internet.[2434] Por otra parte, es difícil mantener la integridad del sistema informático del sospechoso.[2435] En lo que respecta a estas últimas consideraciones, por lo general el software judicial a distancia no puede remplazar el examen físico del sistema informático del sospechoso.

Además, antes de llevar a efecto una disposición que autoriza a los investigadores a instalar software judiciales a distancia, también se han de tener en cuenta varios aspectos jurídicos. Las garantías que contienen los códigos de derecho penal y las constituciones de muchos países limitan las funciones que puede tener ese software. Además de las consideraciones meramente nacionales, la instalación de software judicial a distancia podría violar el principio de soberanía nacional.[2436] Si el software está instalado en un ordenador portátil que sale del país después de su instalación, el software puede ayudar a los investigadores a llevar a cabo investigaciones judiciales en un país extranjero sin haber recibido permiso de las autoridades competentes.

Ejemplo

En el texto legislativo desarrollado por los Estados beneficiarios en el marco de la iniciativa HIPCAR se presenta una manera de enfocar la cuestión.[2437]

Software forense

27. *(1) Si, sobre la base de la [información facilitada bajo juramento/declaración jurada], un [juez] [magistrado] considera que en la investigación de un delito enumerado en el párrafo 5 infra existen motivos razonables para creer que no pueden recabarse pruebas fundamentales por medio de otros instrumentos indicados en la Parte IV, pero que dichas pruebas son razonablemente necesarias para la investigación penal, el [juez] [magistrado] [podrá/deberá] autorizar, previa solicitud, al agente policial a utilizar software forense con la finalidad específica de la investigación e instalarlo en el sistema informático del sospechoso con el fin de obtener las pruebas pertinentes. La solicitud deberá contener la siguiente información:*

(a) el sospechoso del delito, con nombre y dirección si es posible,

(b) una descripción del sistema informático objeto del procedimiento,

(c) una descripción de lo que se desea medir, la amplitud y duración de la utilización, y

(d) los motivos por los que se ha de recurrir a este procedimiento.

(2) En el marco una investigación de esta índole, es necesario garantizar que la modificación del sistema informático del sospechoso se limita a lo estrictamente necesario para la investigación y que dicha modificación es reversible una vez concluida la investigación. Durante la investigación se habrá de registrar:

(a) el mecanismo técnico utilizado y la hora y fecha de su aplicación;

(b) la identificación del sistema informático y las modificaciones introducidas en el marco de la investigación; y

c) toda la información obtenida.

La información obtenida mediante este software debe protegerse contra cualquier alteración, supresión o acceso no autorizados.
(3) la duración de la autorización estipulada en la sección 27 1) se limita a [3 meses]. Si se dejaran de cumplir las condiciones de la autorización, se detendrá inmediatamente el procedimiento.
(4) la autorización de instalar el software comprende el acceso a distancia al sistema informático del sospechoso.
(5) Si el proceso de instalación requiere el acceso físico, se habrán de cumplir lo estipulado en la sección 20.
(6) En caso necesario, un agente [encargado de hacer cumplir de la ley] [de policía] podrá, en virtud de la orden judicial concedida en 1) supra, solicitar que el juzgado exija la colaboración del proveedor de servicios en el proceso de instalación.
(7) [Lista de delitos]
(8) El país podrán tomar la decisión de no aplicar la sección 27.

Los redactores del texto legislativo señalaron que son conscientes de que la aplicación del instrumento podría ser muy intrusiva y atentar contra los derechos fundamentales del sospechoso.[2438] Por ese motivo se han impuesto diversas salvaguardias. En primer lugar, este software sólo puede emplearse cuando no se pueda obtener pruebas por otros medios. En segundo lugar, se requiere una orden de un juez o magistrado. En tercer lugar, la aplicación tiene que contener cuatro elementos esenciales. Además, los actos autorizados se limitan en los párrafos 1 y 2.

6.5.13 Obligación de autorización

El infractor puede tomar varias medidas para complicar las investigaciones. Además de utilizar software de comunicación anónima,[2439] la identificación puede complicarse si el sospechoso utiliza terminales Internet públicos o redes inalámbricas abiertas. La limitación de la producción de software que ayuda al usuario a ocultar su identidad, y de la posibilidad de utilizar terminales públicos que no exigen identificación para acceder a Internet, podría ayudar a las autoridades competentes a llevar a cabo más eficazmente sus investigaciones. Un ejemplo de limitación de la utilización de terminales públicos para cometer delitos es el Artículo 7[2440] del Decreto 144[2441] italiano, que tomó carácter de ley en 2005 (Legge Nº 155/2005). [2442] En esta disposición se obliga a todo el que proyecte ofrecer acceso Internet público (por ejemplo, cafés Internet o universidades [2443]) a solicitar una autorización. Además, tiene la obligación de exigir que sus clientes se identifiquen antes de darles acceso al servicio. En lo que respecta al hecho de que una persona física que crea un punto de acceso inalámbrico no suele estar afectada por esta obligación, los infractores pueden eludir la vigilancia con relativa facilidad si utilizan redes privadas no protegidas para ocultar su identidad.[2444]

Es discutible que la voluntad de mejorar la eficacia de las investigaciones justifique la limitación del acceso a Internet y a servicios de comunicación anónimos. Todos reconocen hoy que el acceso libre a Internet es un elemento importante del derecho a acceder libremente a la información, y que está protegido por la constitución de varios países. La obligación de registrarse puede atentar contra el derecho a utilizar servicios Internet sin autorización, como se subraya en la Declaración Conjunta de 2005 del Relator Especial de las Naciones Unidas para la libertad de opinión y de expresión, el Representante de la OSCE para la Libertad de los Medios de Comunicación y el Relator Especial de la OEA para la Libertad de Expresión.[2445] Es probable que la obligación de identificarse afecte a los usuarios de Internet, ya que siempre temerán que se vigilen sus actividades en Internet. Aun cuando los usuarios saben que sus actividades son legales, pueden modificar su comportamiento y utilización. [2446] Por otra parte, los infractores que desean permanecer anónimos pueden eludir fácilmente el procedimiento de identificación utilizando, por ejemplo, tarjetas telefónicas de pago previo adquiridas en un país extranjero que no exige identificación para acceder a Internet.

La legislación sobre los servicios de comunicaciones anónimas también suscita inquietudes similares. Hay un debate abierto sobre si debe aplicarse la tecnología de encriptación a los servicios y tecnologías de comunicaciones anónimas.[2447] Aparte del conflicto entre proteger la privacidad y garantizar la posibilidad de investigar delitos, los argumentos sobre la viabilidad de las diversas formas legales de enfocar el

problema de la encriptación (especialmente la falta de capacidad para obligar a utilizarla) se aplican igualmente a la comunicación anónima.

6.6 Cooperación internacional

Bibliografía (seleccionada): *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4; *Choo,* Trends in Organized Crime, 2008, page 273 *et seq.*; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005; *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992; *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2; *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296; *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931; *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9; *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.6.1 Introducción

Cada vez más, los ciberdelitos adquieren dimensión internacional.[2448] Como ya se ha indicado, esto se debe a que prácticamente no es necesario que el delincuente esté físicamente presente en el lugar en que se ofrece un servicio.[2449] Por este motivo, tampoco necesitan estar presentes en el lugar en que se localiza a la víctima. Como no existe un marco jurídico internacional exhaustivo ni una entidad supranacional facultada para investigar tales delitos, la investigación de la delincuencia transnacional exige la cooperación de las autoridades de los países implicados.[2450] La movilidad de los infractores, la independencia del lugar donde éstos se encuentra y la incidencia del delito hacen imprescindible que las fuerzas de seguridad y las autoridades judiciales colaboren y ayuden al país que ha asumido la jurisdicción del caso.[2451] Debido a las diferencias en la legislación nacional y a los escasos instrumentos, la cooperación internacional se considera una de las principales dificultades que entraña la globalización de la delincuencia.[2452], tanto en lo que respecta a las formas tradicionales de delito como a la ciberdelincuencia. En el marco de una investigación transnacional, una de las principales exigencias de los investigadores es la reacción inmediata de sus homólogos en el país en que se ha localizado al delincuente.[2453] . En lo que se refiere a esta cuestión en especial, los instrumentos tradicionales de asistencia mutua no cumplen, en la mayoría de los casos, los requisitos relativos a la rapidez de las investigaciones en Internet.[2454]

6.6.2 Mecanismos de cooperación internacional

Los mecanismos oficiales más importantes de cooperación internacional para la investigación de ciberdelitos son la asistencia mutua y la extradición. Otros mecanismos, tales como la transferencia de prisioneros, la transferencia de procedimientos en materia legal, el decomiso y la confiscación de activos,

revisten menos importancia en la práctica. Además de los mecanismos oficiales, existen formas oficiosas de cooperar, como el intercambio de información entre las autoridades competentes de varios países.

6.6.3 Descripción de los instrumentos aplicables

Para determinar el instrumento aplicable de cooperación internacional pueden distinguirse tres casos principales. En primer lugar, los procedimientos pertinentes pueden formar parte de acuerdos internacionales, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC)[2455] y sus tres Protocolos[2456], o convenios regionales, tales como la a Convención Interamericana sobre Asistencia Mutua en Materia Penal[2457], Convenio Europeo de Asistencia Mutua en Materia Penal [2458] y el Convenio del Consejo de Europa sobre la Ciberdelincuencia.[2459] La segunda posibilidad es reglamentar los procedimientos mediante acuerdo bilaterales. Estos acuerdo se refieren, en general, a solicitudes específicas que pueden presentarse y a definir los correspondientes procedimientos y las formas de entrar en contacto, así como los derechos y obligaciones de los Estados que presentan y reciben dichas solicitudes.[2460] Australia, por ejemplo, ha firmado más de 30 acuerdos bilaterales con otros países en materia de extradición.[2461] En la negociación de tales acuerdos se ha tenido en cuenta en algunos casos el tema de la ciberdelincuencia, por no se sabe a ciencia cierta en qué medida los acuerdos existentes rigen adecuadamente el ciberdelito. [2462] Si no existe ningún acuerdo multilateral o bilateral aplicable, la cooperación internacional tendrá que basarse generalmente en cortesía internacional, es decir en la reciprocidad. [2463] Dado que la cooperación basada en acuerdos bilaterales y en la cortesía depende sobremanera de las circunstancias reales del caso y de los países implicados, a continuación se resumen los convenios internacionales y regionales.

6.6.4 Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC) es el principal instrumento internacional para la cooperación judicial en materia penal. [2464] Esta Convención consta de importantes instrumentos de cooperación, pero no se ha concebido para tratar específicamente problemas de ciberdelincuencia, ni tampoco dispone de disposiciones específicas relativas a solicitudes urgentes para preservar datos.

Aplicación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

En virtud del párrafo 1 del Artículo 3, la Convención sólo es aplicable a los casos de ciberdelincuencia en los que el infractor forma parte de un grupo delictivo organizado. En el Artículo 2 de la UNTOC se define como un grupo estructurado de tres o más personas.

> ***Artículo 2. Definiciones***
> *Para los fines de la presente Convención:*
> *(a) Por "grupo delictivo organizado" se entenderá un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material;*
> *[...]*
>
> ***Artículo 3. Ámbito de aplicación***
> *1. A menos que contenga una disposición en contrario, la presente Convención se aplicará a la prevención, la investigación y el enjuiciamiento de:*
> *(a) Los delitos tipificados con arreglo a los Artículos 5, 6, 8 y 23 de la presente Convención; y*
> *(b) Los delitos graves que se definen en el Artículo 2 de la presente Convención; cuando esos delitos sean de carácter transnacional y entrañen la participación de un grupo delictivo organizado.*

Así, la Convención es particularmente pertinente para los casos en los que participa el crimen organizado. No cabe duda de que el crimen organizado también se dedica a la ciberdelincuencia. No obstante, se

desconoce su grado de implicación y, por ende, la pertinencia de la UNTOC en la investigación de la ciberdelincuencia internacional es incierta. De hecho, determinar la participación del crimen organizado es importantísimo. Sin embargo, analizar el vínculo entre los delitos relacionados con la identidad y el crimen organizado presenta dificultades. El principal obstáculo es la falta de un investigación científicamente fiable en este campo. A diferencia de los aspectos técnicos de los delitos, la implicación del crimen organizado no se analiza en gran profundidad. Si bien algunas investigaciones han logrado identificar diversas bandas criminales implicadas en ciberdelitos, la estructura de dichas bandas no es comparable a las de los grupos tradicionales del crimen organizado. Los grupos de ciberdelincuentes tienen una estructura más dispersa y flexible.[2465] Por otra parte, suelen ser grupos mucho más pequeños que los grupos tradicionales del crimen organizado.[2466] Internet permite una estrecha cooperación y coordinación de actividades sin tener que haberse conocido en persona. [2467] Por eso es factible que los infractores colaboren en grupos ad hoc cambiantes.[2468].

Solicitudes de asistencia judicial recíproca

Los procedimientos de asistencia judicial recíproca se definen en el Art. 18, que contiene un conjunto completo de procedimientos.

Artículo 18. Asistencia judicial recíproca
1. Los Estados Parte se prestarán la más amplia asistencia judicial recíproca respecto de investigaciones, procesos y actuaciones judiciales relacionados con los delitos comprendidos en la presente Convención con arreglo a lo dispuesto en el Artículo 3 y se prestarán también asistencia de esa índole cuando el Estado Parte requirente tenga motivos razonables para sospechar que el delito a que se hace referencia en los apartados a) o b) del párrafo 1 del Artículo 3 es de carácter
transnacional, así como que las víctimas, los testigos, el producto, los instrumentos A/RES/55/25
17 o las pruebas de esos delitos se encuentran en el Estado Parte requerido y que el delito entraña la participación de un grupo delictivo organizado.
2. Se prestará asistencia judicial recíproca en la mayor medida posible conforme a las leyes, tratados, acuerdos y arreglos pertinentes del Estado Parte requerido con respecto a investigaciones, procesos y actuaciones judiciales relacionados con los delitos de los que una persona jurídica pueda ser considerada responsable de conformidad con el Artículo 10 de la presente Convención en el Estado Parte requirente. [...]

Los párrafos 1) - 2) del Artículo 18 describen los principios generales para la cooperación internacional.[2469] Estos principios se aplican tanto a la investigación de ciberdelitos como a la investigación tradicional. El Convenio del Consejo de Europa sobre la Ciberdelincuencia contiene una reglamentación similar.

Artículo 18. Asistencia judicial recíproca
[...]
3. La asistencia judicial recíproca que se preste de conformidad con el presente artículo podrá solicitarse para cualquiera de los fines siguientes:
(a) Recibir testimonios o tomar declaración a personas;
(b) Presentar documentos judiciales;
(c) Efectuar inspecciones e incautaciones y embargos preventivos;
(d) Examinar objetos y lugares;
(e) Facilitar información, elementos de prueba y evaluaciones de peritos;
(f) Entregar originales o copias certificadas de los documentos y expedientes pertinentes, incluida la documentación pública, bancaria y financiera, así como la documentación social o comercial de sociedades mercantiles;
(g) Identificar o localizar el producto del delito, los bienes, los instrumentos u otros elementos con fines probatorios;
(h) Facilitar la comparecencia voluntaria de personas en el Estado Parte requirente;
(i) Cualquier otro tipo de asistencia autorizada por el derecho interno del Estado Parte requerido.
[…]

En el párrafo 3) del Art. 18 se especifican las solicitudes de asistencia judicial recíproca. La lista es compleja y varía desde facilitar pruebas a localizar el producto del delito. Como ya se ha indicado antes, la UNTOC no contiene texto específico sobre solicitudes relacionadas con datos, como las de intervenir la comunicación o preservar datos. Ahora bien, el Art. 18 (3) i) deja abierta la posibilidad de solicitar otro tipo de asistencia, por lo que puede apelarse a la UNTOC para solicitudes relacionadas con datos. Aunque en general merece la pena examinar las ventajas de disponer una reglamentación específica en materia de solicitudes de asistencia, instrumentos regionales comparables que contemplan solicitudes específicas, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia, se suelen referir únicamente a instrumentos de procedimiento en la legislación nacional, sin definir procedimientos específicos para la solicitud de asistencia judicial recíproca.

Artículo 18. Asistencia judicial recíproca
[...]
4. Sin menoscabo del derecho interno, las autoridades competentes de un Estado Parte podrán, sin que se les solicite previamente, transmitir información relativa a cuestiones penales a una autoridad competente de otro Estado Parte si creen que esa información podría ayudar a la autoridad a emprender o concluir con éxito indagaciones y procesos penales o podría dar lugar a una petición formulada por este último Estado Parte con arreglo a la presente Convención.
5. La transmisión de información con arreglo al párrafo 4 del presente artículo se hará sin perjuicio de las indagaciones y procesos penales que tengan lugar en el Estado de las autoridades competentes que facilitan la información. Las autoridades competentes que reciben la información deberán acceder a toda solicitud de que se respete su carácter confidencial, incluso temporalmente, o de que se impongan restricciones a su utilización. Sin embargo, ello no obstará para que el Estado Parte receptor revele, en sus actuaciones, información que sea exculpatoria de una persona acusada. En tal caso, el Estado Parte receptor notificará al Estado Parte transmisor antes de revelar dicha información y, si así se le solicita, consultará al Estado Parte transmisor. Si, en un caso excepcional, no es posible notificar con antelación, el Estado Parte receptor informará sin demora al Estado Parte transmisor de dicha revelación.
[…]

Los párrafos 4)-5) del Artículo 18 tratan del intercambio de información. Estipulan una forma de cooperación[2470] voluntaria, sin necesidad de que la parte requirente presente una solicitud de asistencia judicial recíproca.[2471] Comprende información relativa a cuestiones penales, como la relativa a posibles consumidores de pornografía infantil residentes en otro país que se han descubierto durante una investigación. Especialmente en el caso de investigaciones complejas, cuando recurrir a instrumentos oficiales recíprocos conlleva mucho tiempo y, por lo tanto, pueden entorpecer las investigaciones, las fuerzas del orden tenderán a recurrir a mecanismo de cooperación no oficiales. Ahora bien, la compartición de información sólo será de utilidad si el Estado que la recibe es capaz de recabar por su cuenta todas las pruebas necesarias. En todos los demás casos, suele ser necesaria la cooperación oficial en cualquier evento para garantizar la cadena de custodia. Al debatir acerca de la evolución de la cooperación internacional desde la solicitud oficial hacia el intercambio espontáneo de información, es necesario tener presente que el proceso oficial se elaboró para proteger la integridad del Estado y los derechos del acusado. Por consiguiente, el intercambio de información no debería sortear la estructura dogmática de la asistencia jurídica recíproca.

Artículo 18. Asistencia judicial recíproca
[...]
6. Lo dispuesto en el presente artículo no afectará a las obligaciones dimanantes de otros tratados bilaterales o multilaterales vigentes o futuros que rijan, total o parcialmente, la asistencia judicial recíproca.

7. Los párrafos 9 a 29 del presente artículo se aplicarán a las solicitudes que se formulen con arreglo al presente artículo siempre que no medie entre los Estados Parte interesados un tratado de asistencia judicial recíproca. Cuando esos Estados Parte estén vinculados por un tratado de esa índole se aplicarán las disposiciones correspondientes de dicho tratado, salvo que los Estados Parte convengan en aplicar, en su lugar, los párrafos 9 a 29 del presente artículo. Se insta encarecidamente a los Estados Parte a que apliquen estos párrafos si facilitan la cooperación.
8. Los Estados Parte no invocarán el secreto bancario para denegar la asistencia judicial recíproca con arreglo al presente artículo.
9. Los Estados Parte podrán negarse a prestar la asistencia judicial recíproca con arreglo al presente artículo invocando la ausencia de doble incriminación. Sin embargo, de estimarlo necesario, el Estado Parte requerido podrá prestar asistencia, en la medida en que decida hacerlo a discreción propia, independientemente de que la conducta esté o no tipificada como delito en el derecho interno del Estado Parte requerido.

