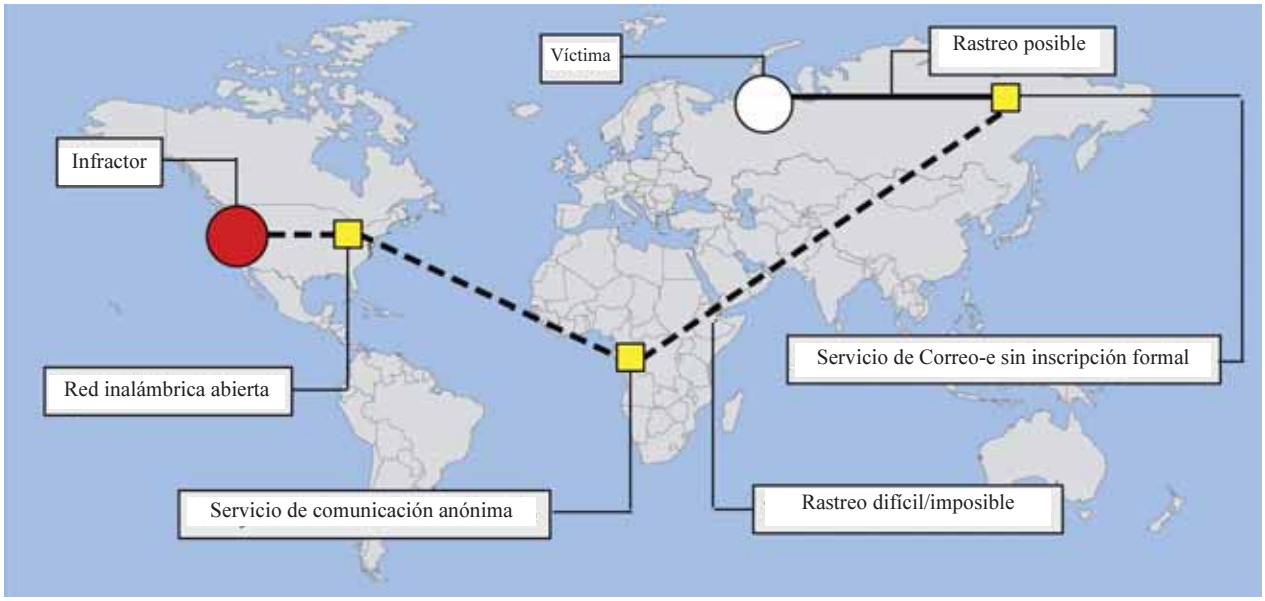
Unión Internacional de Telecomunicaciones

Recursos jurídicos contra el ciberdelito



EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO

División de Aplicaciones TIC y Ciberseguridad
Departamento de Políticas y Estrategias
Sector de Desarrollo de las Telecomunicaciones de la UIT

Proyecto de abril de 2009

Para mayor información póngase en contacto con la
División de Aplicaciones TIC y Ciberseguridad del UIT-D en cybmail@itu.int

Unión Internacional de Telecomunicaciones

Agradecimientos

Este Informe fue encargado por la División de Aplicaciones TIC y Ciberseguridad del Sector de Desarrollo de la UIT.

El Ciberdelito: Guía para los países en desarrollo, fue elaborado por el Dr. Marco Gercke. El autor desea agradecer al equipo del Sector de Desarrollo de las Telecomunicaciones su apoyo y al Gunhild Scheer los amplios debates celebrados al respecto.

Las denominaciones y clasificaciones empleadas en esta publicación no implican ninguna opinión sobre la categoría jurídica o de otro tipo de cualquier territorio ni cualquier responsabilidad o aceptación de ninguna frontera. Cuando aparece la denominación "país" en esta publicación se refiere a países y territorios.

La publicación de la UIT "El Ciberdelito: Guía para los países en desarrollo" está disponible en línea en la siguiente dirección:

www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

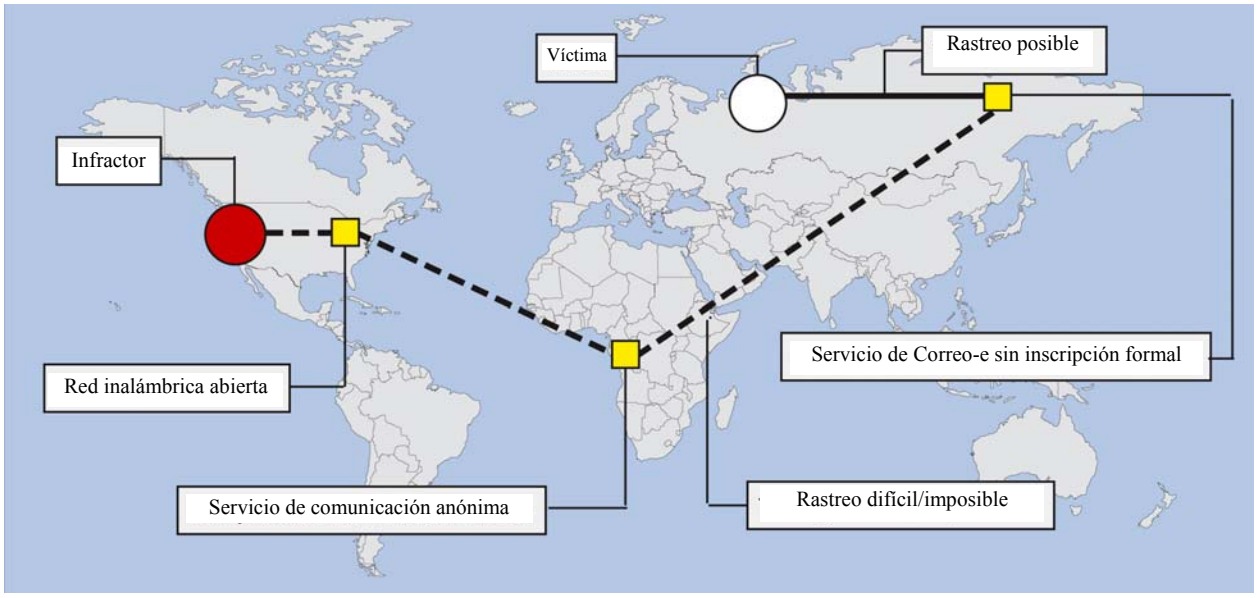
Este documento se ha formateado para su impresión recto-verso. El documento se ha publicado sin edición formal. Para más información sobre la publicación póngase en contacto con:

División de Aplicaciones TIC y Ciberseguridad (CYB)
Departamento de Políticas y Estrategias
Oficina de Desarrollo de las Telecomunicaciones
Unión Internacional de Telecomunicaciones
Place des Nations
1211 Ginebra 20
Suiza

Teléfono: +41 22 730 5825/6052
Fax: +41 22 730 5484
Correo-e: cybmail@itu.int
Dirección web: www.itu.int/ITU-D/cyb/

Cláusula de exención de responsabilidad

Las opiniones expresadas en este Informe son las del autor y no representan necesariamente las opiniones de la Unión Internacional de Telecomunicaciones (UIT) o de sus miembros. Las denominaciones utilizadas y la presentación del material, incluidos los mapas, no implican la expresión de opinión alguna por parte de la UIT sobre la situación jurídica de cualquier país, territorio, ciudad o zona, o relativa a la delimitación de sus límites o fronteras. La mención y referencia a empresas, productos, iniciativas, directrices o países específicos no implica su aprobación ni recomendación por parte de la UIT con preferencia a otros de naturaleza similar que no se hayan mencionado.



EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO

División de Aplicaciones TIC y Ciberseguridad
Departamento de Políticas y Estrategias
Sector de Desarrollo de las Telecomunicaciones de la UIT

Proyecto de abril de 2009

Para mayor información póngase en contacto con la
División de Aplicaciones TIC y Ciberseguridad del UIT-D en cybmail@itu.int

Unión Internacional de Telecomunicaciones

ABREVIATURAS

ABA	Asociación de Abogados de Estados Unidos (*American Bar Association*)
APEC	Foro de cooperación económica de Asia-Pacífico (*Asia-Pacific Economic Cooperation Forum*)
APIG	Grupo Internet multipartito (*All Party Internet Group*)
ASEAN	Asociación de Naciones del Sudeste Asiático (*Association of Southeast Asian Nations*)
CFAA	Ley sobre el fraude y abuso informáticos (EE.UU.) (*Computer Fraud and Abuse Act (U.S.)*)
CMA	Ley sobre utilización fraudulenta informática (Reino Unido y Singapur) (*Computer Misuse Act (U.K.) & Computer Misuse Act (Singapore)*)
CoE	Consejo de Europa (*Council of Europe*)
DDoS	Denegación de servicio distribuida (*Distributed Denial of Service*)
CE	Comisión Europea
Regulaciones	Regulaciones sobre comunicaciones privadas y electrónicas, 2003 (Reino Unido) de la CE
ECPA	Ley sobre privacidad de las comunicaciones electrónicas (Estados Unidos) (*Electronic Communications Privacy Act (U.S.)*)
UE	Unión Europea
G8	Grupo de las Ocho Naciones
GCA	Agenda sobre Ciberseguridad Global (*Global Cybersecurity Agenda*)
IAG	Grupo de asistencia internacionales (Canadá) (*International Assistance Group (Canada)*)
TIC	Tecnologías de la información y la comunicación
IRG	Ley sobre recursos internacionales contra el delito (*Gesetz über die Internationale Rechtshilfe in Strafsachen*)
UIT	Unión Internacional de Telecomunicaciones
OCDE	Organización de Cooperación y Desarrollo Económicos
OWig	Ley sobre irregularidades (Alemania) (*Gesetz über Ordnungswidrigkeiten (Germany)*)
PACC	Comisión de la ABA sobre delitos contra la privacidad e informáticos (*ABA Privacy & Computer Crime Committee*)
RIPA	Ley de poderes de regulación de la investigación (Reino Unido) (*Regulation of Investigatory Powers Act (United Kingdom)*)
StGB	Código Penal de Alemania (*German Criminal Code (Strafgesetzbuch)*)
StPO	Código alemán de procedimiento penal (*German Code of Criminal Procedure (Strafprozessordnung)*)
TKG	Ley de Telecomunicaciones de Alemania (*German Telecommunications Act (Telekommunikationgesetz)*)
RU	Reino Unido
NU	Naciones Unidas
UrhG	Ley de Propiedad Intelectual de Alemania (*German Copyright Act (Urheberrechtsgesecht)*)
EE.UU.	Estados Unidos
CMSI	Cumbre Mundial sobre la Sociedad de la Información

OBJETIVO

El objetivo de la publicación de la UIT **El Ciberdelito: Guía para los países en desarrollo** es ayudar a los países a comprender los aspectos jurídicos de la ciberseguridad y armonizar el marco legal. Por consiguiente, la Guía tiene por objeto ayudar a los países en desarrollo a entender mejor las implicaciones nacionales e internacionales de las ciberamenazas en constante crecimiento, evaluar los requisitos de los actuales instrumentos nacionales, regionales e internacionales y colaborar con los países para establecer unas bases jurídicas sólidas.

La Guía proporciona una perspectiva completa de los temas más importantes vinculados a los aspectos jurídicos del ciberdelito. En su enfoque, la Guía se centra en las demandas de los países en desarrollo. Debido a la dimensión transnacional del ciberdelito, los instrumentos jurídicos son los mismos para los países desarrollados y en desarrollo. No obstante, las referencias utilizadas se seleccionaron en beneficio de los países en desarrollo. La Guía ofrece una amplia selección de recursos para un estudio más profundo de los diferentes temas. Siempre que ha sido posible se han utilizado fuentes públicamente disponibles, incluidas muchas ediciones gratuitas de boletines jurídicos en línea.

La Guía consta de seis Capítulos principales. Tras una introducción (*Capítulo 1*) la Guía presenta el fenómeno del ciberdelito (*Capítulo 2*). Ello incluye la descripción de la forma en que se cometen los delitos y explicaciones sobre los ciberdelitos más habituales tales como el pirateo, el robo de identidad y los ataques contra la denegación de servicio. La Guía también proporciona un resumen de los retos a los que se enfrenta la investigación y procesamiento del ciberdelito (*Capítulos 3* y *4*). Tras resumir algunas de las actividades emprendidas por las organizaciones internacionales y regionales en su lucha contra el ciberdelito (*Capítulo 5*), la Guía continúa con un análisis de los distintos enfoques jurídicos con respecto a leyes penales sustantivas, leyes de procedimiento, cooperación internacional y responsabilidad de los suministradores del servicio Internet (*Capítulo 6*), incluyendo ejemplos de métodos internacionales y de prácticas idóneas adaptadas a partir de soluciones nacionales.

La publicación **El Ciberdelito: Guía para los países en desarrollo** aborda el primero de los siete objetivos estratégicos de la Agenda sobre Ciberseguridad Global (GCA) de la UIT, que recomienda la preparación de estrategias que promuevan el desarrollo de una legislación sobre ciberdelitos, que resulte aplicable a escala mundial y sea compatible con las medidas legislativas ya adoptadas en los diferentes países y regiones. También aborda el enfoque de la C.22/1 de la Comisión de Estudio 1 del UIT-D en el sentido de organizar los esfuerzos de la ciberseguridad nacional. La adopción por todos los países de las medidas jurídicas apropiadas contra la utilización fraudulenta de las tecnologías de la información y la comunicación con propósitos delictivos o de otro tipo, incluidas las actividades destinadas a afectar la integridad de las infraestructuras de la información crítica nacional, es fundamental para lograr la ciberseguridad global. Como las amenazas pueden proceder de cualquier parte del mundo, los retos son intrínsecamente internacionales y requieren la cooperación internacional, la asistencia en la investigación y las provisiones comunes sustantivas y de procedimiento. En consecuencia, es importante que los países armonicen sus marcos jurídicos para combatir el ciberdelito y facilitar la cooperación internacional.

ÍNDICE

Página

1 Introducción

1.1 Infraestructuras y servicios

Internet es una de las áreas de más rápido crecimiento en el desarrollo de la infraestructura técnica[1]. Actualmente, las tecnologías de la información y la comunicación (TIC) están omnipresentes y cada vez es mayor la tendencia hacia la digitalización. La demanda de Internet y la conectividad informática ha dado lugar a la integración de la tecnología informática en productos que normalmente funcionaban sin ella, tales como los automóviles y los edificios[2]. El suministro de energía eléctrica, la infraestructura del transporte, los servicios y logística miliares y prácticamente todos los servicios modernos dependen de la utilización de las TIC[3].

Aunque el desarrollo de las nuevas tecnologías se centra principalmente en satisfacer la demanda del usuario en los países occidentales, los países en desarrollo también pueden beneficiarse de estas nuevas tecnologías[4]. Con la aparición de tecnologías de comunicaciones inalámbricas a larga distancia tales como WiMAX[5] y los sistemas informáticos actualmente disponibles por menos de 200 USD[6], muchos más habitantes de los países en desarrollo pueden tener acceso más fácil a Internet y a sus productos y servicios conexos[7].

La repercusión de las TIC en la sociedad va mucho más allá de la infraestructura de información básica establecida. La disponibilidad de las TIC es fundamental para impulsar la creación, disponibilidad y utilización de los servicios basados en la red[8]. Los correos electrónicos han desplazado a las cartas tradicionales[9]; la presentación web en línea es actualmente más importante para las actividades comerciales que el material de

---

1 Related to 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: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to the ITU, there were 1,13 billion Internet users by the end of 2007, available at: http://www.itu.int/ITU-D/.

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 seqq., available at: http://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 computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. 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: http://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: http://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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

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

7 Current reports highlight that less than 4 per cent of the African population has access to the Internet. See Waters, Africa waiting for net revolution, BBC News, 29.10.2007, available at: http://news.bbc.co.uk/1/hi/technology/7063682.stm.

8 Regarding the impact of ICT on the 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 Defence had to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

publicidad impreso[10]; y tanto las comunicaciones como los servicios de telefonía basados en Internet crecen más rápidamente que las comunicaciones por líneas terrestres[11].

La disponibilidad de las TIC y los nuevos servicios basados en la red ofrecen cierto número de ventajas para la sociedad en general, especialmente para países en desarrollo.

Las aplicaciones TIC, tales como el cibergobierno, el cibercomercio, la cibereducación, la cibersalud y el ciberentorno se consideran habilitantes para el desarrollo puesto que proporcionan un canal eficaz para distribuir una amplia gama de servicios básicos en zonas remotas y rurales. Las aplicaciones TIC pueden facilitar el logro de los objetivos de desarrollo del milenium, disminuir la pobreza y mejorar las condiciones sanitarias y medioambientales en los países en desarrollo. Aplicando los enfoques adecuados, el contexto y los procesos de implementación correctos, las inversiones en aplicaciones y herramientas en las TIC pueden mejorar la productividad y la calidad. A su vez, las aplicaciones TIC pueden liberar la capacidad técnica y humana y permitir un mayor acceso a los servicios básicos. A este respecto, el robo de la identidad en línea y el hecho de apropiarse de las credenciales de otra persona y/o de la información personal a través de Internet con objeto de utilizar esta información de manera fraudulenta para fines delictivos es actualmente una de las principales amenazas que obstaculizan un mayor desarrollo de los servicios de cibergobierno y cibercomercio[12].

Los costes de los servicios que ofrece Internet a menudo son muy inferiores a los costes de los servicios comparables obtenidos fuera de la red[13]. Los servicios de correo electrónico a menudo están disponibles de manera gratuita o cuestan muy poco en comparación con los servicios postales tradicionales[14]. La enciclopedia en línea Wikipedia[15] puede utilizarse de manera gratuita al igual que cientos de servicios en línea[16]. Es muy importante la reducción en los costes pues ello permite la utilización de los servicios a muchos más usuarios, incluidas las personas con ingresos limitados. Teniendo en cuenta los escasos recursos financieros de muchas personas en los países en desarrollo, Internet les permite utilizar servicios a los que de otra forma no tendrían acceso fuera de la red.

1.2 Ventajas y riesgos

La introducción de las TIC en muchos aspectos de la vida cotidiana ha dado lugar al desarrollo del moderno concepto de sociedad de la información[17]. Este desarrollo de la sociedad de la información ofrece grandes

---

10 Regarding the ability to block Internet-based information services by denial-of-service attacks see below 2.4.e.

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

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

14 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: http://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: http://www.email-marketing-reports.com/metrics/email-statistics.htm.

15 http://www.wikipedia.org.

16 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: http://www.symantec.com/business/resources/articles/article.jsp?aid=20080513_symantec_reports_malicious_web_attacks_are_on_the_rise.

17 Unlike in the Industrial Society, members of the Information Society are no longer connected by their participation in industrialisation, 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.

oportunidades[18]. Un acceso sin obstáculos a la información supone un apoyo a la democracia puesto que el flujo de la información cae fuera del control de las autoridades estatales (como ha sucedido, por ejemplo, en Europa Oriental)[19]. Los desarrollos técnicos han mejorado la vida diaria; por ejemplo, los servicios bancarios y de compra en línea, la utilización de los servicios de datos móviles y la telefonía de voz por Internet (VoIP) son sólo ejemplos del avanzado grado de integración de las TIC en nuestras vidas diarias[20].

Sin embargo, el crecimiento de la sociedad de la información viene acompañado por nuevas e importantes amenazas[21]. Servicios esenciales tales como el suministro de agua y electricidad se basan actualmente en las TIC[22]. Los automóviles, el control de tráfico, los ascensores, el aire acondicionado y los teléfonos también dependen del correcto funcionamiento de las TIC[23]. Los ataques contra la infraestructura de la información y los servicios de Internet pueden causar actualmente daños a la sociedad de una forma nueva y crítica[24].

Ya se han producido ataques contra la infraestructura de la información y los servicios de Internet[25]. El fraude en línea, la difusión de pornografía infantil y los ataques de los piratas son sólo ejemplos de delitos relacionados con la informática que se cometen a gran escala todos los días[26]. Los daños financieros causados por el ciberdelito son enormes[27]. Sólo en 2003 el software fraudulento causó daños de hasta 17 000 millones USD[28]. Según algunas estimaciones los ingresos por los ciberdelitos fueron superiores a 100 000 millones USD en 2007 superando por primera vez las ganancias obtenidas por el tráfico ilegal de drogas[29]. Casi el 60 por ciento de los

---

18 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.

19 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: http://www.jiti.com/v1n1/white.pdf.

20 Regarding the extend of integration of ICTs into the daily lives and the related threats see below 3.2.a 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.

21 See *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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

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

23 *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 seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf.

24 See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, page 1; *Wilshuse*n, 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: http://www.gao.gov/new.items/d08212t.pdf.

25 Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: http://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: http://www.projects.ncassr.org/hackback/ethics00.pdf.

26 The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in one month (August 2007). Source: http://www.hackerwatch.org.

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

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

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

negocios en Estados Unidos consideran que el ciberdelito es más costoso actualmente que el delito físico[30]. Estas estimaciones demuestran claramente la importancia que tiene la protección de las infraestructuras de la información[31].

1.3 Ciberseguridad y ciberdelito

La ciberseguridad[32] desempeña un papel importante en el desarrollo en curso de la tecnología de la información, así como de los servicios de Internet[33]. Mejorar la ciberseguridad y proteger las infraestructuras de la información críticas es esencial para lograr la seguridad y el bienestar económico de cada país. Conseguir un servicio de Internet más seguro (y proteger a los usuarios de Internet) se ha convertido en parte integrante del desarrollo de nuevos servicios así como de la política gubernamental[34]. La disuasión del ciberdelito es una componente integrante de la ciberseguridad nacional y de la estrategia de protección de la infraestructura de la información crítica. En particular, ello incluye la adopción de las medidas jurídicas adecuadas contra la utilización fraudulenta de las TIC a efectos delictivos o de otro tipo y contra las actividades destinadas a afectar la integridad de las infraestructuras críticas nacionales. A nivel nacional, se trata de una responsabilidad compartida que requiere una acción coordinada para la prevención, preparación, respuesta y recuperación de la normalidad tras los incidentes por parte de las autoridades gubernamentales, del sector privado y de los ciudadanos. A nivel regional e internacional, ello supone la cooperación y coordinación con los socios pertinentes. La formulación e implantación de un marco y estrategias nacionales para la ciberseguridad exige, por tanto, un enfoque amplio y completo[35]. Las estrategias sobre ciberseguridad, por ejemplo el desarrollo de sistemas de protección técnica o la educación de los usuarios para evitar que se conviertan en víctimas de

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

31 *Wilshuse*n, 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: http://www.gao.gov/new.items/d08212t.pdf.For more information on the economic impact of Cybercrime see below 2.9.

32 The term "Cybersecurity" is used to summarise various activities such as 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 cyber environment 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 cyber environment. 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. Regarding the definition of cybersecurity, 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 cyber environment 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 cyber environment. 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: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

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

34 See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://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: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

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

ciberdelitos, pueden ayudar a reducir el riesgo de ciberdelito[36]. El desarrollo y apoyo de las estrategias de ciberseguridad son un elemento vital en la lucha contra el ciberdelito[37].

Los retos de tipo jurídico, técnico e institucional que plantea el tema de la ciberseguridad son de carácter mundial y de gran alcance y pueden abordarse únicamente mediante una estrategia coherente que tenga en cuenta el cometido de los distintos interesados y las iniciativas actuales dentro de un marco de cooperación internacional[38]. A este respecto, la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[39] reconoció los riesgos reales y significativos planteados por una ciberseguridad inadecuada y la proliferación del ciberdelito. En los párrafos 108-110 de la *Agenda de Túnez para la Sociedad de la Información*[40], incluido el Anexo, se establece un plan para la implementación por las múltiples partes interesadas a nivel internacional del *Plan de Acción de Ginebra de la CMSI*[41] describiendo el proceso de implementación por las múltiples partes interesadas de acuerdo con once líneas de acción y asignando responsabilidades para facilitar la implementación de las distintas líneas de acción. En la CMSI, los líderes mundiales y los gobiernos designaron a la UIT como organismo facilitador de la implementación de la Línea de Acción C5 de la CMSI dedicada a la creación de confianza y seguridad en la utilización de las TIC[42].

A este respecto, el Secretario General de la UIT lanzó la Agenda sobre Ciberseguridad Global (GCA)[43] el 17 de mayo de 2007 junto con socios procedentes de los gobiernos, la industria, las organizaciones regionales e internacionales y las instituciones académicas y de investigación. La GCA es un marco mundial 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 de mejorar la confianza y seguridad en la sociedad de la información. Se basa en los trabajos, iniciativas y asociaciones existentes con el objetivo de proponer estrategias globales que aborden los retos actuales relativos a la creación de confianza y seguridad en la utilización de las TIC. En el seno de la UIT, la Agenda sobre Ciberseguridad Global complementa los actuales programas de trabajo de la Unión facilitando la implementación de las actividades referentes a la ciberseguridad en el seno de los tres Sectores de la UIT y en un marco de cooperación internacional.

La GCA tiene siete objetivos estratégicos principales basados en las cinco áreas de trabajo siguientes: 1) medidas legales; 2) medidas técnicas y de procedimiento; 3) estructuras institucionales; 4) creación de capacidades y 5) cooperación internacional[44].

La lucha contra el ciberdelito exige un enfoque global. Teniendo en cuenta que las medidas técnicas únicamente no pueden evitar ningún delito, es fundamental que se permita a las autoridades competentes investigar y perseguir el ciberdelito de manera efectiva[45]. Entre las áreas de trabajo de la GCA, las "medidas legales" se centran en la forma de abordar de una manera compatible internacionalmente los retos jurídicos que plantean las actividades delictivas cometidas a través de las redes de las TIC. "Las medidas técnicas y de procedimiento" se centran en las medidas clave para promover la adopción de métodos mejorados que aumenten la gestión de la seguridad y el riesgo en el ciberespacio, incluidos los esquemas, protocolos y normas de acreditación. Las "estructuras institucionales" se centran en la predicción, detección, respuesta y gestión de crisis de los ciberataques, incluida la protección de los sistemas de infraestructura de la información crítica. La "creación de

---

36 For more information see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

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

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

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

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

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

42 For more information on WSIS action line C5: Building confidence and security in the use of ICTs see: http://www.itu.int/wsis/c5/.

43 For more information on the Global Cybersecurity Agenda (GCA) see: http://www.itu.int/cybersecurity/gca/.

44 For more information see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

45 For an overview about the most important instruments in the fight against Cybercrime see below: Chapter 6.2.

capacidades" se centra en la elaboración de estrategias para los mecanismos de creación de capacidad a fin de aumentar la concienciación, transferir los conocimientos e impulsar la ciberseguridad en la agenda política nacional. Por último, la "cooperación internacional" se centra en la cooperación, el diálogo y la coordinación internacional a la hora de abordar las ciberamenazas.

El desarrollo de la legislación adecuada y, dentro de este enfoque, del desarrollo de un marco jurídico relativo al ciberdelito es una parte esencial de la estrategia de ciberseguridad. Ello requiere en primer lugar la elaboración de las leyes penales sustantivas necesarias para criminalizar actos tales como fraude informático, acceso ilegal, interferencia en los datos, violaciones del derecho de propiedad intelectual y pornografía infantil[46]. El hecho de que existan disposiciones en el Código Penal que son aplicables a actos similares cometidos fuera de la red no significa que puedan aplicarse también a los actos cometidos a través de Internet[47]. Por consiguiente, es muy importante realizar un análisis profundo de la actual legislación nacional a fin de identificar posibles lagunas[48]. Además de las disposiciones jurídicas penales sustantivas[49], las autoridades competentes necesitan las herramientas e instrumentos jurídicos necesarios para investigar el ciberdelito[50]. Estas investigaciones suponen un cierto número de retos[51]. Los delincuentes pueden actuar desde cualquier lugar del mundo y tomar las medidas necesarias para enmascarar su identidad[52]. Las herramientas e instrumentos jurídicos necesarios para investigar el ciberdelito pueden ser muy distintos de los que se utilizan en la investigación de los delitos ordinarios[53].