10. La persona que se encuentre detenida o cumpliendo una condena en el territorio de un Estado Parte y cuya presencia se solicite en otro Estado Parte para fines de identificación, para prestar testimonio o para que ayude de alguna otra forma a obtener pruebas necesarias para investigaciones, procesos o actuaciones judiciales respecto de delitos comprendidos en la presente Convención podrá ser trasladada si se cumplen las condiciones siguientes:

(a) La persona, debidamente informada, da su libre consentimiento;

(b) Las autoridades competentes de ambos Estados Parte están de acuerdo, con sujeción a las condiciones que éstos consideren apropiadas.

11. A los efectos del párrafo 10 del presente artículo:

(a) El Estado Parte al que se traslade a la persona tendrá la competencia y la obligación de mantenerla detenida, salvo que el Estado Parte del que ha sido trasladada solicite o autorice otra cosa;

(b) El Estado Parte al que se traslade a la persona cumplirá sin dilación su obligación de devolverla a la custodia del Estado Parte del que ha sido trasladada, según convengan de antemano o de otro modo las autoridades competentes de ambos Estados Parte;

(c) El Estado Parte al que se traslade a la persona no podrá exigir al Estado Parte del que ha sido trasladada que inicie procedimientos de extradición para su devolución;

(d) El tiempo que la persona haya permanecido detenida en el Estado Parte al que ha sido trasladada se computará como parte de la pena que ha de cumplir en el Estado del que ha sido trasladada.

12. A menos que el Estado Parte desde el cual se ha de trasladar a una persona de conformidad con los párrafos 10 y 11 del presente artículo esté de acuerdo, dicha persona, cualquiera que sea su nacionalidad, no podrá ser enjuiciada, detenida, condenada ni sometida a ninguna otra restricción de su libertad personal en el territorio del Estado al que sea trasladada en relación con actos, omisiones o condenas anteriores a su salida del territorio del Estado del que ha sido trasladada
[…]

Los párrafo 6)-12) del Art. 18 versan sobre los procedimientos relativos a la asistencia judicial recíproca. Los párrafos 8 y 9 revisten especial interés para los casos de ciberdelincuencia. El párrafo 9 autoriza a los Estados a negarse a prestar asistencia judicial recíproca por razones de ausencia de doble incriminación. Esto es especialmente importante ya que por el momento el alcance de los métodos para armonizar las disposiciones penales sustantivas relativas a la ciberdelincuencia – como el Convenio del Consejo de Europa sobre la Ciberdelincuencia – es muy limitado. A mediados del decenio de 2010, sólo 30 países habían ratificado este instrumento y establecido las correspondientes normas mínimas sobre ciberdelitos, lo que puede dificultar la cooperación basada en la UNTOC.

Artículo 18. Asistencia judicial recíproca
[...]
13. Cada Estado Parte designará a una autoridad central encargada de recibir solicitudes de asistencia judicial recíproca y facultada para darles cumplimiento o para transmitirlas a las autoridades competentes para su ejecución. Cuando alguna región o algún territorio especial de un Estado Parte disponga de un régimen distinto de asistencia judicial recíproca, el Estado Parte podrá designar a otra autoridad central que desempeñará la misma función para dicha región o dicho territorio. Las autoridades centrales velarán por el rápido y adecuado cumplimiento o transmisión de las solicitudes recibidas. Cuando la autoridad central transmita la solicitud a una autoridad competente para su ejecución, alentará la rápida y adecuada ejecución de la solicitud por parte de dicha autoridad. Cada Estado Parte notificará al Secretario General de las Naciones Unidas, en el momento de depositar su instrumento de ratificación, aceptación o aprobación de la presente Convención o de adhesión a ella, el nombre de la autoridad central que haya sido designada a tal fin. Las solicitudes de asistencia judicial recíproca y cualquier otra comunicación pertinente serán transmitidas a las autoridades centrales designadas por los Estados Parte. La presente disposición no afectará al derecho de cualquiera de los Estados Parte a exigir que estas solicitudes y comunicaciones le sean enviadas por vía diplomática y, en circunstancias urgentes, cuando los Estados Parte convengan en ello, por conducto de la Organización Internacional de Policía Criminal, de ser posible.
14. Las solicitudes se presentarán por escrito o, cuando sea posible, por cualquier medio capaz de registrar un texto escrito, en un idioma aceptable para el Estado Parte requerido, en condiciones que permitan a dicho Estado Parte determinar la autenticidad. Cada Estado Parte notificará al Secretario General de las Naciones Unidas, en el momento de depositar su instrumento de ratificación, aceptación o aprobación de la presente Convención o de adhesión a ella, el idioma o idiomas que sean aceptables para cada Estado Parte. En situaciones de urgencia, y cuando los Estados Parte convengan en ello, las solicitudes podrán hacerse oralmente, debiendo ser confirmadas sin demora por escrito.
15. Toda solicitud de asistencia judicial recíproca contendrá lo siguiente:
(a) La identidad de la autoridad que hace la solicitud;
(b) El objeto y la índole de las investigaciones, los procesos o las actuaciones judiciales a que se refiere la solicitud y el nombre y las funciones de la autoridad encargada de efectuar dichas investigaciones, procesos o actuaciones;
(c) Un resumen de los hechos pertinentes, salvo cuando se trate de solicitudes de presentación de documentos judiciales;
(d) Una descripción de la asistencia solicitada y pormenores sobre cualquier procedimiento particular que el Estado Parte requirente desee que se aplique;
(e) De ser posible, la identidad, ubicación y nacionalidad de toda persona interesada; y
(f) La finalidad para la que se solicita la prueba, información o actuación.
16. El Estado Parte requerido podrá pedir información complementaria cuando sea necesaria para dar cumplimiento a la solicitud de conformidad con su derecho interno o para facilitar dicho cumplimiento.
[…]

Los párrafos 13-16) del Artículo 18 definen el formato y el contenido de las solicitudes, así como los canales de comunicación. En lo que respecta a estos canales, la Convención se basa en la idea de que las solicitudes se transmiten de una autoridad central a otra.[2472] La Convención subraya la importancia de este procedimiento para acelerar y ejecutar adecuadamente la solicitud. Las funciones de la autoridad central pueden ser diferentes y variar desde la participación directa en la tramitación y ejecución de las solicitudes hasta su transmisión a las autoridades competentes. El Convenio deja a los Estados la opción de transmitir las solicitudes por canales diplomáticos. Esta opción es un proceso lento, que ralentizaría excesivamente la transmisión e impediría especialmente la adopción de medidas urgentes, tales como la preservación de los datos de tráfico. A diferencia del Convenio del Consejo de Europa sobre la Ciberdelincuencia[2473], la UNTOC no define mecanismos de cooperación acelerada, pero ofrece un procedimiento general para casos urgentes. Si el Estado está de acuerdo, puede recurrirse a la Organización Internacional de Policía Criminal (Interpol) como canal de comunicación. Para facilitar la identificación de la autoridad competente en otro país, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) mantiene un directorio en

línea.[2474] Proporciona a la autoridad requirente información detallada sobre la autoridad central del Estados requerido, los canales de comunicación y otra información pertinente.[2475]

Al presentar la solicitud, es necesario cumplir los requisitos oficiales definidos en los párrafos 14 y 15. Las solicitudes podrán hacerse oralmente sólo en caso de emergencia y habrán de ser confirmadas sin demora por escrito. Los informes de los Estados Parte relativos a la aplicación de la Convención muestran que si bien la legislación de muchos Estados exige que las solicitudes de asistencia judicial recíproca se hagan por escrito, sólo unos cuantos admiten que se les transmita por correo electrónico una solicitud temporal previa.[2476] A este respecto, la UNTOC difiere del Convenio del Consejo de Europa sobre la Ciberdelincuencia, que insta a los Estados a utilizar medios de comunicación electrónica en casos urgentes.[2477] La UNODC suministra un software para redactar tales solicitudes con el fin de garantizar su integridad (Programa para redactar solicitudes de asistencia judicial recíproca).[2478]

Artículo 18. Asistencia judicial recíproca

[...]

17. Se dará cumplimiento a toda solicitud con arreglo al derecho interno del Estado Parte requerido y en la medida en que ello no lo contravenga y sea factible, de conformidad con los procedimientos especificados en la solicitud.

18. Siempre que sea posible y compatible con los principios fundamentales del derecho interno, cuando una persona se encuentre en el territorio de un Estado Parte y tenga que prestar declaración como testigo o perito ante autoridades judiciales de otro Estado Parte, el primer Estado Parte, a solicitud del otro, podrá permitir que la audiencia se celebre por videoconferencia si no es posible o conveniente que la persona en cuestión comparezca personalmente en el territorio del Estado Parte requirente. Los Estados Parte podrán convenir en que la audiencia esté a cargo de una autoridad judicial del Estado Parte requirente y en que asista a ella una autoridad judicial del Estado Parte requerido.

19. El Estado Parte requirente no transmitirá ni utilizará, sin previo consentimiento del Estado Parte requerido, la información o las pruebas proporcionadas por el Estado Parte requerido para investigaciones, procesos o actuaciones judiciales distintos de los indicados en la solicitud. Nada de lo dispuesto en el presente párrafo impedirá que el Estado Parte requirente revele, en sus actuaciones, información o pruebas que sean exculpatorias de una persona acusada. En este último caso, el Estado Parte requirente notificará al Estado Parte requerido antes de revelar la información o las pruebas y, si así se le solicita, consultará al Estado Parte requerido. Si, en un caso excepcional, no es posible notificar con antelación, el Estado Parte requirente informará sin demora al Estado Parte requerido de dicha revelación.

20. El Estado Parte requirente podrá exigir que el Estado Parte requerido mantenga reserva acerca de la existencia y el contenido de la solicitud, salvo en la medida necesaria para darle cumplimiento. Si el Estado Parte requerido no puede mantener esa reserva, lo hará saber de inmediato al Estado Parte requirente.

21. La asistencia judicial recíproca podrá ser denegada:

(a) Cuando la solicitud no se haga de conformidad con lo dispuesto en el presente artículo;

(b) Cuando el Estado Parte requerido considere que el cumplimiento de lo solicitado podría menoscabar su soberanía, su seguridad, su orden público u otros intereses fundamentales;

(c) Cuando el derecho interno del Estado Parte requerido prohíba a sus autoridades actuar en la forma solicitada con respecto a un delito análogo, si éste hubiera sido objeto de investigaciones, procesos o actuaciones judiciales en el ejercicio de su propia competencia;

(d) Cuando acceder a la solicitud sea contrario al ordenamiento jurídico del Estado Parte requerido en lo relativo a la asistencia judicial recíproca.

22. Los Estados Parte no podrán denegar una solicitud de asistencia judicial recíproca únicamente porque se considere que el delito también entraña asuntos fiscales.

23. Toda denegación de asistencia judicial recíproca deberá fundamentarse debidamente.

24. El Estado Parte requerido cumplirá la solicitud de asistencia judicial recíproca lo antes posible y tendrá plenamente en cuenta, en la medida de sus posibilidades, los plazos que sugiera el Estado Parte requirente y que estén debidamente fundamentados, de preferencia en la solicitud. El Estado Parte requerido responderá a las solicitudes razonables que formule el Estado Parte requirente respecto de la evolución del trámite de la solicitud. El Estado Parte requirente informará con prontitud cuando ya no necesite la asistencia solicitada.

25. La asistencia judicial recíproca podrá ser diferida por el Estado Parte requerido si perturbase investigaciones, procesos o actuaciones judiciales en curso.
26. Antes de denegar una solicitud presentada con arreglo al párrafo 21 del presente artículo o de diferir su cumplimiento con arreglo al párrafo 25 del presente artículo, el Estado Parte requerido consultará al Estado Parte requirente para considerar si es posible prestar la asistencia solicitada supeditándola a las condiciones que estime necesarias. Si el Estado Parte requirente acepta la asistencia con arreglo a esas condiciones, ese Estado Parte deberá observar las condiciones impuestas.

27. Sin perjuicio de la aplicación del párrafo 12 del presente artículo, el testigo, perito u otra persona que, a instancias del Estado Parte requirente, consienta en prestar testimonio en un juicio o en colaborar en una investigación, proceso o actuación judicial en el territorio del Estado Parte requirente no podrá ser enjuiciado, detenido, condenado ni sometido a ninguna otra restricción de su libertad personal en ese territorio por actos, omisiones o declaraciones de culpabilidad anteriores a la fecha en que abandonó el territorio del Estado Parte requerido. Ese salvoconducto cesará cuando el testigo, perito u otra persona haya tenido, durante quince días consecutivos o durante el período acordado por los Estados Parte después de la fecha en que se le haya informado oficialmente de que las autoridades judiciales ya no requerían su presencia, la oportunidad de salir del país y no obstante permanezca voluntariamente en ese territorio o regrese libremente a él después de haberlo abandonado.
28. Los gastos ordinarios que ocasione el cumplimiento de una solicitud serán sufragados por el Estado Parte requerido, a menos que los Estados Parte interesados hayan acordado otra cosa. Cuando se requieran a este fin gastos cuantiosos o de carácter extraordinario, los Estados Parte se consultarán para determinar las condiciones en que se dará cumplimiento a la solicitud, así como la manera en que se sufragarán los gastos.
29. El Estado Parte requerido:
(a) Facilitará al Estado Parte requirente una copia de los documentos oficiales y otros documentos o datos que obren en su poder y a los que, conforme a su derecho interno, tenga acceso el público en general;
(b) Podrá, a su arbitrio y con sujeción a las condiciones que juzgue apropiadas, proporcionar al Estado Parte requirente una copia total o parcial de los documentos oficiales o de otros documentos o datos que obren en su poder y que, conforme a su derecho interno, no estén al alcance del público en general.
30. Los Estados Partes contemplarán, en su caso, la posibilidad de concluir acuerdos o arreglos bilaterales o multilaterales a los efectos de las disposiciones de este artículo, o para darles efecto práctico o mejorarlas.

6.6.5 Convenio del Consejo de Europa sobre la Ciberdelincuencia

El Convenio del Consejo de Europa sobre la Ciberdelincuencia (el "Convenio sobre la Ciberdelincuencia") aborda la cada vez más importante cuestión de la cooperación internacional en sus Artículos 23 a 35.

Principios generales de la cooperación internacional

El Artículo 23 del Convenio sobre la Ciberdelincuencia define tres principios generales relativos a la cooperación internacional entre los Miembros en las investigaciones sobre ciberdelitos.

Artículo 23 – Principios generales relativos a la cooperación internacional
Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

En primer lugar, se da por descontado que los Miembros cooperarán en la mayor medida posible en las investigaciones internacionales. Esta obligación pone de manifiesto la importancia de la cooperación

internacional en las investigaciones sobre ciberdelitos. Asimismo, el Artículo 23 estipula que los principios generales no sólo se aplican a las investigaciones sobre ciberdelitos sino también a cualquier otra investigación para la cual sea necesaria la obtención de pruebas electrónicas de los delitos. Ello abarca tanto a las investigaciones sobre ciberdelitos como a las de delitos tradicionales. Si una persona sospechosa de haber cometido un asesinato utilizó un servicio de correo electrónico en el extranjero, el Artículo 23 se aplicaría a las investigaciones necesarias con respecto a los datos almacenados por el proveedor.[2479] El tercer principio recuerda que las disposiciones relativas a la cooperación internacional no sustituyen las correspondientes a acuerdos internacionales en lo que concierne a la asistencia jurídica mutua y a la extradición ni las disposiciones pertinentes de la legislación nacional sobre cooperación internacional. Los redactores del Convenio pusieron de relieve que la asistencia mutua se llevará en general a la práctica mediante la aplicación de los correspondientes tratados y acuerdos similares en la materia. Por consiguiente, el Convenio no procura crear un régimen general autónomo de asistencia mutua. A raíz de ello, únicamente cuando los tratados, la legislación y los acuerdos en vigor no contemplen ya dichas disposiciones, se solicita a cada Parte el establecimiento de una base jurídica que propicie la cooperación internacional definida en el Convenio.[2480]

Extradición

La extradición de nacionales sigue siendo uno de los aspectos más difíciles de la cooperación internacional.[2481] Las solicitudes de extradición plantean a menudo un conflicto entre la necesidad de proteger al ciudadano y la necesidad de respaldar una investigación en curso en otro país. El Artículo 24 define los principios de extradición. A diferencia del Artículo 23, la disposición se limita a los delitos mencionados en el Convenio y no se aplica en delitos menores (privación de libertad de una duración máxima de un año como mínimo[2482]). Para evitar los conflictos que pudieran plantearse con respecto a la capacidad de las Partes de formular reservas, el Artículo 24 se funda en el principio de la doble tipificación penal.[2483]

Artículo 24 – Extradición
1a. El presente Artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los Artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.
b. Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE Nº 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.
2. Se considerará que los delitos mencionados en el apartado 1 del presente Artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.
3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente Artículo.
4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el apartado 1 del presente Artículo como delitos que pueden dar lugar a extradición entre ellas.
5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente Artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.
7a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.
b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Principios generales de asistencia mutua

Con respecto a la asistencia mutua, el Artículo 25 contempla disposiciones complementarias de los principios establecidos en el Artículo 23. Una de las disposiciones más importantes del Artículo 25 figura en el apartado 3, que hace hincapié en la importancia que adquieren los medios rápidos de comunicación en las investigaciones sobre ciberdelitos.[2484] . Como se ha indicado anteriormente, numerosas investigaciones sobre ciberdelitos en el ámbito nacional no han prosperado debido a su prolongada duración y a la consiguiente eliminación de datos importantes antes de que se adoptaran medidas de procedimiento para preservarlos. [2485] En general, las investigaciones que necesitan la asistencia jurídica mutua son más prolongadas aún a causa del tiempo que consumen las comunicaciones oficiales entre las autoridades competentes. El Convenio tiene en cuenta este problema e insiste en la importancia de facilitar la utilización de medios rápidos de comunicación.[2486]

Artículo 25** – **Principios generales relativos a la asistencia mutua
1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.
2. Cada Parte adoptará también las medidas legislativas y de otro tipo que resulten necesarias para cumplir las obligaciones establecidas en los Artículos 27 a 35.
3. En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.
4. Salvo que se establezca específicamente otra cosa en los Artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los Artículos 2 a 11 únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.
5. Cuando, de conformidad con las disposiciones del presente Capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente.

En las investigaciones sobre ciberdelitos emprendidas en el ámbito nacional podrían descubrirse ciertos nexos con delitos cometidos en otro país. Si las autoridades competentes, por ejemplo, investigan un delito de pornografía infantil, podrían hallar información de otros países con respecto a pedófilos que han participado en el intercambio de pornografía infantil.[2487] El Artículo 26 estipula las disposiciones necesarias para que dichas autoridades comuniquen a sus homólogos en el extranjero la información correspondiente sin poner en peligro su propia investigación.[2488]

Artículo 26** – **Información espontánea
1. Dentro de los límites de su derecho interno, y sin petición previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente Capítulo.

2. Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

Como se ha mencionado antes, la sustitución de la asistencia judicial recíproca por información espontánea suscita cierta preocupación. la compartición de información sólo será de utilidad si el Estado que la recibe es capaz de recabar por su cuenta todas las pruebas necesarias. En todos los demás casos, suele ser necesaria la cooperación oficial en cualquier evento para garantizar la cadena de custodia. Al debatir acerca de la evolución de la cooperación internacional desde la solicitud oficial hacia el intercambio espontáneo de información, es necesario tener presente que el proceso oficial se elaboró para proteger la integridad del Estado y los derechos del acusado. Por consiguiente, el intercambio de información no debería sortear la estructura dogmática de la asistencia jurídica recíproca.