1.4 Dimensiones internacionales del ciberdelito

El ciberdelito a menudo adquiere una dimensión internacional[54]. Los correos electrónicos con contenido ilegal a menudo atraviesan un cierto número de países durante el envío del remitente al destinatario o el contenido ilegal se almacena fuera del país[55]. En las investigaciones contra los ciberdelitos, es muy importante establecer una

---

46 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

47 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 et. Seqq.

48 For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at:

http://www.coe.int/cybercrime/. 48 See for example the following surveys on national Cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at:
http://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: https://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: http://www.mosstingrett.no/info/legal.html.

49 See below: Chapter 6.1.

50 See below: Chapter 6.1.

51 For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.2.

52 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 seqq., available at:
http://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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Design", 2005.

53 Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.11.

54 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.

55 Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplyfing Data Storage and Management, 2005.

estrecha cooperación entre los países implicados[56]. Los actuales acuerdos de asistencia jurídica mutua se basan en procedimientos formales complejos y de excesiva duración[57]. Por consiguiente, es fundamental articular procedimientos para dar una rápida respuesta a los incidentes así como a las solicitudes de cooperación internacional[58].

Un cierto número de países basan su régimen de asistencia jurídica mutua en el principio de "criminalidad doble"[59]. Las investigaciones a nivel global se limitan generalmente a los delitos penalizados en todos los países participantes. Aunque existe un cierto número de delitos que pueden procesarse en cualquier parte del mundo, las diferencias regionales desempeñan un papel importante[60]. Un ejemplo es el contenido ilegal. La penalización del contenido ilegal difiere según los distintos países[61]. El material que puede distribuirse legalmente en un país puede fácilmente ser ilegal en otro país[62].

La tecnología informática actualmente utilizada es básicamente la misma en todo el mundo[63]. Aparte de los temas relativos a los idiomas y los adaptadores de potencia, existe muy poca diferencia entre los sistemas informáticos y los teléfonos celulares que se venden en Asia y en Europa. La situación en Internet es análoga. Debido a la normalización, los protocolos utilizados en países del continente africano son los mismos que se emplean en Estados Unidos[64]. La normalización permite a los usuarios de todo el mundo acceder a los mismos servicios a través de Internet[65].

La cuestión consiste en determinar el efecto que tiene la armonización de las normas técnicas mundiales sobre el desarrollo de la jurisdicción penal nacional. En términos de contenido ilegal, los usuarios de Internet pueden

---

56 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 seqq., 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 seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf.

57 See below: Chapter 6.3.

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

59 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://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. seqq., available at: http://www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

60 See below: Chapter 5.5. See for example the following surveys on national Cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: http://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: https://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: http://www.mosstingrett.no/info/legal.html.

61 The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Convention on Cybercrime, but addressed in an additional protocol. See below: Chapter 2.5.

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

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

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

65 Regarding the technical standardisation 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: http://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. seqq.

acceder a información procedente de cualquier parte del mundo, lo que les permite tener acceso a una información legalmente disponible en el extranjero que podría ser ilegal en su propio país.

Teóricamente, los desarrollos derivados de la normalización técnica van más allá de la globalización de la tecnología y los servicios y podrían desembocar en la armonización de las leyes nacionales. Sin embargo, como han demostrado las negociaciones sobre el Primer Protocolo de la Convención del Consejo de Europa sobre Ciberdelito[66], los principios jurídicos nacionales varían mucho más lentamente que los desarrollos técnicos[67].

Aunque Internet puede no reconocer controles fronterizos, existen medios para restringir el acceso a cierta información[68]. El proveedor de acceso puede generalmente bloquear ciertas direcciones web y el suministrador del servicio que almacena una dirección web puede impedir a los usuarios el acceso a la información basándose en las direcciones IP vinculadas a un cierto país ("determinación por IP")[69]. Aunque ambas medidas pueden sortearse se trata no obstante de instrumentos que pueden emplearse para mantener las diferencias territoriales en una red mundial[70]. La Iniciativa OpenNet[71] informa que este tipo de censura se practica en unos doce países[72].

1.5 Consecuencias para los países en desarrollo

Encontrar estrategias y soluciones de respuesta a la amenaza del ciberdelito es un reto importante, especialmente para los países en desarrollo. Una estrategia anticiberdelito completa, generalmente contiene medidas de protección técnica así como instrumentos jurídicos[73]. El desarrollo e implementación de estos instrumentos toma su tiempo. Las medidas de protección técnica son especialmente costosas[74]. Los países en desarrollo necesitan integrar las medidas de protección en la instalación de Internet desde el principio ya que aunque ello inicialmente elevaría el coste de los servicios de Internet las ventajas a largo plazo que supone evitar los costes y daños causados por el ciberdelito compensan sobremanera cualquier desembolso inicial realizado para establecer medidas de protección técnica y de salvaguarda de la red[75].

Los riesgos que suponen unas medidas de protección débiles afectarían de hecho a los países en desarrollo de manera más directa, debido a sus métodos de salvaguarda y protección menos estrictos[76]. La capacidad de proteger a los usuarios, así como a las empresas, es un requisito fundamental no sólo para las actividades comerciales regulares sino también para las actividades comerciales en línea o basadas en Internet. Sin una

---

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

67 Since parties participating in the negotiation could not agree on a common position on the criminalisation 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.

68 See *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq*.

69 This was for example discussed within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: http://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*.

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

71 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: http://www.opennet.net.

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

73 See below: Chapter 4.

74 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 http://www.oecd.org/dataoecd/5/47/34935342.pdf.

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

76 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: http://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 industrialised countries. See OECD: "Spam Issue in Developing Countries", DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

seguridad de Internet garantizada, los países en desarrollo tropezarían con grandes dificultades a la hora de promover el cibercomercio y participar en las industrias de servicio en línea.

El desarrollo de medidas técnicas para promover la ciberseguridad y proponer una adecuada legislación contra el ciberdelito es vital tanto para los países desarrollados como para los países en desarrollo. Comparados con los costes que supone insertar medidas de salvaguarda y protección en las redes informáticas en fecha posterior, es probable que las medidas iniciales tomadas desde el principio sean mucho menos costosas. Los países en desarrollo deben aplicar sus estrategias anticiberdelito en coherencia con las normas internacionales desde el principio[77].

2 El fenómeno de la ciberdelincuencia

2.1 Definiciones relacionadas con la ciberdelincuencia

La mayoría de los Informes, guías o publicaciones sobre este fenómeno comienzan definiendo el término "ciberdelito"[78]. Una definición bastante común de este término es cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva[79]. Como ejemplo de perspectiva internacional puede citarse el Artículo 1.1 del Proyecto de Convenio Internacional para la Protección contra la Ciberdelincuencia y el Ciberterrorismo (CISAC)[80], en el que por ciberdelincuencia se refiere a los actos relativos a los cibersistemas[81]. Algunas definiciones tratan de integrar los objetivos o intenciones y de definir el término con mayor precisión[82], por ejemplo, constituye ciberdelito "la actividad realizada mediante un computador que es *ilícita* o que algunas Partes *considera ilícita* y que puede realizarse *a través de las redes electrónicas mundiales*"[83].

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 ciberdelito en ciertos acuerdos

---

77 For more details about the elements of an anti-cybercrime strategy see below: Chapter 4.

78 Regarding approaches to define and categorise cybercrime see for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: http://www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the 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: http://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: http://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: http://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: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1.

79 See for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: http://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. seqq.; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

80 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 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: http://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.

81 *Arti*cle 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;
[...]

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

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

internacionales, tales como el "Convenio sobre la Ciberdelincuencia"[84]. Por ejemplo, una persona que produce software pernicioso para dispositivos USB[85] que destruye los datos del computador cuando se le conecta el dispositivo está cometiendo un delito definido en el Artículo 4 del Convenio sobre la Ciberdelincuencia del Consejo de Europa[86]. Ahora bien, el acto de borrar datos utilizando un dispositivo físico que copia código pernicioso no se efectúa a través de las redes electrónicas mundiales y 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.

Así pues, la definición del término "ciberdelito" presenta dificultades considerables[87]. 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 el Proyecto de Convenio de Stanford sobre la ciberdelincuencia 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[88].

2.2 Tipología del ciberdelito

El término "ciberdelito" abarca muy diversos tipos de delitos[89]. Los delitos reconocidos comprenden una gran variedad de infracciones, lo que dificulta su tipología o clasificación.[90] Un sistema de clasificación interesante

---

84 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: Chapter 6.1.; *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 Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *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: http://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*.

85 Universal Serial Bus (USB).

86 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.

87 For difficulties related to the application of 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: http://www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

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

89 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.

90 *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: http://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: http://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

es el definido por el Convenio sobre la Ciberdelincuencia del Consejo de Europa[91], en el que se distinguen cuatro tipos diferentes de infracciones[92]:

- delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos[93];
- delitos informáticos[94];
- delitos relacionados con el contenido[95]; y
- delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines[96].

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"[97]; "delitos informáticos"[98] y "delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines"[99]. La cuarta categoría "delitos informáticos"[100] 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"[101] o "*peska*" (*phishing*)[102]) 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.

---

91 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 Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *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: http://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*.

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

93 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: Chapter 6.1.

94 Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences see below: Chapter 6.1.

95 Art. 9 (Offences related to child pornography). For more information about the offences see below: Chapter 6.1.

96 Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences see below: Chapter 6.1.

97 See below: Chapter 2.4.

98 See below: Chapter 2.5.

99 See below: Chapter 2.6.

100 See below: Chapter 2.7.

101 See below: Chapter 2.8.1.

102 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 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. seqq.

2.3 Indicadores estadísticos sobre ciberdelitos

No resulta nada fácil cuantificar la incidencia del ciberdelito en la sociedad[103]. Las pérdidas financieras causadas por el ciberdelito, así como el número de delitos, son muy difíciles de calcular. Algunas fuentes estiman que las pérdidas de las empresas e instituciones en Estados Unidos[104] causadas por el ciberdelito pueden llegar hasta los 67 000 mil millones USD. Ahora bien, no es seguro que puedan extrapolarse los resultados de esta encuesta[105]. Esta crítica a la metodología se refiere no sólo a las pérdidas, sino también al número de delitos reconocidos[106].

Resulta difícil cuantificar el número de ciberdelitos, dado que las víctimas no siempre informan de ello[107]. Sin embargo, las estadísticas pueden ayudar a comprender la incidencia del ciberdelito. En vez del número exacto de ciberdelitos en un año determinado, resulta más interesante conocer la tendencia, que puede observarse comparando los resultados de varios años.

Como ejemplo puede citarse la encuesta sobre ciberdelitos y seguridad informática de 2007 realizada por el CSI[108] de Estados Unidos, en la que se analiza la tendencia del número de delitos informáticos cometidos y otras tendencias[109]. 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[110]. 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). Ahora bien, aunque en el estudio no se explica las razones de esta disminución del número de delitos reconocidos, ésta ha quedado demostrada por las encuestas realizadas por otras instituciones (a diferencia de lo que sugieren los informativos de algunos medios de comunicación)[111]. Al analizar las estadísticas de delitos se observa una evolución similar -por ejemplo, según las estadísticas de delitos de Alemania[112], tras alcanzar un máximo en 2004, el número de delitos informáticos se ha reducido a casi el nivel de 2002.

Las estadísticas sobre ciberdelitos no proporcionan información fiable sobre la escala o magnitud de los delitos[113]. Debido a la incertidumbre acerca de cuál es la proporción de delitos que los afectados informan[114] 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.

---

103 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

104 See 2005 FBI Computer Crime Survey, page 10 As well as *Evers*, Computer crimes cost $67 billion, FBI says, ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

105 See below: Chapter 2.9.

106 Regarding the economic impact of Cybercrime see below: Chapter 2.9.

107 "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: http://www.heise-security.co.uk/news/80152.

108 Computer Security Institute (CSI), United States.

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

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

111 See, for example, the 2005 FBI Computer Crime Survey, page 10.

112 See Polizeiliche Kriminalstatisik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

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

114 See below: Chapter 2.9.2.

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

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[115]. 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[116]. En esta sección se expone una descripción general de los delitos de esta categoría que se producen con mayor frecuencia.

Figura 1

El gráfico muestra un sitio web que ha sido pirateado. El pirata ha modificado la primera página para que los usuarios sepan que su ataque ha sido un éxito.

2.4.1 Acceso ilícito (piratería de sistemas y programas)[117]

Los delitos clasificados como "piratería" se refieren al acceso ilícito a un sistema informático[118], uno de los delitos más antiguos en este campo[119]. Con el advenimiento de las redes de computadores (especialmente Internet), este delito se ha convertido en un fenómeno popular[120]. Los objetivos más conocidos de los ataques de piratería son la Administración Nacional de Aeronáutica y del Espacio (NASA), la Fuerzas Aéreas de Estados Unidos, el Pentágono, Yahoo, Google, Ebay y el Gobierno de Alemania[121]. Ejemplos de delitos de piratería son:

- la irrupción en sistios web protegidos con contraseña[122]; y
- la burla de la protección de contraseña en un computador.

---

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

116 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."

117 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.

118 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.

119 See Levy, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: http://www.aic.gov.au/publications/htcb/htcb005.pdf.; Taylor, Hacktivism: In Search of lost ethics? in Wall, Crime and the Internet, 2001, page 61.

120 See the statistics provides 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: http://www.hackerwatch.org.

121 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 sq.; Regarding the impact see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et. seq.

122 *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

Como ejemplos de actos preparatorios pueden citarse:

- utilización de equipos o programas para obtener una contraseña e irrumpir en el sistema informático[123];
- Creación de sitios web "falsos" para lograr que el usuario revele su contraseña[124]; y
- La instalación por hardware y 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[125].

Los motivos de los delincuentes son diversos. Algunos se limitan a burlar las medidas de seguridad para probar sus capacidades (véase el ejemplo de la Figura 1)[126]. Otros actúan por motivos políticos (conocido como piratería activista o "*hacktivism*"[127]), como es el caso del incidente reciente acaecido en el sitio web de las Naciones Unidas[128]. 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[129]. En muchos casos el acceso ilícito al sistema informático, aunque esencial, es tan solo el primer paso[130].

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[131]. Este aumento del número de ataques de piratería se debe a tres factores principales:

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[132]. 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[133]. 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[134].

---

123 *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

124 *Sieber*, Council of Europe Organised Crime Report 2004, page 66.

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

126 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 Chapter 6.1.a and Chapter 6.1.d.

127 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: http://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: http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

128 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.

129 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.

130 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.

131 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: http://www.hackerwatch.org.

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

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

134 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, No5 – page 825 et sqq.

Aparición de herramientas informáticas que automatizan los ataques

Últimamente se ha comenzado a utilizar herramientas software que permiten automatizar los ataques[135]. Con la ayuda de programas instalados previamente, un mismo pirata puede atacar miles de computadoras en un sólo día utilizando sólo un computador[136]. Si además el pirata tiene acceso a más computadores – por ejemplo, una red zombi[137] – puede atacar a mayor escala. Dado que la mayoría de estas herramientas informáticas utilizan métodos de ataque preprogramados, no todos lo 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[138] -algunas son gratuitas, pero las más eficientes cuestan fácilmente del orden de miles de USD[139]. 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[140].

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[141]. Dado que los computadores de las empresas están por lo general mejor protegidos que los privados, es más difícil atacar a los primeros utilizan herramientas informáticas configuradas de antemano[142]. 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[143].

---

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

136 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: http://www.212cafe.com/download/e-book/A.pdf.

137 Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf; See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

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

139 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: http://www.212cafe.com/download/e-book/A.pdf.

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

141 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

142 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: http://www.212cafe.com/download/e-book/A.pdf; *Erickson*, Hacking: The Art of Exploitation, 2003.

143 Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: Chapter 3.2.i.

El acceso ilícito a sistemas informáticos puede considerarse equivalente al acceso ilícito a un edificio, que en muchos países es un delito[144]. 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[145]; y/o
- el autor tiene malas intenciones[146]; y/o
- se obtienen, modifican o dañan datos.

Otros sistemas jurídicos no consideran delito el mero acceso, sino que se concentran en los delitos derivados del mismo[147].

2.4.2 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[148]. Internet se utiliza cada vez más para obtener secretos comerciales[149]. 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 la Unión Soviética[150].

Los delincuentes recurren a diversas técnicas para acceder a los computadores de sus víctimas[151], entre las que cabe citar:

- software para explorar los puertos desprotegidos[152];
- software para burlar las medidas de protección[153]; e
- "ingeniería social"[154].

---

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

145 See in this context Art. 2, sentence 2 Convention on Cybercrime.

146 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

147 One example of this is the German Criminal Code, that criminalised 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.

148 For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq. *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, No5 – page 825 et sqq.

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

150 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.

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

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

153 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.

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[155]. La "ingeniería social" no es para nada el menos eficaz de los métodos de ataque a sistemas informáticos bien protegidos. En realidad consiste en la manipulación de seres humanos con la finalidad de obtener acceso a sistemas informáticos[156]. 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[157] 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[158]. La OCDE subraya la importancia que reviste la criptografía para los usuarios, por cuanto aumenta la protección de los datos[159]. 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[160]. El éxito de los delincuentes en la obtención de información confidencial suele radicar en la ausencia de mecanismos de protección.

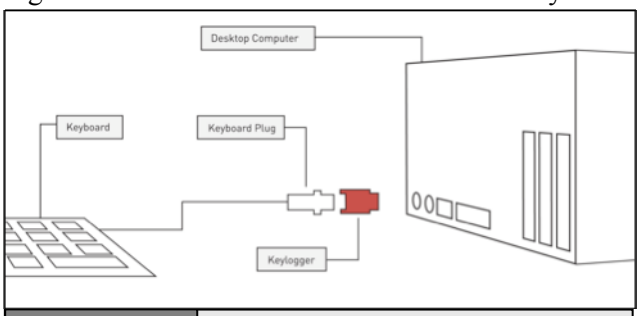


Figura 2

El gráfico muestra cómo se instalan los interceptores de teclado. Muchas de estas herramientas – que parecen adaptadores – se sitúan entre el conector del teclado y el computador. Los modelos más modernos se instalan dentro del teclado, por lo que resulta imposible encontrarlo sin abrirlo. Los programas antivirus no pueden detectar los interceptores de teclado físicos.

Por lo general los delincuentes buscan secretos comerciales, aunque cada vez más dirigen sus ataques a computadores privados[161]. Los usuarios privados suelen guardar información sobre sus cuentas bancarias y tarjetas de crédito en sus computadores[162]. Los delincuentes pueden utilizar esta información para sus propios fines

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

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

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

157 See the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: http://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 "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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

158 Regarding the elements of an Anti-Cybercrime Strategy, see below: Chapter 4.

159 "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: http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

160 Physical researches prove 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: Chapter 3.2.m.

161 Regarding the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq.

162 Regarding the impact of this behaviour for identity-theft see *Gercke*, Internet-related Identity Theft, 2007, available at: http://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.

(por ejemplo, los datos bancarios para efectuar transferencias monetarias) o para venderla a terceros[163]. Por ejemplo, el precio de venta de datos de una tarjeta de crédito puede alcanzar los 60 USD[164]. 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, a saber:

- acceder a sistemas informáticos o a un dispositivo de almacenamiento y extraer la información; o
- manipular a los usuarios para que revelen la información o los códigos de acceso que permitan al delincuente 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[165]. En los últimos años se han detectado diversos tipos de programas espía, por ejemplo los interceptores de teclado (*keyloggers*)[166]. Estos interceptores son herramientas informáticas que registran cada una de las teclas pulsadas en el teclado del computador infectado[167]. 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[168]) 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 (véase la Figura 4). Obviamente los dispositivos físicos son más difíciles de instalar y detectar, dado que requieren el acceso físico al sistema informático[169]. Por ese motivo, los programas antivirus y antiespías clásicos son en general incapaces de identificarlos[170].

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[171]. La "*peska*" se ha convertido recientemente en uno de los crímenes más importantes en el ciberespacio[172]. El término "*peska*" se utiliza para describir un tipo de delito que se caracteriza

---

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

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

165 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.

166 See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

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

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

169 One approach to gain access to a computer system to install a key-logger 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.

170 Regular hardware checks are a vital part of any computer security strategy.

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

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

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[173].

El espionaje de datos es otro ejemplo de delito dirigido a uno de los puntos más débiles de cualquier sistema informático, a saber, el usuario. Así pues es evidente que los riesgos van a la par con los timos. Pero existe solución. 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[174].

Por otra parte, cada vez se almacena más información confidencial en sistemas informáticos. Es esencial evaluar si las medidas de protección técnica adoptadas por los usuarios resultan adecuadas o si los legisladores han de establecer protección adicional para penalizar el espionaje de datos[175].

2.4.3 Intervención ilícita

Los delincuentes pueden intervenir las comunicaciones entre usuarios[176] (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[177]) 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[178]).

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[179]. Sin embargo, los delincuentes buscan los puntos débiles del sistema. Las tecnologías inalámbricas gozan de mayor popularidad y anteriormente eran vulnerables[180]. 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[181]. 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[182].

---

173 For more information on the phenomenon of phishing see below: Chapter 2.8.4.

174 Regarding the elements of an Anti-Cybercrime Strategy see below: Chapter 4.

175 The Council of Europe Convention on Cybercrime contains no provision criminalising data espionage.

176 *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.

177 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.

178 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 http://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: http://www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

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

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

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

182 With regard to the time necessary for decryption see below: Chapter 3.2.13.

Para conseguir acceder a la información confidencial, algunos delincuentes configuran puntos de acceso cerca de los lugares donde hay gran demanda de acceso inalámbrico[183] (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[184]. Al pasar a través de un cable las transmisiones de datos emiten energía electromagnética[185]. Con un equipo adecuado, es posible detectar y registrar dichas emisiones[186] y es posible registrar transferencias de datos entre los computadores y el sistema conectado, así como las transmisiones internas del sistema informático[187].

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[188].

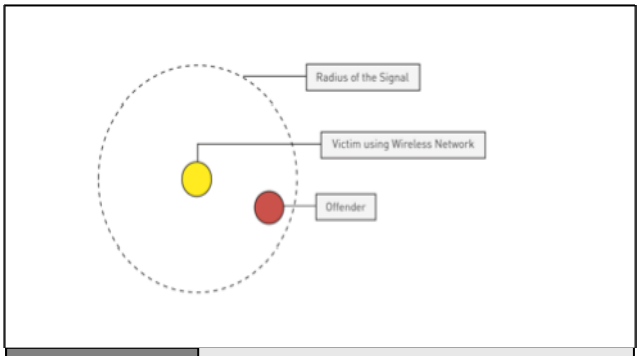


Figura 3

Este gráfico muestra el caso de un ataque dirigido a un usuario con conexión inalámbrica. El delincuente que desea interceptar los datos que se envían y reciben puede actuar desde cualquier punto situado dentro del radio de la señal. Dependiendo del encaminador inalámbrico y de su emplazamiento, las señales pueden recibirse en un radio de hasta 100 metros.

2.4.4 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[189]. La carencia de acceso a los datos puede causar daños (económicos) considerables. Los infractores pueden atentar contra la integridad de los datos de las siguientes formas[190]:

- borrarlos; y/o
- suprimirlos; y/o
- alterarlos; y/o
- restringir el acceso a los mismos.

183 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: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

184 *Sieber*, Council of Europe Organised Crime Report 2004, page 97.

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

186 See http://en.wikipedia.org/wiki/Computer_surveillance#Surveillance_techniques.

187 E.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

188 For more details on legal solutions see below: Chapter 6.1.3.

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

190 *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

Los virus son un ejemplo bastante común de supresión de datos[191]. Desde los albores de la tecnología informática, los virus han constituido una amenaza para los usuarios que no tienen instalada la debida protección[192]. Con el tiempo el número de virus informáticos ha aumentado considerablemente[193]. Entre los adelantos más recientes cabe citar:

- la manera en que los virus se distribuyen; y
- los efectos[194].

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[195]. 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[196] infectó el 90 por ciento de los sistemas informáticos vulnerables en los diez 10 minutos posteriores a su distribución[197]. Las pérdidas económicas causadas por ataques de virus en 2000 se calculó en 17 000 millones USD aproximadamente[198]. En 2003 esta cifra fue superior a los 12 000 millones USD[199].

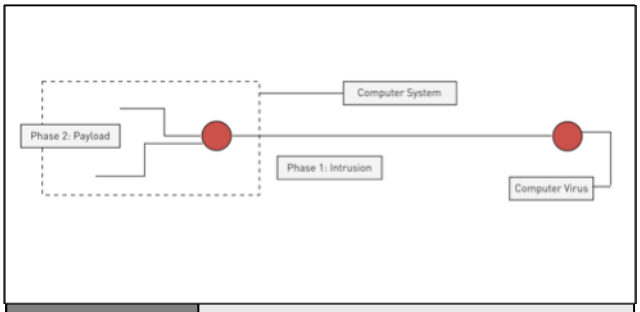


Figura 4

El gráfico muestra la función de un virus informático. Una vez infectado el sistema (fase 1), el virus realiza la función programada (fase 2), por ejemplo, borrar o cifrar determinados ficheros.

La mayoría de los virus informáticos de primera generación se limitaban a borrar información o mostrar mensajes (véase la Figura 4). Recientemente, los efectos se han diversificado[200]. Los virus modernos son capaces de abrir puertas traseras por las que los piratas pueden tomar el control del computador o cifrar los

---

191 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. *Cohen*, "Computer Viruses"; *Adleman*, "An Abstract Theory of Computer Viruses". 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/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

192 One of the first computer virus was called (c)Brain and was created by *Basit* and *Amjad Farooq Alvi*. For further details, see: http://en.wikipedia.org/wiki/Computer_virus.

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

194 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.

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

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

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

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

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

200 See *Szor*, The Art of Computer Virus Research and Defence, 2005.

ficheros del mismo de modo que las víctimas no puedan acceder a sus propios ficheros, a no ser que paguen para obtener la clave[201].

2.4.5 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[202]. Al impedir que los sistemas informáticos funcionen correctamente, los infractores consiguen causar grandes pérdidas económicas a sus víctimas[203].

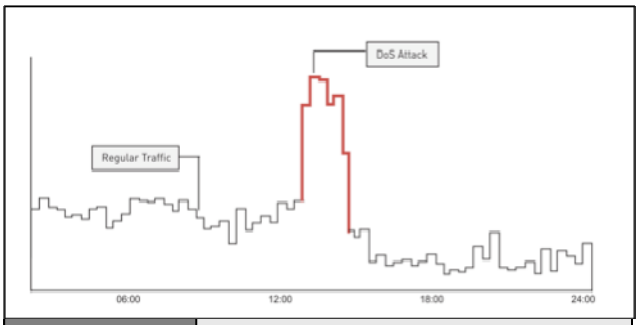


Figura 5

El gráfico muestra el número de solicitudes de acceso a un sitio web durante condiciones normales de funcionamiento (negro) y durante un ataque de denegación del servicio (DoS). Si el servidor atacado es incapaz de gestionar el elevado número de solicitudes, el ataque puede ralentizar la velocidad de respuesta del sitio web o anular completamente el servicio.

También es posible realizar ataques físicos a los sistemas informáticos[204]. 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[205].

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:

- gusanos informáticos[206]; o
- ataques de denegación del servicio (DoS)[207].

---

201 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 license' 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.

202 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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

203 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.

204 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.

205 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.