Una de las disposiciones más importantes del Artículo 26 es la confidencialidad de la información. En relación con el hecho de que numerosas investigaciones sólo podrán llegar a buen término si el delincuente no tiene conocimiento de ellas, el Artículo 26 autoriza a la Parte informante a solicitar que se preserve la confidencialidad de la información transmitida. Si no puede preservarse dicha confidencialidad, la Parte informante puede negarse a facilitar esa información.

Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Al igual que el Artículo 25, el Artículo 27 está inspirado en la idea de la conveniencia de que la asistencia jurídica mutua se lleve a cabo a través de la aplicación de tratados y acuerdos similares en la materia y no esté sujeta únicamente a las disposiciones del Convenio. Los redactores del Convenio decidieron no establecer un régimen autónomo de asistencia jurídica mutua obligatoria.[2489] Si otros instrumentos estuvieran vigentes, no se aplicarán los Artículos 27 y 28 a una solicitud concreta. Únicamente en casos en que no se apliquen otras disposiciones, los Artículos 27 y 28 estipulan una serie de mecanismos a los que se puede recurrir para formular solicitudes de asistencia jurídica mutua.

Los aspectos más importantes estipulados en el Artículo 27 son la obligación de establecer un punto de contacto disponible para las solicitudes de asistencia jurídica mutua [2490], la comunicación directa entre puntos de contacto para evitar procedimientos excesivamente prolongados [2491] y la creación de una base de datos con todos los puntos de contacto por parte del Secretario General del Consejo de Europa.

Por otra parte, el Artículo 27 define ciertos límites con respecto a las solicitudes de asistencia. Las Partes en el Convenio pueden denegar su cooperación especialmente en relación con delitos políticos, o si consideran que la cooperación podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Si bien, por un lado, los redactores del Convenio consideraron que era necesario habilitar a las Partes a denegar en ciertos casos su cooperación, señalaron, por el otro, que las Partes deberían recurrir a ese derecho con moderación para evitar entrar en conflicto con principios establecidos con anterioridad.[2492] Por consiguiente, reviste especial importancia definir con exactitud la expresión "otros intereses esenciales". En el Informe Explicativo del Convenio sobre la Ciberdelincuencia se indica que con esa expresión se contemplaría el caso en que la cooperación planteara dificultades de carácter fundamental a la Parte requerida.[2493] Desde la perspectiva de los redactores del Convenio, los aspectos vinculados a la aplicación de una legislación inadecuada en materia de protección de datos no se consideran intereses esenciales.[2494]

Asistencia mutua en materia de medidas provisionales

Los Artículos 28 a 33 contemplan los instrumentos de procedimiento del Convenio sobre la Ciberdelincuencia.[2495] Los numerosos instrumentos de este tipo concebidos en el Convenio tienen por finalidad mejorar los resultados de las investigaciones llevadas a cabo en los Estados Miembros.[2496] En lo que concierne al principio de soberanía nacional, dichos instrumentos sólo podrán ser aplicados en el ámbito nacional[2497], dichos instrumentos sólo podrán ser aplicados en el ámbito nacional.[2498] Si los investigadores estiman necesario obtener pruebas fuera de su territorio, deberán solicitar asistencia jurídica mutua. A excepción del Artículo 18, a cada uno de los instrumentos establecidos por los Artículos 16 a 21 corresponde una disposición en los Artículos 28 a 33, que habilita a las autoridades competentes a aplicar los instrumentos de procedimiento a petición de una autoridad competente en el extranjero.

Instrumento de procedimiento	Disposición correspondiente
Artículo 16 – Conservación rápida de datos informáticos almacenados[2499]	Artículo 29
Artículo 17 – Conservación y revelación parcial rápidas de datos sobre el tráfico[2500]	Artículo 30
Artículo 18 – Orden de presentación[2501]	Ninguna
Artículo 19 – Registro y confiscación de datos informáticos almacenados[2502]	Artículo 31
Artículo 20 – Obtención en tiempo real de datos sobre el tráfico[2503]	Artículo 33
Artículo 21 – Interceptación de datos sobre el contenido[2504]	Artículo 34

Acceso transfronterizo a datos informáticos almacenados

Aparte de la atención consagrada a las disposiciones en materia de procedimiento, los redactores del Convenio examinaron las circunstancias en el marco de las cuales las autoridades competentes están autorizadas a tener acceso a datos informáticos no almacenados en su territorio ni sujetos al control de una persona en ese mismo territorio. Los redactores sólo se pusieron de acuerdo con respecto a dos situaciones en que la investigación debería quedar en manos de una autoridad competente sin necesidad de solicitar asistencia jurídica mutua.[2505] No se pudieron concertar nuevos acuerdos [2506] e incluso los Estados Miembros del Consejo de Europa siguen poniendo en tela de juicio la solución alcanzada.[2507]

Las dos situaciones mencionadas se refieren:

- a la información a disposición del público; y/o
- al acceso con el consentimiento de la persona autorizada a divulgar esos datos.

Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público

Una Parte podrá, sin la autorización de otra Parte:

a. tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o

b. tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

El Artículo 32 no abarca otras situaciones, pero tampoco las prohíbe.[2508]

Por otra parte, el Artículo 32 estipula que si los datos se encuentran a disposición del público, las autoridades extranjeras competentes están autorizadas a tener acceso a esa información. Un ejemplo de este tipo de información es la que figura en las páginas web sin control de acceso (como las contraseñas). Si los investigadores a diferencia de cualquier otro usuario no estuvieran autorizados a acceder a esas páginas web, su labor podría tener serias dificultades. Por consiguiente, se logró la aceptación general de la primera situación contemplada por el Artículo 32.

La segunda situación en la que se autoriza a las autoridades competentes el acceso a datos informáticos almacenados fuera de su territorio tiene lugar cuando los investigadores han obtenido el consentimiento legal y voluntario de la persona autorizada a divulgar esos datos. Esta autorización ha sido objeto de intensas críticas.[2509]

Una de las mayores preocupaciones es que, en su redacción actual, la disposición es probablemente contraria a los principios fundamentales del derecho internacional.[2510] Según éste, los investigadores deben respetar la soberanía nacional durante una investigación.[2511] En particular, no están autorizados a llevar a cabo investigaciones en otro Estado sin el consentimiento de las autoridades competentes de dicho Estado. La decisión de conceder dicha autorización no depende de un individuo, sino de las autoridades del Estado, dado que la injerencia en la soberanía nacional no afecta exclusivamente a los derechos del individuo, sino también al Estado. Al ratificar el Convenio sobre la Ciberdelincuencia, los países renuncian en parte este principio y permiten a otros países realizar investigaciones que afectan a su territorio.

Otro aspecto que suscita inquietud es que el Artículo 32b no define los procedimientos de la investigación. Según el texto del mismo, no es necesario aplicar las mismas limitaciones que existen en la legislación nacional para investigaciones comparables de ámbito nacional. Resulta bastante curioso que en el proyecto de texto del Convenio sobre la Ciberdelincuencia presentado a principios de 2000 figuraba dicha restricción, pero luego se eliminó en el 22º proyecto.[2512]

Al crear el punto b del Artículo 32, los redactores del Convenio sobre la Ciberdelincuencia contravinieron en última instancia la estructura dogmática del régimen de asistencia judicial recíproca de este Convenio. Mediante el Artículo 18, los redactores del Convenio permiten a los investigadores ordenar la comunicación de datos en las investigaciones de ámbito nacional. Si se desea autorizar a las fuerzas del orden a utilizar este instrumento en las investigaciones de alcance internacional, bastaría con incluirlo en el catálogo de instrumentos mencionados en el contexto de la asistencia judicial recíproca. Sin embargo, el instrumento no puede aplicarse en investigaciones internacionales debido a la ausencia de la correspondiente disposición en el Capítulo 3 del Convenio. En lugar de renunciar a la estructura dogmática permitiendo a los investigadores que se pongan directamente en contacto con la persona autorizada a divulgar esos datos y le soliciten su presentación, los redactores podrían haber incluido simplemente la correspondiente disposición en el Capítulo 3 del Convenio.[2513]

El acceso transfronterizo a datos informáticos almacenados también se debatió en la Conferencia Ministerial del G8 sobre la Lucha contra el Delito Transnacional, celebrada en Moscó el año 1999.[2514] Uno de los resultados de la reunión fue la compilación de principios relativos al acceso transfronterizo.[2515] Este fue con toda probabilidad el modelo utilizado por los redactores del Convenio sobre la Ciberdelincuencia, con el que guarda ciertas similitudes.

6. Acceso transfronterizo a datos informáticos almacenados que no requiere asistencia judicial
Salvo que se estipule lo contrario en estos Principios, no será necesario que un Estado obtengan la autorización de otro Estado cuando actúe de conformidad con su legislación nacional para los fines de:

(a) tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos

(b) acceder, buscar, copiar o incautar datos almacenados en sistemas informáticos situados en otro Estado, siempre y cuando actúe de conformidad con el consentimiento legal y voluntario de la persona autorizada a divulgar esos datos. El Estado que busca estos datos debe considerar la posibilidad de notificarlo al Estado donde éstos se encuentran, siempre que dicha notificación esté autorizada en la legislación nacional y los datos revelen un quebrantamiento del derecho penal o pueden resultar de interés para el Estado afectado.

La principal diferencia radica en el procedimiento de notificación estipulado en el punto 6 b). El propósito de esta disposición es la compartición inteligente. Ahora bien, la introducción de algunas modificaciones podría garantizar que los Estados afectados estuvieran al corriente de las investigaciones que tienen lugar en su territorio. Aunque no evitaría el conflicto con el derecho internacional, al menos garantizaría cierto grado de transparencia.

Red de contactos 24/7

Las investigaciones sobre ciberdelitos exigen habitualmente una reacción inmediata.[2516] Como ya se ha indicado, esto ocurre especialmente cuando se trata de obtener datos de tráfico necesarios para identificar a un sospechoso, dado que a menudo se eliminan con bastante rapidez.[2517] Para acelerar las investigaciones internacionales, el Convenio sobre la Ciberdelincuencia europeo, en su Artículo 25, pone de relieve la importancia de propiciar la utilización de medios rápidos de comunicación. Con miras a lograr que las solicitudes de asistencia mutua sean más eficaces, los redactores del Convenio han obligado a las Partes a designar un punto de contacto disponible sin limitaciones de tiempo para garantizar la prestación de asistencia inmediata.[2518] Los redactores del Convenio recordaron que esta disposición es uno de los instrumentos más importantes del Convenio sobre la Ciberdelincuencia.[2519] Sin embargo, el examen reciente de la utilización de los puntos de contacto 24/7 en países que han ratificado el Convenio sobre la ciberdelincuencia indica que su utilización es muy limitada.

Artículo 35 – Red 24/7
1. Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a. el asesoramiento técnico;

b. la conservación de datos en aplicación de los Artículos 29 y 30;

c. la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

2a. El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.
b. Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.
3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

La Red 24/7 está inspirada en la red de contactos durante las 24 horas del día de International High Tech Crime del G8[2520]. Con la creación de una red de puntos de contacto 24/7, los redactores del Convenio procuran tener en cuenta los problemas que plantea la lucha contra el ciberdelito, en particular los vinculados a la rapidez de los procedimientos de intercambio de datos[2521] y que adquieren dimensión internacional.[2522] Las Partes en el Convenio están obligadas a establecer esos puntos de contacto, a

garantizar que estén en condiciones de realizar ciertas acciones inmediatas y a mantener dicho servicio. Como se estipula en el apartado 3 del Artículo 35 del Convenio, se debe garantizar la disponibilidad de personal debidamente formado y equipado.

En lo que respecta al procedimiento para establecer los puntos de contacto y, en especial, a los principios fundamentales de esta estructura, el Convenio otorga máxima flexibilidad a los Estados Miembros. El Convenio no impone la creación de una nueva autoridad ni determina a qué autoridad ya existente podría o debería adscribirse el punto de contacto. Los redactores del Convenio hicieron además hincapié en que el hecho de que el objetivo de la red de puntos de contacto 24/7 sea prestar asistencia técnica y jurídica dará lugar a diversas opciones posibles con respecto a su realización.

Con respecto a las investigaciones sobre ciberdelitos, la instalación de puntos de contacto tiene dos funciones principales, a saber facilitar la rapidez de la comunicación proporcionando un sólo punto de contacto, y acelerar las investigaciones autorizando al punto de contacto a llevar a cabo inmediatamente ciertas investigaciones. Combinando ambas funciones se puede lograr que la celeridad de las investigaciones internacionales sea equivalente a la de las investigaciones nacionales.

El Artículo 32 del Convenio sobre la Ciberdelincuencia define las aptitudes mínimas requeridas del punto de contacto. Aparte de proporcionar asistencia técnica e información jurídica, sus principales tareas son la preservación de los datos, la obtención de pruebas, y la localización de sospechosos.

También en este contexto resulta importante recordar que el Convenio no define qué autoridad convendría que fuera responsable del funcionamiento de la red de puntos de contacto 24/7. Si el punto de contacto está en manos de una autoridad con atribuciones para ordenar la preservación de los datos,[2523] y un punto de contacto en el extranjero solicita dicha preservación, el punto de contacto local puede ordenar inmediatamente esa medida. Si la autoridad a cargo del punto de contacto no tiene esa atribución, es importante que el punto de contacto pueda, sin ninguna demora, ponerse en contacto con las autoridades competentes para garantizar la aplicación inmediata de esa medida.[2524]

En la 2ª Reunión de la Comisión del Convenio sobre la Ciberdelincuencia se destacó explícitamente que la participación en la red de puntos de contacto 24/7 no requiere la firma del Convenio ni su ratificación.[2525]

En 2008, el Consejo de Europa publicó un estudio que analiza la eficacia de la cooperación internacional contra la ciberdelincuencia.[2526] En 2009, se llevó a cabo un estudio específico sobre el funcionamiento de los puntos de contacto 24/7.[2527] Uno de los resultados de estos estudios es que no todos los países que han ratificado el Convenio sobre la Ciberdelincuencia han creado los puntos de contacto 24/7 que exige el mismo. Otro resultado es que los países que sí han creado puntos de contacto los suelen utilizar para fines muy limitados, tales como la preservación de datos de tráfico.

6.6.6 Cooperación internacional en el Proyecto de Convenio Internacional de Stanford

Los redactores del Proyecto de Convenio Internacional de Stanford (el "Proyecto de Stanford") [2528] reconocieron la importancia de la dimensión internacional del ciberdelito y los problemas que entraña. Para afrontarlos, incorporaron disposiciones específicas que tienen en cuenta la cooperación internacional. Las disposiciones del Proyecto abarcan los siguientes temas:

- Artículo 6 – Asistencia jurídica mutua
- Artículo 7 – Extradición
- Artículo 8 – Actuaciones penales
- Artículo 9 – Medidas paliativas provisorias
- Artículo 10 – Derechos de una persona acusada
- Artículo 11 – Cooperación en el cumplimiento de la ley

Se observan numerosas similitudes entre este enfoque y el adoptado en el Convenio sobre la Ciberdelincuencia. La principal diferencia radica en que las disposiciones del Convenio europeo son más estrictas, más complejas y su definición más precisa en comparación con las del Proyecto de Convenio de

Stanford. Como señalaron los redactores de este Proyecto, el Convenio sobre la Ciberdelincuencia tiene un carácter más práctico y, por consiguiente, algunas ventajas claras con respecto a su aplicación real.[2529] Por lo tanto, los redactores del Proyecto decidieron seguir un enfoque diferente puesto que previeron que la implantación de nuevas tecnologías podría plantear ciertas dificultades. A raíz de ello, sólo formularon algunas instrucciones generales sin especificarlas más detalladamente.[2530]

6.7 Responsabilidad de los proveedores de Internet

Bibliografía (seleccionada): *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Luotonen*, Web Proxy Servers, 1997; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.7.1 Introducción

Cometer un ciberdelito implica automáticamente a numerosas personas y actividades, aunque el delincuente haya actuado solo. Dada la estructura de Internet, la transmisión de un simple mensaje electrónico requiere el servicio de un cierto número de proveedores.[2531] Además del proveedor de correo electrónico, en la transmisión participan proveedores de acceso y encaminadores que envían el correo al destinatario. Con la descarga de películas que contienen imágenes de pornografía infantil, ocurre algo similar. En el procedimiento de descarga intervienen el proveedor de contenido que colocó las imágenes (por ejemplo, en una página web), el proveedor de alojamiento de datos que facilita los medios de almacenamiento en la página web, los encaminadores que envían los archivos al usuario y, por último, el proveedor que autoriza el acceso del usuario a Internet.

Debido a las numerosas partes que intervienen en este proceso, los proveedores de servicios Internet (PSI) han sido siempre el centro de interés de investigaciones de delitos en los que se utilizan los servicios que esos proveedores proporcionan.[2532] Uno de los principales motivos de dicho interés radica en que cuando la acción del delincuente se sitúa en el extranjero, los proveedores localizados dentro de los límites de las fronteras nacionales pueden ser objeto de investigación sin que se viole el principio de la soberanía nacional.[2533]

Dado que, por una parte, un ciberdelito no puede cometerse sin la intervención de los proveedores y que, por otra parte, los proveedores no tienen generalmente la capacidad de evitarlo, se ha planteado la pregunta de si resulta conveniente o no poner límites a la responsabilidad de los proveedores de Internet.[2534] Hallar la respuesta es esencial para el desarrollo económico de la infraestructura de las TIC. Los proveedores explotarán sus servicios únicamente si pueden evitar que se tipifique como delito su modo de funcionamiento habitual. Por otra parte, las autoridades competentes también tienen gran interés en esta cuestión puesto que, con suma frecuencia, su labor depende de la cooperación de los proveedores de

Internet y de la que puedan mantener con ellos. Esta situación despierta ciertas inquietudes en el sentido de que poner límites a la responsabilidad de los proveedores de Internet por actos cometidos por sus usuarios podría afectar la cooperación y respaldo de dichos proveedores en las investigaciones sobre ciberdelitos, así como la prevención real de los mismos.

6.7.2 El enfoque utilizado en los Estados Unidos

Se han adoptado diferentes enfoques que tratan de establecer un equilibrio entre la necesidad, por un lado, de la participación activa de los proveedores en las investigaciones y, por el otro, de la limitación de los riesgos de la responsabilidad penal de la acción de terceros.[2535] Puede hallarse un ejemplo de este enfoque legislativo en los § 517(a) y (b) del 17 USC (Código de los Estados Unidos).

§ 512. Limitaciones de responsabilidad con respecto al material en línea
(a) Comunicaciones de redes digitales transitorias
Un proveedor de servicio no estará obligado a conceder una compensación económica ni, salvo en el caso estipulado en la subsección (j), un desagravio por mandato judicial ni otro tipo de reparación equitativa, por la violación de derechos de autor debido a la transmisión o encaminamiento de material a través de un sistema o red controlados o explotados por o para el proveedor de servicio, o al establecimiento de conexión para tales fines, ni debido al almacenamiento intermedio o transitorio de dicho material en el curso de la transmisión, encaminamiento o establecimiento de conexión, si –

(1) la transmisión del material fue iniciada por una persona distinta del proveedor de servicio o en una dirección distinta a la de ese proveedor;

(2) la transmisión, el encaminamiento, el establecimiento de conexión o el almacenamiento se llevan a cabo a través de un procedimiento técnico automático sin selección del material por parte del proveedor de servicio;

(3) el proveedor de servicio no selecciona los destinatarios del material, salvo como respuesta automática a la solicitud de otra persona;

(4) en el sistema o red no se mantiene, de manera habitualmente accesible a cualquiera aparte de los destinatarios previstos, ninguna copia del material efectuada por el proveedor de servicio en el curso de ese tipo de almacenamiento intermedio o transitorio, y si en el sistema o red no se mantiene ninguna de dichas copias de manera habitualmente accesible a los destinatarios previstos durante un periodo de tiempo tan prolongado como sea razonablemente necesario para la transmisión, encaminamiento o establecimiento de conexión; y si

(5) el material es transmitido a través del sistema o red sin modificación de su contenido.