206 *Sieber*, "Council of Europe Organised Crime Report 2004", page 107.

Los gusanos informáticos[208] 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 es la siguiente:

- En función de los efectos del gusano, la infección puede detener el buen funcionamiento del sistema informático y utilizar los recursos del sistema para reproducirse a sí mismo por Internet.
- La producción de tráfico de red adicional puede reducir la disponibilidad de ciertos servicios (por ejemplo, sitios web).

A diferencia de los gusanos informáticos que afectan generalmente a toda la red sin atacar directamente un sistema informático en particular, los ataques de DoS están dirigidos a sistemas informáticos concretos. Los ataques DoS hacen que los recursos informáticos queden indisponibles para los usuarios previstos[209]. Al enviar a un sistema informático más solicitudes de las que puede gestionar (véase la Figura 7), los infractores pueden impedir que los usuarios accedan a dicho sistema para consultar su correo, leer las noticias, reservar un vuelo o descargar ficheros. En 2000, en sólo un breve intervalo de tiempo, se lanzaron diversos ataques DoS contra empresas conocidas tales como CNN, Ebay y Amazon[210]. Como resultado de ello, algunos de los servicio quedaron indisponibles durante horas e incluso días[211].

La interposición de una acción judicial contra los ataques de DoS y de gusanos informáticos plantea grandes dificultades a la mayoría de las legislaciones penales, por cuanto no implican ningún daño físico contra los sistemas víctimas de tales ataques. Además de la necesidad de penalizar los ataques por la web[212], la cuestión de si la prevención y denuncia de ataques contra la infraestructura esencial requiere un enfoque legislativo independiente sigue siendo objeto de debate.

2.5 Delitos relacionados con el contenido

Esta categoría comprende el contenido que se considera ilícito, como la pornografía infantil, el material xenófobo y los insultos dirigidos a símbolos religiosos[213]. La creación de instrumentos jurídicos para tratar esta categoría se ve influenciada sobre todo por los enfoques nacionales, que pueden tomar en consideración principios jurídicos y culturales 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

---

207 A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

208 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 programme running loose through a computer network.

209 For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://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".

210 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: http://www.projects.ncassr.org/hackback/ethics00.pdf.

211 *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.

212 Regarding the different approaches see below: Chapter 6.1.5.

213 For reports on cases involving illegal content, see *Sieber*, "Council of Europe Organised Crime Report 2004", page 137 et seqq.

muchos países de Europa[214], mientras que en Estados Unidos queda protegido por el principio de libertad de expresión[215], [216]. La utilización de comentarios despectivos al referirse al Sagrado Profeta se considera un acto criminal en muchos países islámicos[217], pero no en algunos países europeos.

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[218]. 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, si no imposible[219].

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[220].

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[221]. Otra solución

---

214 One example of the wide criminalisation of illegal content is Sec. 86a German Penal Code. The provision criminalises 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.

215 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

216 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 criminalisation was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

217 See e.g. Sec. 295C 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 Muhammad (peace be upon him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

218 See below: Chapter 3.2.6 and Chapter 3.2.7.

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

220 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: http://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: http://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: http://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: http://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.

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

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)[222].

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[223], cerca de dos docenas de países practican la censura actualmente[224].

2.5.1 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:

- intercambiar medios (tales como imágenes, películas, cámaras en directo) ahorrándose los onerosos gastos de envío[225];
- acceso mundial[226], 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[227]) -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 con acceso en cualquier instante asciende hasta 4,2 millones[228]. Además de los sitios web, el material pornográfico puede distribuirse a través de:

- sistemas de intercambio de ficheros[229];
- en salas de charla cerradas.

---

222 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.

223 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: http://www.opennet.net.

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

225 Depending on the availability of broadband access.

226 Access is in some countries is limited by filter technology. 226 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: http://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: http://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: http://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: http://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.

227 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: Chapter 6.2.

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

229 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.

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[230], a los efectos de protección del menor[231]. Según los estudios, el acceso a material pornográfico puede afectar negativamente el desarrollo del menor[232]. Para hacer cumplir estas leyes, se han creado "sistemas de verificación de la edad" (véase la Figura 6)[233]. En otros países se penaliza todo intercambio de material pornográfico incluso entre adultos[234], 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.

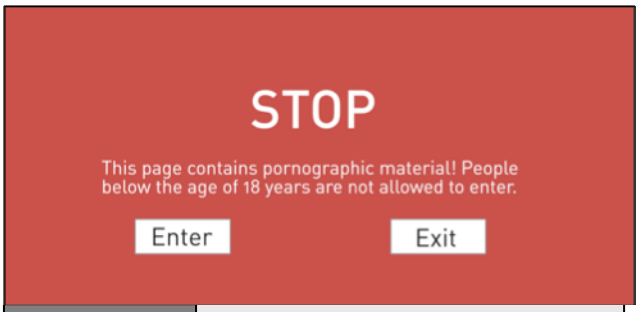


Figura 6

El gráfico muestra un método de impedir a los menores el acceso a sitios web con contenido pornográfico. Dado que esta solución no permite la verificación de la respuesta dada por el usuario, en muchos países se considera insuficiente.

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[235]. 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[236]. 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[237]) a determinados sitios web[238].

---

230 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; […]

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

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

233 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: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

234 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.

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

236 Regarding the principle of "dual criminality", see below: Chapter 6.3.2.

237 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: http://www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

2.5.2 Pornografía infantil

Al contario que en el caso de la pornografía de adultos, donde existe divergencia de opiniones, cuando se trata de pornografía infantil hay unanimidad en su condena y los delitos relacionados con la pornografía infantil se consideran generalmente actos criminales[239]. Diversas organizaciones internacionales se dedican a luchar contra la pornografía infantil en Internet[240] en el marco de varias iniciativas jurídicas internacionales, entre las que cabe citar: la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989[241]; 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[242]; y el Convenio del Consejo de Europa, de 2007, sobre la protección de los niños contra la explotación sexual y el abuso sexual[243].

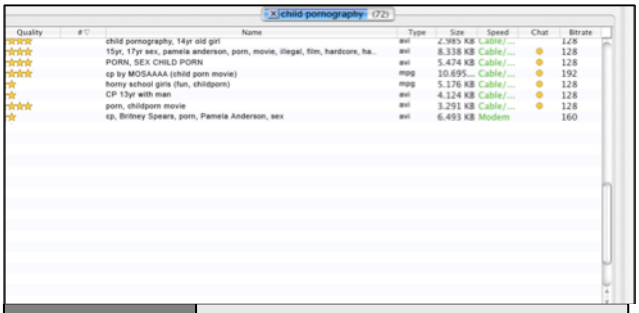


Figura 7

El gráfico muestra la interfaz de usuario de un programa para el intercambio de ficheros. Tras buscar el término "pornografía infantil", el programa enumera todos los ficheros disponibles en el sistema de compartición que contienen dicho término.

Lamentablemente, estas iniciativas destinadas a controlar la distribución de pornografía por la red han resultado poco disuasorias para los autores de dicha distribución, que utilizan Internet para comunicarse e intercambiar material de pornografía infantil (véase la Figura 7)[244]. El aumento de la anchura de banda ha contribuido al intercambio de archivos de vídeo e imágenes.

Según las investigaciones sobre el comportamiento de los infractores de pornografía infantil, el 15 por ciento de los detenidos por delitos de pornografía infantil por 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[245]; el

---

238 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: http://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: http://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: http://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: http://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.

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

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

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

242 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.

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

244 *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: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

245 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

19 por ciento tenían imágenes de niños menores de 3 años[246]; y el 21 por ciento de imágenes con escenas violentas[247].

La venta de material de pornografía infantil es muy lucrativa[248], dado que los coleccionistas están dispuestos a pagar grandes cantidades por películas e imágenes que muestren niños en un contexto sexual[249]. Los motores de búsqueda permiten encontrar este tipo de material con rapidez[250]. 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[251].

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[252]:

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[253]. 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[254]. Sin embargo, cuando los infractores efectúan pagos anónimos resulta difícil rastrearlos.

2) La utilización de tecnología de cifrado[255]:

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[256], lo que dificulta sobremanera las investigaciones penales[257].

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

---

246 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

247 For more information, see "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

248 See *Walden*, "Computer Crimes and Digital Investigations", page 66.

249 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.

250 "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: http://www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

251 See ABA "International Guide to Combating Cybercrime", page 73.

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

253 For more information, see *Wilson*, "Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond".

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

255 See below: Chapter 3.2.13.

256 Based on the "National Juvenile Online Victimisation Study", 12% 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

257 See below: Chapter 3.2.13.

de registrar a los usuarios o de bloquear o filtrar el acceso a sitios web que contengan contenido de pornografía infantil[258].

2.5.3 Racismo, lenguaje ofensivo, exaltación de la violencia

Los grupos radicales utilizan los medios de comunicación de masas, como Internet, para divulgar propaganda (Figura 8)[259]. El número de sitios web con contenido racista y lenguaje ofensivo ha aumentado recientemente[260], 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[261]. En 2006 existían en Internet más de 6 000 sitios web de este tipo[262].

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[263]. 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[264]. 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.

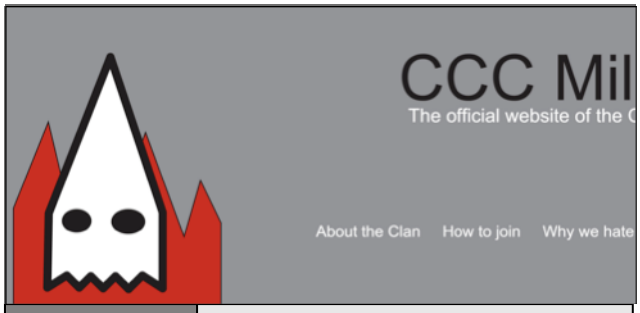


Figura 8

El gráfico muestra un sitio web de un grupo radical. Estos grupos utilizan mucho Internet para hacer propaganda de su ideología y reclutar nuevos miembros.

Estos actos no están penalizados en todos los países[265]. En algunos países, este tipo de contenido está protegido por el principio de libertad de expresión[266]. 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,

258 For an overview about 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.

259 Radical groups in the United States recognised 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.

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

261 *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: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

262 See "Digital Terrorism & Hate 2006", available at: http://www.wiesenthal.com.

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

264 See "ABA International Guide to Combating Cybercrime", page 53.

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

266 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

cuando un tribunal francés dictó a Yahoo! (con sede en Estados Unidos) que bloqueara el acceso de usuarios franceses a material nazi[267]. 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[268].

La discrepancia de opiniones entre los países sobre estos asuntos quedó patente durante la redacción del Convenio sobre la Ciberdelincuencia del Consejo de Europa. 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[269]. 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[270]. De lo contrario, algunos países (con inclusión de Estados Unidos) no lo hubieran firmado.

2.5.4 Delitos contra la religión

Son cada vez más[271] los sitios web con material que algunos países consideran que atenta contra la religión, por ejemplo declaraciones antirreligiosas por escrito[272]. 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 (Figura 9).

Figura 9

El gráfico muestra un sitio web con contenido de carácter religioso, accesible desde cualquir lugar del mundo.

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[273]. 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[274]. 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.

---

267 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, page1041.

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

269 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, 144.

270 See "Explanatory Report to the First Additional Protocol", No. 4.

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

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

273 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

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

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[275].

Figura 10

El gráfico muestra una interfaz de usuario de un casino en línea. Tras registrarse y transferir dinero, el usuario puede jugar en línea. Muchos de estos casinos permiten utilizar servicios sin tener que registrarse oficialmente.

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[276] o la profanación de copias del Corán[277], mientras que otros adoptan una posición más liberal y no penalizan tales actos.

2.5.5 Juegos ilegales y juegos en línea

Los juegos por Internet son uno de los campos que experimenta un mayor crecimiento en este medio[278]. Según Linden Labs, el creador del juego en línea "Segunda Vida"[279], se han abierto unos diez millones de cuentas[280]. Los Informes muestran que algunos de estos juegos se han utilizado para cometer delitos, en particular[281]:

- intercambio y presentación de pornografía infantil[282];
- fraude[283];
- casinos en línea[284]; y

---

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

276 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.

277 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.

278 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: http://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: http://www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

279 http://www.secondlife.com.

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

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

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

283 *Leapman*, "Second Life world may be haven for terrorists", Sunday Telegraph, 14.05.2007, available at: http://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/.

- 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[285] (si bien es cierto que comparadas con las cifras que mueve el juego tradicional, éstas son relativamente pequeñas[286]).

La reglamentación del juego dentro y fuera de Internet varía de un país a otro[287] -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)[288]. El éxito en Macao se debe al hecho de que el juego es ilegal en China[289] 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[290]. Los casinos en línea han proliferado (véase la Figura 10), 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[291]. Los casinos en línea también pueden utilizarse para lavar dinero y financiar el terrorismo[292]. Al efectuar 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[293]. Ha habido varios intentos de impedir la participación en los juegos en línea[294], 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[295].

---

284 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.

285 Christiansen Capital Advisor. See http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

286 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: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf.

287 See, for example, GAO, "Internet Gambling – An Overview of the Issues", available at: http://www.gao.gov/new.items/d0389.pdf; Regarding the WTO Proceedings, "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: http://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.

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

289 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.

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

291 For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

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

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

294 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.

295 See § 5367 Internet Gambling Prohibition Enforcement Act.

2.5.6 Difamación e información falsa

Internet puede utilizarse para divulgar información errónea con la misma facilidad que la información fidedigna[296]. 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[297]. Los menores utilizan cada vez más los foros web y los sitios de relaciones sociales donde también puede publicarse este tipo de información[298]. El comportamiento delictivo[299] puede consistir, por ejemplo, en la publicación de fotografías de carácter íntimo o información falsa sobre hábitos sexuales[300].

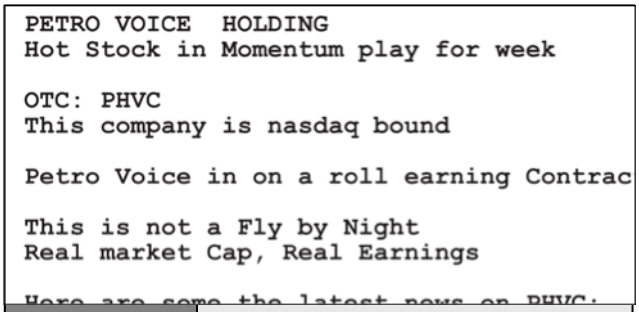


Figura 11

Los Correos-e basura representan un serio problema. Estos correos electrónicos se refieren a una amplia gama de temas. Además de promocionar diferentes productos, la información que proporcionan sobre valores y acciones es muy pupular.

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[301], lo que complica la identificación de los mismos. Además, los moderadores de foros controlan muy poco o nada el contenido publicado (Figura 11). No obstante, ello no es óbice para que se hayan desarrollado proyectos interesantes tales como Wikipedia, una enciclopedia en línea creada por los usuarios[302], 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 los rivales)[303];
- difamar (por ejemplo, escribir mensajes difamatorios o calumnias)[304];
- 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

---

296 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 http://www.mttlr.org/voleight/Reder.pdf.

297 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.

298 Regarding the privacy concerns related to those 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: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

299 Regarding the controversial discussion about the criminalisation 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: http://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: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://www.article19.org/pdfs/standards/definingdefamation.pdf.

300 See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

301 With regard to the challenges of investigating offences linked to anonymous services see below: Chapter 3.2.l2.

302 See: http://www.wikipedia.org.

303 See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

304 See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

retirarla o suprimirla. En tal caso, la información permanecerá en Internet aunque la fuente original de la misma se haya suprimido o corregido[305]. 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 entre la libertad de expresión[306] y la protección de las posibles víctimas de calumnias[307].

2.5.7 Correo basura y amenazas conexas

Por "correo basura" se entiende el envío masivo de mensajes no solicitados (Figura 12)[308]. 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[309], la oleada de este tipo de mensajes ha experimentado un aumento espectacular[310]. 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[311]. 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)[312].

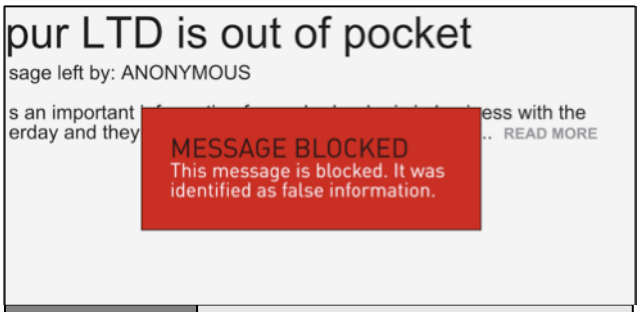


Figura 12

Los foros Internet, en los que se pueden escribir mensajes sin registro oficial, han adquirido mucha popularidad para escribir mensajes con información falsa.

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

---

305 Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as http://www.archive.org.

306 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

307 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.

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

309 *Tempelton*, "Reaction to the DEC Spam of 1978", available at: http://www.templetons.com/brad/spamreact.html.

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

311 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: http://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 http://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; http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html, available April 2007.

312 "2007 Sophos Report on Spam-relaying countries", available at: http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

filtrado de palabras clave o listas negras de direcciones IP de los remitentes de este tipo de correo[313]. 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[314].

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[315]), la mayoría de los infractores utilizan redes zombi (*botnets*)[316] para distribuir correo electrónico no solicitado. Al recurrir a redes zombi (o robot) constituidas por miles de sistemas informáticos[317], 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[318]. Algunos expertos opinan que la única solución real en la lucha contra el correo indeseado es aumentar el costo de envío para los remitentes[319]. 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[320]. 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[321].

En 2005, la OCDE publicó un Informe en que se analiza la incidencia del correo basura en los países en desarrollo[322]. 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

---

313 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: http://www.ciac.org/ciac/bulletins/i-005c.shtml; For an overview on different approaches see: BIAC ICC Discussion Paper on SPAM, 2004, available at: http://www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf

314 Lui/Stamm, "Fighting Unicode-Obfuscated Spam", 2007, page 1, available at: http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

315 Re 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, "Consumer Perspectives On Spam: Challenges And Challenges", available at: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20 perspective%20on%20spam.pdf.

316 Botnets is a short term for a group of compromised computers running programmes 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: http://www.fas.org/sgp/crs/terror/RL32114.pdf.

317 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.

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

319 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: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

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

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

322 "Spam Issue in Developing Countries", available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

banda y el acceso a Internet son más escasos y caros que en los países industrializados[323]. El correo consume tiempo y recursos en los países donde los recursos de Internet son más escasos y costosos.

2.5.8 Otras formas de contenido ilícito

Internet no sólo se utiliza para ataques directos, sino también como foro para:

- solicitar, ofrecer e incitar el crimen[324];
- 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[325]. 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[326]. El contrabando dificulta el control de ciertos productos restringidos en un territorio[327]. 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.

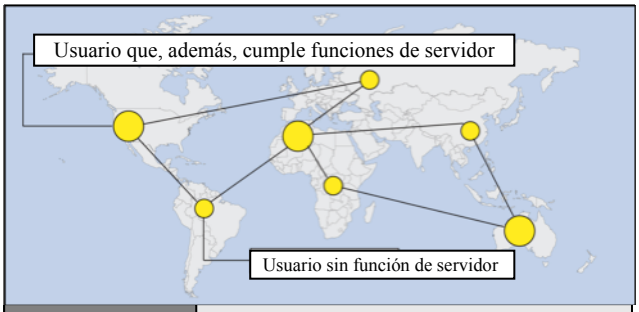


Figura 13

En el gráfico se observa el funcionamiento de sistemas de intercambio de archivos de la segunda generación. Mientras que los sistemas de intercambio de archivos de la primera generación se basaban en servidores centralizados que alojaban listas de documentos disponibles, en los de la segunda generación la función de servidor se delega a los usuarios, con lo cual resulta más difícil suprimir las actividades de la red e impedir las violaciones de los derechos de autor.

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[328] y cuanto más fácil es el acceso a esta información mayor es la probabilidad de que se produzcan atentados.

2.6 Delitos en materia de derechos de autor y de marcas

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

---

323 See "Spam Issue in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

324 See *Sieber*, Council of Europe Organised Crime Report 2004, page 140.

325 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: http://www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement.

326 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.

327 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: http://www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, "What's a Legal System to Do? The Problem of Regulating Internet Pharmacies", available at: https://www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

328 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: http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.

Internet[329] pueden tener problemas de carácter jurídico con las violaciones de los derechos de autor puesto que sus productos se pueden teledescargar, copiar y distribuir.

2.6.1 Delitos en materia de derechos de autor

Con el paso de los sistemas analógicos a los digitales[330], la digitalización[331] 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[332].

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 pueden mencionarse las siguientes:

- intercambio, en sistemas de intercambio de archivos, de programas informáticos, archivos y temas musicales protegidos con derechos de autor[333];
- elusión de los sistemas de gestión de derechos en el ámbito digital[334].

Los sistemas de intercambio de archivos son servicios de red entre pares[335] que habilitan a los usuarios a compartir archivos[336], por lo general, con otros millones de usuarios[337]. 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[338]. 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

---

329 E.g. by offering the download of files containing music, movies or books.

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

331 See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.

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

333 *Sieber*, Council of Europe "Organised Crime Report 2004", page 148.

334 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://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: http://www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

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

336 GAO, File Sharing, "Selected Universities Report Taking Action to Reduce Copyright Infringement", available at: http://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: http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

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

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

teledescargado música o archivos mediante sistemas de intercambio de archivos[339], y una tendencia similar se observa en otros países de la OCDE[340]. Estos sistemas pueden utilizarse para intercambiar todo tipo de datos informáticos, en especial, música, películas y software[341]. Históricamente se han utilizado ante todo para intercambiar música, pero el intercambio de vídeo es cada vez más importante[342].

La tecnología empleada en los servicios de intercambio de archivos, sumamente compleja, permite intercambiar grandes archivos en cortos periodos de tiempo[343]. 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[344]. 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[345]. Con la descentralización de las redes de intercambio de archivos de la segunda generación (véase la Figura 13) 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[346]. 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[347].

La tecnología de intercambio de archivos no sólo es utilizada por los ciudadanos de a pie y los delincuentes, sino también por las empresas[348]. No todos los archivos intercambiados con estos sistemas violan los derechos

---

339 See: "OECD Information Technology Outlook 2004", page 192, available at: http://www.oecd.org/dataoecd/22/18/37620123.pdf.

340 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: http://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.

341 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.

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

343 *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking", 2005, page 11, available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Cope, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: http://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.

344 Regarding Napster and the legal response see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: http://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.

345 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: http://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: http://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: http://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.

346 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 seqq., available at: http://www.ncjrs.gov/pdffiles1/nij/210798.pdf.

347 *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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing", 2005.

348 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: http://www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

de autor. Hay ciertos usos legítimos como, por ejemplo, el intercambio de obras de arte o de copias autorizadas dentro del dominio público[349].

Con todo, la utilización de los sistemas de intercambio de archivos plantea problemas a la industria del ocio[350]. 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[351] y miles de millones de archivos teledescargados[352]. En sistemas de intercambio de archivos han aparecido copias de películas antes de su estreno oficial en los cines[353], 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[354].

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*)[355], una tecnología de encriptación que impide la copia de contenidos en DVD[356]. 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)[357] 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[358]. 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[359]. 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

---

349 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.

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

351 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% of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

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

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

354 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.

355 Content Scrambling Systems (CSS) is a Digital Rights Management system that is used is most DVD videos discs. For details about the encryption used, see *Stevenson*, "Cryptanalysis of Contents Scrambling System", available at: http://www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

356 Regarding further responses of the entertainment industry (especially lawsuits against Internet user) 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.

357 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, "Digital Rights Management: The Skeptics' View", available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

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

359 *Sieber*, Council of Europe Organised Crime Report 2004, page 152.

falsificar equipos utilizados como control de acceso o eliminar la encriptación a través de herramientas informáticas[360].

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[361].

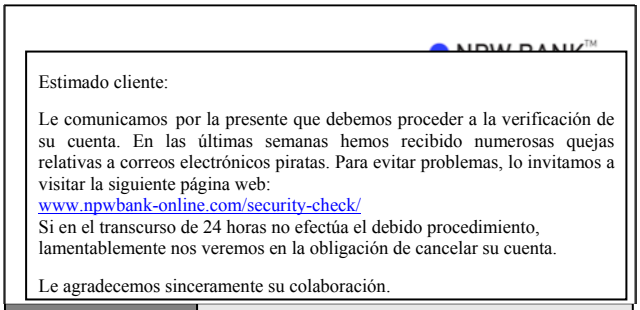


Figura 14

Se observa en esta figura el texto de un mensaje electrónico de *peska*. Estos mensajes se asemejan a las comunicaciones enviadas por empresas legítimas. Los delincuentes suelen utilizar logotipos originales de marcas protegidas.

2.6.2 Delitos en materia de marcas

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[362]. Los delitos más graves son, entre otros:

- la utilización de marcas en actividades delictivas con el propósito de engañar a las víctimas; 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* (véase la Figura 14)[363], 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[364].

Otro aspecto de las violaciones de marcas son los delitos en materia de dominios[365], por ejemplo la ciberocupación ilegal[366], 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[367]. En la mayoría de los casos, los delincuentes intentan

---

360 See: http://www.golem.de/0112/17243.html.

361 Regarding the similar discussion with regard to tools used to design viruses, see below: Chapter 2.7.4.

362 See Bakken, Unauthorised 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: http://www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf.

363 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 *Gercke*, The criminalisation of Phishing and Identity Theft, Computer und Recht, 2005, 606; *Ollmann*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: Chapter 2.8.d.

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

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

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

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

vender el dominio a la empresa a un precio más elevado[368] o utilizarlo para vender productos o servicios engañando a los usuarios con su supuesta conexión a la marca[369]. Otro ejemplo de infracción en materia de dominio es la "apropiación indebida de dominio" o registro de nombres de dominio que han caducado accidentalmente[370].

2.7 Delitos informáticos

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, incluyen:

- el fraude informático;
- la falsificación informática, la *peska* y el robo de identidad;
- la utilización indebida de dispositivos.

2.7.1 Fraude y fraude informático

El fraude informático es uno de los delitos más populares cometidos por Internet[371], puesto que con la automatización[372] y herramientas informáticas se pueden encubrir identidades delictivas.

Gracias a la automatización, los delincuentes obtienen importantes beneficios a partir de un cierto número de pequeñas acciones[373]. 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[374]. Un ejemplo de este timo es la estafa nigeriana, que consiste en el pago de una suma por adelantado (véase la Figura 15)[375].

Estimado amigo:
Ante todo, quiero presentarme. Me llamo Mbuto Butalia y soy la esposa del antiguo Presidente de la República de Thalia. Mi querido esposo ha muerto recientemente en un accidente aéreo. Mientras revisaba unos documentos, descubrí que mi marido era titular de una cuenta secreta de 10 000 000 USD.
Tengo la intención de transferir ese dinero a mi familia, que vive en los Estados Unidos. Como lamentablemente no puedo hacerlo en forma directa, me atrevo a solicitar su ayuda.
Me gustaría enviar los 10 000 000 USD a su cuenta, y pedirle que haga una transferencia de 9 000 000 USD a mi familia. El 1 000 000 USD restante sería para usted. Si está de acuerdo, quisiera que enviara primero a mi cuenta 10 USD para verificar la información de su cuenta bancaria.
...

Figura 15

En este recuadro puede leerse el texto de un correo electrónico clásico inspirado en la estafa nigeriana. Para recibir una supuesta fortuna, se pide a las víctimas que adelanten una cierta cantidad de dinero. Es un fraude muy difundido pero, dado que no se manipula ningún sistema informático, no se trata de un delito informático.