(b) Sistema de almacenamiento especial

(1) Limitaciones de responsabilidad.– Un proveedor de servicio no estará obligado a conceder una compensación económica ni, salvo en el caso estipulado en la subsección (j), un desagravio por mandato judicial ni otro tipo de reparación equitativa, por la violación de derechos de autor debido al almacenamiento intermedio o temporal de material en un sistema o red controlados o explotados por o para dicho proveedor en caso de que –

(A) el material haya sido colocado en línea por una persona distinta del proveedor de servicio;

(B) el material es transmitido por la persona descrita en el subapartado (A) a través del sistema o red a otra persona que no sea la descrita en dicho subapartado, a la dirección de esa otra persona; y

(C) el almacenamiento se realice a través de un procedimiento técnico automático con la finalidad de poner el material a disposición de los usuarios del sistema o red quienes, una vez que el material es transmitido tal como se indica en el subapartado (B), solicitan el acceso al material de la persona descrita en el subapartado (A),

si se cumplen las condiciones estipuladas en el apartado (2).

[…]

Esta disposición se inspira en la DMCA (Ley de Derechos de Autor del Milenio Digital), promulgada en 1998.[2536] Mediante la creación de un régimen de protección, la DMCA exceptúa de responsabilidad a los proveedores de ciertos servicios por violaciones de derechos de autor cometidas por terceros.[2537] En este contexto, es importante en primer lugar poner de relieve que no todos los proveedores están abarcados en la limitación.[2538] Las limitaciones de responsabilidad se aplican únicamente a proveedores de servicio[2539] y proveedores de sistemas de almacenamiento especial.[2540] También es importante recordar que la responsabilidad está vinculada a ciertos requisitos. Con respecto a los proveedores de servicio, esos requisitos son los siguientes:

- la transmisión del material fue iniciada por una persona distinta del proveedor de servicio o en una dirección distinta a la de ese proveedor;
- la transmisión se lleva a cabo a través de un procedimiento técnico automático sin selección del material por parte del proveedor de servicio;
- el proveedor de servicio no selecciona los destinatarios del material;
- en el sistema o red no se mantiene, de manera habitualmente accesible a cualquiera aparte de los destinatarios previstos, ninguna copia del material efectuada por el proveedor de servicio en el curso de ese tipo de almacenamiento intermedio o transitorio.

Otro ejemplo de limitaciones de responsabilidad a proveedores de Internet basada en la Ley de Decencia de las Comunicaciones [2541] puede consultarse en el § 230(c) del 47 USC:

> ***§ 230. Protección del particular que bloquea y filtra material ofensivo***
> *[...]*
> ***(c) Protección del "Buen Samaritano" que bloquea y filtra material ofensivo***
> *(1) Tratamiento de editor y portavoz*
> *Ningún proveedor ni usuario de un servicio informático interactivo será considerado editor o portavoz de ningún tipo de información proporcionada por otro proveedor de contenido.*
> *(2) Responsabilidad civil*
> *Ningún proveedor ni usuario de un servicio informático interactivo podrá ser considerado responsable de:*
> *(A) ninguna acción llevada a cabo voluntariamente y de buena fe con objeto de restringir el acceso a material que considere obsceno, lascivo, excesivamente violento, hostil u objetable por otros motivos, o la disponibilidad del mismo, esté o no dicho material protegido por instrumentos constitucionales; ni de*
> *(B) ninguna acción llevada a cabo para facilitar o poner a disposición de proveedores de contenido u otros proveedores los medios técnicos necesarios para restringir el acceso al tipo de material descrito en el apartado (1).*
> *[…]*

Las disposiciones del § 512(a) del 17 USC y del § 230(c) del 47 USC, tienen en común que otorgan prioridad a la responsabilidad con respecto a grupos especiales de proveedores y ámbitos especiales de la ley. En lo que resta del Capítulo se dará por tanto una visión general del enfoque legislativo adoptado por la Unión Europea, que es partidaria de un concepto más amplio.

6.7.3 Directiva de la Unión Europea sobre comercio electrónico

La Directiva de la Unión Europea sobre comercio electrónico es un ejemplo de enfoque legislativo destinado a la reglamentación de la responsabilidad de los proveedores de Internet.[2542] Confrontados a las dificultades derivadas de la dimensión internacional que ha adquirido Internet, los redactores de la Directiva decidieron elaborar normas que faciliten un marco jurídico para la construcción general de la sociedad de la información, y de esta forma respaldar el desarrollo económico global así como la labor de las autoridades competentes. [2543] Las disposiciones relativas a la responsabilidad se inspiran en el principio de responsabilidad progresiva.

La Directiva estipula numerosas disposiciones que limitan la responsabilidad de ciertos proveedores.[2544] Las limitaciones están relacionadas con las diferentes categorías de servicios prestados por el proveedor.[2545] Todos los demás casos no están necesariamente exceptuados de responsabilidad y, al menos que otras disposiciones estipulen esas limitaciones, el aludido es plenamente responsable. La finalidad de la Directiva es limitar la responsabilidad a los casos en que el proveedor tiene sólo posibilidades mínimas, debido posiblemente a cuestiones de carácter técnico, de evitar el delito. Por ejemplo, los encaminadores, sin una pérdida considerable de velocidad, no pueden filtrar los datos que les transfieren y difícilmente evitar procedimientos de intercambio de datos. Los proveedores de alojamiento de datos pueden eliminar datos si tienen conocimiento de actividades delictivas. Sin embargo, como ocurre con los encaminadores, los grandes proveedores de alojamiento de datos no tienen la capacidad de controlar todos los datos almacenados en sus servidores.

En lo que concierne a la capacidad variable para controlar realmente las actividades delictivas, la responsabilidad de los proveedores de alojamiento de datos y de los proveedores de acceso no es la misma. En este sentido, hay que tener en cuenta que el equilibrio de la Directiva se basa en normas técnicas vigentes. Por ahora, no se dispone de herramientas que permitan detectar automáticamente imágenes pornográficas desconocidas. Si los avances técnicos en esta esfera continúan, tal vez haya que evaluar en el futuro la capacidad técnica de los proveedores y, en caso necesario, adaptar el sistema.

6.7.4 Responsabilidad del proveedor de acceso (Directiva de la Unión Europea sobre comercio electrónico)

Los Artículo 12 a 15 de la Directiva citada definen el grado de responsabilidad de los diferentes proveedores. Según el Artículo 12, se exceptúa completamente de responsabilidad a los proveedores de acceso y a los encaminadores siempre que cumplan las tres condiciones estipuladas en dicho Artículo. Por consiguiente, el proveedor de acceso, por lo general, no es responsable de los delitos cometidos por sus usuarios. La plena exención de responsabilidad no exceptúa al proveedor de la obligación de evitar un delito o una infracción si lo exige un tribunal o una autoridad administrativa.[2546]

Sección 4: Responsabilidad de los proveedores de servicio intermediarios
Artículo 12
"Mera transmisión"
1. Los Estados Miembros garantizarán que, en el caso de un servicio de la sociedad de la información que consista en transmitir en una red de comunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a una red de comunicaciones, no se pueda considerar al prestador de servicios de este tipo responsable de los datos transmitidos, a condición de que el prestador de servicios:

(a) no haya originado él mismo la transmisión;
(b) no seleccione al destinatario de la transmisión; y
(c) no seleccione ni modifique los datos transmitidos.

2. Las actividades de transmisión y concesión de acceso enumeradas en el apartado 1 engloban el almacenamiento automático, provisional y transitorio de los datos transmitidos siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión.
3. El presente Artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados Miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida.

Este enfoque es comparable al presentado en el § 512(a) del 17 USC[2547] Ambas disposiciones apuntan a determinar la responsabilidad de los proveedores de servicio vinculándola a requisitos similares. La diferencia principal consiste en que la aplicación del Artículo 12 de la Directiva de la Unión Europea sobre comercio electrónico no se limita a las violaciones de los derechos de autor sino que exceptúa de responsabilidad a los proveedores con respecto a todo otro tipo de delito.

6.7.5 Responsabilidad por la memoria tampón (Directiva de la Unión Europea sobre comercio electrónico)

En este contexto, el término "caching" describe el almacenamiento de páginas web muy populares en medios locales con la finalidad de reducir la anchura de banda y facilitar un acceso más eficaz a los datos.[2548] Una técnica utilizada para reducir la anchura de banda es la instalación de servidores intermediarios.[2549] Con este fin, un servidor intermediario puede solicitar servicios sin ponerse en contacto con el servidor específico (el usuario introduce el nombre de dominio) retirando el contenido salvado en el medio de almacenamiento local de una petición anterior. Los redactores de la Directiva reconocieron la importancia económica de la memoria tampón y decidieron exceptuar de responsabilidad al proveedor por almacenamiento temporal automático siempre que dicho proveedor cumpla las condiciones definidas en el Artículo 13. Una de esas condiciones estipula que el proveedor cumpla las normas sobre actualización de la información ampliamente reconocidas.

Artículo 13
"Memoria tampón (caching)"
1. Los Estados Miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, el prestador del servicio no pueda ser considerado responsable del almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de éstos, a condición de que:

(a) el prestador de servicios no modifique la información;

(b) el prestador de servicios cumpla las condiciones de acceso a la información;

(c) el prestador de servicios cumpla las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada por el sector;

(d) el prestador de servicios no interfiera en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información; y

(e) el prestador de servicios actúe con prontitud para retirar la información que haya almacenado, o hacer que el acceso a ella será imposible, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se encontraba inicialmente, de que se ha imposibilitado el acceso a dicha información o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir que se acceda a ella.

2. El presente Artículo no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados Miembros, exija al prestador de servicios poner fin a una infracción o impedirla.

El Artículo 13 de la Directiva de la Unión Europea sobre comercio electrónico constituye otro ejemplo de similitud entre la estructura dogmática de los Estados Unidos y el enfoque europeo. El enfoque de la Unión Europea puede compararse al § 512(b) del 17 USC[2550] Ambas disposiciones apuntan a determinar la responsabilidad de los proveedores de sistemas de almacenamiento especial vinculándola a requisitos similares. Con respecto a la responsabilidad de los proveedores de servicio[2551], la diferencia principal entre ambos enfoques radica en que la aplicación del Artículo 13 de la Directiva de la Unión Europea sobre comercio electrónico no se limita a las violaciones de los derechos de autor sino que exceptúa de responsabilidad a los proveedores con respecto a todo otro tipo de delito.

6.7.6 Responsabilidad del proveedor de alojamiento de datos (Directiva de la Unión Europea)

Especialmente con respecto al contenido ilícito, el proveedor de alojamiento de datos desempeña una función importante en el marco de la perpetración del delito. Los delincuentes que colocan contenidos ilícitos en línea, generalmente no los almacenan en sus propios servidores. La mayoría de páginas web están almacenadas en servidores facilitados por proveedores de alojamiento de datos. Cualquiera que desee crear una página web puede arrendar a esos proveedores capacidad de almacenamiento para su página web. Algunos proveedores ofrecen incluso, en forma gratuita, espacio web con auspicio publicitario.[2552]

La identificación de contenido ilícito constituye un problema para el proveedor de alojamiento de datos. En especial cuando se trata de proveedores muy solicitados con numerosos sitios web, la búsqueda manual de contenido ilícito por todas esas páginas podría resultar imposible. A raíz de ello, los redactores de la Directiva decidieron limitar la responsabilidad de este tipo de proveedores. Sin embargo, a diferencia de lo que ocurre con el proveedor de acceso, no se exceptúa de responsabilidad al proveedor de alojamiento de datos. No se lo considera responsable en la medida en que no tiene conocimiento efectivo de las actividades ilícitas o de los contenidos ilícitos almacenados en sus servidores. La presunción de que el contenido ilícito podría ser almacenado en los servidores no se considera aquí equivalente a tener conocimiento efectivo al respecto. Si el proveedor tiene conocimiento concreto con respecto a actividades ilícitas o contenidos ilícitos, únicamente podrá evitar que se lo considere responsable si elimina inmediatamente la información ilícita. [2553] La ausencia de una reacción inmediata dará lugar a la imputación de responsabilidad del proveedor de alojamiento de datos.[2554]

Artículo 14
Alojamiento de datos
1. Los Estados Miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que:

(a) el prestador de servicios no tenga conocimiento efectivo de que la actividad a la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que,

(b) en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.

2. El apartado 1 no se aplicará cuando el destinatario del servicio actúe bajo la autoridad o control del prestador de servicios.
3. El presente Artículo no afectará la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados Miembros, exijan al prestador de servicios de poner fin a una infracción o impedirla, ni a la posibilidad de que los Estados Miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos.

El Artículo 14 no sólo se aplica al proveedor que limita sus servicios al arrendamiento de una infraestructura técnica de almacenamiento de datos. También algunos servicios Internet de gran difusión, como las plataformas de subastas, ofrecen ese tipo de servicios.[2555]

6.7.7 Responsabilidad del proveedor de alojamiento de datos (HIPCAR)

Otra forma de enfocar la responsabilidad el proveedor de alojamiento de datos es la que figura en el texto legislativo elaborado por los Estados beneficiarios de la iniciativa HIPCAR.[2556]

Proveedor de alojamiento de datos
30 *(1) El proveedor de alojamiento de datos no incurre en responsabilidades penales por la información almacenada a petición de los usuarios del servicio, siempre y cuando:*

(a) el proveedor de alojamiento de datos borre o corte el acceso a la información rápidamente en cuanto reciba una orden de cualquier autoridad pública o tribunal de suprimir la información ilícita específica que tiene almacenada; o

(b) el proveedor de alojamiento de datos, en cuanto tenga conocimiento o descubra por otros medios aparte de una orden de una autoridad pública que tiene almacenada información ilegal específica, informe sin dilación a una autoridad pública para que ésta pueda evaluar la información y, si procede, emitir la orden para eliminar el contenido.

(2) El párrafo 1 no será de aplicación cuando el usuario del servicio actúa bajo la autoridad o el control del proveedor de almacenamiento de datos.

(3) Si el proveedor de almacenamiento de datos elimina el contenido tras recibir una orden con arreglo al párrafo 1, quedará exento de obligaciones contractuales con su cliente en cuanto a la disponibilidad del servicio.

Al igual que en el enfoque adoptado por la Unión Europea, el punto 30(1)a. de la Parte V de la Sección II limita la responsabilidad del proveedor de alojamiento de datos si éste borra sin dilación el contenido tras recibir una orden de cualquier autoridad pública o de un tribunal. Por lo general, sin dilación significa dentro de las 24 horas.[2557] La principal diferencia respecto de la EU se encuentra en la Sección 30(1)(b). A diferencia del enfoque de la EU, el proveedor no tiene que determinar si el contenido que ha descubierto es ilegal. En cuanto tenga conocimiento del mismo, su obligación se limita exclusivamente a informar a la autoridad pública (designada) acerca del posible contenido ilegal. Los redactores de la disposición decidieron que corresponde a dichas autoridades determinar la naturaleza del contenido y emitir una orden para suprimirlo.[2558] Si la información se considera ilegal, el proveedor tendrá que suprimirla para quedar eximido de toda responsabilidad.

6.7.8 Exclusión de la obligación de supervisión (Directiva de la Unión Europea sobre comercio electrónico)

Antes de la aplicación de la Directiva, algunos Estados Miembros no tenían muy claro si podían entablar una acción judicial contra los proveedores por violación de la obligación de supervisar las actividades de sus usuarios. Dejando de lado posibles conflictos con las normas de protección de datos y la confidencialidad de las telecomunicaciones, esas obligaciones plantearían especialmente dificultades a los proveedores de alojamiento de datos que almacenan millares de páginas web. Para evitarlas, la Directiva decide no imponer a los proveedores una obligación general de supervisar los datos que transmitan o almacenen.

Artículo 15
Inexistencia de obligación general de supervisión
1. Los Estados Miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los Artículos 12, 13 y 14.
2. Los Estados Miembros podrán establecer obligaciones tendentes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades competentes, a solicitud de éstas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento.

6.7.9 Responsabilidad de los hiperenlaces (ECC- Austria)

Los hiperenlaces desempeñan una función importante en Internet puesto que su proveedor orienta al usuario hacia informaciones concretas disponibles en línea. En vez de ofrecer simplemente detalles técnicos sobre la manera de tener acceso a esa información (por ejemplo, facilitando el nombre de dominio de la página web en que figura la información), el usuario puede tener acceso directo a ella con sólo pulsar el hiperenlace activo. El hiperenlace ordena al navegador web abrir la dirección Internet depositada.

Durante la elaboración de la Directiva de la Unión Europea se mantuvo un intenso debate sobre la necesidad de reglamentar los hiperenlaces.[2559] Los redactores decidieron no obligar a los Estados Miembros a armonizar su legislación con respecto a la responsabilidad imputada a los hiperenlaces. En su lugar, aplicaron un procedimiento de reexamen para garantizar que se tuviera en cuenta la necesidad de presentar propuestas relativas a la responsabilidad de los proveedores de hiperenlaces y servicios de instrumentos de localización.[2560] Hasta que no se modifique en el futuro la disposición sobre imputación de responsabilidad a los hiperenlaces, los Estados Miembros tienen la libertad de formular soluciones en el ámbito nacional.[2561] Algunos países de la Unión Europea han decidido contemplar la responsabilidad de los proveedores de hiperenlaces en una disposición especial.[2562] Para ello, estos países se han inspirado en los

mismos principios que sostiene la Directiva con respecto a la responsabilidad de los proveedores de alojamiento de datos.[2563] Este enfoque es la consecuencia lógica de la situación comparable del proveedor de alojamiento de datos y el proveedor de hiperenlaces. En ambos casos, los proveedores controlan el contenido ilícito o, al menos, el enlace a dicho contenido.

Un ejemplo de lo indicado es la Sección 17 de ECC de Austria:[2564]

> ***Sección 17 ECC*** *(Austria) – Responsabilidad de los hiperenlaces*
> *(1) Un proveedor que da acceso a una información proporcionada por terceros facilitando un enlace electrónico no puede ser considerado responsable de esa información si*
> *1. no tiene conocimiento efectivo de que la actividad o la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tiene conocimiento de hechos o circunstancias por los que la actividad o la información hubieran podido revelar al proveedor de servicio su carácter ilícito; o*
> *2. en cuanto tiene conocimiento de esos aspectos, actúa con prontitud para retirar el enlace electrónico.*

6.7.10 Responsabilidad de los motores de búsqueda

Los proveedores de motores de búsqueda ofrecen servicios para identificar documentos de interés especificando ciertos criterios. Esos motores de búsqueda indagarán documentos pertinentes que responden a los criterios indicados por el usuario. Los motores de búsqueda cumplen una función importante en el éxito de la evolución de Internet. Sólo se puede tener acceso al contenido disponible en una página web pero no contemplado en el índice de un motor de búsqueda si la persona que desea acceder a él conoce el URL completo. Introna/Nissenbaum señala que "sin exagerar demasiado, se podría decir que para existir hay que figurar en el índice de un motor de búsqueda".[2565]

Como ocurre con los hiperenlaces, la Directiva de la Unión Europea no contempla normas que definan la responsabilidad de los operadores de motores de búsqueda. Por consiguiente, algunos países de la Unión Europea han decidido contemplar la responsabilidad de dichos operadores en una disposición especial.[2566] A diferencia de lo que ocurre con los hiperenlaces, no todos los países se han basado en los mismos principios.[2567] España[2568] y Portugal, en sus disposiciones relativas a la responsabilidad de los operadores de motores de búsqueda, han tenido en cuenta el Artículo 14 de la Directiva, en tanto que Austria [2569], en cuanto a la limitación de responsabilidad, se ha inspirado en el Artículo 12 de ese instrumento.

> ***Sección 14 ECC*** *(Austria) – Responsabilidad de los operadores de motores de búsqueda*
> *(1) Un proveedor que facilita un motor de búsqueda u otras herramientas electrónicas para buscar información proporcionada por terceros no puede ser considerado responsable, a condición de que:*
> *1. no inicie la transmisión;*
> *2. no seleccione al destinatario de la transmisión; y*
> *3. no seleccione ni modifique la información contenida en la transmisión.*

[1479] For an overview of legal approaches, see also: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 18 *et seq.*, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1480] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.

[1481] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 255.

[1482] Four definitions are included in Art. 1 and an additional provision was included in Art. 9, Council of Europe Convention on Cybercrime.

[1483] For more information related to legal approaches regulating the liability of access provider see below: § 6.7.4

[1484] With regard to the lawful interception of communication see below: § 6.5.9.

[1485] With regard to the liability of caching provider see below: § 6.7.5.

[1486] For more details related to different legal approaches to criminalize child pornography see below: § 6.2.8.

[1487] With regard to the criminalization of such conduct see below: § 6.2.7.

[1488] Art. 2(a) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1489] Art. 3(a) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1490] Sec. 3(3) HIPCAR Model Legislative Text on Cybercrime.

[1491] With regard to details of the criminalization see below: § 6.2.8.

[1492] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1493] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1494] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104..

[1495] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1496] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1497] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1498] Art. 2(c) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1499] Art. 20(2) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1500] With regard to different approaches to criminalize data interference see below: § 6.2.5..

[1501] Regarding the criminalization of data espionage/illegal data acquisition see below: § 6.2.3.

[1502] Art. 1(b) Council of Europe Convention on Cybercrime, ETS 185.

[1503] Art. 1(b) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1504] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1505] Sec. 3(5) HIPCAR Model Legislative Text on Cybercrime.

[1506] Sec.3 (7) HIPCAR Model Legislative Text.

[1507] *Stair/Reynolds/Reynolds*, Fundamentals of Information Systems, 2008, page 167; *Weik*, Computer science and communications dictionary, 2000, page 826; *Stair/Reynolds*, Principles of Information Systems, 2011, page 15..

[1508] Art. 1(a) Council of Europe Convention on Cybercrime, ETS 185.

[1509] Art. 1(a) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The Framework Decision uses the term „information" system instead of computer system.

[1510] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1511] Sec. 3(4) HIPCAR Model Legislative Text on Cybercrime.

[1512] Regarding attacks against critical infrastructure see above: § 1.2.

[1513] Regarding the related challenges see above: § 3.2.14.

[1514] With regard to the legal response see below: § 6.5.11

[1515] Draft African Union Convention on the Establishment of a credible Legal Framework for Cyber Security in Africa, Version 1, January 2011.

[1516] See below: § 6.2.15.

[1517] See Art. 10 (1)(a) HIPCAR Model Legislative Text on Cybercrime.

[1518] See below: § 6.2.6.

[1519] With regard to the liability of different types of provider see below: § 6.7.

[1520] Regarding the liability of search engines see below: § 6.7.10.

[1521] With regard to illegal interception, see below: § 6.2.4.

[1522] For more details related to the interference with computer data see below: § 6.2.5.

[1523] With regard to system interference see below: § 6.2.6.

[1524] See in this regard below: § 6.2.14.

[1525] See below: § 6.5.12.

[1526] Regarding the different legal approaches to seize evidence see below: § 6.5.6.

[1527] See in this regard Art. 19 (3) Council of Europe Convention on Cybercrime.

[1528] Sec. 3 Commonwealth Model Law on Computer and Computer-related Crime.

[1529] Sec. 3(17) HIPCAR Model Legislative Text on Cybercrime.

[1530] See below: § 6.5.9.

[1531] Art. 1 Council of Europe Convention on Cybercrime.

[1532] Sec. 3(18) HIPCAR Model Legislative Text on Cybercrime.

[1533] *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[1534] These range from the simple proof that technical protection measures can be circumvented, to the intent to obtain data stored on the victim computer. Even political motivations have been discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

[1535] Regarding the independence of place of action and the location of the victim, see above § 3.2.7.

[1536] These can, for example, be passwords or fingerprint authorization. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of potential tools, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[1537] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is also highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

[1538] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 729.

[1539] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "The need for protection reflects the interests of organizations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

[1540] With regard to data espionage, see above, § 2.5.2 and below, § 6.1.3.

[1541] With regard to data interference see above, Chapter 2.4.d and below, Chapter 6.1.3.

[1542] *Sieber*, Informationstechnologie und Strafrechtsreform, page 49 *et seq.*

[1543] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1544] Art. 2 of the Convention on Cybercrime enables the Member States to keep those existing limitations that are mentioned in Art. 2, sentence 2. Regarding the possibility of limiting criminalization, see also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

[1545] An example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). This provision was changed in 2007. The following text presents the old version:

Section 202a – Data Espionage

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

[1546] This approach is not only found in national legislation, but was also recommended by Council of Europe Recommendation No. (89) 9.

[1547] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1548] Regarding the system of reservations and restrictions, see *Gercke*, The Convention on Cybercrime, Computer Law Review International, 2006, 144.

[1549] *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1550] With regard to software tools that are designed and used to carry out such attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf. With regard to Internet-related social engineering techniques, see the information offered by the anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1551] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1552] The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5 per cent of the respondents reported that 80-100 per cent of their losses were caused by insiders. Nearly 40 per cent of all respondents reported that between 1 per cent and 40 per cent of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: www.gocsi.com/.

[1553] Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

[1554] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1555] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1556] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1557] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1558] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

[1559] *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, page 7.

[1560] See for example: World Information Technology And Services Alliance (WITSA), Statement On The Council Of Europe Draft Convention On Cybercrime, 2000, available at: www.witsa.org/papers/COEstmt.pdf. Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1561] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62 (dealing with Article 4).

[1562] *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[1563] This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

[1564] *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1565] Article 42 – Reservations: By a written notification addressed to the Secretary-General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[1566] This limits the criminalization of illegal access to those cases where the victim used technical protection measures to protect its computer system. Access an unprotected computer system would therefore not be considered a criminal act.

[1567] The additional mental element/motivation enables Member States to undertake a more focused approach rather than implementing a criminalization of the mere act of hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

[1568] This enables Member States to avoid a criminalization of cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

[1569] Framework Decision on Attacks against Information Systems – 19 April 2002 – COM (2002) 173. For more details, see above: § 5.2.1.

[1570] Article 2 – Illegal access to information systems:

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

committed by infringing a security measure.

[1571] Model Law on Computer and Computer Related Crime, LMM(02)17, available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1572] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1573] See the explanation of the EU Directive 2013/40/EU on attacks against information systems .

[1574] EU Directive 2013/40/EU on attacks against information systems.

[1575] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1576] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1577] See *Sofaer/Goodman/Cuellar/Drozdova and others*. A Proposal for an International Convention on Cybercrime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1578] In this context, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

[1579] Standalone computer systems are covered by Art. 1, paragraph 3, of the Draft Convention because they "control programs". This does not require a network connection.

[1580] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1581] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1582] The Explanatory Report points out that the provision intends to criminalize violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1583] See below: § 6.1.4.

[1584] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

[1585] One key indication of the limitation of application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet, which do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights."* See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1586] See in this context especially a recent case from Hong Kong, People's Republic of China. See above: § 2.5.2.

[1587] ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1588] Regarding the challenges related to the use of encryption technology by offenders, see above: § 3.2.14; *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf; *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html. Regarding the underlying technology, see: *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[1589] One of the consequences related to this aspect is the fact that limitation of the criminalization of illegal access to those cases where the victim of the attack secured the target computer system with technical protection measures could limit the application of such a provision, insofar as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

[1590] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996). See in this context: *Chamblee*, Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 *et seq.*), 177 A.L.R. Fed. 609 (2002); *Fischer*, An Analysis of the Economic Espionage Act of 1996, 25 Seton Hall Legis. J. 239 (2001).

[1591] *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 986, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

[1592] For details, see: US CCIPS, Prosecuting Intellectual Property Crimes, 3rd Edition, 2006, page 138 *et seq.* available at: www.justice.gov/criminal/cybercrime/ipmanual/04ipma.pdf.

[1593] *Loundy*, Computer Crime, Information Warfare, and Economic Espionage, 2009, page 55 *et seq.*; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.* available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[1594] *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 988, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf..

[1595] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1596] The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1597] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1598] This provision has recently been modified and now even criminalizes illegal access to data. The previous version of the provision has been used here, because it is better suited for demonstrating the dogmatic structure.

[1599] See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

[1600] A similar approach of limiting criminalization to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention on Cybercrime: *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.* For more information, see above: § 6.1.1.

[1601] This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement, self-protection measures.

[1602] See in this context for example a recent case in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Herald, 14.02.2008, available at: www.smh.com.au/news/web/stolen-photos-from-laptop-tell-a-tawdry-tale/2008/02/14/1202760468956.html; *Pomfret*, Hong Kong's Edision
Chen quits after sex scandal, Reuters, 21.02.2008, available at: www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

[1603] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1604] With regard to "phishing", see above: § 2.9.4 and below: § 6.1.15 and as well: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Phishing, Computer und Recht, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1605] Regarding the risks related to the use of wireless networks, see above: § 3.2.3. Regarding the difficulties in cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

[1606] Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1607] Regarding the underlying technology and the security related issues, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx. With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[1608] The computer magazine ct reported in 2004 that field tests proved that more than 50 per cent of 1 000 wireless computer networks that were tested in Germany were not protected. See: www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182.

[1609] Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx.

[1610] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1611] Regarding identity theft, see above: § 2.8.3 and below: § 6.1.16 and also: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1612] In the United States, the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes. Regarding offences related to social-security numbers, see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[1613] See: *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1, page 112.

[1614] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1615] The Explanatory Report describes the technical means more in detail: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalization." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53..

[1616] Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering"..

[1617] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

[1618] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf

[1619] See above: § 6.1.3.

[1620] "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 55.

[1621] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

[1622] Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue, see Explanatory Report, No. 57: *"The creation of an offence in relation to "electromagnetic emissions" will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as "data" according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision"*, Explanatory Report to the Council of Europe Convention on Cybercrime, No. 57.

[1623] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1624] *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1625] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 54.

[1626] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39..

[1627] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39..

[1628] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1629] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58..

[1630] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58

[1631] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58..

[1632] Cookies are data sent by a server to a browser and then sent back each time the browser is used to access the server. Cookies are used for authentication, tracking and keeping user information. Regarding the functions of cookies and the controversial legal discussion, see: *Kesan/Shah*, Deconstruction Code, Yale Journal of Law & Technology, 2003-2004, Vol. 6, page 277 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

[1633] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

[1634] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1635] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1636] Model Law on Computer and Computer Related Crime" LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1637] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1638] The difficulty with offences against the integrity of data is that identification of these violations is often difficult to prove. Therefore, the Expert Group which drafted the Convention on Cybercrime identified the possibility of prosecuting violations regarding data interference by means of criminal law as a necessary strategic element in the fight against cybercrime. Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

[1639] The 2007 Computer Economics Malware Report focuses on computer crime and analyses the impact of malware on the worldwide economy by summing up the estimated costs caused by attacks. It identified peaks in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion). For more information, see: 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code. A summary of the report is available at: www.computereconomics.com/article.cfm?id=1225.

[1640] A number of computer fraud scams are including the manipulation of data – e.g. the manipulation of bank-account files, transfer records or data on smart cards. Regarding computer related fraud scams, see above: § 2.8.1 and below: § 6.1.17.

[1641] Regarding the problems related to these gaps, see for example the LOVEBUG case, where a designer of a computer worm could not be prosecuted due to the lack of criminal law provisions related to data interference. See above: § 2.5.4 and: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1642] A similar approach to Art. 4 of the Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 – Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[1643] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

[1644] As pointed out in the Explanatory Report, the two terms overlap. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1645] Regarding the more conventional ways to delete files using Windows XP, see the information provided by Microsoft, available at: www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

[1646] Regarding the consequences for forensic investigations, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq.*, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1647] See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/05hb003.pdf

[1648] The fact that the Explanatory Report mentions that the files are unrecognizable after the process does not give any further indication with regard to the interpretation of the term. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1649] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1650] A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf. In 2000 a number of well-known US e-commerce businesses were targeted by DoS attacks. A full list is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1651] With regard to the criminalization of DoS attacks, see also below: § 6.1.6.

[1652] In addition, criminalization of DoS attacks is provided by Art. 5 of the Convention on Cybercrime. See below: § 6.1.6.

[1653] Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

[1654] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Regarding the different recognized functions of malicious software, see above: § 2.5.4. Regarding the economic impact of malicious software attacks, see above: § 2.5.4.

[1655] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1656] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1657] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report states: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1658] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62: "The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g., encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right." Regarding the liability of Remailer, see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

[1659] For further information, see *du Pont*, The Time Has Come For Limited Liability For Operators Of True Anonymity Remailers In Cyberspace: An Examination Of The Possibilities And Perils, Journal Of Technology Law & Policy, Vol. 6, Issue 2, page 176 *et seq.*, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf

[1660] With regard to the possible difficulties to identify offenders who have made use of anonymous or encrypted information, the Convention leaves the criminalization of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

[1661] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems..

[1662] For further information, see: *Gercke*, The EU Framework Decision on Attacks against Information Systems, Computer und Recht 2005, page 468 *et seq.*

[1663] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1664] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1665] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1666] Sec. 5 (Illegal access), Sec. 8 (Illegal interception) and Sec. 10 (Child pornography).

[1667] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cybercrime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1668] ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1669] A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see above: § 2.5.4 and US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

[1670] For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, Inferring Internet Denial-of-Service Activities, page 1, available at: www.caida.org/papers/2001/BackScatter/usenixsecurity01.pdf; CNN News, One year after DoS attacks, vulnerabilities remain, at: http://edition.cnn.com/2001/TECH/internet/02/08/ddos.anniversary.idg/index.html. *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1671] Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: Campbell/Gordon/Loeb/Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, pages 431-448.

[1672] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding cyberterrorism, see above § 2.9.1 and *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyberterrorism and Cybersecurity, available at: www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeld*t, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at:

www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: *Prados*, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 et *seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.* OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf; *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, pages 221-249.

[1673] The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 65.

[1674] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1675] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1676] The Explanatory Report gives examples for implementation of restrictive criteria for serious hindering: "Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate "denial-of-service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)" – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 67.

[1677] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Although the connotation of "serious" does limit the applicability, it is likely that even serious delays to operations resulting from attacks against a computer system can be covered by the provision.

[1678] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1679] Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection.

[1680] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61. Regarding the fact that the definition does not distinguish between the different ways how information can be deleted, see above: § 6.1.15. Regarding the impact of the different ways of deleting data on computer forensics, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq.*, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1681] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1682] Apart from the input of malicious codes (e.g. viruses and trojan horses), it is therefore likely that the provision could cover unauthorized corrections of faulty information as well. .

[1683] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1684] "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam legislation worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: § 2.5.g.

[1685] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf

[1686] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1687] Regarding legal approaches in the fight against spam, see above: § 6.1.l3.

[1688] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1689] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1690] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1691] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1692] See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1693] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 68: "The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized by this article, even if it causes serious hindering."

[1694] Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

[1695] Article 3 – Illegal system interference: "Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[1696] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1697] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1698] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1699] Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), PC-CY (2000), 19, available at: www.iwar.org.uk/law/resources/eu/cybercrime.htm.

[1700] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/ documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1701] For an overview on hate speech legislation, see for example: the database provided at: www.legislationline.org. For an overview on other cybercrime-related legislation, see: the database provided at: www.cybercrimelaw.net.t.

[1702] Regarding the challenges of international investigation, see above: § 3.2.4 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1703] For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

[1704] *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 5.

[1705] Regarding the influence of pornography on minors, see: *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact, and Prevention, Youth & Society, Vol. 34, 2003, page 330 *et seq.*, available at: www.unh.edu/ccrc/pdf/Exposure_risk.pdf; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002, available at: http://findarticles.com/p/articles/mi_m2372/is_1_39/ai_87080439..

[1706] See Section 11 Subparagraph 3 Penal Code: "Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection".

[1707] *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 28.

[1708] The draft law was not in force by the time this publication was finalized.

[1709] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1710] Regarding the challenges of international investigation, see above: § 3.2.4. See also: *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1711] *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Cox*, Litigating Child Pornography and Obscenity Cases, Journal of Technology Law and Policy, Vol. 4, Issue 2, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB.

[1712] Regarding methods of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication, see above: § 3.2.14.

[1713] It has been reported that some websites containing child pornography register up to a million hits per day. For more information, see: *Jenkins*, Beyond Tolerance: Child Pornography on the Internet, 2001, New York University Press; *Wortley/Smallbone*, Child Pornography on the Internet, page 12, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1714] Regarding the challenges related to investigations involving anonymous communication technology, see above: § 3.2.l.

[1715] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[1716] *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 68.

[1717] *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11, page 6, available at: http://jjlp.law.ucdavis.edu/archives/vol-11-no-1/07%20Liu%2011.1.pdf.

[1718] *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 69.

[1719] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

[1720] *Akdeniz* in *Edwards/Waelde*, Law and the Internet: Regulating Cyberspace; *Williams* in *Miller*, Encyclopaedia of Criminology, page 7. Regarding the extent of criminalization, see: Child Pornography: Model Legislation & Global Review, 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalization of child pornography and freedom of speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws in terms of the criminalization of child pornography.

[1721] Regarding differences in legislation, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 26, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1722] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

[1723] *Walden*, Computer Crimes and Digital Investigations, 2006, page 144.

[1724] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 94.

[1725] Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, ETS 201.

[1726] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 135.

[1727] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1728] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 95.

[1729] Regarding criminalization of the possession of child pornography in Australia, see: *Krone*, Does thinking make it so? Defining online child pornography possession offences, in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalization of child pornography.

[1730] See: Child Pornography: Model Legislation & Global Review, 2006, page 2, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[1731] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 98.

[1732] *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf

[1733] Based on the National Juvenile Online Victimization Study, only 3 per cent of arrested Internet-related child-pornography possessors had morphed pictures. *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1734] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 102.

[1735] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf..

[1736] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1737] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1738] Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49. Article 1. For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

[1739] One example is the current German Penal Code. The term "child" is defined by law in Section 176 to which the provision related to child pornography refers: Section 176: "Whoever commits sexual acts on a person under fourteen years of age (a child) ...".

[1740] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[1741] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, available at: http://conventions.coe.int.

[1742] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1743] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1744] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1745] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1746] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may*

implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1747] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1748] *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

[1749] Regarding the challenges related to the use of encryption technology, see above: § 3.2.14. One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1750] See Explanatory Report to the Convention on the Protection of Children, No. 140.

[1751] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or is just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[1752] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1753] Official Notes:

NOTE: The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.

NOTE: The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read: "commits an offence punishable, on conviction:

(a) in the case of an individual, by a fine not exceeding [amount] or imprisonment for a period not exceeding [period]; or

(b) in the case of a corporation, by a fine not exceeding [a greater amount].

[1754] Official Note:

NOTE: Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.

[1755] See the preface to the Optional Protocol.

[1756] See Art. 2.