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[376]. La distinción principal entre fraude informático y fraude tradicional consiste en el objetivo que se persigue. Si el estafador trata de manipular

368 This happens especially with the introduction of new top-level-domains. To avoid cyber-squatting, 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.

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

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

371 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: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

372 Regarding the related challenges see below: Chapter 3.2.8.

373 In 2006, Nearly 50% 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: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

374 Regarding the related automation process: Chapter 3.2.8.

375 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. 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: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response", "Computer Law & Security Report", Volume 21, Issue 3, 237.

376 For more information, see below: Chapter 6.1.13.

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 *supra*.

Los fraudes más habituales son, entre otros, los siguientes:

1) Subasta en línea[377]

Las subastas en línea constituyen actualmente uno de los servicios más difundidos de cibercomercio. En 2006, se vendieron por eBay, el mercado de subastas en línea más importante del mundo[378], 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[379]. 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[380]. Los dos timos más comunes son[381]:

- ofrecer mercancías no disponibles para la venta y exigir su pago antes de la entrega[382]; 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[383] 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[384]. Con este timo, que se conoce como "apropiación de cuenta"[385], 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.

---

377 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: http://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: http://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

378 See http://www.ebay.com.

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

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

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

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

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

384 Regarding the criminalisation of "account takeovers", see *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

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

2) Estafa nigeriana[386]

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[387]. 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[388]. 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[389].

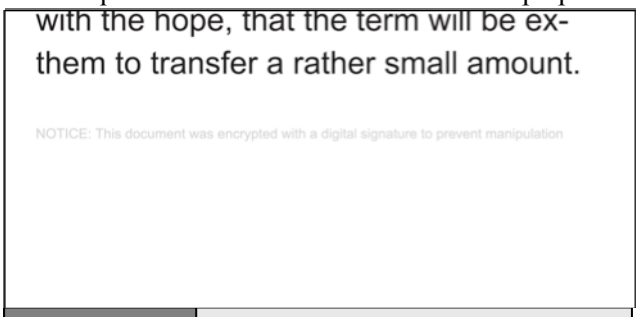


Figura 16

En comparación con la falsificación de documentos clásicos, los datos electrónicos se pueden manipular con bastante facilidad. Soluciones técnicas como las firmas digitales podrían evitar manipulaciones irreconocibles.

2.7.2 Falsificación informática

Por falsificación informática se entiende la manipulación de documentos digitales[390], 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[391]. Este timo consiste en lograr que las víctimas revelen información personal o secreta[392]. Por regla general, los delincuentes envían correos electrónicos que se asemejan a mensajes de instituciones financieras legítimas conocidas por la víctima[393] y están redactados de tal forma que resulta

386 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. 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: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response", "Computer Law & Security Report", Volume 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: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

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

388 For an overview of estimated losses, see *Reich*, "Advance Fee Fraud Scams in-country and across borders", "Cybercrime & Security", IF-1, page 3 et seqq.

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

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

391 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: http://www.usdoj.gov/opa/report_on_phishing.pdf

392 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

393 "Phishing" scams show a number of similarities to spam e-mails. It is likely that those organised crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: Chapter 2.5.g.

difícil creer que son falsos[394]. 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[395].

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 (véase la Figura 16).

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[396] para evitar la falsificación de un documento[397].

2.7.3 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[398]. Estos actos pueden cometerse sin recurrir a medios técnicos[399] o también en línea utilizando la tecnología Internet[400].

Por lo general, este delito consta de tres etapas diferentes[401]:

- 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[402], como ocurre con la venta de ese tipo de información[403]. Se venden, por ejemplo, listas de tarjetas de crédito a un precio de hasta 60 USD[404].

---

394 Regarding related trademark violations, see above: Chapter 2.6.2.

395 For more information about phishing scams see below: Chapter 2.8.4.

396 One technical solution to ensure the integrity of data is the use of digital signatures.

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

398 *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: http://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: http://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.

399 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: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

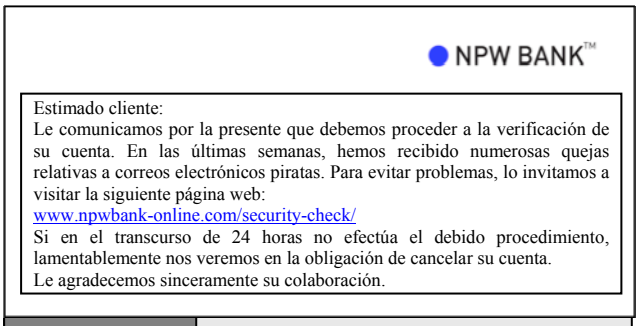
400 Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15% obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://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: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.

401 *Gercke*, Internet-related Identity Theft, 2007, available at: http://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: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

402 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: http://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.

- 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[405] 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[406].

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 deshechos")[407] o proceder al robo de correo[408]. 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[409]. Algunos Informes ponen de relieve los peligros que se corren debido a la utilización legal de motores de búsqueda con fines ilegales[410]. 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[411]. 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[412] 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. 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


NPW BANK™

Estimado cliente:
Le comunicamos por la presente que debemos proceder a la verificación de su cuenta. En las últimas semanas, hemos recibido numerosas quejas relativas a correos electrónicos piratas. Para evitar problemas, lo invitamos a visitar la siguiente página web:
www.npwbank-online.com/security-check/
Si en el transcurso de 24 horas no efectúa el debido procedimiento, lamentablemente nos veremos en la obligación de cancelar su cuenta.
Le agradecemos sinceramente su colaboración.

Figura 17

Se envían mensajes electrónicos de *peska* para obtener información secreta (datos de cuentas, contraseñas y números de transacción) que los delincuentes pueden utilizar para cometer delitos.

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

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

405 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf .

406 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 – available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

407 Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

408 This method is not considered as an Internet-related approach.

409 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.

410 See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

411 See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.

412 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 U.S corporations, government agencies and financial institutions. The Survey is available at: http://www.gocsi.com/.

ingeniosos para obtener información secreta (como datos de cuentas bancarias o de tarjetas de crédito) manipulando a los usuarios con técnicas de ingeniería social (véase la Figura 17)[413].

Hay varios tipos de datos que interesan a los delincuentes[414], siendo los más importantes los siguientes:

- **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[415]. 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[416].

- **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)[417]. 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[418] o porque responde a requisitos legales, como los pies de imprenta de las páginas web[419].

- **Contraseña de cuentas no financieras** – Si conocen la contraseña de una cuenta, los delincuentes pueden modificar sus particularidades y utilizarla para sus propios fines[420]. 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[421].

- **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.

---

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

414 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.

415 *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.

416 See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm.

417 *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: http://www.privacyrights.org/ar/id_theft.htm.

418 Examples is the online community Facebook, available at http://www.facebook.com.

419 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).

420 Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

421 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

El robo de identidad es un problema grave y que está en aumento[422]. Según cifras recientes, en el primer semestre de 2004, el 3 por ciento de los hogares estadounidenses fue víctima de ese delito[423]. 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[424]. 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[425]. 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[426]. Las pérdidas no sólo son financieras ya que contemplan también las estimaciones por daños y perjuicios[427]. 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[428].

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[429].

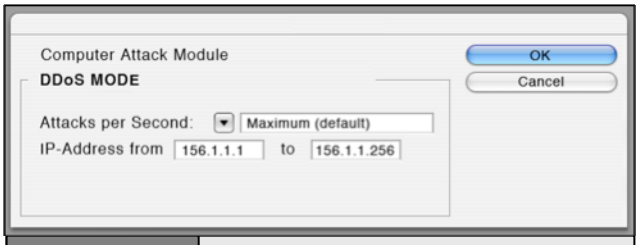


Figura 18

Gracias a un cierto número de herramientas a disposición, los delincuentes pueden efectuar ataques automáticos contra todos los sistemas informáticos utilizando direcciones IP dentro de una gama IP definida previamente. Con ayuda de esos programas, se pueden atacar centenares de sistemas informáticos en pocas horas

2.7.4 Utilización indebida de dispositivos

Para cometer un ciberdelito sólo hace falta un equipo sumamente básico[430]. 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[431] y, generalmente, en forma gratuita. Las más modernas cuestan varios miles de dólares[432]. Con ellas, los

---

422 "Identity Theft, Prevalence and Cost Appear to be Growing", GAO-02-363.

423 United States Bureau of Justice Statistics, 2004, available at http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

424 See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.

425 *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

426 See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.

427 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper", 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

428 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: http://www.heise-security.co.uk/news/80152.

429 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper", 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

430 The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: Chapter 3.2.h.

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

delincuentes pueden atacar otros sistemas informáticos pulsando tan sólo una tecla (véase la Figura 18). 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[433]. Pueden encontrarse herramientas informáticas para[434]:

- cometer ataques por denegación de servicio (DoS)[435];
- 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[436]. 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[437].

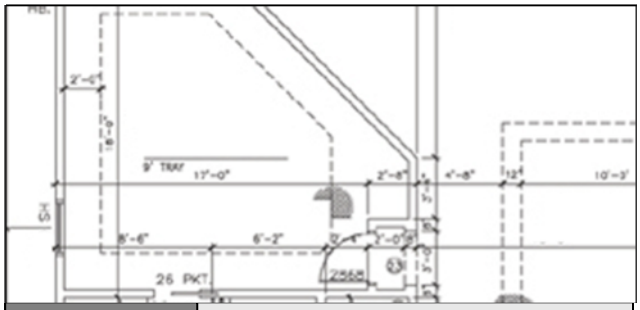


Figura 19

Internet es una fuente importante de información, incluida la información (por ejemplo, planos de arquitectura) sobre posibles objetivos (como edificios públicos), que puede obtenerse en las páginas web (de un arquitecto, por ejemplo), etc.

2.8 Combinación de delitos

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*.

2.8.1 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

---

432 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: http://www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (200 – 500 US Dollar) see: Paget, Identity Theft, White Paper, McAfee, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

433 See above: Chapter 2.4.1.

434 For more examples, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 23 et seq., available at: http://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: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.

435 DoS is an acronym for Denial-of-Service attack. For more information, see above : Chapter 2.4.e.

436 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: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

437 For more details, see below: Chapter 6.1.13.

informática")[438]. 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[439], pero resulta difícil evaluar la importancia de las amenazas[440]; 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 suceso 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[441].

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[442], propiciado por Informes[443] que revelaban el uso de Internet en la preparación del ataque[444]. 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[445]. En el marco de este contexto, se descubrió que las organizaciones terroristas utilizan Internet de distintas formas[446]. 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.

---

438 *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.

439 *Rollins/ Wilson*, "Terrorist Capabilities for Cyberattack", 2007, page 10, available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf.

440 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: http://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 cyber-terrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, "A Framework for Understanding Terrorist Use of the Internet, 2006", available at: http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp.

441 See: Report of the National Security Telecommunications Advisory Committee – Information Assurance Task Force – Electric Power Risk Assessment, available at: http://www.aci.net/kalliste/electric.htm.

442 See: *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://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 seqq., available at: http://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 seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/ lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

443 See: *Rötzer*, Telepolis News, 4.11.2001, available at: http://www.heise.de/tp/r4/artikel/9/9717/1.html.

444 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: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=.

445 CNN, News, 04.08.2004, available at: http://www.cnn.com/2004/US/08/03/terror.threat/index.html.

446 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.

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[447], 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[448]. Uno de los motivos es el reconocimiento de la comunidad internacional de que las amenazas del terrorismo internacional exigen soluciones a escala mundial[449]. 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[450]. No se ha logrado siquiera llegar a un consenso con respecto a la definición de "terrorismo"[451]. 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[452]. 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[453]. 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[454]. Los terroristas también han comenzado a participar en comunidades vídeo (como YouTube) para distribuir mensajes y propaganda[455]. La utilización de páginas web y otros foros es una señal de la importancia que atribuyen los grupos subversivos a relaciones públicas más profesionales[456]. La finalidad de recurrir a páginas web y otros medios reside en distribuir propaganda[457], dar una justificación[458] de sus actividades y reclutar[459] nuevos miembros y donantes así como

---

447 *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

448 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.

449 One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.

450 Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyber Attacks 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 Cyber Terrorism, Cyber War and Other Cyber Threats; *Wilson* in CRS Report, Computer Attack and Cyber Terrorism – Vulnerabilities and Policy Issues for Congress, 2003.

451 See for example *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.

452 *Wilson* in CRS Report, Computer Attack and Cyber Terrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

453 ADL, Terrorism Update 1998, available at: http://www.adl.org/terror/focus/16_focus_a.asp.

454 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes see as well: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

455 Regarding the use of YouTube by terrorist organisations, see Heise News, news from 11.10.2006, available at: http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

456 *Zanini/Edwards*, "The Networking of Terror in the Information Age", in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

457 United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

establecer contacto con los ya existentes[460]. En algunas páginas web se han difundido recientemente vídeos de ejecuciones[461].

Recopilación de información

En Internet puede hallarse información considerable sobre posibles objetivos[462]. 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[463]. 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[464]. 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[465]. 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[466]. 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[467]. Un incidente similar tuvo lugar en Australia, cuando en páginas web del Gobierno apareció información detallada sobre posibles objetivos de atentados terroristas[468]. 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[469].

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[470]. Actualmente se examinan formas más directas de actividades de preparación en línea. Según algunos Informes publicados, los terroristas están utilizando juegos en línea para

---

458 Regarding the justification see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

459 *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 et. seqq.

460 See: *Conway*, "Terrorist Use of the Internet and Fighting Back", "Information and Security", 2006, page 16.

461 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.

462 Regarding the related challenges see *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.

463 *Levine*, Global Security, 27.06.2006, available at: http://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, Goolge Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: http://www.derstandard.at/?url/?id=2952935.

464 For further reference see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.

465 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".

466 "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.

467 See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.

468 *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18.

469 See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: http://www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

470 See below.

preparar sus atentados[471]. 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[472].

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[473]. En 2008, los servicios secretos occidentales descubrieron un servidor de Internet que facilitaba el intercambio de material de capacitación y la comunicación[474]. Según se informó, las organizaciones terroristas se sirven de diferentes páginas web para coordinar sus actividades[475].

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[476]. Los diarios informaron acerca del intercambio de instrucciones detalladas sobre los objetivos y el número de atacantes a través del correo electrónico[477]. 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[478]. 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[479]. 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

---

471 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: http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html*; O'Hear*, Second Life a terrorist camp?, ZDNet.

472 Regarding other terrorist related activities in online games see: *Chen/Thoms*, Cyber Extremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 et seqq.

473 *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.

474 *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

475 *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

476 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

477 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: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=.

478 The Commission analyzing the 9/11 attacks calculated that the costs for the attack could have been between 400.000 and 500.000 USD. 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 have been relatively small. Regarding the related challenges see as well *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

479 See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

datos de una cuenta bancaria destinada a posibles donantes[480]. 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[481]. 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[482].

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[483]. Es lo que ocurre especialmente con los ataques contra sistemas interconectados a través de computadoras y redes de comunicación[484], 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[485]. Investigar o incluso impedir esos ataques supone desafíos singulares[486]. A diferencia de los ataques físicos, los delincuentes no necesitan estar presentes en el lugar afectado[487]. Y mientras llevan a cabo el ataque, pueden utilizar medios de comunicaciones anónimas y tecnologías de encriptación para ocultar su identidad[488]. 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[489].

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[490]. Una infraestructura se considera esencial si su incapacidad o destrucción puede afectar negativamente la defensa o seguridad económica de un Estado[491]. 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

480 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.

481 See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4.

482 Regarding virtual currencies see *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

483 *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

484 *Lewis*, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002.

485 *Shimeall/Williams/Dunlevy*," Countering cyber war", NATO review, Winter 2001/2002, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf.

486 *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 et seq.

487 *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.

488 CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

489 Law Enforcement Tools and Technologies for Investigating Cyber Attacks, DAP Analysis Report 2004, available at: http://www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.

490 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

491 United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17,1996. Vol. 61, No. 138.

servicios a causa del huracán Katrina en los Estados Unidos es un ejemplo de la dependencia de la sociedad en esos servicios[492].

La vulnerabilidad de la infraestructura esencial ante los ataques perpetrados en la red puede demostrarse con algunos incidentes vinculados al transporte aéreo.

- Los servicios de facturación de la mayoría de los aeropuertos del mundo ya disponen de sistemas informáticos interconectados[493]. En 2004, el virus informático Sasser[494] infectó millones de computadoras en todo el mundo, incluidos los sistemas informáticos de las principales compañías aéreas, con la consiguiente cancelación de vuelos[495].

- 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)[496]. En 2000, durante un plazo muy breve, se cometieron varios ataques de ese tipo contra empresas bien conocidas como CNN, Ebay y Amazon[497], a raíz de los cuales algunos servicios fueron interrumpidos durante varias horas e incluso días[498]. Las compañías aéreas también han sido víctimas de ataques DoS, como el cometido contra la página web de Lufthansa en 2001[499].

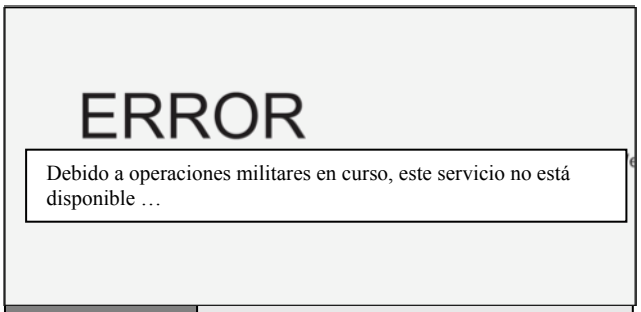


Figura 20

En los últimos años, Internet se ha constituido en un medio importante de intercambio de información y propaganda durante los conflictos armados. Se discute a menudo en qué medida es posible y/o aconsejable interrumpir ciertos servicios Internet durante etapas clave progresivas de un conflicto.

- 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

---

492 Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: http://www.gao.gov/new.items/d07706r.pdf.

493 *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: http://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.

494 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.

495 *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.

496 *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

497 *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.

498 *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.

499 *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

de los Estados Unidos en 1997[500], 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[501].

2.8.2 Guerra informática

Por guerra informática se entiende la utilización de las TIC e Internet para declarar una guerra en el ciberespacio. Este fenómeno tiene características similares al ciberterrorismo[502]. En un principio, los debates se centraron en la sustitución de la guerra clásica por ataques a través de redes informáticas[503] que, por lo general, son menos onerosos que las operaciones militares tradicionales[504] e incluso pequeños Estados pueden llevarlos a cabo.

Protegerse contra los ciberataques no es fácil. Hasta ahora, se conocen muy pocos Informes que se refieran a la sustitución de conflictos armados por ataques a través de Internet[505]. En este momento, los debates dan prioridad a los ataques contra infraestructuras esenciales y al control de la información durante un conflicto (véase la Figura 20).

Teniendo en cuenta tanto las comunicaciones civiles como militares, la infraestructura de la información constituye un objetivo fundamental en los conflictos armados. Sin embargo, no es seguro que esos ataques se cometan por Internet. Los ataques perpetrados a sistemas informáticos en Estonia[506] y los Estados Unidos[507] han sido asociados a la guerra informática. Dada la imposibilidad de determinar a ciencia cierta si un ataque procede de un organismo público oficial, resulta difícil catalogarlo de guerra informática. Ocurre lo mismo con respecto a los ataques físicos -por ejemplo, mediante armas y explosivos - contra infraestructuras[508].

El control de la información ha sido siempre un aspecto importante en los conflictos armados puesto que permite ejercer influencia en el público en general y también en el personal militar enemigo. El control de la información por Internet ha pasado a ser un medio de influencia cada vez más importante durante los conflictos armados.

2.8.3 Ciberblanqueo de dinero

Internet está transformado los métodos de blanqueo de dinero. 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

---

500 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.

501 Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: http://www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: http://www.cio.com/article/print/30933.

502 See above: Chapter 2.8.1.

503 Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, "Strategic Information Warfare, 1996", available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

504 *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

505 *Shimeall/Williams/Dunlevy*, "Countering cyber war", NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf; *Yurcik/Sharma*, "Internet Hack Back as an Active Defense Strategy", 2005, available at: http://www.projects.ncassr.org/hackback/ccsa05.pdf.

506 *Traynor,* "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, 17.05.2007, available at: http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

507 *Thornburgh*, "Inside the Chinese Hack Attack", Time, 25.08.2005, available at: http://www.time.com/time/nation/printout/0,8816,1098371,00.html.

508 One example is the intentional destruction of communication infrastructure by NATO forces during the war in the former Republic of Yugoslavia. Regarding this issue, see: http://www.nato.int/kosovo/press/p990506c.htm.

de transacciones sospechosas en la lucha contra el blanqueo de dinero se basa en obligaciones de las instituciones financieras que intervienen en las transferencias[509].

El ciberblanqueo de dinero se divide por lo general en tres etapas:

1) depósito;

2) estratificación; y

3) integración.

Con respecto al depósito de grandes cantidades de dinero en efectivo, Internet no podría quizás ofrecer esas numerosas ventajas tangibles[510], 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 (véase la Figura 21)[511].

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.

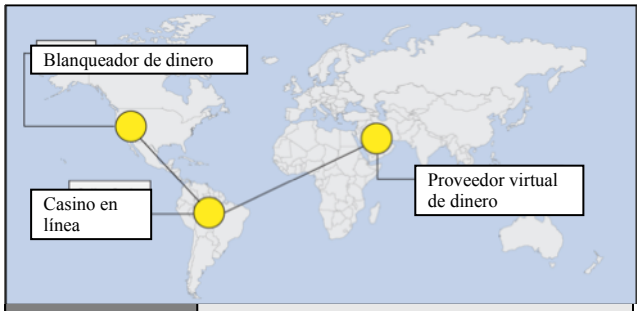


Figura 21

En el gráfico se observa la combinación de casinos en línea y dinero virtual en los delitos de blanqueo de dinero por Internet. Debido a la utilización de esos servicios por parte de delincuentes, las autoridades competentes tienen dificultades en localizar las operaciones de transferencia e identificar a quienes las realizan.

1) 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[512]. 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[513].

2) Utilización de casinos en línea:

En contraposición al establecimiento de un verdadero casino, no se necesitan importantes inversiones para crear casinos en línea[514]. Por otra parte, la reglamentación de los casinos en línea y fuera de línea suele ser diferente según los países[515]. 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.

---

509 One of the most important obligations is the requirement to keep records and to report suspicious transactions.

510 Offenders may tend to make use of the existing instruments e.g., the service of financial organisations to transfer cash, without the need to open an account or transfer money to a certain account.

511 For case studies, see: "Financial Action Task Force on Money Laundering", "Report on Money Laundering Typologies 2000 – 2001", 2001, page 8.

512 See: *Woda*, "Money Laundering Techniques With Electronic Payment Systems", Information & Security, Vol. 18, 2006, page 40.

513 Regarding the related challenges see below: Chapter 3.2.l.

514 The costs of setting up an online casino are not significantly larger than other e-commerce businesses.

515 Regarding approaches to the criminalisation of illegal gambling, see below: Chapter 6.1.j.

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 motivos de los problemas planteados en materia de reglamentación son los siguientes:

- dificultades en la verificación del cliente: la precisión de una verificación puede correr peligro si el proveedor del servicio financiero y el cliente no se han conocido nunca[516];
- falta de contacto personal: resulta difícil aplicar procedimientos tradicionales del tipo "conozca a su cliente";
- participación frecuente, en las transferencias por Internet, de proveedores de diversos países;
- falta de un código legal/penal para supervisar ciertos instrumentos: en particular, plantea dificultades cuando los proveedores autorizan a los clientes a efectuar transferencias de valores con arreglo al modelo "de par a par".

2.8.4 Peska

Los ciberdelincuentes han elaborado técnicas para obtener información personal de los usuarios que van desde los programas espía[517] hasta los ataques destinados a la "*peska*"[518]. El término "*peska*" describe una serie de actos llevados a cabo para que las víctimas revelen información personal y/o secreta[519]. Aunque hay diferentes tipos de ataques de este último tipo[520], 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).

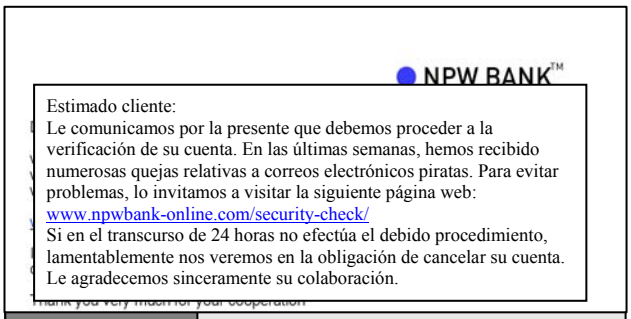


Figura 22

La finalidad de los mensajes electrónicos de *peska*, que se diseñan de tal forma que se asemejan a los enviados por empresas legítimas, es lograr que la víctima revele información secreta. Con suma frecuencia, el objetivo de los delincuentes son los clientes de instituciones bancarias.

Con objeto de guiar a los usuarios hacia sitios pirata, los delincuentes envían mensajes electrónicos similares a los de una empresa legítima (véase la Figura 22)[521], que con frecuencia dan lugar a violaciones en materia de marcas[522]. 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

---

516 See: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000 – 2001", 2001, page 2.

517 Regarding the threat of spyware, see *Hackworth*, "Spyware, Cybercrime and Security", IIA-4.

518 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: http://www.usdoj.gov/opa/report_on_phishing.pdf.

519 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

520 The following section describes email-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: http://www.techweb.com/wire/security/186701001.

521 "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organised 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: Chapter 2.5.7.

522 Regarding related trademark violations, see above 2.6.2.

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[523].

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*[524]. Más de 55 000 sitios de *peska* exclusivos se pusieron en conocimiento del APWG[525] en abril de 2007[526]. 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"[527].

2.9 Repercusiones económicas del ciberdelito

Huelga decir que los daños financieros ocasionados por los delitos perpretados con computadores y los cometidos en la Internet son considerables. Se han publicado recientemente los resultados de varias encuestas en las que se destaca el hecho de que estos efectos[528] resultan apreciables. Además, no son sólo las estadísticas sobre estos delitos las que suscitan en general preocupación, sino también sus daños financieros. Hay que indicar, por otra parte, la incertidumbre imperante en lo que respecta a la medida en que dichas encuestas proporcionan cifras exactas, ya que muchas victimas no informan acerca de estos delitos[529].

2.9.1 Panorama de los resultados de una serie de encuestas

En la Encuesta sobre delitos informáticos y seguridad que efectuó el Instituto de Seguridad Informática (CSI) en 2007, se analizaron las consecuencias económicas de los delitos cibernéticos[530], basándose en las respuestas de 494 personas encargadas de la seguridad informática de empresas, organismos públicos e instituciones financieras de Estados Unidos, por lo que dicha encuesta reviste interés principalmente para este país[531].

A la vista del ciclo económico, la encuesta apuntaba al hecho de que, tras aumentar hasta 2002, las repercusiones financieras del ciberdelito se redujeron los años siguientes. Aunque en la encuesta se sugería que este resultado era motivo de controversia, no resultaba claro en qué medida se había reducido el número de delitos comunicados y las pérdidas medias de sus victimas. En 2006 aumentó una vez más el importe de tales pérdidas. Ahora bien, en la encuesta no se explicaba por qué motivo las pérdidas se redujeron en 2002 o aumentaron en 2006. Basándose en las 21 categorías identificadas en la encuesta, se vio que las pérdidas en dólares más elevadas eran las que correspondían al fraude financiero, la penetración de sistemas por virus venidos del exterior y el robo de datos confidenciales. En 2006 las pérdidas de las personas que habían respondido a la encuesta ascendieron a un total de aproximadamente 66,9 millones USD.

---

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

524 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).

525 Anti-Phishing Working Group. For more details, see: http://www.antiphishing.org.

526 "Phishing Activity Trends", Report for the Month of April 2007, available at: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

527 See above: Chapter 2.7.3.

528 See, for example: "Deloitte 2007 Global Security Survey" – September 2007; "2005 FBI Computer Crime Survey"; "CSI Computer Crime and Security Survey 2007" is available at: http://www.gocsi.com/; "Symantec Internet Security Threat Report", September 2007, available at: http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport; "Sophos Security Threat Report", July 2007, available at: http://www.sophos.com/pressoffice/news/articles/2007/07/securityrep.html.

529 See for example: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, 2002, page 27, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; See also ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

530 The "CSI Computer Crime and Security Survey 2007", available at: http://www.gocsi.com/.

531 See "CSI Computer Crime and Security Survey 2007", page 1, available at: http://www.gocsi.com/.

Tras una serie de años en los que se registró una reducción de las pérdidas medias por persona que habían respondido a la encuesta, asistimos a un cambio de situación. En 2006 la pérdida media se situó en 345 000 USD, mientras que en 2001 fue prácticamente diez veces mayor (3,1 millones USD). Esta pérdida media depende en gran medida de la composición de las personas que responden a una encuesta, así, si un año dado responden esencialmente empresas pequeñas y medianas, al año siguiente lo hacen empresas mayores, dicho cambio afecta considerablemente los resultados estadísticos.

En la Encuesta sobre delitos informáticos efectuada por el FBI en 2005[532] se seguía un enfoque similar a la encuesta del CSI, pero su cobertura era mayor y más extensa[533]. El FBI estimó que el costo de los incidentes de seguridad producidos por delitos informáticos o cometidos en la Internet ascendería a 21,7 millones USD[534]. Los delitos más generalizados que detectaron las organizaciones que respondieron al cuestionario eran ataques con virus, programas maliciosos, lectura de puertos y sabotaje de datos o redes[535]. En la encuesta se incluía una estimación de la pérdida total que estos delitos habían supuesto para la economía de los Estados Unidos[536]. Basándose en las pérdidas medias[537] y en el supuesto de que el 20 por ciento de las organizaciones estadounidenses se veían afectadas por delitos cibernéticos, se calculó que la pérdida total se había situado en 67 mil millones USD[538]. Con todo, preocupaba la representatividad de estas estimaciones y la continuidad de los participantes de un año a otro[539].

El Informe sobre los aspectos económicos de los programas informáticos maliciosos, que se publicó en 2007[540], se centra en el impacto de estos programas maliciosos en la economía mundial, impacto que se calcula sumando los costes estimados[541] de tales ataques. Un descubrimiento crucial de los autores del Informe precitado es el hecho de que los delincuentes que diseñan programas maliciosos han trocado el vandalismo por la obtención de beneficios económicos. En el Informe mencionado se ha descubierto que las pérdidas financieras generadas por ataques perpetrados con soporte malicioso llegaron a un máximo en los años 2000 (17,1 mil millones USD) y 2004 (17,5 mil millones USD), pero se redujeron después de 2004 y se situaron en 13,3 mil millones USD en 2006. Sin embargo, como ocurre con los resultados de la encuesta, no se sabe si las estadísticas sobre los efectos de los programas maliciosos son realistas. Existen grandes discrepancias entre las pérdidas comunicadas y los daños probados, como demuestra el caso del gusano Sasser. En efecto, se ha informado de que este gusano ha infectado millones de sistemas informáticos[542] y en el juicio civil contra el diseñador del soporte lógico implicado, muy pocas empresas y particulares respondieron a la petición de que probaran sus pérdidas y se sumasen a la acción judicial. El caso concluyó con un fallo según el cual el diseñador del virus debía pagar una compensación inferior a diez mil dólares estadounidenses[543].

---

532 "2005 FBI Computer Crime Survey".

533 The 2005 FBI Computer Crime Survey is based on data of 2066 United States institutions (see 2005 FBI Computer Crime Survey, page 1) while the 2007 CSI Computer Crime and Security Survey is based on 494 respondents (See CSI Computer Crime and Security Survey 2007, page 1, available at: http://www.gocsi.com/).

534 See "2005 FBI Computer Crime Survey", page 10.

535 See "2005 FBI Computer Crime Survey", page 6.

536 See *Evers*, "Computer crimes cost $67 billion, FBI says", ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

537 "2005 FBI Computer Crime Survey", page 10.

538 See "2005 FBI Computer Crime Survey", page 10 As well as *Evers*, "Computer crimes cost $67 billion, FBI says", ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

539 The report makes available useful details of those institutions that responded. See "CSI Computer Crime and Security Survey 2007", page 3, available at: http://www.gocsi.com/.

540 "2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code". A summary of the report is available at: http://www.computereconomics.com/article.cfm?id=1225.

541 The costs covered by the report include labour costs to analyze and repair an infected computer system, the loss of user productivity and the loss of revenue due to a loss of performance of infected computer systems. For more information, see the summary of the report available at: http://www.computereconomics.com/article.cfm?id=1225.

542 See: "Sasser Worm rips through the Internet", CNN News, 05.05.2004, available at: http://edition.cnn.com/2004/TECH/internet/05/05/sasser.worm/index.html.

543 See Heise News, 06.07.2005, available at: http://www.heise.de/newsticker/meldung/print/61451.

2.9.2 Dificultades que plantean las estadísticas sobre el ciberdelito

Resulta poco claro que las estadísticas sobre las repercusiones económicas del ciberdelito sean representativas y que proporcionen información fiable acerca del alcance de las pérdidas[544]. En efecto, no se sabe a ciencia cierta en qué grado se informa sobre el ciberdelito, no sólo en las encuestas, sino también a las entidades encargadas de hacer cumplir la ley. Las autoridades que participan en la lucha contra el ciberdelito alientan a las víctimas del mismo a informar sobre tales delitos[545]. El acceso a una información más precisa acerca del grado de incidencia real de los ciberdelitos permitiría que los órganos encargados de hacer cumplir la ley reprimieran más adecuadamente a los delincuentes, impidiesen la realización de ataques y promulgaran legislación más adecuada y eficaz.

Un gran número de entidades públicas y privadas han intentado cuantificar los costes directos e indirectos de los programas informáticos maliciosos. Resulta difícil calcular dichos costes para las empresas, y aún más evaluar las pérdidas financieras que generan los programas maliciosos y el soporte lógico similar en detrimento de los diferentes consumidores, aunque hay pruebas fragmentarias que indican que los daños pueden ser considerables[546]. Ahora bien, dichos costes tienen distintos componentes y pueden traducirse en daños directos para los equipos y programas informáticos, así como en daños financieros y de otro tipo, debido al robo de identidad o a otras acciones fraudulentas aunque las estimaciones realizadas sobre el particular difieren entre sí, empezamos a hacernos una idea coherente de la situación considerada en su conjunto.

Por otra parte, las empresas pueden no informar acerca de delitos cibernéticos por varias razones:

Es posible que las empresas teman que la publicidad negativa a que diese lugar dicha información pudiera atentar contra su reputación[547]. Así por ejemplo, los clientes de una empresa que anuncie que su servidor ha sido pirateado pueden perder confianza en la misma. Los costes totales de estas consecuencias pueden ser mayores que las pérdidas ocasionadas por los ataques de los piratas. No obstante, si no se informa sobre las acciones de éstos y no son enjuiciados, pueden volver a actuar de manera delictiva.

Puede ocurrir que las víctimas de dichos delitos no crean que las entidades encargadas de hacer cumplir la ley puedan identificar a los delincuentes[548]. Si se compara el gran número de ciberdelitos con el reducido número de investigaciones que se han visto coronados por el éxito, las víctimas tendrían poco interés en informar acerca de los delitos de que han sido objeto[549].

Hay que señalar además que la automatización permite que los ciberdelincuentes adopten una estrategia consistente en obtener grandes beneficios realizando un gran número de ataques con el fin de obtener una reducida cantidad de dinero de cada víctima, como sucede con el fraude que entraña la percepción de tasas por adelantado[550]. Tratándose de pequeñas cantidades, las víctimas de dichos ataques no recurrirían seguramente a aplicar procedimientos de información engorrosos. En todo caso, y si se atiende a los casos registrados, lo

---

544 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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

545 "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: http://www.heise-security.co.uk/news/80152.

546 ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

547 See *Mitchison/Urry*, "Crime and Abuse in e-Business, IPTS Report", available at: http://www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm.

548 See Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, page 2, available at: http://www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

549 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: http://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: http://www.interpol.int/Public/THB/vico/Default.asp.

550 See SOCA, "International crackdown on mass marketing fraud revealed, 2007", available at: http://www.soca.gov.uk/downloads/massMarketingFraud.pdf.

harían únicamente cuando se tratara de ataques que redundan en el cobro de tasas muy elevadas[551]. Además, los delincuentes que sólo estafan pequeñas cantidades realizan un delito que no será investigado las más de las veces.

3 Desafíos que suscita la lucha contra el ciberdelito

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

Las entidades encargadas de hacer cumplir la ley 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[552].

Figura 23

En este ejemplo, los expertos en informática forense pudieron deshacer las modificaciones realizadas en una fotografía y reconstruir el rostro del sospechoso.

Puede resultar difícil automatizar los procesos de investigación. Así por ejemplo, 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 desmenuzados sólo tienen éxito cuando las fotografías se han clasificado anteriormente por notas, los valores desmenuzados se almacenan en una base de datos y la fotografía que se analiza no se modifica[553].

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 de 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 (véase la Figura 23). Los expertos en informática forense pudieron deshilvanar las modificaciones y reconstruir el rostro del sospechoso[554]. Si bien el éxito de esta investigación demuestra con claridad las posibilidades de la ciencia forense informática, 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.

---

551 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 5,100 USD each. The number of reported offences is very low, while the average loss of those offences is the high.

552 See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: https://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: https://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.

553 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.

554 For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: http://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: http://www.interpol.int/Public/THB/vico/Default.asp.

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 la Internet; entre otras, las llamadas VoIP y las comunicaciones por correo electrónico[555]. Las TIC se utilizan en nuestros días para ejecutar funciones de control y gestión en edificios[556], vehículos y el campo de los servicios de aviación (véase la Figura 24)[557]. 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[558].

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[559]. Una breve interrupción de un servicio puede ocasionar grandes daños financieros en los mercados de cibercomercio[560] 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[561].

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[562], por lo cual los delincuentes pueden diseñar ataques eficaces, concentrándose únicamente en este objetivo[563].

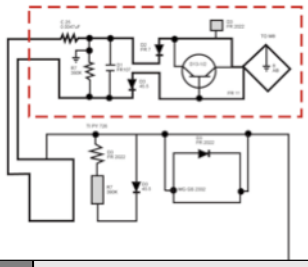


Figura 24

La tecnología de la información y los dispositivos electrónicos reemplazan cada vez más las funciones manuales.

La sociedad depende de las TIC y dicha dependencia no se limita a los países occidentales[564], como demuestra el hecho de que los países en desarrollo deban afrontar los ataques lanzados contra sus infraestructuras y

555 It was reported that the United States Department of Defence had to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

556 Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

557 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.

558 *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 seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf.

559 Re 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.

560 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 computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. 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: http://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.

561 *Shimeall/Williams/Dunlevy*," Countering cyber war", NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf.

562 One analysis by "Red Sheriff" in 2002 stated that more than 90% of the users worldwide use Microsoft`s operating systems (source: http://www.tecchannel.de – 20.09.2002).

563 Re the discussion about 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 http://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.

564 With regards to the effect of spam on developing countries, see: "Spam issues in developing countries, 2005", available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

usuarios[565]. El desarrollo de tecnologías de infraestructura baratas, tales como WiMAX[566], 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[567, 568]. 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[569].

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[570].

3.2.2 Número de usuarios

La popularidad de la Internet y de sus servicios van en rápido aumento, como demuestra la existencia de más de mil millones de usuarios de Internet en todo el mundo (véase la Figura 25)[571]. Los fabricantes de computadores y los ISP tienen la mira puesta en los países en desarrollo, ya que estas naciones presentan el mayor potencial de crecimiento[572]. En 2005 el número de usuarios de Internet en los países en desarrollo sobrepasó al de usuarios en las naciones industrializadas[573], por no hablar de que el desarrollo de equipo barato y acceso inalámbrico permitirá que una mayor cantidad de personas acceda a la Internet[574].

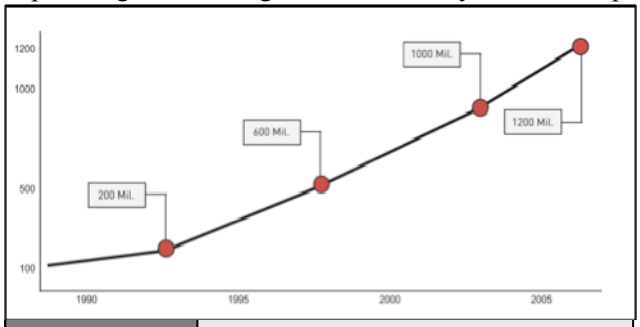


Figura 25

Actualmente sistemas de mil millones de usuarios de Internet.

El continuo incremento de la población conectada a Internet, hace que aumente también el número de víctimas en potencia y de delincuentes[575]. Es difícil calcular cuántas personas emplean la Internet para efectuar

---

565 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: http://www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; "World Information Society Report 2007", page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

566 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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, "WiMAX Technology for Broadband Wireless Access".

567 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

568 See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

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

570 See below: Chapter 4.

571 According to the ITU, there were 1.14 billion Internet users by the start of 2007, available at: http://www.itu.int/ITU-D/icteye.default.asp.

572 See *Wallsten*, "Regulation and Internet Use in Developing Countries", 2002, page 2.

573 See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

574 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 http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

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 la 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[576].

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 fotografías ilegales plantea grandes problemas. Así por ejemplo, los enfoques basados en valores desmenuzados son sólo útiles si se procede previamente a clasificar las fotografías por nota, se almacenan los valores desmenuzados en una base de datos y la fotografía analizada no se ha modificado[577].

3.2.3 Disponibilidad de dispositivos y de acceso

Para cometer delitos informáticos es preciso disponer de un sistema básico, integrado generalmente por los siguientes elementos:

- equipo;
- programas; y
- acceso a Internet.

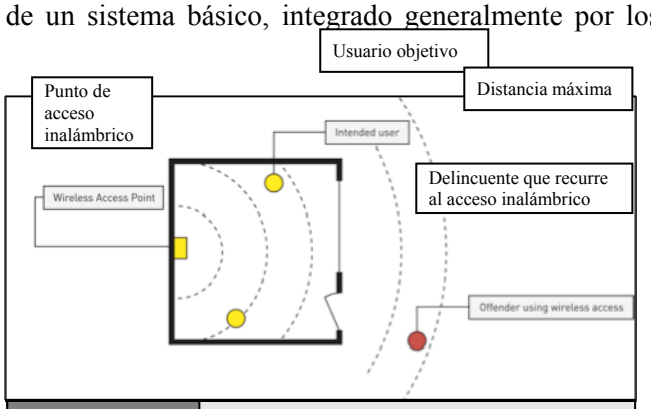


Figura 26

Acceder a Internet sin dejar huella alguna es el objetivo que persiguen muchos delincuentes. En la figura se indica la forma en que un delincuente puede utilizar la señal de una red inalámbrica abierta para acceder a distancia a ésta. De ser así, resulta prácticamente imposible identificar a dicho delincuente.

Por lo que hace al equipo, hay que señalar que la potencia de los computadores se encuentra en continuo aumento[578] 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[579]. 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[580] diseñadas para localizar puertos

---

575 Regarding the necessary steps to improve cybersecurity, see: "World Information Society Report 2007", page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

576 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: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: Chapter 2.8.d.

577 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.

578 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/.

579 Chapter six, "World Information Society Report 2007", ITU, Geneva, available at: http://www.itu.int/wisr/.

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

abiertos o suspender la protección que procuran las contraseñas[581]. Debido a las técnicas de espejo y de intercambio entre pares, resulta difícil limitar la disponibilidad especializada de dichos dispositivos[582].

El último elemento crucial es el acceso a Internet. El costo de dicho acceso[583] 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 la Internet en los países en desarrollo se encuentra en rápido aumento[584]. 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[585]. Para acceder a las conexiones de redes recurren preferentemente a:

- terminales públicos de Internet;
- redes abiertas (inalámbricas) (véase la Figura 26)[586];
- redes pirateadas; y
- 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[587]. Con todo, hay motivos que aconsejan no imponer dicha obligación de identificación[588]. 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[589]. Se ha sugerido que esta limitación del acceso a Internet

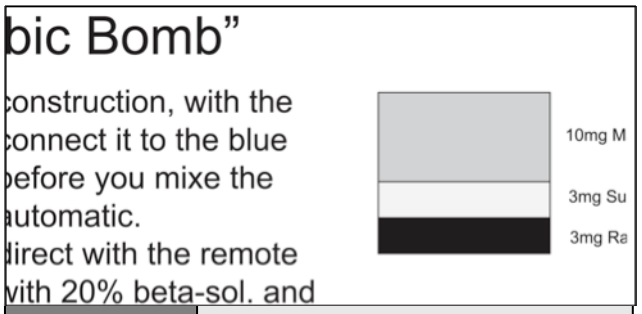


Figura 27

En Internet aparecen en numerosas ocasiones las instrucciones para construir armas y explosivos. El gráfico muestra una explicación sobre la forma de construir una bomba utilizando únicamente componentes disponibles en farmacias.

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

582 In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime. See below: Chapter 6.1.13.

583 Regarding the costs, see: The World Information Society Report, 2007, available at: http://www.itu.int/wisr/.

584 See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

585 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: http://www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf.

586 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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

587 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

588 See below: Chapter 6.2.11.

589 Regarding the impact of censorship and control, see: *Burnheim*, "The right to communicate, The Internet in Africa", 1999, available at: http://www.article19.org/pdfs/publications/africa-internet.pdf.

podría violar ciertos derechos humanos[590]. 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[591], 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

La Internet consta de millones de páginas web[592] 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[593], que es una enciclopedia en línea en la cual cualquier persona puede publicar[594].

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[595]. Se han realizado Informes en los cuales se destaca el riesgo de la utilización de motores de búsquedas con fines ilegales[596]. Hay terroristas que pueden encontrar en Internet información detallada sobre la forma de construir una bomba utilizando productos químicos disponibles en los supermercados (Figura 27)[597]. Aunque este tipo de información estaba disponible aun antes de que se desarrollarse la Internet, resultaba mucho mas difícil procurársela. Hoy en día, empero, cualquier usuario de Internet puede accede 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[598]. 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 la

---

590 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: http://www.undp.org/dpa/annualreport2001/arinfocom.pdf; "Background Paper on Freedom of Expression and Internet Regulation", 2001, available at: http://www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

591 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.

592 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: http://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.

593 http://www.wikipedia.org.

594 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: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

595 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.

596 See Nogguchi, "Search engines lift cover of privacy", The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

597 One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

598 See *Thomas*, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", Parameters 2003, page 112 et seqq., available at: http://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: http://www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

Internet para recoger información sobre posibles objetivos[599]. 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[600].

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 la 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[601], por lo cual la 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[602], 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 la Internet resistiera contra las fuerzas de control externo. Ahora bien, la 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.

La 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[603].

Un ejemplo de los problemas que plantea la ausencia de instrumentos de control es que los usuarios pueden soslayar los dispositivos de filtro[604] recurriendo a servicios de comunicación anónima encriptada[605].Si los

---

599 "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy". The reports about the sources of the quotation varies: 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: http://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: http://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.

600 See Telegraph.co.uk, news from January the 13th 2007.

601 See for example, *Sadowsky/Zambrano/Dandjinou*, "Internet Governance: A Discussion Document", 2004, available at: http://www.internetpolicy.net/governance/20040315paper.pdf.

602 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: http://www.isoc.org/internet/history/brief.shtml.

603 *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

604 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: http://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: http://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: http://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: http://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.

605 For more information regarding anonymous communications, see below: Chapter 3.2.l2.

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 (Figura 28).

3.2.6 Dimensiones internacionales

Muchos procesos de transferencia de datos afectan a más de un país[606]. 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[607]. 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[608]. Además, muchos servicios de Internet se basan en servicios prestados desde el exterior y, así por ejemplo, los proveedores huéspedes pueden arrendar espacio web[609] en un país aprovechando equipo situado en otro[610].

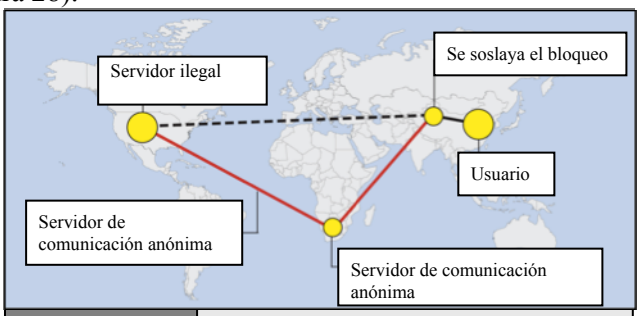


Figura 28

En esta figura puede verse que es posible soslayar los mecanismos de control central instalados por los proveedores de acceso. Si los proveedores de acceso instalan una determinada tecnología de filtro, las peticiones del usuario quedarán bloqueadas. Con todo, este método de control puede soslayarse, si el usuario recurre a servidores de comunicación anónima que encripten sus peticiones. Así por ejemplo, en este caso los proveedores de acceso no pueden acceder a las peticiones enviadas al servidor de comunicación anónima, por lo cual resulta imposible bloquear los correspondientes sitios web.

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[611]. 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[612], 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

606 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.

607 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".

608 See *Kahn/Lukasik*, "Fighting Cyber Crime and Terrorism: The Role of Technology," presentation at the Stanford Conference, December 1999, page 6 et seqq.; *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.

609 One example of the international cooperation of companies and the 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 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)*.

610 See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://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 Simplyfing Data Storage and Management.

611 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 seqq., 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 seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf.

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

las entidades extranjeras encargadas de hacer cumplir la ley suelen obstaculizar las investigaciones[613], que las más de las veces se realizan en periodos muy breves[614]. 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[615]. El principio de doble criminalidad[616] también plantea dificultades, cuando el acto considerado no se tipifica como delito en uno de los países que participan en la investigación[617]. Además, es posible que los delincuentes incluyan deliberadamente a terceros países en sus ataques para obstaculizar las investigaciones[618].

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 (Figura 29)[619]. 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[620] y las disposiciones de cooperación internacional especificadas en el Convenio sobre la Ciberdelincuencia del Consejo de Europa[621].

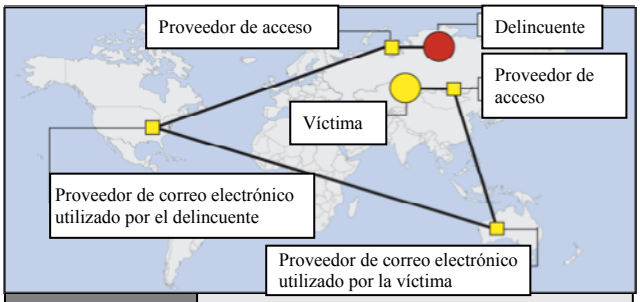


Figura 29

En esta figura puede verse que, incluso en el caso en que los delincuentes y sus objetivos estén situados en el mismo país, el acto de enviar un correo electrónico con contenido ilegal puede realizarse a través de varios países y a partir de los mismos. Incluso cuando éste no es el caso, los procesos de transferencia de datos pueden dirigirse a otro país y ulteriormente una vez más al país interesado.

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 (Figura 30)[622].

---

613 See *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.

614 See below: Chapter 3.2.10.

615 See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142.

616 Dual criminality exists if the offence is a crime under both the requestor 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).

617 Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://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.

618 See: *Lewis*, "Computer Espionage, Titan Rain and China", page 1, available at: http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

619 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: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

620 See below: Chapter 6.3.8.

621 See below: Chapter 6.3.

622 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.

Oponerse a los "refugios seguros" es uno de los desafíos esenciales a la hora de combatir el ciberdelito[623], 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[624], que infectó millones de computadores en todo el mundo[625]. 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[626]. 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;
- 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[627]. 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[628], si se recurre a la automatización[629] (véase la

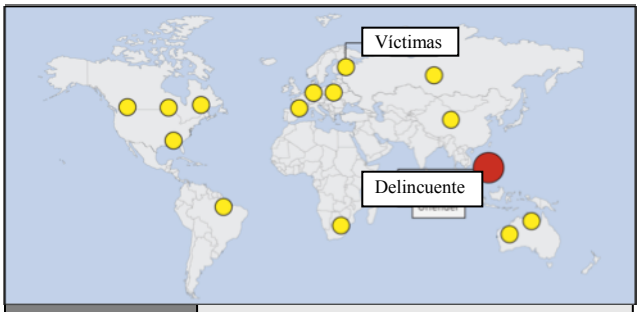


Figura 30

Los delincuentes pueden acceder a la Internet para cometer delitos prácticamente a partir de cualquier país. Entre los diferentes aspectos que los delincuentes toman en consideración a la hora de decidir dónde desean basarse cabe citar los siguientes: la severidad de la legislación sobre el ciberdelito, la eficacia de las entidades encargadas de hacer cumplir la ley y la disponibilidad de acceso anónimo a Internet.

623 This issue was addressed by a number of international organisations. The 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: http://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: Chapter 5.2.

624 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: http://www.gao.gov/archive/2000/ai00181t.pdf.

625 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.

626 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", http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

627 One example of low- cost services that are automated is e-mail. The automation of registration allows providers offer e-mail addresses free of charge. For more information on the difficulties of prosecuting Cybercrime involving e-mail addresses, see below: Chapter 3.2.l.

628 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: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

629 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: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.

Figura 31). Actualmente los piratas suelen llevar a cabo sus ataques de forma automatizada[630] (hasta 80 millones de ataques diarios)[631], recurriendo a programas informáticos[632] que pueden atacar miles de sistemas informáticos en unas cuantas horas[633]. 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[634]. 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[635]. 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.

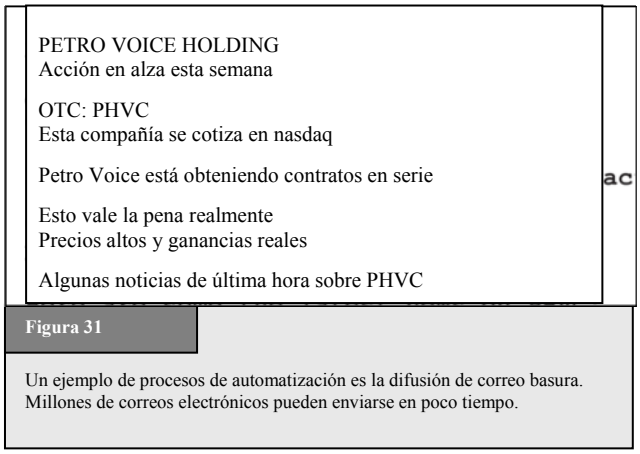


Figura 31

Un ejemplo de procesos de automatización es la difusión de correo basura. Millones de correos electrónicos pueden enviarse en poco tiempo.

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[636] 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[637]. El análisis de estos ataques cometidos por miles de computadores dependientes de una red robot[638] o grupo de computadores comprometidos que ejecutan programas bajo el control de una fuente exterior[639]. 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 (véase la Figura 32). La red de robot se utiliza para tener información acerca de objetivos y para realizar ataques de alto nivel[640].

---

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

631 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: http://www.hackerwatch.org.

632 Regarding the distribution of hacking tools, see: CC Cert, "Overview of Attack Trends", 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.