[1757] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at:

http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1758] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1759] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1760] See in this regard: *Powell*, Paedophiles, Child Abuse and the Internet, 2007; *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010, available at: www.cse.dmu.ac.uk/~bstahl/index_html_files/2010_grooming_ICIS.pdf.

[1761] See: Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

[1762] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1763] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

[1764] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 157.

[1765] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 159.

[1766] International Mechanisms for Promoting Freedom of Expression, Joint Declaration, Challenges to Freedom of Expression in the New Century, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2001.

[1767] For an overview of hate speech legislation, see the database provided at: www.legislationline.org.

[1768] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1769] Regarding the criminalization of hate speech in Europe, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 781 *et seq.* available at: http://law.wlu.edu/ deptimages/Law%20Review/62-2VanBlarcum.pdf. Regarding the situation in Australia, see: *Gelber/Stone*, Hate Speech and Freedom of Speech in Australia, 2007.

[1770] Vienna Summit Declaration, 1993, available at: www.coe.int/t/dghl/monitoring/ecri/archives/other_texts/2-vienna/plan_of_action/plan_of_action_vienna_summit_EN.asp.

[1771] Recommendation No. 1275 on the fight against racism, xenophobia, anti-Semitism and intolerance.

[1772] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4: "The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

[1773] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[1774] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1775] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1776] Regarding the list of states that signed the Additional Protocol, see above: § 5.2.1.

[1777] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

[1778] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at: www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1779] Regarding the challenges of international investigation, see above: § 3.2.5 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1780] Regarding possible reservations, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 792.

[1781] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1782] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1783] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1784] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 29.

[1785] Regarding the definition of "distributing" and "making available", see § 6.1.8 above.

[1786] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 34.

[1787] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1788] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 36.

[1789] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1790] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1791] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1792] Regarding legislation on blasphemy, as well as other religious offences, see: Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf.

[1793] International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2006.

[1794] See above: § 6.1.9, as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1795] The draft law was not in force at the time this publication was finalized.

[1796] Prevention of Electronic Crimes Ordinance 2007, available at: www.upesh.edu.pk/net-infos/cyber-act08.pdf.

[1797] Prevention of Electronic Crimes Ordinance, 2007, published in the Gazette of Pakistan, Extraordinary, Part-I, dated 31 December 2007, available at: www.na.gov.pk/ordinances/ord2008/elect_crimes_10042008.pdf.

[1798] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1799] Regarding the difficulties related to jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

[1800] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1801] Regarding the challenges of international investigation, see above: § 3.2.6 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1802] The 2005 e-gaming data report estimates total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm. Regarding the number of licensed Internet websites related to Internet gambling in selected countries, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 52, available at: www.gao.gov/new.items/d0389.pdf. Regarding the total numbers of Internet gambling websites, see: *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf.

[1803] For an overview of different national Internet gambling legislation, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

[1804] Regarding the situation in the People's Republic of China, see for example: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[1805] Regarding addiction, see: *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: www.european-lotteries.org/data/info_130/Wood.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

[1806] See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

[1807] See *Thumm*, Strafbarkeit des Anbietens von Internetglueckspielen gemaess § 284 StGB, 2004.

[1808] Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which do not know that their services are abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

[1809] For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously, criminalization is limited to those cases where the offender is intentionally making the equipment available.

[1810] This is especially relevant with regard to the location of the server.

[1811] Avoiding the creation of safe havens is a major intention of harmonization processes. The issue of safe havens has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 states that: "*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "*There must be no safe havens for those who abuse information technologies*".

[1812] With regard to the principle of sovereignty, changing the location of a server can have a great impact on the ability of law-enforcement agencies to carry out an investigation. National Sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[1813] Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene, see above: §§ 3.2.6 and 3.2.7.

[1814] For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

[1815] Regarding the vulnerability of Internet gambling to money laundering, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 5, 34 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

[1816] Regarding other recent approaches in the United States, see: *Doyle*, Internet Gambling: A Sketch of Legislative Proposals in the 108th Congress, CRS Report for Congress No. RS21487, 2003, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-4047: *Doyle*, Internet Gambling: Two Approaches in the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

[1817] For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII, page 1183 *et seq.*, available at: http://law.fordham.edu/publications/articles/600flspub8956.pdf.

[1818] *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

[1819] *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm

[1820] Based on Sec. 5366, criminalization is limited to the acceptance of financial instruments for unlawful Internet gambling.

[1821] See: EU opens investigation into US Internet gambling laws, EU Commission press release, 10.03.2008, available at: http://ec.europa.eu/trade/issues/respectrules/tbr/pr100308_en.htm; *Hansen*, EU investigates DOJ internet gambling tactics, The Register, 11.03.2008, available at: www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

[1822] General Agreement on Trade in Services (GATS) – with regard to the United States Unlawful Internet Gambling Enforcement Act especially Articles XVI (dealing with Market Access) and XVII (dealing with National Treatment) could be relevant.

[1823] See above: § 3.2.l.

[1824] See above: § 3.2.2.

[1825] See, for example: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US delegation to OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at:

www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf; *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[1826] See, for example, the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information, see: www.osce.org/documents/rfm/2004/10/14893_en.pdf. See in addition the statement of the representative on Freedom of the Media, Mr Haraszti, at the fourth Winder Meeting of the OSCE Parliamentary Assembly on 25 February 2005.

[1827] Regarding various regional approaches to criminalization of defamation, see: *Greene* (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf.

[1828] For more details, see: the British Crime Survey 2006/2007 published in 2007, available at: www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

[1829] See: Crime Statistic Germany (Polizeiliche Kriminalstatistik), 2006, available at: www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

[1830] The full version of the Criminal Defamation Amendment Bill 2002 is available at: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02_P.pdf. For more information about the Criminal Defamation Amendment Bill 2002, see the Explanatory Notes, available at: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf.

[1831] The full text of the Criminal Code of Queensland, Australia is available at: www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

[1832] The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see: www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails are spam. See: www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

[1833] For more information on the phenomenon, see above: § 2.6.7. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1834] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf

[1835] See ITU Survey on Anti-Spam Legislation Worldwide, 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1836] Regarding the availability of filter technology, see: *Goodman,* Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam Consumer Perspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[1837] Spam Issues in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1838] See Spam Issues in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1839] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1840] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69: "The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law."

[1841] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1842] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1843] The document available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1844] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1845] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1846] Regarding the US legislation on spam, see: *Sorkin*, Spam Legislation in the United States, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Warner*, Spam and Beyond: Freedom, Efficiency, and the Regulation of E-mail Advertising, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Alongi*, Has the US conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 *et seq.*, available at: www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

[1847] For more details about the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM act 2003), see: www.spamlaws.com/f/pdf/pl108-187.pdf.

[1848] See: *Hamel,* Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?, New Eng. Law Review, 39, 2005, 196 *et seq.* 325, 327 (2001).

[1849] For more details, see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1850] For more information, see: *Wong,* The Future Of Spam Litigation After Omega World Travel v. Mummagraphics, Harvard Journal of Law & Technology, Vol. 20, No. 2, 2007, page 459 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech459.pdf.

[1851] Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[1852] One example of this misuse is the publication of passwords used for access control. Once published, a single password can grant access to restricted information to hundreds of users.

[1853] One example is the 2001 EU Framework Decision combating fraud and counterfeiting of non-cash means of payment.

[1854] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 71: "To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries".

[1855] With the definition of "distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report, No. 72), the drafters of the Convention restrict devices to software. Although the Explanatory Report is not definitive in this matter, it is likely that it covers not only software devices, but hardware tools as well.

[1856] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1857] See, in this context: *Biancuzzi*, The Law of Full Disclosure, 2008, available at: www.securityfocus.com/print/columnists/466.

[1858] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

[1859] See for example one approach in the US legislation:

18 USC. § 1029 (Fraud and related activity in connection with access devices)

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both. […]

[1860] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1861] This approach could lead to broad criminalization. Therefore Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

[1862] Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

[1863] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1864] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72: "*This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices*".

[1865] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society.

[1866] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 73: The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

[1867] Regarding the US approach to address the issue, see for example 18 USC. § 2512 (2):

(2) It shall not be unlawful under this section for –

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

[1868] *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1869] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76: "Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'."

[1870] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 731.

[1871] See, for example, the World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1872] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1873] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

[1874] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1875] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 77.

[1876] For more information, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 78.

[1877] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1878] Expert Group's suggestion for an amendment:

Paragraph 3:

A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.

Official Note: Subsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.

[1879] Canada's suggestion for an amendment:

Paragraph 3:

(3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8, unless the person raises a reasonable doubt as to its purpose.

Official Note: Subsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.

[1880] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1881] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1882] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1883] "Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating." See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1884] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1885] See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

[1886] See for example: *Austria*, Forgery in Cyberspace: The Spoof could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, Vol. IV, 2004, available at: http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf.

[1887] See for example 18 USC. § 495:

Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or

Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited –

Shall be fined under this title or imprisoned not more than ten years, or both.

Or Sec. 267 German Penal Code:

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:

1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;

2. causes an asset loss of great magnitude;

3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or

4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

[1888] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 82.

[1889] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

[1890] See Art. 1 (b) Convention on Cybercrime.

[1891] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

[1892] For example, by filling in a form or adding data to an existing document.

[1893] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

[1894] With regard the definition of "alteration" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1895] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1896] With regard the definition of "suppression" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1897] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1898] With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1899] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

[1900] If only part of a document is deleted the act might also be covered by the term "alteration".

[1901] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1902] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1903] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1904] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 85.

[1905] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1906] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1907] See, for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: http://edition.cnn.com/2006/US/05/18/identity.theft/; Identity Fraud, NY Times Topics, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html; *Stone*, US Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: www.iht.com/articles/2007/03/21/business/identity.php.

[1908] See, for example, the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1909] See, for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the US: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[1910] Regarding the phenomenon of identity theft, see above: § 2.8.3.

[1911] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1912] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1913] *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

[1914] *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[1915] This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data, see: *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007, available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1 ; ID Analytics, www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

[1916] The reason for the success is the fact that the provisions focus on the most relevant aspect of phase 1: transfer of the information from the victim to the offender.

[1917] Examples of acts that are not covered include the illegal access to a computer system in order to obtain identity related information.

[1918] One of the most common ways the information obtained is used is fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1919] Furthermore, it is uncertain whether the provisions criminalize possession if the offender does not intend to use the data but to sell them. Prosecution could in this case in general be based on fact that 18 USC. § 1028 not only criminalizes possession with the intent to use it to commit a crime, but also to aid or abet any unlawful activity.

[1920] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1921] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1922] See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[1923] Similar provisions are included in the Commonwealth Model Law and the Stanford Draft International Convention. For more information about the Commonwealth model law, see: Model Law on Computer and Computer Related Crime, LMM(02)17. The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Stanford Draft International Convention, see: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1924] See above: § 6.1.1.

[1925] See above: § 6.1.4.

[1926] See above: § 6.1.5.

[1927] *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1928] See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1929] See above: § 2.8.1.

[1930] Regarding the criminalization of computer-related fraud in the UK, see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 *et seq.*

[1931] One example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does not therefore cover the majority of computer-related fraud cases:

Section 263 Fraud

(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

[1932] A national approach that is explicitly address computer-related fraud is 18 USC. § 1030:

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

[1933] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1934] The drafters highlighted that the four elements have the same meaning as in the previous articles: "To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer program or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1935] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1936] With regard to the definition of "alteration" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1937] With regard to the definition of "suppression" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1938] With regard to the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1939] As a result, not only data-related offences, but also hardware manipulations, are covered by the provision.

[1940] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 87.

[1941] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 88.

[1942] "The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another."

[1943] The drafters of the Convention point out that these acts are not meant to be included in the offence established by Article 8 – Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

[1944] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1945] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

[1946] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1947] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1948] Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

[1949] For more information on the effects of digitization on the entertainment industry, see above: § 2.7.1.

[1950] The technology that is used is called digital rights management – DRM. The term digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies or other digital data. One of the key functions is copy protection, which aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[1951] Regarding the technical approach to copyright protection, see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

[1952] For details see above: § 2.7.1.

[1953] Examples are 17 USC. § 506 and 18 USC. § 2319:

Section 506. Criminal offenses

(a) Criminal Infringement. –- Any person who infringes a copyright willfully either –

(1) for purposes of commercial advantage or private financial gain, or

(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.

[...]

Section 2319. Criminal infringement of a copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506(a)(1) of title 17 –

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;

(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.

(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements shall include –

(A) producers and sellers of legitimate works affected by conduct involved in the offense;

(B) holders of intellectual property rights in such works; and

(C) the legal representatives of such producers, sellers, and holders.

(e) As used in this section –

(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and

(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.

Regarding the development of legislation in the United States, see: *Rayburn*, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

[1954] Regarding the international instruments, see: *Sonoda*, Historical Overview of Formation of International Copyright Agreements in the Process of Development of International Copyright Law from the 1830s to 1960s, 2006, available at: www.iip.or.jp/e/summary/pdf/detail2006/e18_22.pdf; *Okediji*, The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, 2006, available at: www.unctad.org/en/docs/iteipc200610_en.pdf. Regarding international approaches to anti-circumvention laws, see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

[1955] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 109.

[1956] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 110: "With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

[1957] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 111: "The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

[1958] Explanatory Report to the Council of Europe Convention on Cybercrime, Nos. 16 and 108.

[1959] *Article 61:*

Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.

[1960] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 113.

[1961] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 114.

[1962] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1963] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 115. In addition, the drafters pointed out: The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

[1964] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1965] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1966] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1967] See, for example, Art. 5 of the Convention on Cybercrime.

[1968] Convention on Cybercrime, ETS 185.

[1969] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1970] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1971] EU Framework Decision on Combating Terrorism, COM (2007) 650.

[1972] EU Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[1973] EU Framework Decision 2008/919/JHA of 28 November 2008, No. 4.

[1974] The intention of the drafters to cover online and offline activities was highlighted several times. See, for example: EU Framework Decision 2008/919/JHA of 28 November 2008, No. 11. "These forms of behavior should be equally punishable in all Member States irrespective of whether they are committed through the Internet or not."

[1975] Regarding the motivation, see: *Russell*, A History of the United Nations Charter, 1958.

[1976] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

[1977] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 59.

[1978] *Mani*, Basic Principles of Modern International Law: A Study of the United Nations Debates on the Principles of International Law Concerning Friendly Relations and Co-operation among States, 1993, page 263 *et seq.*

[1979] *Bond*, Peacetime foreign Data Manipulations as one Aspect of Offensive Information Warfare, 1996.

[1980] *Brownlie*, International Law and the Use of Force, 1993, page 362.

[1981] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 80.

[1982] *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyber force, Alb. Law Journal of Science and Technology, Vol. 18, page 304.

[1983] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57..

[1984] *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1 000 Centrifuges at the Nataz Enrichment Plant?, Preliminary Assessment, Institute for Science and International Security, 2010.

[1985] Regarding proliferation concerns, see: *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 58.

[1986] With regard to the development, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[1987] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5.

[1988] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 6.

[1989] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[1990] Regarding the admissibility and reliability of digital images, see: *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy, page 267 *et seq.*

[1991] *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7, page 71 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 14. Regarding the legal frameworks in different countries, see: *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 76; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213.

[1992] See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

[1993] For a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

[1994] The Council of Europe Convention on Cybercrime therefore contains a provision that clarifies that the procedural instruments in the Convention shall not only be applicable with regard to cybercrime-related offences, but also to "other criminal offences committed by means of a computer system" and "the collection of evidence in electronic form of a criminal offence" (Art. 14).

[1995] *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

[1996] Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

[1997] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

[1998] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq*

[1999] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 1.

[2000] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[2001] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286. With more reference to national law: *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213; *Vaciago*, Digital Evidence, 2012, Chapter I.1 (with an overview about the discussion about digital evidence in different jurisdictions).

[2002] Police and Criminal Evidence Code (PACE).

[2003] *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

[2004] Regarding the different models of cybercrime investigation, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[2005] This includes the development of investigation strategies.

[2006] The second phase covers, in particular, the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2007] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[2008] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

[2009] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2010] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[2011] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2012] This includes, for example, the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[2013] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2014] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59

[2015] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq*.

[2016] *Vaciago*, Digital Evidence, 2012, Chapter II.

[2017] *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

[2018] Regarding geo-recognition, see: *Friedland/Sommer*; Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, available at: www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf; *Strawn*, Expanding the Potential for GPS Evidence Acquisition, Small Scale Digital Device Forensics Journal, 2009, Vol. 3, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V3_1_Strawn.pdf; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

[2019] See *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010, page 95 *et seq.*, available at: www.dfrws.org/2010/proceedings/2010-311.pdf.

[2020] Regarding the use of metadata for investigations, see: *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf..

[2021] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

[2022] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217. Regarding the challenges of witnesses as a source of evidence, see: *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002.

[2023] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2024] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.

[2025] Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

[2026] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161..

[2027] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2028] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2029] Daubert v. Merrell Dow Pharmaceutical, Inc. (1993) 113 S. Ct. 2786, available at: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=509&invol=579.

[2030] *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3, page 1.

[2031] The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

[2032] Regarding the status of national legislation, see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2033] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2034] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2035] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

[2036] *Casey*, Digital Evidence and Computer Crime, 2004, page 15.

[2037] *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2Dpage 38F31AF079F9.pdf; With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2038] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf. Criteria for Admissibility of Expert Opinion, Utah Law Review, 1978, page 546 *et seq.*

[2039] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2040] See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39

[2041] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

[2042] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2043] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2044] See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

[2045] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 92.

[2046] *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

[2047] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2048] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[2049] *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

[2050] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2051] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2052] For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

[2053] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[2054] *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

[2055] *Casey*, Digital Evidence and Computer Crime, 2004, page 16..

[2056] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf..

[2057] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[2058] Regarding the design of courtrooms, see: *Youngblood*, Courtroom Design, 1976; *Smith/Larson*, Courtroom design, 1976.

[2059] Scientific Evidence Review: Admissibility of Expert Evidence, ABA, 2003, page 159 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 169; *Nilsson*, Digital Evidence in the Courtroom, 2010; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12, Issue 1.

[2060] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2061] See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 538.

[2062] Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

[2063] *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

[2064] *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

[2065] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 218

[2066] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

[2067] See in this context: *Nikali*, The Substitution of Letter Mail in Targeted Communication, 2007, available at: http://hsepubl.lib.hse.fi/pdf/diss/a136.pdf.

[2068] See in this context *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Hayes*, Forensic Handwriting Examination, 2006.

[2069] *Houck/Siegel*, Fundamentals of Forensic Science, 2010, page 512 *et seq.*; FBI Handbook of Crime Scene Forensics, 2008, page 111 *et seq.*; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962, Vol. 7, Issue 3, page 286 *et seq.*; *Miller*, An Analysis of the Identification Value of Defects in IBM Selectric Typewriters, American Academy of Forensic Science annual meeting, presented paper, Ohio, 1983; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007, page 207 *et seq.*

[2070] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[2071] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

[2072] *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No. 1, page 16 *et seq.*, available at: http://airccse.org/journal/nsa/0409s2.pdf.

[2073] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2074] Regarding approaches to link a suspect to stored computer records, see for example: *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 165.

[2075] Regarding the obligation to register prior to the use of public Internet terminals in Italy, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, page 94.

[2076] See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

[2077] Regarding a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

[2078] Regarding the extent of commercial child pornography, see: IWF 2007 Annual and Charity Report, page 7.

[2079] See *Schnabel,* The Mikado Principle, Datenschutz und Datensicherheit, 2006, page 426 *et seq.*

[2080] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 206.

[2081] Regarding the legitimacy principle, see: *Grans/Palmer*, Australian Principles of Evidence, 2005, page 10.

[2082] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 219.

[2083] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.