633 See CC Cert, "Overview of Attack Trends", 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.

634 Nearly 50% of all fraud complains reported to the United States Federal Trade Commission are related to a amount paid between 0 and 25 USD. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission , available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

635 See "Spam Issue in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

636 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

637 Regarding the attacks, see: Lewis, "Cyber Attacks Explained", 2007, available at: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; "A cyber-riot", The Economist, 10.05.2007, available at: http://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: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

638 See: *Toth*, "Estonia under cyber attack", http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

639 See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, page 3, available at: http://www.cert.org/archive/pdf/Botnets.pdf.

640 See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, available at: http://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".

En los últimos años las redes robot se han convertido en una gran amenaza para la ciberseguridad[641].

El tamaño de las redes robot es variable, ya que va de unos cuantos computadores a más de un millón de máquinas[642]. 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[643]. La red robot puede utilizarse para realizar actividades delictivas de diverso tipo; entre otras:

- ataques que conllevan la denegación del servicio[644];
- envío de correo basura[645];
- ataques de piratas;
- redes que comparten ficheros.

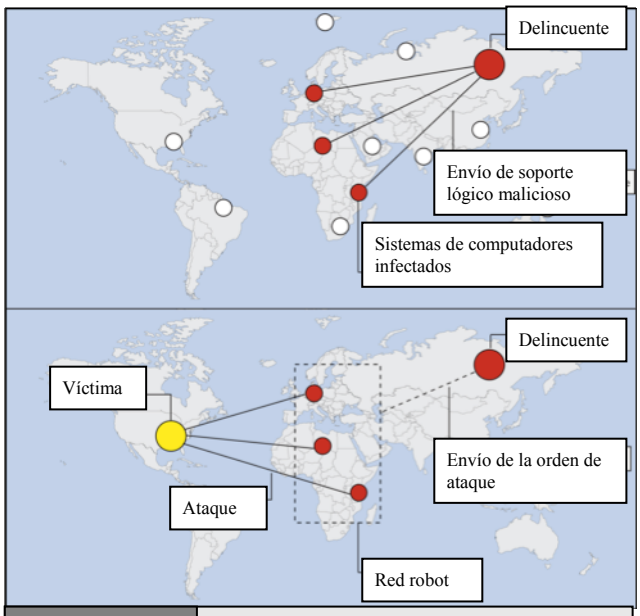


Figura 32

En los dos gráficos se representa la creación y el uso de una red robot.

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[646]. En segundo lugar, las redes 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 la 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 ley para investigar o recoger pruebas (el proceso tradicional de investigación es mucho más largo)[647].

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.

---

641 See "Emerging Cybersecurity Issues Threaten Federal Information Systems", GAO, 2005, available at: http://www.gao.gov/new.items/d05231.pdf.

642 *Keizer*, Duch "Botnet Suspects Ran 1.5 Million Machines", TechWeb, 21.10.2005, available at http://www.techweb.com/wire/172303160.

643 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.

644 E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, "Estonia under cyber attack", http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

645 "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: http://www.ic3.gov/media/initiatives/BotRoast.pdf.

646 *Staniford/Paxson/Weaver*, "How to Own the Internet in Your Space Time", 2002, available at: http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

647 *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International, 2006, page 142.

Los correos electrónicos demuestran la importancia de contar con herramientas de respuesta inmediata que puedan ser usadas sin tardanza (véase la Figura 33). Para localizar e identificar a sospechosos, los investigadores suelen necesitar datos que pueden borrarse poco después de ser transferidos[648]. 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[649].

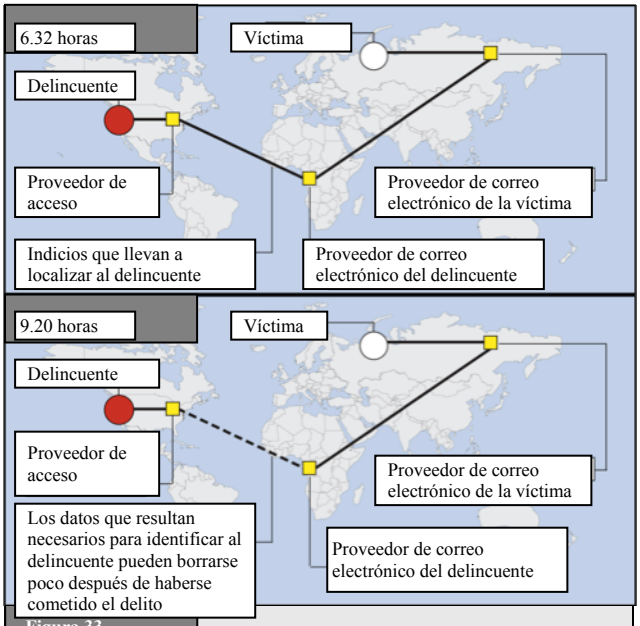


Figura 33

En este cuadro se indica la importancia de la respuesta inmediata en las investigaciones sobre el ciberdelito. Algunos datos importantes generados durante el envío de un correo electrónico y que permitirían identificar al delincuente suelen borrarse poco después del envío del correo electrónico. La identificación del delincuente resulta prácticamente imposible si no se dispone de dicha información.

Los procedimientos de "rápida congelación"[650] y los puntos de redes 24/7[651] 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

La Internet se ha desarrollado constantemente y la creación de la interfaz de usuario gráfica (WWW[652]) 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[653], 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;
- 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[654].

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.

---

648 *Gercke*, DUD 2003, 477 et seq.; *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

649 Regarding the necessary instruments, see below: Chapter 6.2. One solution that is currently being discussed is data retention. Re 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.

650 The term "quick freeze" is used to describe the immediate preservation of data on request of law enforcement agencies. For more information, see below : Chapter 6.2.4.

651 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: Chapter 6.3.8.

652 The graphical user interface called World Wide Web (WWW) was created in 1989.

653 The development of the graphical user interface supported content-related offences in particular. For more information, see above : Chapter 2.5.

654 For more information see above: Chapter 2.5.5.

Si se aplicase el mismo principio a las comunicaciones VoIP, las entidades encargadas de hacer cumplir la ley actuarían por conducto de los ISP 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[655]. En consecuencia, se requieren nuevas técnicas[656].

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 la Internet a través de redes inalámbricas[657]. 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[658]. 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.

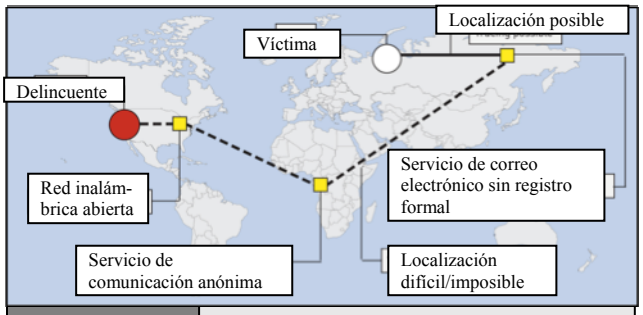


Figura 34

En esta Figura puede verse la forma en que los delincuentes pueden actuar anónimamente combinando diferentes métodos. La utilización de las redes inalámbricas abiertas hace que sea prácticamente imposible identificar a los delincuentes. Por otra parte, recurriendo a servicios de comunicación anónima y de correo electrónico en los que no se verifica la información de registro, los delincuentes pueden reducir la posibilidad de ser identificados.

3.2.12 Comunicaciones anónimas

Ciertos servicios Internet complican la tarea de identificar sospechosos[659]. Las comunicaciones anónimas pueden ser únicamente un producto de un servicio u ofrecerse con la intención de evitar desventajas para el usuario. Entre estos servicios (que pueden combinarse incluso) (véanse las Figuras 34 y 35), cabe citar los siguientes:

- terminales públicos de Internet (por ejemplo, terminales en el aeropuerto, o cibercafés)[660];
- redes inalámbricas[661];
- servicios móviles de prepago que no requieren registro;

---

655 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 http://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.

656 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.

657 Regarding the implication of the use of cell phones as storage media on 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.

658 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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

659 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: http://www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

660 Re 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: Chapter 6.2.14.

661 Regarding the difficulties that are caused if offenders use open wireless networks, see above: Chapter 3.2.3.

- capacidades de almacenamiento de páginas ofrecidas sin registro;
- servidores de comunicación anónimas[662];
- repetidores de correo anónimo[663].

Los delincuentes pueden encubrir sus identidades recurriendo, entre otras cosas, a direcciones falsas de correo electrónico[664]. 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[665].

Figura 35

En esta Figura se indica de qué forma la información puede ocultarse en una fotografía. El soporte lógico de encriptado incorpora información, alterando la referente al color de ciertos píxeles. Si la fotografía es suficientemente grande, resulta difícil identificar los cambios sin tener acceso al original y a la fotografía modificada. Sirviéndose de esta tecnología, los delincuentes pueden ocultar el hecho de que se encuentran intercambiando información adicional.

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[666]. 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[667]. 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[668]. No obstante, algunos países abordan los desafíos suscitados por las comunicaciones anónimas, aplicando restricciones jurídicas[669];

---

662 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

663 See: *Claessens/Preneel/Vandewalle*, "Solutions for Anonymous Communication on the Internet", 1999.

664 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.

665 *Donath*, "Sociable Media", 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

666 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.

667 (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).

668 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.

669 See below: Chapter 6.2.11.

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[670].

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 la Internet debería desempeñar un cometido de mayor alcance en las estrategias de ciberseguridad[671].

3.2.13 Tecnología de encriptado

Otro factor que puede complicar la investigación del ciberdelito es la tecnología de encriptado[672], 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[673]. Al igual que el anonimato, la encriptación no es un concepto novedoso[674], pero la tecnología informática ha transformado la situación. En efecto, actualmente es posible encriptar datos informáticos sin necesidad de cliquear un ratón, por lo que a las entidades encargadas de hacer cumplir la ley[675] les resulta difícil descifrar encriptados y acceder a datos. No es claro en qué medida los delincuentes utilizan ya tecnología de encriptación para encubrir sus actividades: así por ejemplo, se ha informado de que hay terroristas que utilizan tecnología de encriptación[676]. Aunque una encuesta realizada sobre pornografía infantil apuntaba al hecho de que sólo el 6 por ciento de los poseedores de pornografía infantil arrestados se servían de tecnología de encriptación[677], algunos expertos han subrayado la amenaza que supone un mayor uso de la tecnología de encriptación en los casos de ciberdelito[678].

---

670 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: http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

671 Regarding the technical discussion about traceability and anonymity, see: "CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

672 Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/ Publications/Computer_Forensics_Past_Present_Future.pdf.

673 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: http://www.cert.org/archive/pdf/ecrimesurvey06.pdf.

674 *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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

675 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

676 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: http://www.terrorismcentral.com/Library/Teasers/Flamm.html.

677 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

678 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: http://www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

Hoy en día se dispone de herramientas para descifrar encriptados[679] y existen varios productos informáticos a los que puede recurrirse para proteger ficheros contra accesos no autorizados[680]. Resulta posible descifrar encriptados, aunque ésta sea una tarea difícil y lenta. Así, los investigadores que tienen acceso al programa informático utilizado para encriptar ficheros, pueden descifrarlos[681]. Por otra parte, están también en condiciones de descifrar ficheros recurriendo a un ataque masivo[682].

Dependiendo de la técnica de encriptación y la magnitud de la llave utilizadas, podría tomar décadas descifrar un encriptado[683]. 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[684]. 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[685]. 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[686]. 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[687], 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[688] que pueden enviarse utilizando

679 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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

680 Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see http://www.truecrypt.org).

681 See "Data Encryption, Parliament Office for Science and Technology No. 270", UK, 2006, page 3, available at: http://www.parliament.uk/documents/upload/postpn270.pdf.

682 Brute force attack is one method of defeating a cryptographic scheme by trying a large number of possible codes.

683 *Schneier*, "Applied Cryptography", Page 185; *Bellare/Rogaway*, "Introduction to Modern Cryptography", 2005, page 36, available at: http://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

684 1099512 seconds.

685 Equivalent to 10790283070806000000 years.

686 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.

687 See *Leyden*, "Vista encryption 'no threat' to computer forensics", The Register, 02.02.2007, available at: http://www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

688 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, "Skype Security Evaluation", 2005, available at: http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

VoIP[689]. Recurriendo a la tecnología de encriptación VoIP, los delincuentes podrían proteger conversaciones vocales contra su intercepción[690].

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[691]. Resulta difícil que las autoridades de investigación puedan distinguir el intercambio inocuo de fotografías de vacaciones del intercambio de fotografía con mensajes encriptados ocultos[692].

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[693]; 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[694]. 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[695], la autoprotección es un importante elemento de la ciberseguridad.

3.2.14 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.

---

689 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: http://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.

690 *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.

691 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: http://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

692 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: https://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.

693 See below: Chapter 6.2.9.

694 See below: Chapter 6.2.9.

695 See above: Chapter 3.2.8.

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[696]. 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[697]. 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[698]. Por regla general, el proceso de ajuste consta de tres etapas:

Los ajustes a las leyes nacionales 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)[699], 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.

La segunda etapa consiste en identificar las 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.

La tercera etapa es la 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[700]. 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

---

696 See BBC News, "Hacking: A history", 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

697 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."

698 Within this process the case law based Anglo-American Law System shows advantage with regard to the reaction time.

699 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 percent of internet systems to a halt in November 1988. For more information on the history of the CERT CC see: http://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.

700 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and the UN Resolution 55/63.

legislaciones nacionales. En consecuencia, cada vez adquieren más importancia los intentos internacionales para armonizar las diferentes leyes penales nacionales[701]. 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[702]. 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[703]. 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")[704]. Se están descubriendo constantemente nuevas actividades delictivas; en los juegos en línea pueden "robarse" divisas virtuales y comercializarse en subastas[705]. Algunas divisas virtuales tienen valor en términos de moneda real (basándose en el tipo de cambio), dando al delito una dimensión "real"[706]. 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[707]. Las autoridades competentes necesitan disponer de instrumentos adecuados para investigar los posibles actos delictivos. Algunos instrumentos (tales como la retención de datos)[708] podrían interferir con los derechos de los usuarios de Internet inocentes[709]. 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

---

701 See below: Chapter 5.

702 See above: Chapter 2.7.1.

703 Regarding the offences recognised in relation to online games see above: Chapter 2.5.5.

704 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/.

705 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 et seqq.

706 *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/.

707 Re 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.

708 Data retention describes the collection of certain data (such as traffic data) through obliged institutions e.g., Access Providers. For more details, see below: Chapter 6.2.5.

709 Related 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.

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[710] comparados con los que supone el almacenamiento de documentos físicos, el número de documentos digitales es cada vez mayor[711]. 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[712]. Como consecuencia de estos desarrollos, la evidencia digital se introdujo como una nueva fuente de evidencia [713]. 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[714]. El manejo de la evidencia digital viene acompañado por retos peculiares y requiere la aplicación de procedimientos específicos[715]. Uno de los aspectos más difíciles consiste en mantener la integridad de esta evidencia digital[716]. Los datos digitales son extremadamente frágiles y pueden borrarse o modificarse fácilmente[717]. 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[718] y, por consiguiente, requiere la utilización de técnicas de mantenimiento especiales[719]. 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[720].

La evidencia digital desempeña un papel importante en varias fases de las investigaciones del ciberdelito. En general es posible distinguir cuatro fases[721]:

- identificación de la evidencia pertinente[722];
- recopilación y mantenimiento de la evidencia[723];

---

710 *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.

711 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

712 *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.

713 *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.

714 *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: http://www.cybex.es/agis2005/elegir_idioma_pdf.htm.

715 Regarding the difficulties of dealing with digital evidence on the basis of the 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.

716 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

717 *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.

718 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

719 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

720 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

721 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 as well *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 are differentiating between six different phases.

722 This includes the development of investigation strategies.

- análisis de la tecnología informática y la evidencia digital; y,
- presentación de la evidencia 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[724]. El hecho de que el volumen de datos almacenados en formato digital aumenta constantemente pone en evidencia los retos logísticos que suponen tales investigaciones[725]. Los enfoques de los procedimientos forenses automatizados, por ejemplo realizando búsquedas basadas en los valores de troceo para localizar imágenes de pornografía infantil[726] o búsqueda por teclado[727], desempeñan un papel importante además de las investigaciones manuales[728].

Dependiendo del requisito de la investigación específica, los procedimientos forenses informáticos podrían por ejemplo incluir lo siguiente:

- análisis del hardware y el software utilizados por un sospechoso[729];
- apoyo a los investigadores para identificar la evidencia pertinente[730];
- recuperación de ficheros suprimidos[731];
- decodificación de ficheros[732]; e
- identificación de usuarios de Internet analizando los datos de tráfico[733].

4 Estrategias anticiberdelito

El número cada vez mayor de ciberdelitos reconocidos y las herramientas técnicas para automatizar estos tipos de delitos (incluidos los sistemas[734] de compartición de ficheros anónimos y los productos de software

723 The second phase does especially cover 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.

724 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.

725 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol 119, page 532.

726 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

727 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.

728 *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.

729 This does for example include the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

730 This does for example include the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

731 *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.

732 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion 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.

733 Regarding the differnet 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.

diseñados para crear virus informáticos[735]) hace que la lucha contra el ciberdelito se haya convertido en un elemento esencial de las actividades relativas al cumplimiento de la ley en todo el mundo. El ciberdelito constituye un reto para las autoridades competentes tanto de los países desarrollados como en desarrollo. Como las TIC crecen de manera tan rápida, especialmente en los países en desarrollo, es esencial la creación e implementación de una estrategia anticiberdelito eficaz como parte de la estrategia de ciberseguridad nacional.

4.1 Legislación contra el ciberdelito como parte integrante de una estrategia de ciberseguridad

Como se ha indicado anteriormente, la ciberseguridad[736] desempeña un papel importante en el desarrollo en curso de la tecnología de la información así como de los servicios de Internet[737]. Hacer que Internet sea más seguro (y proteger a los usuarios de Internet) se ha convertido en parte integrante del desarrollo de nuevos servicios así como de la política gubernamental[738]. 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[739].

Una estrategia anticiberdelito debe ser un elemento integrante de una estrategia de ciberseguridad. La Agenda sobre Ciberseguridad Global de la UIT[740], 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 de mejorar la confianza y ciberseguridad en la sociedad de la información, se basa en los trabajos, iniciativas y asociaciones existentes con el objetivo de proponer estrategias a escala mundial que aborden estos retos conexos. Todas las medidas requeridas e 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 los cinco pilares[741].

---

734 *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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Design", 2005. See also above: Chapter 3.2.l.

735 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: http://www.212cafe.com/download/e-book/A.pdf. For more information, see above: Chapter 3.2.h.

736 The term "Cybersecurity" is used to summarise various activities such as 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 cyber environment 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 cyber environment. 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. Regarding the definition of cybersecurity, 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 cyber environment 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 cyber environment. 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: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

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

738 See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://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: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

739 For more information see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

740 For more information see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

741 See below: Chapter 4.4.

4.2 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 la ventaja de una disminución en los costes y en el tiempo para su desarrollo. La implementación de estrategias existentes podría permitir a los países en desarrollo beneficiarse de los actuales conocimientos y experiencia.

No obstante, la implementación de una estrategia anticiberdelito ya existente plantea un cierto número de dificultades. Aunque tanto los países en desarrollo como los países desarrollados se enfrentan a retos similares, las soluciones óptimas que pueden 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 costosos.

Existen otros temas que deben tener en cuenta los países en desarrollo que adopten estrategias anticiberdelito existentes:

- compatibilidad de los respectivos sistemas jurídicos;
- situación de las iniciativas de apoyo (por ejemplo, educación de la sociedad);
- ampliación de las medidas de autoprotección *in situ*; y
- ampliación del soporte por parte del sector privado (por ejemplo, mediante asociaciones públicas/privadas), entre otros temas.

4.3 Diferencias regionales

Teniendo en cuenta el carácter internacional del ciberdelito, la armonización de las leyes nacionales y de las técnicas es vital en la lucha contra el mismo. Sin embargo, esta armonización debe tener en cuenta la demanda y capacidad regionales. La importancia de los aspectos regionales en la implementación de estrategias anticiberdelito viene destacada por el hecho de que muchas normas jurídicas y técnicas fueron acordadas entre países industrializados y no incluyen varios aspectos importantes relativos a los países en desarrollo[742]. Por lo tanto, es necesario incluir en alguna parte los factores y diferencias regionales en su implementación.

4.4 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 de una manera compatible internacionalmente los retos jurídicos planteados por las actividades delictivas cometidas sobre las redes TIC.

4.4.1 Medidas legales

En los cinco pilares, las medidas legales son probablemente las más importantes con respecto a una estrategia anticiberdelito. Ello requiere en primer lugar la elaboración de las leyes penales sustantivas necesarias para criminalizar actos tales como fraude informático, acceso ilegal, interferencia en los datos, violaciones del derecho de propiedad intelectual y pornografía infantil[743]. El hecho de que existan disposiciones en el Código Penal que son aplicables a actos similares cometidos fuera de la red no significa que puedan aplicarse también a los actos cometidos a través de Internet[744]. Por consiguiente, es muy importante realizar un análisis profundo de

742 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States of America, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arabic regions.

743 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

744 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 et. Seqq.

la actual legislación nacional a fin de identificar posibles lagunas jurídicas[745]. Además de las disposiciones jurídicas penales sustantivas[746], las autoridades competentes necesitan las herramientas e instrumentos jurídicos pertinentes para investigar el ciberdelito[747]. Estas investigaciones se enfrentan a un cierto número de retos[748]. Los delincuentes pueden actuar desde cualquier lugar del mundo y tomar las medidas necesarias para enmascarar su identidad[749]. Las herramientas e instrumentos jurídicos necesarios para investigar el ciberdelito pueden ser muy distintos de los que se utilizan en la investigación de los delitos ordinarios[750]. Debido a la dimensión internacional[751] de los ciberdelitos es preciso, además, desarrollar un marco jurídico nacional capaz de cooperar con las autoridades competentes exteriores[752].

4.4.2 Medidas técnicas y de procedimiento

Las investigaciones relativas al ciberdelito a menudo tienen una fuerte componente técnica[753]. 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[754] a ITAN[755]) 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

---

745 For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at: http://www.coe.int/cybercrime/. 745 See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005 -, page 5, available at: http://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: https://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: http://www.mosstingrett.no/info/legal.html.

746 See below: Chapter 6.1.

747 See below: Chapter 6.1.

748 For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.1.

749 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 seqq., available at: http://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: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing", 2005.

750 Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.10 and Chapter 6.2.11.

751 See above: Chapter: 3.2.6.

752 See in this context below: Chapter 6.3.

753 *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: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://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.

754 Transaction Authentication Number – for more information, see: "Authentication in an Internet Banking Environment", United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

755 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 relavant 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.

técnicas[756]. 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
- suministradores de servicio 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 para proteger a 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 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 servicio Internet y los vendedores de producto (por ejemplo, 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)[757].

4.4.3 Estructuras institucionales

Una lucha eficaz contra el ciberdelito exige unas estructuras institucionales altamente desarrolladas. Sin contar con las adecuadas estructuras que eviten la duplicación de medidas y se basen en unas competencias claramente establecidas difícilmente será posible llevar a cabo las complejas investigaciones que exige la asistencia de distintos expertos jurídicos y técnicos.

4.4.4 Creación de capacidad y educación del usuario

El ciberdelito es un fenómeno global. Para poder investigar eficazmente estos delitos es necesario establecer una armonización de las leyes y desarrollar los métodos 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 la creación de capacidad[758].

Además de la creación de capacidad se requiere la educación del usuario[759]. Algunos ciberdelitos, especialmente los relativos al fraude tales como usurpación de identidad ("*phishing*") y falsificación de direcciones de origen o piratería ("*spoofing*"), no se producen generalmente debido a la ausencia de protección

---

756 Re the various approaches of authentication in Internet banking, see: "Authentication in an Internet Banking Environment", United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

757 Regarding the 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: http://www.coe.int/cybercrime/.

758 Capcity Buidling 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, adding that, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations and water user groups, professional associations, academics and others.

759 At the G8 Conference in Paris in 2000, *Jean-Pieree 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: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf. Re sceptical views regarding user education, see: *Görling*, "The Myth Of User Education", 2006, available at: http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

técnica sino a causa de una falta de atención por parte de las víctimas[760]. Existen varios productos de software que pueden identificar automáticamente direcciones web fraudulentas[761], pero hasta ahora estos productos no pueden identificar todas las direcciones web sospechosas. Una estrategia de protección del usuario basada únicamente en productos de software presenta una capacidad limitada para proteger a los usuarios[762]. 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 educación del usuario[763]. Por ejemplo, si los usuarios son conscientes de que sus instituciones financieras nunca se pondrán en contacto con ellos mediante correo electrónico solicitándoles sus claves o los detalles de sus cuentas bancarias, no pueden ser víctimas de la usurpación de identidad o de ataques fraudulentos. La educación de los usuarios de Internet reduce el número de objetivos potenciales. Los usuarios pueden educarse mediante:

- campañas públicas;
- lecciones en los colegios, bibliotecas, centros de TI y universidades;
- asociaciones privadas-públicas (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 están 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 y que informen sobre los ciberdelitos[764]. Con objeto de determinar los niveles de amenaza, así como de informar a los usuarios, es fundamental mejorar la recopilación y publicación de la información pertinente[765].

4.4.5 Cooperación internacional

En un gran número de casos los procesos de transferencia de datos en Internet afectan a más de un país[766]. Ello es el resultado del diseño de la red así como del hecho de que pueden crearse protocolos que garantizan el éxito de las transmisiones, aun cuando las líneas directas se encuentren temporalmente bloqueadas[767]. Además, un

---

760 "Anti-Phishing Best Practices for ISPs and Mailbox Providers", 2006, page 6, available at: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; Milletary, "Technical Trends in Phishing Attacks", available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf.

761 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: http://www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

762 For a different opinion, see: *Görling*, "The Myth Of User Education", 2006, at:http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

763 At the G8 Conference in Paris in 2000, *Jean-Pieree 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."

764 "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: http://www.heise-security.co.uk/news/80152.

765 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: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

766 Regarding the extend of transnational attacks in the the most damaging cyber attacks 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.

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

gran número de servicios de Internet (por ejemplo los servicios anfitriones) son ofrecidos por empresas basadas en el extranjero[768].

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 que resulten afectados[769]. 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 el expreso permiso de las autoridades locales[770]. Por lo tanto, las investigaciones deben realizarse con el apoyo de las autoridades de todos los países implicados. Con relación al hecho de que en la mayoría de los casos sólo se dispone de un breve intervalo de tiempo en el que puede llevarse a cabo con éxito las investigaciones, la aplicación del clásico régimen de asistencia jurídica mutua presenta evidentes dificultades cuando se trata de investigaciones de ciberdelitos. Ello se debe al hecho de que normalmente la asistencia jurídica mutua exige procedimientos muy largos. En consecuencia, reviste una gran importancia la mejora de los mecanismos de cooperación internacional y es fundamental en el desarrollo y aplicación de las adecuadas estrategias de seguridad y estrategias anticiberdelito.

5 Panorama de los enfoques legislativos internacionales

En el presente Capítulo se traza un panorama de los enfoques legislativos internacionales[771] 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 G8[772]

En 1997 el Grupo de los Ocho (G8) estableció un Subcomité[773] sobre delitos de alta tecnología, cuyo objetivo era luchar contra el ciberdelito[774]. 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

---

768 See Huebner/Bem/Bem, Computer Forensics – Past, Present And Future, No.6, available at: http://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.

769 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 seqq. , 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 seqq. , available at: http://media.hoover.org/documents/0817999825_1.pdf.

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

771 This includes regional approaches.

772 The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, Great Britain, United States and the Russian Federation. The Presidency of the group that represents more than 60% of the world economy (Source: http://undp.org) rotates every year.

773 The idea of the creation of five Subgroups – among them, one on High-Tech Crimes – was to improve the implementation of the Forty Recommendations adopted by G8 Heads of State in 1996.

774 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 organised crime, that started with the launch of the Senior Experts Group on Organised Crimes (the "Lyon Group") in 1995. At the Halifax summit in 199,5 the G8 expressed: "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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

para combatir el delito de alta tecnología[775]. 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[776]. 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[777].

---

775 Regarding the G8 activities in the fight against Cybercrime see as well: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

776 "Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October, 1999.

777 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.

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[778].

En la Conferencia del G8 organizada en París, Francia, en 2008, 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 sobre la Ciberdelincuencia del Consejo de Europa[779]. El G8 debatió sobre una serie de instrumentos de procedimiento para luchar contra el ciberdelito en un taller celebrado en Tokio en 2001[780], 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[781].

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[782]. Una vez más el G8 tomó nota del Convenio sobre la Ciberdelincuencia del Consejo de Europa[783].

---

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.

778 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. […]

779 *Jean-Pieree Chevenement*, the French Minister of 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."

780 G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

781 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.

782 G8 Justice and Home Affairs Communiqué, Washington DC, May 11, 2004.

783 G8 Justice and Home Affairs Communiqué Washington DC, May 11, 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."

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[784]. 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[785] la cuestión que representaba el ciberterrorismo[786].

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 terroristas, y los Ministros convinieron en tipificar como delito la utilización abusiva de Internet por grupos terroristas[787]. Hay que agregar que este acuerdo no incluía ciertos actos específicos que los Estados deberían tipificar penalmente.

5.1.2 Naciones Unidas[788]

En el 8º Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente (celebrado en La Habana, Cuba, del 27 de agosto al 7 de septiembre de 1990), la Asamblea General de Naciones Unidas adoptó una Resolución que tenía por objeto la legislación contra el ciberdelito[789]. Basándose en esta Resolución (Resolución 45/121 (1990)), las Naciones Unidas publicaron en 1994 un Manual sobre la prevención y el control de delitos informáticos[790].

En 2000 la Asamblea General aprobó una Resolución sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, que presenta cierta semejanza con el Plan de Acción de Diez Puntos adoptado por el G8 en 1997[791]. En esta Resolución la Asamblea General especifica una serie de medidas destinadas a combatir la utilización debida a la tecnología de la información, por ejemplo:

> *Los Estados deben velar por que en su legislación y práctica se eliminan 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.*

---

784 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: http://www.g7.utoronto.ca/justice/justice2006.htm.

785 Regarding the topic Cyberterrorism see above: Chapter 2.8.1; In addition see See: *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; Lewis, "Cyber-terrorism and Cybersecurity"; http://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 seqq., available at: http://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 seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://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 seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/ lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

786 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.

787 For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

788 The United Nations (UN) is an international organisation founded in 1945 that had 191 Member States in 2007.

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

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

791 A/RES/55/63. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

En 2002 la Asamblea General aprobó otra Resolución sobre la lucha contra la utilización de la tecnología de la información con fines delictivos[792] en la que se señalan los métodos existentes en el plano internacional para combatir el ciberdelito y se destacan varias 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 la Ciberdelincuencia, 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. Tomando nota del valor de las medidas enunciadas en su Resolución 55/63, invita nuevamente a los Estados Miembros a que las tengan en cuenta en su lucha contra la utilización de la tecnología en 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.*

En 2004, las Naciones Unidas crearon un Grupo de Trabajo para ocuparse del correo basura, el ciberdelito y otros aspectos relacionados con la Internet, lo que reflejaba el interés que tenían las Naciones Unidas en participar en el debate internacional en curso sobre las amenazas planteadas por el ciberdelito[793].

En el 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, organizado en Bangkok, Tailandia, en 2005, se aprobó una Declaración en la que se destacaba la necesidad de armonizar el combate contra el ciberdelito[794]. En la Declaración se señalaba lo siguiente:

> *Reafirmamos la importancia fundamental que reviste la traducción a la práctica de los instrumentos vigentes y la preparación de medidas nacionales y el desarrollo de la cooperación internacional en el ámbito penal, de modo tal que se tome en consideración el fortalecimiento y la ampliación de medidas, en particular, contra el ciberdelito, el blanqueo de dinero y el tráfico indebido de bienes culturales, así como en relación con la extradición, la existencia jurídica mutua y la confiscación, recuperación y devolución de ingresos delictivos.*
>
> *Observamos que, en el actual periodo de mundialización, la tecnología de la información y el rápido desarrollo de nuevos sistemas de telecomunicaciones y redes de computadores ha venido acompañado por la utilización indebida de tecnologías con propósitos delictivos. En consecuencia, vemos con buenos ojos los esfuerzos emprendidos para fomentar y complementar la cooperación existente para prevenir, investigar y castigar los delitos de alta tecnología y cometidos con ayuda de computadores, lo que incluye la creación de asociaciones con el sector privado. Reconocemos la importante contribución de las Naciones Unidas a foros regionales e internacionales en la lucha contra el ciberdelito e invitamos a la Comisión sobre Prevención del Delito y Justicia Penal, a que, tomando en cuenta dicha experiencia, examine la posibilidad de proporcionar mayor asistencia en este campo bajo la égida de las Naciones Unidas y en colaboración con otras organizaciones que persiguen los mismos objetivos.*

Asimismo, en el sistema de las Naciones Unidas se han aprobado Decisiones, Resoluciones y Recomendaciones sobre temas relacionados con el ciberdelito y entre las cuales, cabe citar por su importancia, las siguientes:

- La Comisión de Prevención del Delito y Justicia Penal (Oficina de las Naciones Unidas[795] contra la Droga y el Delito) adoptó una Resolución sobre respuestas eficaces en el plano de la prevención del delito y de la justicia penal en el marco de la lucha contra la explotación sexual de los niños[796].

---

792 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.

793 Regarding the Creation of the Working Group, see the UN press release, 21st of September 2004, available at: http://www.un.org/apps/news/story.asp?NewsID=11991&Cr=internet&Cr1=.

794 "Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice", available at: http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

- En 2004 el Consejo Económico y Social de las Naciones Unidas[797] adoptó una Resolución sobre cooperación internacional para prevenir, investigar, enjuiciar y castigar el fraude, la utilización delictiva y la falsificación de identidad y delitos afines[798]. En 2007 el Consejo adoptó una Resolución sobre cooperación internacional para impedir, investigar, enjuiciar y castigar el fraude económico y los delitos de usurpación de identidad conexos[799]. Aunque ambas resoluciones no abordan explícitamente los problemas planteados por los delitos relacionados por la Internet[800], resultan aplicables también a dichos delitos.

  En 2004 el Consejo adoptó una Resolución sobre la venta de drogas ilícitas a través de Internet en la que se contemplaba expresamente el fenómeno relacionado con un delito cibernético[801].

5.1.3 Unión Internacional de Telecomunicaciones[802]

Como organismo especializado del sistema de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT) desempeña un cometido rector en lo que concierne a la normalización y el desarrollo de las telecomunicaciones, así como a los diferentes aspectos de la ciberseguridad. Entre otras actividades, la UIT hizo las veces de organismo rector de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) que se organizó en dos fases, la primera en Ginebra, Suiza (2003) y la segunda en Túnez, Túnez (2005). En la Cumbre gobiernos, formuladores de políticas y expertos de todo el mundo intercambiaron ideas y experiencias acerca de la forma más adecuada de abordar las cuestiones que empezaba a plantear el desarrollo de una sociedad de la información mundial, lo que incluía la definición de normas y leyes compatibles.
Los resultados de la Cumbre se consignan 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.

En el Plan de Acción de Ginebra se destaca la importancia de las medidas adoptadas para combatir el ciberdelito[803]:

> ***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*

---

795 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

796 CCPCJ Resolution 16/2 on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process within the development of the resolution and for an overview about 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: http://www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative to the resolution see: http://www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

797 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: http://www.un.org/ecosoc/.

798 ECOSOC Resolution 2004/26 International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

799 ECOSOC Resolution 2007/20 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: http://www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

800 Regarding Internet-related ID-Theft, see above: Chapter 2.7.3 and below: Chapter 6.1.15.

801 ECOSOC Resolution 2004/42 on sale of internationally controlled licit drugs to individuals via the Internet, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

802 The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates. For more information see http://www.itu.int.

803 WSIS Geneva Plan of Action, 2003, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

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 delito cibernético se discutió, igualmente, en la segunda fase de la CMSI, organizada en Túnez en 2005. En la Agenda de Túnez para la Sociedad de la Información[804] se hacía hincapié en la necesidad de promover la cooperación internacional para combatir el ciberdelito y se señalan los instrumentos legislativos existentes tales como las Resoluciones de la Asamblea General de las Naciones Unidas y el Convenio sobre Delito Cibernético del Consejo de Europa:

> ***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.*

Como resultado de la CMSI, la UIT fue designada como el único facilitador de la Línea de Acción C5 consagrada a la creación de confianza y seguridad en cuanto a la utilización de la tecnología de la información y la comunicación[805]. En la segunda reunión de facilitación relativa a la Línea de Acción C5 de la CMSI, convocada en 2007, el Secretario General de la UIT, destacó la importancia de la cooperación internacional en lo que respecta a la lucha contra el ciberdelito y anunció el lanzamiento de la Agenda sobre Ciberseguridad Global de la UIT[806]. La Agenda contiene siete objetivos clave[807], basados, a su vez, en cinco pilares estratégicos[808], entre otros, la elaboración de estrategias para la formulación de legislación modelo contra el ciberdelito. Los objetivos precitados 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.*

---

804 WSIS Tunis Agenda for the Information Society, 2005, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

805 For more information on C5 Action Line see http://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: http://www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the Meetign Report of the Third Facilitation Meeting for WSIS Action Line C5, 2008, available at: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008 pdf.

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

807 http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

808 The five pillars are: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, International Cooperation. For more information, see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

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.

Se creó un Grupo de Expertos para definir estrategias relacionadas por la Agenda sobre Ciberseguridad Global[809].

5.1.4 Consejo de Europa[810]

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[811]. En 1985, el Consejo de Europa designó a un Comité de Expertos[812] para analizar los aspectos jurídicos de los delitos cibernéticos[813]. En 1989, el Comité Europeo para Asuntos Delictivos adoptó el "Informe de Expertos sobre el delito cibernético"[814], 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[815], en 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[816]. Las directrices para preparar la legislación idónea se resumen en el Apéndice a dicha Recomendación[817].

---

809 See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

810 The Council of Europe, based in Strasbourg and founded in 1949, is an international organisation 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 organisation.

811 Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

812 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.

813 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

814 *Nilsson* in Sieber, "Information Technology Crime", Page 576.

815 Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

816 Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

817 The Guidelines deal with investigative instruments (e.g. Search and Seizure) as well as electronic evidence and international cooperation.

En 1996 el Comité Europeo para Asuntos Delictivos (CDPC) decidió establecer un Comité de Expertos para abordar el ciberdelito[818]. 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[819]. 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[820]. 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. 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 abril de 2009 habían firmado el Convenio sobre la Ciberdelincuencia 46 Estados [821] y 25 Estados[822] lo habían ratificado[823]. Países tales como Argentina[824], Pakistán[825], Filipinas[826], Egipto[827], Botswana[828] y Nigeria[829] han redactado ya partes de su legislación con arreglo al Convenio. Si bien dichos países no han firmado aún el Convenio, apoyan el proyecto de armonización y normalización propuesto por los redactores del Convenio. Actualmente, se reconoce que el

818 Decision CDPC/103/211196. The CDPC explained their 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."

819 Explanatory Report of the Convention on Cybercrime (185), No. 10.

820 The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: http://www.coe.int.

821 Albania, 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, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

822 Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

823 The need for a ratification is laid down in Article 36 of the Convention:

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.

824 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).

825 Draft Electronic Crime Act 2006.

826 Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

827 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

828 Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

829 Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

Convenio es un importante instrumento internacional para luchar contra el ciberdelito y como tal ha recabado el apoyo de diferentes organizaciones internacionales[830].

Se aprobó el Primer Protocolo Adicional del Convenio sobre la Ciberdelincuencia[831]. Durante las negociaciones del texto del Convenio se vio que penalizar especialmente el racismo y la distribución de material xenófobo era objeto de controversia[832]. Algunos de los países en los que se protege apreciablemente el principio de libertad de expresión[833] señalaron con preocupación que si se incluían disposiciones en el Convenio que violaran la libertad de expresión, no podrían firmar el Convenio[834]. De ahí que estas cuestiones se integrasen en un Protocolo separado. En octubre de 2008 habían firmado el Protocolo Adicional 20 Estados[835] y 13 Estados[836] lo habían ratificado.

Dada su óptica de mejorar la protección de menores contra la explotación sexual, el Consejo de Europa preparó un nuevo Convenio en 2007[837]. El primer día en que se abrió a la firma el Convenio sobre la Protección de los niños, 23 Estados lo firmaron[838]. Uno de los objetivos esenciales del Convenio es armonizar las disposiciones de derecho penal encaminadas a proteger a los menores contra la explotación sexual[839]. Para lograr este objetivo, el Convenio contiene un conjunto de disposiciones penales. Aparte de la penalización del abuso sexual

---

830 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 Cyber Crime 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: http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda points out: „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: http://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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

831 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

832 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."

833 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

834 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

835 Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine.

836 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine.

837 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

838 Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Irland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Turkey. Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).

839 For more details see *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

de niños (Artículo 18), el Convenio contiene una disposición sobre el intercambio de pornografía infantil (Artículo 20) y la solicitación de niños con propósitos sexuales (Artículo 23).

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 Unión Europea[840]

Los poderes de la Unión Europea son limitados cuando se trata de legislar en la esfera del derecho penal[841]. En efecto, la Unión sólo tiene la posibilidad de armonizar el derecho penal de los Estados Miembros en esferas especiales, tales como la protección de los intereses financieros de la Unión Europea y el ciberdelito[842].

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"[843]. En 2000 el Consejo Europeo adoptó un "Plan de Acción e-Europa" detallado y pidió que se tradujese a la práctica antes de fines de 2002.

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[844]. 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[845].

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[846].

---

840 The European Union is a supranational and intergovernmental union of today 27 member states from the European continent.

841 *Satzger*, International and European Criminal Law, Page 84; *Kapteyn/VerLooren van Themaat*, Introduction to the Law of the European Communities, Page 1395.

842 Regarding the Cybercrime legislation in respect of Computer and Network Misuse in EU Countries see: *Baleri/Somers/Robinson/Graux/Dumontier*, Handbook of Legal Procedures of Computer Network Misuse in EU Countries, 2006.

843 Communication of 8 December 1999 on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000 – *e*Europe – An information society for all – COM 1999, 687.

844 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 Crime26.1.2001, COM(2000) 890.

845 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.

846 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.

La Comisión formulará propuestas legislativas en el marco del Título VI del Tratado de la Unión Europea:

[...] 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 la 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[847].

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[848].

Asimismo, la Comisión publicó una Comunicación, que versaba sobre la seguridad de las redes y la información[849], Comunicación 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[850]. Tras dicha estrategia, la Comisión presentó en 2002[851] una propuesta relativa a la formulación de una Decisión Marco sobre los ataques lanzados contra los sistemas de información. Esta propuesta se modificó en parte y fue adoptada finalmente por el Consejo[852].

En la Decisión Marco mencionada se toma nota de que el Convenio sobre la Ciberdelincuencia del Consejo de Europa[853] se concentra en la armonización de las disposiciones del derecho penal sustantivo tendentes a proteger los elementos de las infraestructuras.

Artículo 2 – Acceso ilícito a sistemas de información

1. Los Estados Miembros tomarán las medidas necesarias para garantizar que se sancione penalmente el acceso deliberado e ilegítimo a la totalidad de un sistema de información o parte del mismo, al menos en casos graves.

2. Los Estados Miembros podrán decidir que la conducta especificada en el párrafo 1 se tipifique en su derecho penal solamente cuando el delito se cometa infringiendo una medida de seguridad, y se sancione penalmente de manera proporcional y disuasiva.

---

847 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.

848 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.

849 "Network and Information Security" A European Policy approach – adopted 6 June 2001.

850 For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

851 Proposal of the Commission for a Council Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. 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.

852 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

853 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:

Artículo 3 – Interferencia legítima en los sistemas

Los Estados Miembros tomarán las medidas necesarias para garantizar que se sancione penalmente el intento de obstaculizar o interrumpir en grado considerable y de manera deliberada e ilegítima el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, al menos en casos graves.

Artículo 4 – Interferencia ilegal en los datos

Los Estados Miembros tomarán las medidas necesarias para garantizar que se sancione penalmente el intento de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos en un sistema de información, al menos en casos graves.

En 2005, el Tribunal de Justicia de las Comunidades Europeas declaró ilegal la Decisión Marco del Consejo relativa a la protección del medio ambiente mediante el derecho penal[854],[855]. Gracias a su decisión, el Tribunal precisó la distribución de poderes entre el primer y tercer pilares en lo que concierne a las disposiciones del derecho penal. El Tribunal decidió que siendo indivisible, la Decisión Marco mencionada infringía el Artículo 47 de la Unión Europea, ya que se arrogaba los poderes conferidos a la Comunidad en virtud del Artículo 175 de las Comunidades Europeas[856]. En una comunicación sobre la Decisión[857] del Tribunal, la Comisión señaló que:

> *"Desde el punto de vista del asunto tratado, aparte de la protección ambiental, el razonamiento del Tribunal puede aplicarse, en consecuencia, a todas las políticas y libertades de la comunidad que entrañen legislación vinculante que traiga consigo sanciones de derecho penal para garantizar su eficacia."*

La Comisión señaló que como consecuencia del fallo del Tribunal varias Decisiones Marco que versaban sobre derecho penal eran incorrectas íntegra o parcialmente, ya que algunas de sus disposiciones o todas ellas se habían adoptado a partir de una base jurídica errónea. La Decisión Marco relativa a los ataques contra los sistemas de información se señalaba explícitamente en la enmienda a la Comunicación mencionada.

En la Decisión Marco no se integraron una serie de aspectos de derecho procesal, especialmente la armonización de los instrumentos necesarios para investigar y enjuiciar el ciberdelito. Con todo, en 2005 la Comisión preparó una propuesta de Directiva de la Unión Europea, que versaba sobre la retención de datos. El Consejo adoptó dicha propuesta, sólo tres meses después de su presentación al Parlamento Europeo[858]. El elemento clave de la Directiva precitada es la obligación de los proveedores de Internet a almacenar ciertos datos sobre el tráfico necesarios para identificar a delincuentes en el ciberespacio:

Artículo 3 – Obligación de retener datos

1. No obstante lo dispuesto en los Artículos 5, 6 y 9 de la Directiva 2002/58/EC, los Estados Miembros deberán adoptar medidas para garantizar que los datos especificados en el Artículo 5 de la presente Directiva se retengan de conformidad con lo dispuesto sobre el particular siempre que los datos sean generados y tramitados por proveedores de servicios de comunicaciones electrónicas disponibles para el público por una red de comunicaciones pública dentro de su jurisdicción, cuando dichos proveedores suministren los servicios de comunicaciones de que se trate.

---

854 Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

855 Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03.

856 "It follows from the foregoing that, on account of both their aim and their content, Articles 1 to 7 of the framework decision have as their main purpose the protection of the environment and they could have been properly adopted on the basis of Article 175 EC. That finding is not called into question by the fact that Articles 135 EC and 280(4) EC reserve to the Member States, in the spheres of customs cooperation and the protection of the Community's financial interests respectively, the application of national criminal law and the administration of justice. It is not possible to infer from those provisions that, for the purposes of the implementation of environmental policy, any harmonisation of criminal law, even as limited as that resulting from the framework decision, must be ruled out even where it is necessary in order to ensure the effectiveness of Community law. In those circumstances, the entire framework decision, being indivisible, infringes Article 47 EU as it encroaches on the powers which Article 175 EC confers on the Community."

857 Communication From The Commission To The European Parliament And The Council on the implications of the Court's judgment of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

858 2005/0182/COD.

2. La obligación de conservar datos señalada en el párrafo 1 incluirá la conservación de los datos especificados en el Artículo 5, relativo a los intentos de llamada no fructuosos, cuando dichos datos sean generados o tramitados, y almacenados (datos telefónicos) o registrados (datos de Internet) por proveedores de servicios de comunicaciones electrónicas disponibles para el público o por una red de comunicaciones pública dentro de la jurisdicción de los Estados Miembros y durante la prestación de los servicios de comunicaciones de que se trate. La presente Directiva no exigirá retener los datos relacionados con llamadas no conectadas.

El hecho de que las organizaciones de derechos humanos hayan criticado repetidamente que la información esencial sobre cualesquiera comunicaciones que se efectúen en Internet sea objeto de la Directiva mencionada podría llevar a que los tribunales constitucionales revisen la Directiva y su aplicación[859].

En 2007, la Comisión publicó una Comunicación relativa a una política general en cuanto a la lucha contra el ciberdelito[860]. 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.

En 2008 la Unión Europea inició un debate acerca de un proyecto de enmienda de la Decisión Marco sobre la lucha contra el terrorismo[861]. 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 la Internet[862]. 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.

---

859 *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, 286.

860 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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

861 Draft Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism, COM(2007) 650.

862 "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."

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, párrafo 1 (c)[863] 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 "regulares" 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).

5.2.2 Organización de Cooperación y Desarrollo Económicos[864]

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[865]. La OCDE publicó en 1985 un Informe que analizaba la legislación vigente y formuló propuestas para combatir el ciberdelito[866]. 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[867]. 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

863 "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.

864 The Organisation for Economic Co-operation and Development was founded 1961. It has 30 member states and is based in Paris. For more information see: http://www.oecd.org.

865 *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.

866 OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

867 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.

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 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 se adoptaron como Recomendación del Consejo de la OCDE[868]. 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[869] 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 occidentales[870].

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

868 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: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

869 Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

870 See Spam Issue in Developing Countries, Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

publicó en 2007 un Informe sobre el tratamiento legislativo del "ciberterror" en las legislaciones de los diferentes Estados[871].

5.2.3 Foro de Cooperación Económica Asia-Pacífico[872]

En 2002 los dirigentes del Foro de Cooperación Económica Asia-Pacífico (APEC) publicaron una declaración sobre la lucha contra el terrorismo y la promoción del crecimiento, para dar aplicación a leyes detalladas sobre el ciberdelito y desarrollar capacidades nacionales e investigación de los delitos cibernéticos[873]. Los dirigentes se comprometieron a:

- Intentar promulgar en octubre de 2003 un conjunto detallado de leyes sobre ciberseguridad y ciberdelito que fueran conformes a lo dispuesto en los instrumentos jurídicos internacionales, incluida la Resolución 55/63 (2000) aprobada por la Asamblea General de las Naciones Unidas y el Convenio sobre la Ciberdelincuencia (2001).
- Identificar las unidades nacionales que se encargan del ciberdelito y los coordinadores de la asistencia internacional en materia de alta tecnología, y crear las correspondientes capacidades, siempre que éstas no existan ya, todo ello a más tardar en octubre de 2003.
- Establecer a más tardar en octubre de 2003 instituciones que intercambien evaluaciones sobre amenazas y vulnerabilidad (tales como equipos de respuesta de emergencia ante incidentes informáticos).

Los dirigentes del APEC hicieron un llamamiento para promover una cooperación más estrecha entre los funcionarios que participan en la lucha contra el ciberdelito[874]. En 2005 el APEC organizó la Conferencia sobre Legislación en materia de Ciberdelito[875]. Los principales objetivos de dicha Conferencia eran los siguientes:

- 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;
- promover la cooperación entre los investigadores y el ciberdelito en la región.

El Grupo de Trabajo sobre telecomunicaciones e información del APEC[876] participó activamente en la definición de enfoques del APEC para acrecentar la ciberseguridad[877]. En 2002 el Grupo de Trabajo adoptó la estrategia de ciberseguridad del APEC[878]. 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

---

871 The report is available at: http://www.legislationline.org/upload/ lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

872 The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties that has 21 members.

873 APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico 26 October 2002. Regarding the national legislation on Cybercrime in the Asian-Pacific Region see: Urbas, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: http://www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf; See in this regards as well: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

874 "*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.

875 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.

876 "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."

877 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: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

878 For more information see: http://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

de las Naciones Unidas al Consejo de Europa[879]. 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[880].

5.2.4 La Commonwealth

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 sobre la Ciberdelincuencia del Consejo de Europa[881]. 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[882]. El Grupo de Expertos presentó su Informe y recomendaciones en marzo de 2002[883]. En la fecha ulterior de dicho año se presentó el proyecto de Ley Modelo sobre el ciberdelito y los actos delictivos afines[884]. 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.

5.2.5 La Liga Árabe y el Consejo de Cooperación del Golfo[885]

Varios países de la Región Árabe han tomado ya medidas nacionales y adoptado diferentes enfoques para luchar contra el ciberdelito, o se encuentran preparando legislación al respecto[886]. Entre estos países, cabe citar: Pakistán[887], Egipto[888] y Emiratos Árabes Unidos[889]. El Consejo de Cooperación del Golfo[890] recomendó en una Conferencia celebrada en 2007 que los países del Consejo de Cooperación del Golfo intentasen definir un enfoque común en el que se tomaran en consideración diferentes normas internacionales[891].

---

879 See: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

880 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: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

881 See "Model Law on Computer and Computer Related Crime", LMM(02)17, Background information.

882 *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.

883 See: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

884 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

885 The League of Arab States is a regional organisation with currently 22 members.

886 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

887 Draft Electronic Crime Act 2006.

888 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

889 Law No.2 of 2006, enacted in February 2006.

890 Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE.

891 Non official transation of the Recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18th of 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.

5.2.6 Organización de los Estados Americanos[892]

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 dentro del mandato y alcance de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA).[893]

En 1999, la REMJA recomendó el establecimiento de un Grupo de Expertos Intergubernamental sobre el ciberdelito. Se encomendó a este Grupo:

- Que preparase un diagnóstico sobre las actividades delictivas en el campo de la informática de la información, o cuya realización requiere el empleo de computadores.
- Efectuar un diagnóstico de la legislación, políticas y prácticas nacionales relativas a dichas actividades delictivas.
- Identificar entidades nacionales e internacionales que dispongan de conocimientos especializados sobre el particular.
- Identificar mecanismos de cooperación con el sistema interamericano de lucha contra el delito cibernético.

En 2000, los Ministros de Justicia o Ministros o Procuradores Generales de las Américas abordaron el tema que representaba el ciberdelito y convinieron en una serie de recomendaciones.[894] Estas recomendaciones, entre las cuales cabe citar las siguientes, fueron reiteradas en la reunión de 2003[895]:

- Que se apoye el examen de las recomendaciones efectuado por el Grupo de Expertos Gubernamentales en su reunión inicial, como contribución de la REMJA a la elaboración de la Estrategia Comprensiva Interamericana de la OEA para combatir amenazas a la ciberseguridad cibernética, señalada en la Resolución de la Asamblea General de la OEA AG/RES. 1939 /XXXIII-O/03), y pedir al Grupo que, a través de su Presidente, siga apoyando la preparación de la Estrategia.
- Que en el contexto del Grupo de Expertos, los Estados Miembros examinen mecanismos para facilitar la amplia y eficiente cooperación entre los mismos con el fin de combatir el ciberdelito y estudiar, en la medida de lo posible, la constitución de las capacidades técnicas y jurídicas que exigiría participar en la red establecida por el G8 para contribuir a las investigaciones sobre el delito las 24 horas del día y siete días por semana.
- Que los Estados Miembros evalúen la conveniencia de implementar los principios del Convenio sobre la Ciberdelincuencia (2001) del Consejo de Europa, y que consideren la posibilidad de acceder al Convenio.
- Que los Estados Miembros examinen y, si así procede, actualicen la estructura y las actividades de los órganos nacionales o las entidades encargadas de hacer cumplir la ley con el fin de ajustarse a la naturaleza cambiante del ciberdelito, lo que incluye analizar la relación existente entre los organismos que luchan contra el ciberdelito y los que proporcionan tradicionalmente asistencia de política o se prestan mutuamente ayuda.