[2084] *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

[2085] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

[2086] Regarding necessary procedures, see: *Chawki*, The Digital Evidence in the Information Era, available at: www.droit-tic.com/pdf/digital_evid.pdf; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

[2087] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[2088] *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

[2089] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2090] See in this context also: *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

[2091] Regarding the consequences of the fruit of the poisonous tree doctrine for computer-crime investigations, see: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 563.

[2092] *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

[2093] Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.

[2094] Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332.

[2095] *Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563, [2001] EMLR 654. The primary evidence rule was in any event inapplicable to recordings on film or tape, which may be proven by copies under common law (*Kajala v Noble*

(1982) 75 Cr App Rep 149, DC; R v. Wayte (1982) 76 Cr App Rep 110, CA) and if lost or destroyed their contents may be proven by oral evidence from persons who have previously viewed or heard them (*Taylor v Chief Constable of Cheshire* [1987] 1 All ER 225, 84 Cr App Rep 191, DC). Also, see now the Criminal Justice Act 2003 s 133; and para 1464 post.

[2096] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; *Permanent Trustee Co of New South Wales v Fels* [1918] AC 879, PC.

[2097] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; The admission of documentary copies is subject to the Civil Evidence Act 1995: see PARA 808 *et seq.*

[2098] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

[2099] *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

[2100] With regard to different exemptions, see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 *et seq.*; Best Evidence Rule, California Law Review Commission, 1996, available at: www.clrc.ca.gov/pub/Printed-Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf..

[2101] For further reference, see: *Eltgroth*, Best Evidence and the Wayback Machine, Fordham Law Review, 2009, 193, available at: http://law.fordham.edu/assets/LawReview/Eltgroth_October_2009.pdf.

[2102] With regard to European common law countries (UK, Ireland), this development was especially supported by EU Directive 1999/93/EC. See also Sec. 4 and 6 of the Commonwealth model law on electronic evidence.

[2103] *Munday*, Evidence, 2007, page 380; *Allen*, Practical Guide to Evidence, 2008, page 189.

[2104] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567.

[2105] Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567 and *R v Sharp* [1988] 1WLR 7, HL; *R v Kearley* [1992] 2 AC 228, [1992] 2 All ER 345. HL. See also Civil Evidence Act 1995 ss1-7.

[2106] Per Lord Havers in *R v Sharp* [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion.

[2107] *Keane*, Modern Law of Evidence, 2005, pages 246-266.

[2108] *Dennis*, The Law of Evidence, 2002, Chapters 16-17.

[2109] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

[2110] Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006.

[2111] See in this context, for example, Part II of the Irish Criminal Evidence Act 1992.

[2112] R v Dodson [1984] 1 WLR 971, 79 CrApp Rep 220, CA (photographic evidence); R v Maqsud Ali [1966] 1 QB 688, 49 Cr App Rep 230, CCA (tape recorded conversation); R v Wood (1982) 76 Cr App Rep 23, CA; Castle v Cross [1984] 1 WLR 1372, DPP v McKeown [1997] 1 All ER 737, 2 Cr App Rep 155, HL (computer evidence).

[2113] A "statement" is now defined as any representation of fact or opinion made by a person by whatever means; and it includes a representation made in a sketch, photo or other pictorial form: Criminal Justice Act 2003 ss 115(2), 134 (2).

[2114] See in this context, for example, the Statue of Liberty case, [1968] 1 W.L.R. 739.

[2115] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

[2116] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

[2117] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

[2118] *Insa/Lazaro*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 214; *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 205.

[2119] Model Law on Electronic Evidence (LMM(02)12.

[2120] Singapore Evidence Act, Section 35.

[2121] Canada Uniform Electronic Evidence Act.

[2122] See above.

[2123] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. For more information, see: *Dumortier*, The European Directive 1999/93/EC on a Community Framework for Electronic Signatures, in Lodder/Kaspersen, eDirectives, 2000, page 33 *et seq.*, available at: www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf.

[2124] *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

[2125] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

[2126] *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

[2127] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2128] United Nations Report oft he International Law Commission, Fifty-eigth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm

[2129] *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

[2130] For a general overview see: *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

[2131] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2132] National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2133] *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

[2134] *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 6; *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

[2135] *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

[2136] International Court of Justice, Case of S.S."Lotus", Series A – No. 10, 1927, available at: www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

[2137] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.html; Dunn/Krishna-Hensel/Mauer (eds), The Resurgence of the State, Trends and Progress in Cyberspace Governance, 2007, page 69.

[2138] *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 8, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

[2139] For an overview about relevant case examples for conflicts see: *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 10 et seq.

[2140] *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 21.

[2141] See in this regard for example: *Ali/Ragothaman/Bhagavathula/Pendse*, Security Issues in Airplane Data Networks, available at: http://soar.wichita.edu/dspace/bitstream/handle/10057/398/GRASP-4.pdf?sequence=1; The Developments in Satellite Hardware, Satellite Executive Briefing, Vol. 3, No. 12, 2010, available at: www.satellitemarkets.com/pdf/aug10.pdf.

[2142] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2143] See *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Cameron*, Protective Principle of International Criminal Jurisdiction, 1994.

[2144] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2145] *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72. Regarding the use of the principle within the US see for example United States v. Gallaxy Sports.

[2146] See in this regard below: § 6.2.8.

[2147] *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72.

[2148] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2149] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2150] See: *Kobrick*, The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes, Columbia Law Review, Vol 87, 1987, page 1523 et seq; Regarding the discussion about scope and application of the principle of universal jurisdiction within the UN see the information provided by the Sixth Committee, available at: www.un.org/en/ga/sixth/64/UnivJur.shtml.

[2151] For an overview about the implementation of the principle in European countries see: Universal Jurisdiction in Europe – The State of the Art, Human Rights Watch, 2006, available at: www.hrw.org/sites/default/files/reports/ij0606web.pdf.

[2152] See above: §§ 4.5.4 and 6.1.

[2153] This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132. Regarding the substantive criminal law provisions related to cybercrime, see above: § 6.1.

[2154] Regarding the elements of an anti-cybercrime strategy, see above: § 4. Regarding user-based approaches in the fight against cybercrime, see: *Görling*, The Myth Of User Education, 2006, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[2155] Due to the protocols used in Internet communication and worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence, see above: § 3.2.7.

[2156] Regarding the challenges of fighting cybercrime, see above: § 3.2.

[2157] The pure fact that the offender is acting from a different country can result in additional challenges for law-enforcement agencies' investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases, the investigation nevertheless requires international cooperation between the authorities in both countries, which in general is more time consuming compared to investigations concentrating on a single country.

[2158] See in this context also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 134.

[2159] For an overview of the current status of the implementation of the Convention on Cybercrime and its procedural law provisions in selected countries, see the country profiles made available on the Council of Europe website: www.coe.int/cybercrime/.

[2160] See Articles 15-21 of the Council of Europe Convention on Cybercrime.

[2161] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[2162] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21.

[2163] *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

[2164] *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

[2165] For an overview of different kinds of evidence that can be collected by computer forensic experts, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[2166] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

[2167] For an overview of different forensic investigation techniques related to the most common technologies, see: *Carney/Rogers*, The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Vol. 2, Issue 4; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Urnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, Vol. 5, Issue 1; *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2; *Gupta/Mazumdar*; Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4; Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Vol. 5, Issue 1; *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233; *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

[2168] *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

[2169] Regarding the different models of Cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[2170] This includes the development of investigation strategies.

[2171] The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2172] With regard to developments, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[2173] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2174] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2175] *Vaciago*, Digital Evidence, 2012, Chapter II.1; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

[2176] For guidelines on how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2177] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[2178] Regarding investigation techniques, see: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, page 283 *et seq.*

[2179] *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No. 1.

[2180] *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, Vol. 19, page 1227 *et seq.*; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 54.

[2181] See below: § 6.3.8.

[2182] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 171.

[2183] Regarding the challenges of encryption, see § 3.2.14 as well as *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, Issue 3.

[2184] Regarding possible counter strategies for law enforcement, see: *Haldeman/Schoen/Heninger* and other, Lest we Remember: Cold Boot Attacks on Encryption keys, 2008, available at: http://citp.princeton.edu/memory.

[2185] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2186] *Vaciago*, Digital Evidence, 2012, Chapter II.1.

[2187] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 59.

[2188] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2189] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2190] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2191] *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

[2192] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, page 297.

[2193] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process in forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[2194] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the forensic software magic lantern, developed as a keylogger used by law enforcement in the US, see: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[2195] Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

[2196] *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2..

[2197] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 52.

[2198] For an overview of the debate, see: *Gercke*, The Role of Internet Service Providers in the Fight Against Child Pornography Computer Law Review International, 2009, page 65 *et seq.*

[2199] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 15.

[2200] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 24.

[2201] See *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime – Toward common best-of-breed guidelines?, 2008, available at: www.coe.int/cybercrime/.

[2202] For more information about the Guidelines, see: *Gercke,* The Council of Europe Guidelines for the Cooperation between LEAs and ISPs against Cybercrime, Computer Law Review International, 2008, page 97 *et seq.*

[2203] See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 29.

[2204] See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 30.

[2205] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2206] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

[2207] Regarding the impact on tracing offenders, see: *Nicoll*, Concealing and Revealing Identity on the Internet in *Nicoll/Prins/Dellen*, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 *et seq.*

[2208] *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

[2209] For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

[2210] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, No. 4.

[2211] For more information, see: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, § 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, page 149.

[2212] The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, The criminalization of Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide: Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

[2213] *Casey*, Digital Evidence and Computer Crime, 2004, page 19.

[2214] For more information, see: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten, 08.01.2007, available at: www.spiegel.de/panorama/justiz/0,1518,457844,00.html.

[2215] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 472.

[2216] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2217] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 90, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[2218] Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

[2219] *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

[2220] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2221] A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

[2222] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 64, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[2223] For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

[2224] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.

[2225] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[2226] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

[2227] With regard to the criminalization of illegal devices, see below: § 6.1.15.

[2228] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[2229] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2230] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 29.

[2231] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2232] Regarding the ability to manipulate the time information and the response in forensic investigations, see: *Gladyshev/Patel*, Formalizing Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1. Regarding dynamic time analysis, see: *Weil*, Dynamic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

[2233] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[2234] *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2235] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2236] See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

[2237] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[2238] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2239] For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

[2240] Regarding the related procedural instrument, see: Art. 19, paragraph 3 Convention on Cybercrime.

[2241] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 12.

[2242] *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf. With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2243] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2244] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 62.

[2245] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

[2246] See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801, for further reference

[2247] Taylor, The Council of Europe Cybercrime Convention – A civil liberties perspective, available at http://crime-research.org/library/CoE_Cybercrime.html; Cybercrime: Lizenz zum Schnueffeln Financial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at www.ccc.de.

[2248] See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 *et seq.*

[2249] Regarding the possibilities of making reservations, see Article 42 of the Convention on Cybercrime:

Article 42

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[2250] See above: § 5.2.1..

[2251] "Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

[2252] "There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

[2253] For the transformation of safeguards for Internet-related investigation techniques, see: *Taylor*, The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/taylor.pdf..

[2254] This is especially relevant with regard to the protection of the suspect of an investigation.

[2255] See: Article 37 – Accession to the Convention.

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

[2256] ABA International Guide to Combating Cybercrime, page 139.

[2257] "Interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" – Case of Kruslin v. France, Application No. 11801/85.

[2258] "The requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly", Case of Malone v. United Kingdom, Application No. 8691/79.

[2259] "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

[2260] "The expression "in accordance with the law", within the meaning of Article 8 § 2 (Art. 8-2), requires firstly that the impugned measure should have some basis in domestic law", Case of Kruslin v. France, Application No. 11801/85.

[2261] "Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject", Case of Doerga v. The Netherlands, Application No. 50210/99.

[2262] "It also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law", Case of Kruslin v. France, Application No. 11801/85.

"Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence." Case of Malone v. United Kingdom, Application No. 8691/79.

[2263] "The cardinal issue arising under Article 8 (Art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (Art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

[2264] "Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

[2265] The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

[2266] "National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 147.

[2267] See below: § 6.2.9.

[2268] See below: § 6.2.10.

[2269] "Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 230.

[2270] See below: § 6.3.4.

[2271] See below: § 6.3.7.

[2272] As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorizes the law-enforcement agencies to prevent the deletion of the relevant data. The advantage of separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application.

[2273] A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 of the Convention on Cybercrime.

[2274] A definition of the term "computer data" is provided in Art. 1 of the Convention on Cybercrime

[2275] As described more in detail below, the differentiation between "computer data" and "subscriber information" in Art. 18 of the Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.

[2276] "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 155. Regarding the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq*.

[2277] *Gercke*, Preservation of User Data, DUD 2002, 578.

[2278] The cost issue was especially raised within the discussion on data retention legislation in the EU. See, for example: E-communications service providers remain seriously concerned with the agreement reached by European Union Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005, available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

[2279] Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[2280] The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report of the Workshop on Potential Consequences for Data Retention of

Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001. A similar discussion took place during the negotiation of the Convention on Cybercrime. The drafters explicitly pointed out that the Convention does not establish a data retention obligation. See Explanatory Report to the Convention on Cybercrime, No. 151, available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[2281] Regarding The Data Retention Directive in the European Union, see: *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1, available at: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

[2282] Art. 6 Periods of Retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[2283] See: Preface 11 of the European Union Data Retention Directive: "Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."

[2284] Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[2285] See, for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes – Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US, see: ABA International Guide to Combating Cybercrime, page 59.

[2286] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

[2287] However, it is recommended that states consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

[2288] *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[2289] See: *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

[2290] "Preservation" requires that data which already exists in a stored form be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

[2291] Explanatory Report, No. 152.

[2292] Regarding the advantages of a system of graded safeguards, see above: § 6.3.3.

[2293] "The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)". See Explanatory Report to the Convention on Cybercrime, No. 160.

[2294] The drafters of the Convention on Cybercrime tried to approach the problems related to the need for immediate action from law-enforcement agencies on the one hand and the importance of ensuring safeguards on the other in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law-enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime, No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the

submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

[2295] *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[2296] An IP address does not necessary immediately identify the offender. If law-enforcement agencies know the IP address an offender used to commit an offence, this information only enables them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café), further investigations are necessary to identify the offender

[2297] If the offender is using services that do not require a registration or if the subscriber information provided by the user is not verified, Art. 18 Subparagraph 1b) will not enable the law-enforcement agencies to immediately identify the offender. Art. 18 Subparagraph 1b) is therefore especially relevant with regard to commercial services (like providing Internet access, commercial e-mail or hosting services).

[2298] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

[2299] "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

[2300] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2301] Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

[2302] The Commonwealth Model Law contains an alternative provision:

"Sec. 16: If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

(b) the path through which the communication was transmitted."

[2303] For an introduction to data retention, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*; *Blanchette/Johnson*, Data retention and the panoptic society: The social benefits of forgetfulness, available at: http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

[2304] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[2305] Judgement in Joined Cases C-293/12 and C-594/12.

[2306] See, for example: Briefing for the Members of the European Parliament on Data Retention, available at: www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: www.vibe.at/aktionen/200205/data_retention_30may2002.pdf. Regarding the concerns relating to violation of the European Convention on Human Rights, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

[2307] See: Heise News, 13 000 determined to file suit against data retention legislation, 17.11.2007, available at: www.heise.de/english/newsticker/news/99161/from/rss09.

[2308] Case C-275/06.

[2309] See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

[2310] In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

[2311] Regarding the challenges for law-enforcement agencies related to the use of means of anonymous communication, see above: § 3.2.12.

[2312] Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[2313] An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2314] See: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

[2315] Regarding the impact of use of anonymous communication technology on the work of law-enforcement agencies, see above: § 3.2.12.

[2316] Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2317] Regarding protection of the use of anonymous means of communication by the United States constitution, see: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 82, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

[2318] Judgement in Joined Cases C-293/12 and C-594/12.

[2319] A detailed overview of the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.* Regarding remote live search and possible difficulties with regard to the principle of chain of custody, see: *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law and Technology Vol. 9, Issue 2, 2005, available at: www.lawtechjournal.com/articles/2005/05_051201_Kenneally.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2320] Regarding the involvement of computer forensic experts in investigations, see above: § 6.3.2

[2321] Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants

to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

[2322] See below: § 6.3.12.

[2323] Apart from the fact that direct access enables the law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[2324] See Explanatory Report to the Convention on Cybercrime, No. 184.

[2325] "However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data." Explanatory Report to the Convention on Cybercrime, No. 184. Regarding the special demands with regard to computer-related search and seizure procedures, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2326] Explanatory Report, No. 184.

[2327] Regarding the difficulties of online search procedures, see below: § 6.3.12.

[2328] See in this context: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

[2329] Regarding the requirements in the US, see for example: *Brenner*, Michigan Telecommunications and Technology Law Review, 2001-2002, Vol. 8, page 41 *et seq.*; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2330] "However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record." Explanatory Report to the Convention on Cybercrime, No. 187.

[2331] *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[2332] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[2333] The importance of being able to extend the search to connected computer systems was already addressed by Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the recommendation is available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf.

[2334] In this context, it is important to keep in mind the principle of national sovereignty. If the information is stored on a computer system outside the territory, an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be in its territory"– Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue, see also: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2335] For guidelines how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2336] Regarding the classification of the act of copying the data, see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*

[2337] "Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data". Explanatory Report to the Convention on Cybercrime, No. 197.

[2338] This principle also applies with regard to the seizure of hardware. Compared to maintaining the integrity of copied data it is often easier to maintain the integrity of data on a storage device.

[2339] See above: § 2.6.

[2340] One possibility to prevent access to the information without deleting it is the use of encryption technology.

[2341] See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

[2342] The fact that law-enforcement agencies are able to access certain data stored outside the country through a computer system in their territory does not automatically legalize the access. See Explanatory Report to the Convention on Cybercrime, No. 195. "This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation." Two cases of transborder access to stored computer data are regulated in Art. 32 Convention on Cybercrime:

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[2343] "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

[2344] "A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data." Explanatory Report to the Convention on Cybercrime, No. 201.

[2345] Explanatory Report to the Convention on Cybercrime, No. 202.

[2346] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2347] Official Note: If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.

[2348] Official Note: A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self-incrimination.

[2349] Regarding the motivation of the drafters, see Explanatory Report to the Convention on Cybercrime, No. 171.

[2350] "A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be

beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability." Explanatory Report to the Convention on Cybercrime, No. 171.

[2351] Explanatory Report to the Convention on Cybercrime, No. 173.

[2352] "At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement." Explanatory Report to the Convention on Cybercrime, No. 173.

[2353] Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication, see above: § 3.2.12.

[2354] If the providers offer their service free of charge, they do often either require an identification of the user nor do at least not verify the registration information.

[2355] See above: § 6.3.5.

[2356] Explanatory Report to the Convention on Cybercrime, No. 172.

[2357] This can be, for example, information that was provided on a classic registration form and kept by the provider as paper records.

[2358] The Explanatory Report even points out that the parties to the Convention can adjust their safeguards with regard to specific data within each of the categories. See Explanatory Report to the Convention on Cybercrime, No. 174: "Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

[2359] For example, the requirement of a court order.

[2360] The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 21) shows that the drafters of the Convention realized the importance of separating instruments with different impact.

[2361] See below: § 6.3.9.

[2362] See below: § 6.3.10.

[2363] Art. 21 of the Convention on Cybercrime obliges the signatory states to implement the possibility to intercept content data only with regard to serious offences ("Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law"). On the contrary, Art. 20 of the Convention on Cybercrime is not limited to serious offences. "Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

[2364] Regarding the advantages of a graded system of safeguards, see above: § 6.3.3.

[2365] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2366] Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other

countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

[2367] Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel, see: Legal Opinion on Intercept Communication, 2006, available at: www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

[2368] In these cases, other technical solutions for surveillance need to be evaluated. Regarding possible physical surveillance techniques, see: *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997, page 384 *et seq.*

[2369] Regarding the interception of VoIP to assist law-enforcement agencies, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2370] Regarding the interception of VoIP to assist law-enforcement agencies, see: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 48, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.htm; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2371] In particular, lack of technical preparation of Internet providers to collect the relevant data in real time.

[2372] Explanatory Report to the Convention on Cybercrime, No. 205.

[2373] ABA International Guide to Combating Cybercrime, page 125.

[2374] ABA International Guide to Combating Cybercrime, page 125.

[2375] The "origin" refers to a telephone number, Internet protocol (IP) address or similar identification of a communications facility to which a service provider renders services. Explanatory Report to the Convention on Cybercrime, No. 30.

[2376] "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in cybercrime investigations, see also: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 *et seq.*

[2377] "In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a))." Explanatory Report to the Convention on Cybercrime, No. 223.

[2378] The Convention does not define technical standards regarding the design of such an interface. Explanatory Report to the Convention on Cybercrime, No. 220.

[2379] Explanatory Report to the Convention on Cybercrime, No. 223.

[2380] "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Explanatory Report to the Convention on Cybercrime, No. 221.

[2381] See above: § 3.2.12.

[2382] Tor is a software that enables users to protect against traffic analysis. For more information about the software, see: http://tor.eff.org/.

[2383] An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request an identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2384] This advantage is also relevant for remote forensic investigations. See below: § 6.3.12.

[2385] Such obligation might be legal or contractual.

[2386] Explanatory Report to the Convention on Cybercrime, No. 226.

[2387] Regarding the key intention, see Explanatory Report on the Convention on Cybercrime No. 16: "The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation."

[2388] The drafters of the Convention point out that the signatory states should limit the use of the right to make reservations in this context: Explanatory Report to the Convention on Cybercrime, No. 213.

Regarding the possibilities of making reservations, see Art. 42 Convention on Cybercrime:

Article 42

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No. other reservation may be made.

[2389] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at:

www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers,* Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2390] One possibility to prevent law-enforcement agencies from analysing the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures, see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[2391] Regarding the impact of encryption technology on computer forensic and criminal investigations, see: *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge, see below: § 6.3.11.

[2392] *Schneier*, Applied Cryptography, page 185.

[2393] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2394] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[2395] *Schneier*, Applied Cryptography, page 185.

[2396] Regarding practical approaches to recover encrypted evidence, see: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at:

[2397] The issue is, for example, addressed by Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with information, 11 September 1995: "14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary" and the G8 in the 1997 Meeting in Denver: "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines. Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies."

[2398] For more information, see: *Koops*, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

[2399] The need for such authorization is mentioned, for example, in principle 6 of the 1997 Guidelines for Cryptography Policy: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

[2400] This topic was discussed in the deliberations of the US District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow law-enforcement agencies to make use of a software to record keystrokes on a suspect's computer (keylogger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers). See: www.epic.org/crypto/scarfo/opinion.html.

[2401] Export limitations on encryption software capable of processing strong keys are not designed to facilitate the work of law-enforcement agencies in the country. The intention of such regulations is to prevent the availability of the technology outside the country. For detailed information on import and export restrictions with regard to encryption technology, see: http://rechten.uvt.nl/koops/cryptolaw/index.htm.

[2402] The limitation of the import of such powerful software is even characterized as "misguided and harsh to the privacy rights of all citizens". See, for example: The Walsh Report – Review of Policy relating to Encryption Technologies 1.1.16 available at: www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

[2403] See: *Lewis*, Encryption Again, available at: www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

[2404] The key escrow system was promoted by the United States Government and implemented in France for a period in 1996. For more information, see: Cryptography and Liberty 2000 – An International Survey of Encryption Policy, available at: www2.epic.org/reports/crypto2000/overview.html#Heading9.

[2405] See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 *et seq.*

[2406] "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management. which may allow, consistent with these guidelines. lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies", www.g7.utoronto.ca/summit/1997denver/formin.htm.

[2407] See, for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf; Australia, Cybercrime Act, Art. 12, available at: http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf; Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at: http://staatsbladclip.zita.be/staatsblad/wetten/2001/02/03/wet-2001009035.html; France, Loi pour la confiance dans l'économie numérique, Section 4, Art. 37, available at: www.legifrance.gouv.fr/affichTexte.do;jsessionid=B78A2A8ED919529E3B420C082708C031.tpdjo12v_3?cidTexte=JORFTEXT000000801164&dateTexte=20080823; United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at: www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative à l'échange électronique de données juridiques, Chapter III, available at: http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/; Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: www.info.gov.za/gazette/acts/2002/a70-02.pdf; Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

[2408] An example can be found in Sec. 69 of the Indian Information Technology Act 2000: "Directions of Controller to a subscriber to extend facilities to decrypt information.(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." For more information about the Indian Information Technology Act 2000, see: *Duggal*, India's Information Technology Act 2000, available under: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf.

[2409] For general information on the Act, see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses, available at: www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

[2410] For an overview of the regulation, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

[2411] Regarding the discussion of protection against self-incrimination under United States law, see for example: *Clemens*, No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private key, UCLA Journal of Law and Technology, Vol. 8, Issue 1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: www.richmond.edu/jolt/v2i1/sergienko.html; *O'Neil*, Encryption and the First Amendment, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art1.pdf; *Fraser*, The Use of Encrypted, Coded and Secret Communication is an "Ancient Liberty" Protected by the United States Constitution, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art2.pdf; *Park*, Protecting the Core Values of the First Amendment in an age of New Technology: Scientific Expression vs. National Security, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art3.pdf; Hearing before the Subcommittee on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary, United States Senate, 150 Congress, Second Session on Examining the Use of Encryption, available at: www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe on self-incrimination, in particular with regard to the European Convention on Human Rights (ECHR), see: *Moules*, The Privilege against self-incrimination and the real evidence, The Cambridge Law Journal, 66, page 528 *et seq.*; *Mahoney*, The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR, Judicial Studies Institute Journal, 2004, page 107 *et seq.*; *Birdling*, Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom, International Journal of Evidence and Proof, Vol. 12, Issue 1, 2008, page 58 *et seq.*; Commission of the European Communities, Green Paper on the Presumption of Innocence, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:pdf.

[2412] Regarding the situation in the US, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

[2413] In this context, see also: *Walker*, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: www.bileta.ac.uk/01papers/walker.html.

[2414] *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

[2415] Regarding possibilities to circumvent the obligations, see: *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm.

[2416] A detailed overview of the elements of search procedures as well as the challenges of carrying them out is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the

office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.*

[2417] Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an ongoing investigation based on Art. 20 confidential, see above: § 6.3.9.

[2418] There are disadvantages related to remote investigations. Apart from the fact that direct access enables law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system it is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[2419] Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

[2420] See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.200, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[2421] See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: www.heise-security.co.uk/news/92950.

[2422] Computer and Internet protocol address verifier.

[2423] A copy of the search warrant is available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search, see: www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf. For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

[2424] Regarding the discussion in Germany, see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware "specialists" to bug terrorists, The Register, 21.11.2007, available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: www.spiegel.de/international/germany/0,1518,502955,00.html.

[2425] See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: www.tagesspiegel.de/politik/;art771,1989104.

[2426] For an overview, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

[2427] The search function was the focus of the decision of the German Supreme Court in 2007. See: Online police searches found illegal in Germany, 14.02.2007, available at: www.edri.org/edrigram/number5.3/online-searches.

[2428] Regarding investigations involving VoIP, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2429] See: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf. Keylogging is the focus of the FBI software "magic lantern". See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf. See also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[2430] This is the focus of the US investigation software CIPAV. Regarding the functions of the software, see the search warrant, available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf.

[2431] Regarding these functions, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

[2432] Regarding the possible ways of infecting a computer system by spyware, see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

[2433] With regard to the efficiency of virus scanners and protection measures implemented in the operating systems, it is likely that the functioning of a remote forensic software would require the cooperation of software companies. If software companies agree to prevent detection of remote forensic software, this could result in serious risks for computer security. For more information, see: *Gercke*, Computer und Recht 2007, page 249.

[2434] If the offender stores illegal content on an external storage device that is not connected to a computer system, the investigators will in general not be able to identify the content if they only have access to the computer system via remote forensic software.

[2435] Regarding the importance of maintaining integrity during a forensic investigation, see: *Hosmer*, Providing the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2436] National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2437] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2438] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2439] See above: § 3.2.12.

[2440] Based on Art. 7, "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electrnic data transmission or other communications, are made available to the public, to customers or members" is obliged to require a licence from local authorities and identify persons using the service. For more information, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

[2441] Decree 144/2005, 27 July 2005 ("Decreto-legge"). Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article, Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[2442] For more details, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

[2443] *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

[2444] Regarding the related challenges, see: *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

[2445] International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005.

[2446] *Büllingen/Gillet/Gries/Hillebrand/Stamm*, Situation and Perspectives of Data Retention in an international comparison (Stand und Perspectiven der Vorratsdatenspeichung im internationalen Vergleich), 2004, page 10, available at: www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

[2447] *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

[2448] Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[2449] See above: § 3.2.7.

[2450] See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2451] See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2452] *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[2453] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

[2454] The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2455] Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

[2456] The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

[2457] Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

[2458] European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

[2459] Council of Europe Convention on Cybercrime, ETS 185.

[2460] See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2461] A full list of agreements is available at: www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

[2462] Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

[2463] See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, page 119.

[2464] Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.

[2465] *Choo,* Trends in Organized Crime, 2008, page 273.

[2466] *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4, page 27.

[2467] See, for example: Great Britain Crown Prosecution Service, Convictions for internet rape plan, Media release, 01.12.2006.

[2468] *Choo,* Trends in Organized Crime, 2008, page 273.

[2469] For further details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2470] According to the report of the expert meeting held between 8 and 10 October 2008, there are certain states which require special provisions in their internal law to allow such spontaneous information, while others can transmit information spontaneously without such internal provisions in force: see CTOC/COP/2008/18 page 5.

[2471] For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 226, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2472] For details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 225, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf..

[2473] See, for example, Art. 29 and Art. 35 Convention on Cybercrime.

[2474] The directory is available at: www.unodc.org/compauth/en/index.html. Access requires registration and is reserved for competent national authorities.

[2475] The directory indicates the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific requests of the receiving states and sometimes even extracts from domestic legislation of that state.

[2476] See CTOC/COP/2008/18, paragraph 27.

[2477] See Art. 25, paragraph 3 of the Convention on Cybercrime.

[2478] The software is available at: www.unodc.org/mla/index.html

[2479] See Explanatory Report to the Convention on Cybercrime, No. 243. The Member States have the possibility to limit the international cooperation with regard to certain measures (extradition, real time collection of traffic data and the interception of content data).

[2480] If, for example, two countries involved in a cybercrime investigation already have bilateral agreements in place that contain the relevant instruments, those agreements will remain a valid basis for the international cooperation.

[2481] Regarding the difficulties with the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

[2482] The Explanatory Report clarifies that the determination of the covered offences does not depend on the actual penalty imposed in the particular cases. See: Explanatory Report to the Convention on Cybercrime, No. 245.

[2483] Regarding the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

[2484] See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2485] See above: § 3.2.10.

[2486] See Explanatory Report to the Convention on Cybercrime, No. 256.

[2487] This information often leads to successful international investigations. For an overview of large-scale international investigations related to child pornography, see: *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296, page 4, available at: www.ecpat.se/upl/files/279.pdf.

[2488] Similar instruments can be found in other Council of Europe conventions. For example, Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 28 of the Criminal Law Convention on Corruption. Council of Europe conventions are available at: www.coe.int.

[2489] See Explanatory Report to the Convention on Cybercrime, No. 262.

[2490] Regarding the 24/7 network points of contact, see below: § 6.4.12.

[2491] See Explanatory Report to the Convention on Cybercrime, No. 265: "Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly."

[2492] See Explanatory Report to the Convention on Cybercrime, No. 268.

[2493] See Explanatory Report to the Convention on Cybercrime, No. 269. "Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal."

[2494] See Explanatory Report to the Convention on Cybercrime, No. 269.

[2495] See above: § 6.3.

[2496] The most important instruments established by the Convention on Cybercrime are: Expedited preservation of stored computer data (Art. 16), Expedited preservation and partial disclosure of traffic data (Art. 17), Production order (Art. 18), Search and seizure of stored computer data (Art. 19), Real-time collection of traffic data (Art. 20), Interception of content data (Art. 21).

[2497] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2498] An exemption is Art. 32 of the Convention on Cybercrime – See below. Regarding the concerns related to this instrument, see: Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: " […] Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32b in particular in the light of experience gained from the use of this Article).

[2499] See above: § 6.3.4.

[2500] See above: § 6.3.4.

[2501] See above: § 6.3.7.

[2502] See above: § 6.3.6.

[2503] See above: § 6.3.9.

[2504] See above: § 6.3.10.

[2505] See Explanatory Report to the Convention on Cybercrime, No. 293.

[2506] "The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules." See Explanatory Report to the Convention on Cybercrime, No. 293.

[2507] See below in this chapter.

[2508] See Explanatory Report to the Convention on Cybercrime, No. 293.

[2509] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

[2510] See: Challenges and Best Practices in Cybercrime Investigation, 2008, available at: www.unafei.or.jp/english/pdf/PDF_rms/no79/15_P107-112.pdf.

[2511] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2512] For more information, see: A Draft Commentary on the Council of Europe Convention, October 2000, available at: www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf.

[2513] In this context, it is necessary to point out a difference between Art. 32 and Art. 18. Unlike Art. 18, Art. 32 does not enable a foreign law-enforcement agency to order the submission of the relevant data. It can only seek permission.

[2514] Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, 19-20 October 1999.

[2515] Principles on Transborder Access to Stored Computer Data, available at: www.justice.gov/criminal/cybercrime/g82004/99TransborderAccessPrinciples.pdf.

[2516] The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2517] See above: § 6.3.4.

[2518] Availability 24 hours a day and 7 days a week is especially important with regard to the international dimension of cybercrime, as requests can potentially come from any time zone in the world. Regarding the international dimension of cybercrime and the related challenges, see above: § 3.2.6.

[2519] See Explanatory Report to the Convention on Cybercrime, No. 298.

[2520] Regarding the activities of the G8 in the fight against cybercrime, see above: § 5.1.1. For more information on the 24/7 Network, see: *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 484, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.

[2521] See above: § 3.2.10.

[2522] See above: § 3.2.6.

[2523] Regarding the question of which authorities should be authorized to order the preservation of data, see above: § 6.3.4.

[2524] Explanatory Report to the Convention on Cybercrime, No. 301.

[2525] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

[2526] *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

[2527] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

[2528] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[2529] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[2530] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[2531] Regarding the network architecture and the consequences with regard to the involvement of service providers, see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003, available at: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[2532] See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

[2533] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2534] For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2535] In the decision Recording Industry Association Of America v. Charter Communications, Inc., the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the United States DMCA by pointing out the balance. In the opinion of the court, DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

[2536] Regarding the history of DMCA and pre-DMCA case law in the United States, see: *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Salow*, Liability Immunity for Internet Service Providers – How is it working?, Journal of Technology Law and Policy, Vol. 6, Issue 1, 2001, available at: http://grove.ufl.edu/~techlaw/vol6/issue1/pearlman.html.

[2537] Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html.

[2538] Regarding the application of DMCA to search engines, see: *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

[2539] 17 USC. § 512(a)

[2540] 17 USC. § 512(b)

[2541] Regarding the Communications Decency Act, see: *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf;

[2542] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union e-commerce regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches
To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*, available at: www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

[2543] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[2544] Art. 12 – Art. 15 EU of the E-Commerce Directive.

[2545] With the number of different services covered, the E-Commerce Directive aims for a broader regulation than 17 USC. § 517(a). Regarding 17 USC. § 517(a).

[2546] See Art. 12 paragraph 3 of the E-Commerce Directive.

[2547] The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2548] Regarding traditional caching as well as active caching, see: *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

[2549] For more information on proxy servers, see: *Luotonen*, Web Proxy Servers, 1997.

[2550] The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2551] See above: § 6.5.4.

[2552] Regarding the impact of free webspace on criminal investigations, see: *Evers*, Blogging sites harbouring cybercriminals, CNET News, 26.07.2005, available at: http://news.zdnet.co.uk/security/0,1000000189,39210633,00.htm.

[2553] This procedure is called "notice and takedown".

[2554] The hosting provider is quite often in a difficult situation. On the one hand, it needs to react immediately to avoid liability; on the other hand, it has certain obligations to its customers. If it removes legal information that was just at first sight illegal, this could lead to claims for indemnity.

[2555] By enabling their customers to offer products, they provide the necessary storage capacity for the required information.

[2556] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2557] See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2558] See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[2559] *Spindler*, Multimedia und Recht 1999, page 204.

[2560] Art. 21 – Re-examination

1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.

2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, 'notice and take down' procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

[2561] *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

[2562] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[2563] See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[2564] § 17 – Ausschluss der Verantwortlichkeit bei Links

(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

[2565] *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, page 5, available at: www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

[2566] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

[2567] See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

[2568] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) – Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (Spain)

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No. tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

[2569] Ausschluss der Verantwortlichkeit bei Suchmaschinen

§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er

1. die Übermittlung der abgefragten Informationen nicht veranlasst,

2. den Empfänger der abgefragten Informationen nicht auswählt und

3. die abgefragten Informationen weder auswählt noch verändert.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Unión International de las Telecomunicaciones (UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Oficina del Director
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Director Adjunto y
Jefe del Departamento de
Administración y Coordinación
de las Operaciones (DDR)
Correo-e: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Departamento de Infraestructura,
Entorno Habilitador y
Ciberaplicaciones (IEE)
Correo-e: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Departamento de Innovación y
Asociaciones (IP)
Correo-e: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Departamento de Apoyo a los
Proyectos y Gestión del
Conocimiento (PKM)
Correo-e: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

África

Etiopía

International Telecommunication
Union (ITU)
Oficina Regional
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Etiopía

Correo-e: itu-addis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Camerún

Union internationale des
télécommunications (UIT)
Oficina de Zona
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Camerún

Correo-e: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des
télécommunications (UIT)
Oficina de Zona
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Senegal

Correo-e: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication
Union (ITU)
Oficina de Zona de la UIT
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Correo-e: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Américas

Brasil

União Internacional de
Telecomunicações (UIT)
Oficina Regional
SAUS Quadra 06, Bloco "E"
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Correo-e: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication
Union (ITU)
Oficina de Zona
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Correo-e: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chile

Correo-e: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Correo-e: ituteguciglapa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Estados Árabes

Egipto

International Telecommunication
Union (ITU)
Oficina Regional
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egipto

Correo-e: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacífico

Tailandia

International Telecommunication
Union (ITU)
Oficina de Zona
Thailand Post Training Center ,5th floor
111 Chaengwattana Road, Laksi
Bangkok 10210 – Tailandia

Dirección postal:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Tailandia

Correo-e: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication
Union (ITU)
Oficina de Zona
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Dirección postal:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

Correo-e: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

Países de la CEI

Federación de Rusia

International Telecommunication
Union (ITU)
Oficina de Zona
4, Building 1
Sergiy Radonezhsky Str.
Moscú 105120 – Federación de Rusia

Dirección postal:
P.O. Box 25 – Moscú 105120
Federación de Rusia

Correo-e: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europa

Suiza

Union internationale des
télécommunications (UIT)
Oficina de Desarrollo de las
Telecomunicaciones (BDT)
Unidade Europa (EUR)
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: eurregion@itu.int
Tel.: +41 22 730 5111

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza
www.itu.int

ISBN 978-92-61-15643-5 SAP id 39679

Impreso en Suiza
Ginebra, 2014

11/2014