---

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 proofs 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.

892 The Organisation of American States is an international organisation with 34 active Member States. For more information see: http://www.oas.org/documents/eng/memberstates.asp.

893 For more information see http://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: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

894 The full list of recommendations from the 2000 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber; The full list of recommendations from the 2003 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

895 The full list of recommendations is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

La Cuarta Reunión de Ministros de Justicia, de Ministros o Procuradores Generales de las Américas recomendó que, en el marco de las actividades emprendida por el Grupo de Trabajo de la OEA para dar aplicación a las recomendaciones de la REMJA, el Grupo de Expertos Gubernamentales sobre ciberdelito[896] se vuelva a convocar y que se otorgue a éste el mandato necesario para:

- Vigilar la aplicación de las recomendaciones preparadas por el Grupo y adoptadas por la REMJA-III.
- Estudiar la preparación de los correspondientes instrumentos jurídicos y legislación modelo interamericanos, con el propósito de fortalecer la cooperación hemisférica para combatir el ciberdelito, habida cuenta de la normativa relativa a la privacidad, de la protección de la información, de los aspectos de procedimientos y de la prevención del delito.

Los Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) han celebrado siete reuniones hasta la fecha[897]. Las reuniones más recientes fueron las organizadas en Washington D.C., Estados Unidos, en abril de 2006 y abril de 2008. Entre las recomendaciones formuladas en la reunión de 2006 pueden citarse las siguientes[898]:

- Que prosiga el fortalecimiento de la cooperación con el Consejo de Europa, con el fin de que los Estados Miembros de la OEA puedan considerar la aplicación de los principios del Convenio sobre la Ciberdelincuencia del Consejo de Europa[899] y adherirse a dicho instrumento, así como adoptar las medidas jurídicas y de otro tipo que requiere la implementación del Convenio. Asimismo, que se sigan realizando esfuerzos para fortalecer los mecanismos de intercambio de información y cooperación con otras organizaciones internacionales en la esfera del ciberdelito, tales como las Naciones Unidas, la Unión Europea, el Foro de Cooperación Económica Asia-Pacífico, la OCDE, el G8, la Commonwealth e INTERPOL, para que los Estados Miembros de la OEA aprovechen los progresos alcanzados en dichos foros.
- Que los Estados Miembros establezcan unidades especializadas para investigar el ciberdelito e identificar a las autoridades que se encargan de la coordinación a este respecto, así como para acelerar el intercambio de información y la obtención de pruebas. Asimismo, que se promueva la cooperación para que las autoridades gubernamentales, los proveedores de servicios de Internet, y las empresas privadas que proporcionan servicios de transmisión de datos desplieguen esfuerzos con el fin de luchar contra el ciberdelito.

Estas recomendaciones fueron reiteradas en la reunión de 2008, en la cual se señaló, igualmente[900]:

- Que, teniendo presente las recomendaciones adoptadas por el Grupo de Expertos Gubernamentales y por las anteriores reuniones REMJA, los Estados consideren la posibilidad de aplicar los principios del Convenio sobre la Ciberdelincuencia del Consejo de Europa, así como de adherirse a dicho instrumento, y de adoptar las medidas jurídicas y de otro tipo que exija la implementación del Convenio. Asimismo, que se sigan realizando actividades de cooperación técnica bajo los auspicios de la Secretaría General de la OEA y por conducto de la Secretaría de Asuntos Jurídicos y el Consejo de Europa. Asimismo, que se sigan desplegando esfuerzos para fortalecer el intercambio de información y la cooperación con otras organizaciones internacionales en la esfera del ciberdelito, para que los Estados Miembros de la OEA aprovechen los progresos alcanzados en tales foros.

---

896 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: http://www.oas.org/dil/department_office_legal_cooperation.htm.

897 The Conclusions and Recommendation of the Meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas and Cyber Crime are available at: http://www.oas.org/juridico/english/cyber_meet.htm.

898 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 program be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G-8 to help conduct cyber-crime investigations. Pursuant to such recommendation, three OAS Regional Technical Workshops were held during 2006 and 2007, with the first being offered by Brazil and the United States, and the second and third offered by the United States. The List of Technical Workshops is available at: http://www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

899 In the meantime the 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: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

900 Conclusions and Recommendations of REMJA-VII, 2008, available at: http://www.oas.org/juridico/english/cybVII_CR.pdf.

- Que las Secretarías del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Trabajo sobre Ciberdelito, sigan realizando actividades permanentes de coordinación y cooperación para garantizar la implementación de la Estrategia Comprensiva Interamericana de la OEA para combatir amenazas a la seguridad cibernética, adoptada por la Asamblea General de la OEA en la Resolución AG/RES. 2004 (XXXIV-O/04).

5.3 Enfoques científicos

Un ejemplo muy conocido de enfoque científico para desarrollar un marco jurídico con el fin de afrontar globalmente el ciberdelito es el Proyecto de Convención Internacional de Standford (CISAC)[901]. Esta Convención fue preparada como resultado de una Conferencia celebrada en la Universidad de Standford en Estados Unidos en 1999[902]. Dicha Convención y el Convenio sobre la Ciberdelincuencia del Consejo Europeo[903] guardan cierto parecido. Ambos instrumentos versan sobre el derecho penal sustantivo, el derecho procesal y la cooperación internacional. De otro lado, la diferencia más importante es el hecho de que los delitos y los instrumentos procesales contemplados en el Proyecto de Convención de Standford resultan únicamente aplicables a los ataques contra la infraestructura de la información y los ataques terroristas, mientras que los instrumentos procesales y la cooperación internacional especificados en el Convenio sobre la Ciberdelincuencia pueden aplicarse también a delitos tradicionales[904].

5.4 Relaciones entre diferentes enfoques internacionales y legislativos

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[905]. En la actualidad, el Convenio sobre la Ciberdelincuencia es el principal instrumento internacional vigente para abordar todos los aspectos pertinentes del ciberdelito, pese a que se están discutiendo otras iniciativas en este sentido. Un segundo enfoque internacional es el adoptado actualmente por la Unión Internacional de Telecomunicaciones[906]. En la Cumbre Mundial sobre la Sociedad de la Información, la UIT fue designada facilitador de la así llamada Línea de Acción C5 de la CMSI. Como se definió en la fase de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en 2003, la Línea de Acción C5 versa sobre la creación de confianza en la seguridad en la

---

901 *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.

902 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: http://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.

903 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: Chapter 6.1.; *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. seqq; *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: http://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*.

904 Regarding the application of Art. 23 et seq. with regard to tradition crimes see: Explanatory Report to the Convention on Cybercrime, No. 243.

905 For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 et seq.

906 The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates.

utilización de las TIC[907]. En la segunda reunión de facilitación al seguimiento a la Línea de Acción C5, el Secretario General de la UIT destacó la importancia de la cooperación internacional para luchar contra el ciberdelito. Acto seguido, se anunció que se prepararía la Agenda de Ciberseguridad Global de la UIT[908]. La Agenda contiene siete objetivos clave[909]. Una de tales metas es la elaboración de estrategias para definir un modelo de legislación sobre ciberdelito. Asimismo se estableció un Grupo de Expertos para preparar estrategias en relación con la Agenda[910]. La compatibilidad entre una posible Ley Modelo y las normas existentes dependerá del enfoque que se adopte al redactar una nueva Ley Modelo. En este contexto pueden plantearse tres tipos de relación:

- Reglamentación controvertida

  Una nueva Ley Modelo que defina normas no conformes con las vigentes, podría, al menos en una fase inicial, afectar adversamente el proceso de armonización requerido.

- Duplicación parcial de las normas del Convenio

Una nueva Ley Modelo podría basarse en el Convenio sobre la Ciberdelincuencia y eliminar las disposiciones que plantean dificultades o que incluso disuadieron de firmar el Convenio a una serie de países. En ese sentido, un ejemplo es la muy discutida reglamentación contenida en el Artículo 32b del Convenio sobre la Ciberdelincuencia. Esta disposición fue criticada por la Delegación de Rusia en la reunión del Comité sobre Ciberdelito de 2007[911].

- Complementación de las normas del Convenio

  Una nueva Ley Modelo podría ir más allá de las normas definidas en el Convenio sobre la Ciberdelincuencia y, por ejemplo, tipificar como delitos ciertos actos relacionados con el delito cibernético, así como definir instrumentos procesales aún no contemplados por el Convenio. Desde 2001 se han registrado varios hechos importantes en este campo. En la época en que se redactó el Convenio el "*phishing*"[912], el "hurto de identidad"[913] y los delitos relacionados con los juegos en línea y

---

907 For more information on the C5 Action Line see Meeting Report of 2nd Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/meetingreport.pdf.

908 For more information see http://www.itu.int/osg/csd/cybersecurity/gca/.

909 1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, 2. Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime. 3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems. 4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.5. Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries. 6. Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas. 7. Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

910 See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

911 Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: http://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.

912 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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon 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: http://www.usdoj.gov/opa/report_on_phishing.pdf.

913 For an overview about the different legal approaches see: *Gercke*, Internet-related Identity Theft, 2007, available at: http://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; See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://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: http://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.

las redes sociales eran menos importantes de lo que fueron después. Un nuevo modelo de ley podría contribuir a proseguir el proceso de armonización, tipificando como delitos otras acciones de magnitud transnacional[914].

En este contexto, el Conjunto de herramientas de legislación sobre ciberdelito preparado por la UIT[915] tiene por objetivo proporcionar a los países material de referencia que pueda ayudar a éstos a establecer un régimen legislativo encaminado a frenar el ciberdelito. En el Conjunto de herramientas se destaca la importancia de la armonización de los marcos jurídicos nacionales para combatir más eficazmente el ciberdelito y facilitar la cooperación internacional. El Conjunto de herramientas de legislación del ciberdelito fue preparado por un Grupo de Expertos internacional y multidisciplinario que puso a disposición un primer esbozo a principios de 2009.

5.5 Relaciones entre los enfoques legislativos internacionales y nacionales

Como se indicó anteriormente los ciberdelitos son acciones que tienen carácter internacional[916]. A la vista de que los delincuentes pueden dirigirse, en general, a usuarios en todo el mundo, la cooperación internacional de los organismos encargados de hacer cumplir la ley es un requisito indispensable, o cuando se trata de realizar investigaciones internacionales en materia del delito cibernético[917]. Estas investigaciones exigen dotarse de los medios de cooperación necesarios, así como armonizar las leyes. Habida cuenta del principio común de doble delincuencia[918], 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[919]. 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[920]. 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, si no una necesidad, en cualquier estrategia nacional que se emprenda contra el ciberdelito.

5.5.1 Motivos de 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[921]. 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

---

914 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 criminalisation that go beyond the standards of the Convention will proceed with difficulties.

915 Further information on the ITU Cybercrime Legislation Toolkit is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.

916 Regarding the extent of transnational attacks in the most damaging cyber attacks 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.

917 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.

918 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties 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 the surrender procedures between Member States (2002/584/JHA).

919 Regarding the dual criminality principle in international investigations see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

920 See Convention on Cybercrime, Art. 23 – Art. 35.

921 See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq*.

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[922]. 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[923]. 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[924]. 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 y 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 aquellos que desean conectarse en la Internet deben utilizar los protocolos normalizados (técnicos) establecidos[925]. 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[926]. Habrá que preguntarse si es posible seguir aplicando enfoques nacionales, dada la naturaleza internacional del ciberdelito[927]. 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[928].

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[929]. 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. Esta 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 relativa a los ataques contra los sistemas de información adoptada por la Unión Europea 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[930]. 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.

---

922 See above: Chapter 2.6.7.

923 See Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

924 See Spam Issue in Developing Countries, Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

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

926 See for example the following surveys on national Cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005 -, page 5, available at: http://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: https://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: http://www.mosstingrett.no/info/legal.html.

927 Regarding the international dimension see above: Chapter 3.2.6.

928 With regard to the Convention on Cybercrime see: Explanatory Report to the Convention on Cybercrime, No. 33.

929 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.

930 See below: Chapter 6.1.9.

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[931]. 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[932], motivo por el cual la viabilidad práctica de los enfoques nacionales exige en general la adopción de medidas auxiliares adicionales[933]. Las medidas auxiliares más populares son las siguientes:

- **Tipificar como delitos no sólo las conductas de los proveedores de contenido ilegal, sino también las de sus usuarios**

Lo que puede hacerse es no sólo tipificar como delito 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.

- **Tipificación penal de los servicios utilizados para cometer delitos**

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[934].

El establecimiento de la obligación de filtrar ciertos contenidos disponibles en Internet es una medida estrechamente relacionada con la anterior[935]. Este enfoque se discutió en el marco de la célebre decisión sobre Yahoo[936] 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

---

931 See above: Chapter 3.2.6 and Chapter 3.2.7.

932 The issue was addressed by a number of international organisations. The 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: http://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".

933 For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.

934 For an overview about the law see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm. For more information see below: Chapter 6.1.j.

935 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: http://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: http://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: http://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: http://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.*

936 See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *http://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.*

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. OpenNet Initiative[937] ha informado de que unos veinticuatro países practican la censura en este contexto[938].

6 Respuesta jurídica

El presente Capítulo contiene un panorama general de las respuestas jurídicas al fenómeno de la ciberdelincuencia, y en éste se describen los enfoques jurídicos para la penalización de ciertos actos[939]. Toda vez que sea posible se expondrán enfoques internacionales, y cuando no se disponga de ellos se presentarán otros enfoques a escala nacional o regional.

6.1 Derecho penal sustantivo

6.1.1 Acceso ilícito (piratería)

Desde que se desarrollaron las redes informáticas, su capacidad para conectar a los ordenadores y ofrecer a los usuarios acceso a otros sistemas informáticos ha sido aprovechada por piratas con fines delictivos[940]. Las motivaciones que mueven a los piratas son muy diversas[941]: no es necesario que estén presentes en la escena del delito[942]; basta con que éstos eludan los sistemas de protección que aseguran a la red[943]. 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[944].

El acceso ilícito a los sistemas informáticos dificulta a los operadores una gestión, explotación y control de sus sistemas sin perturbación o impedimento[945]. La finalidad de la protección es mantener la integridad de los sistemas informáticos[946]. Es esencial hacer una distinción entre el acceso ilícito y las subsiguientes infracciones (tales como el espionaje de datos[947]), 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,

---

937 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: http://www.opennet.net.

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

939 For an overview about legal approaches see also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18 et seq., available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

940 *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, No5 – page 825 et sqq.

941 These range from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimised computer. Even political motivations have been discovered. See: *Anderson*, "Hacktivism and Politically Motivated Computer Crime", 2005, available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

942 Regarding the independence of place of action and the location of the victim, see above 3.2.7.

943 These can for example be passwords or fingerprint authorisation. 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: http://www.212cafe.com/download/e-book/A.pdf.

944 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.

945 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 729.

946 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "*The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner*".

947 With regard to data espionage see above, Chapter 2.4.b and below, Chapter 6.1.2.

tales como la modificación u obtención de datos almacenados (cuando la ley trata de proteger la integridad y la confidencialidad de los datos)[948].

La cuestión consiste en determinar si se debe penalizar o no el acto de acceso ilícito, además de los subsiguientes delitos[949]. 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[950]. En algunos países se penaliza el mero acceso, mientras que en otros se limita la penalización únicamente a los casos en los cuales 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[951]. En otros países no se penaliza el acceso propiamente dicho, sino únicamente los delitos subsiguientes[952]. 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[953].

Convenio sobre la Ciberdelincuencia

El Convenio 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[954], 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[955].

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.*

---

948 With regard to data interference see above, Chapter 2.4.d and below, Chapter 6.1.3.

949 *Sieber*, Informationstechnologie und Strafrechtsreform, Page 49 et seq.

950 For an overview of the various legal approaches towards criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003", available at: http://www.mosstingrett.no/info/legal.html.

951 Art. 2 Convention on Cybercrime enables the member states to keep those existing limitations that are mentioned in Art. 2, sentence 2 Convention on Cybercrime. Regarding the possibility to limit the criminalisation see as well: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

952 An example of this is the German Criminal Code, which criminalised 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.

953 This approach is not only found in national legislation, but was also recommended by the Council of Europe Recommendation N° (89) 9.

954 For an overview of the various legal approaches in criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003", available at: http://www.mosstingrett.no/info/legal.html.

955 Regarding the system of reservations and restrictions, see *Gercke*, "The Convention on Cybercrime", Computer Law Review International, 2006, 144.

Actos contemplados

El término "acceso" no especifica un medio concreto de comunicación, sino que admite diversas connotaciones y está abierto a nuevos adelantos técnicos[956]. Este término se refiere a todos los medios de ingresar en otro sistema informático, con inclusión de los ataques por Internet[957], 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)[958]. 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[959]. La segunda frase del Artículo 2 ofrece la posibilidad de limitar la penalización del acceso ilícito al acceso a través de una red[960].

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[961].

Predisposición

Al igual que todos los otros delitos definidos en el Convenio sobre la Ciberdelincuencia, en el Artículo 12 se exige que para penalizar un delito el delincuente lo haya efectuado de manera intencional[962]. El Convenio no contiene una definición del término "internacionalmente". Los redactores del Informe Explicativo subrayaron que la definición de "intencionalmente" debe considerarse a nivel nacional[963].

---

956 *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

957 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 seqq., available at: http://www.212cafe.com/download/e-book/A.pdf. With regard to Internet related social engineering techniques see the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing , available at: http://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 "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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

958 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

959 The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5% of the respondents reported that 80-100% of their losses were caused by insiders. Nearly 40% of all respondents reported that between 1% and 40% 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: http://www.gocsi.com/.

960 Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

961 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

962 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

963 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

Sin derecho

A tenor del Artículo 2 del Convenio, el acceso a un ordenador sólo puede penalizarse si éste tiene lugar "sin derecho"[964]. 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"[965]. Además del tema del acceso libre, también se aborda la legitimidad de los procedimientos de ensayo de seguridad[966]. 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[967]. 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"[968].

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[969], es necesario verificar si la autorización concedida por la víctima incluye al acto efectuado por el delincuente[970]. 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 ofrece la posibilidad de limitar la penalización con elementos adicionales, tal como se enumeran en la segunda frase[971]. En el Artículo 42 del Convenio se describe el procedimiento adecuado para recurrir a esta reserva[972]. Las posibles reservas guardan relación con las

---

964 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.

965 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

966 *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, Page 7.

967 See for example: World Information Technology And Services Alliance (WITSA), "Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000", available at: http://www.witsa.org/papers/COEstmt.pdf; "Industry group still concerned about draft Cybercrime Convention, 2000", available at: http://www.out-law.com/page-1217.

968 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).

969 *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.

970 This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: http://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 "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: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

971 *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

972 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.*

medidas de seguridad[973], la intención especial de obtener datos informáticos[974], 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[975]. La Decisión Marco de la Unión Europea[976] sobre ataques contra sistemas de información[977] 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[978].

> ***Sección 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 principal diferencia con el Convenio sobre la Ciberdelincuencia es el hecho de que en esta Sección 5 de la Ley Modelo de la Commonwealth no se ofrece ninguna opción para formular reservas, como se hace en el Artículo 2 del mencionado Convenio.

Proyecto de Convenio Stanford

En el Proyecto de Convenio Stanford de 1999, de carácter oficioso[979], se reconoce que el acceso ilícito es uno de los delitos que deben penalizar los Estados signatarios.

Disposición

> ***Artículo 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:*
>
> *[...]*

---

973 This limits the criminalisation of illegal access to those cases where the victim used technical protection measures to protect it's computer system. Access an unprotected computer system would therefore not be considered a criminal act.

974 The additional mental element/motivation enables the member states to undertake a more focused approach not implement a criminalisation of the mere 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

975 This enables the member states to avoid a criminalisation 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.

976 Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. For more details see above: Chapter 5.1.e.

977 *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.

978 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

979 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: http://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.

(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 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"[980] utilizado en el Convenio sobre la Ciberdelincuencia y apunta explícitamente a incorporar el concepto de autodefensa[981]. La principal diferencia con el Convenio es el hecho de 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 sobre la Ciberdelincuencia[982]. Aunque el Proyecto de Convenio 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[983].

6.1.2 Espionaje de datos

El Convenio sobre la Ciberdelincuencia, así como la Ley Modelo de la Commonwealth y el Proyecto de Convenio de Stanford, proporcionan soluciones jurídicas únicamente para la interceptación ilícita[984]. Cabe poner en tela de juicio si el Artículo 3 del Convenio 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[985], 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[986]. 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 que la interceptación de los procesos de transferencia[987].

---

980 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.

981 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

982 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.

983 Stand alone computer system are covered by Art. 1, paragraph 3 of the Draft Convention because they "control programs". This does not require a network connection.

984 The Explanatory Report points out, that the provision intends to criminalise violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

985 See below: Chapter 6.1.c.

986 See *Gercke*, "The Convention on Cybercrime", Multimedia und Recht 2004, page 730.

987 One key indication of the limitation of the 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 that 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.

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[988].

Puesto que hoy en día 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[989]. 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[990]. 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[991]. 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.

Ejemplos

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 U.S.C. § 1831 que penaliza el espionaje económico. Esta disposición no sólo abarca el espionaje de datos, sino también otros medios de obtener información secreta.

> ***§ 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,*

---

988 See in this context especially a recent case from Hong Kong, People's Republic of China. See above: Chapter 2.4.2.

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

990 Regarding the challenges related to the use of encryption technology by offenders see above: Chapter 3.2.m; *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://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: http://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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

991 One of the consequences related to this aspect is the fact, that the limitation of a criminalisation 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 provision as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

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 $.

Otros países han adoptado un enfoque más amplio y han penalizado el acto de obtener datos informáticos almacenados, aunque éstos no contengan ningún secreto económico. Un ejemplo de ello es la anterior versión del § 202a del Código Penal alemán[992].

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[993]. En lo que respecta a sus objetos de protección, este enfoque es más amplio que el consignado en el § 1831 U.S.C., 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[994]. 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[995].

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[996]. En lo tocante al hecho de que el permiso cubre el acceso al sistema informático, en general no es posible abarcar este aspecto con las disposiciones que penalizan el acceso ilegal.

Sin derecho

En general para aplicar las disposiciones sobre espionaje de datos es necesario que los datos hayan sido obtenidos sin el consentimiento de la víctima. El éxito de los ataques de usurpación de identidad[997] demuestra

---

992 This provision has recently been modified and now even criminalises illegal access to data. The previous version of the provision was used, because it is suitable to demonstrate the dogmatic structure in a better way.

993 See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

994 A similar approach of limiting criminalisation 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: Chapter 6.1.1.

995 This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement self protection measures.

996 See in this context for example a recent cases in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: http://www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadro*s, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Harald, 14.02.2008, available at: http://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: http://www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: http://www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

997 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*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see above: Chapter 2.8.d.

claramente el éxito de las estafas basadas en la manipulación de los usuarios[998]. 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.

6.1.3 Interceptación ilegal

La utilización de las TIC comporta varios riesgos relacionados con la seguridad de la transferencia de información[999]. 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[1000]. 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[1001]. 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[1002]. 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[1003].

En el pasado, los perpetradores concentraron sus interceptaciones ilegales principalmente en redes empresariales[1004], pues en éstas era más probable encontrar información útil que en los datos transferidos por redes privadas. No obstante, el creciente número de casos de usurpación de identidad para robar datos

---

998 With regard to "phishing" see above: Chapter 2.8.d and below: Chapter 6.1.n and as well: *Jakobsson*, The Human Factor in Phishing, available at: http://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 "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, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

999 Regarding the risks related to the use of wireless networks, see above: Chapter 3.2.c. 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: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

1000 Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1001 Regarding the underlying technology and the security related issues see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: http://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: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

1002 The computer magazine ct reported in 2004 that field tests proved that more than 50% of 1000 wireless computer networks that were tested in Germany were not protected. See: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182.

1003 Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, "Information Technology Security Handbook", page 60, available at: http://www.infodev.org/en/Document.18.aspx.

1004 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

personales privados señala que tal vez los perpetradores hayan cambiado de objetivo[1005]; actualmente los delincuentes manifiestan gran interés por datos privados tales como los números de tarjeta de crédito, los números de seguridad social[1006], las contraseñas y la información sobre cuentas bancarias[1007].

Convenio sobre la Ciberdelincuencia

El Convenio 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 ilícitas que ya existe actualmente en la mayor parte de los sistemas jurídicos[1008].

Disposición

> ***Artículo 3 – Interceptación ilícita***
>
> *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[1009]. Las interceptaciones relacionadas con los datos electrónicos pueden definirse como cualquier acto de adquisición de datos durante un proceso de transferencia[1010].

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[1011]. En general la disposición se aplica únicamente a la interceptación de las transmisiones, pues el acceso a la información almacenada no se considera

---

1005 Regarding Identity Theft, see above: Chapter: 2.7.3 and below: Chapter 6.1.15 and as well: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://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: http://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: http://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: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1006 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: http://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.

1007 See: *Hopkins*, "Cybercrime Convention: A Positive Beginning to a Long Road Ahead", Journal of High Technology Law, 2003, Vol. II, No. 1; Page 112.

1008 Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

1009 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-criminalisation." Explanatory Report to the Council of Europe Convention on Cybercrime No. 53.

1010 Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering".

1011 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 730.

como una interceptación de transmisión[1012]. 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 sobre la Ciberdelincuencia no contiene ninguna disposición relacionada con el espionaje de datos[1013] 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[1014]. 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 propio delincuente opera el computador.
- 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"[1015]. Si los delincuentes obtienen acceso a un sistema informático y lo utilizan para hacer copias no autorizadas de datos almacenados en un disco externo, y 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[1016].

El término "transmisión" se aplica a todas las transferencias de datos, ya sean por teléfono, facsímil, correo electrónico o transferencia de ficheros[1017]. El delito consignado a tenor del Artículo 3 se aplica únicamente a las transmisiones no públicas[1018]. Una transmisión es "no pública" si el proceso de transmisión es confidencial[1019]. 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 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[1020]. El Convenio no contiene una definición del término "internacionalmente". Los

---

1012 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1013 See above: Chapter 6.1.2.

1014 "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.

1015 Explanatory Report to the Council of Europe Convention on Cybercrime No. 53.

1016 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.

1017 Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

1018 *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

1019 Explanatory Report to the Council of Europe Convention on Cybercrime No. 54.

1020 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

redactores del Informe Explicativo destacaron que la definición de "intencionalmente" debe considerarse a escala nacional[1021].

Sin derecho

Sólo se puede entablar juicio por interceptación de comunicaciones a tenor del Artículo 3 del Convenio si ésta tiene lugar "sin derecho"[1022]. Los redactores del Convenio proporcionaron un conjunto de ejemplos de interceptación efectuada sin derecho:

- acción sobre la base de instrucciones o por autorización de los participantes en la transmisión[1023];
- actividades de protección o ensayo autorizadas y convenidas por los participantes[1024];
- interceptación legal sobre la base de las disposiciones de derecho penal o en favor del interés de la seguridad nacional[1025].

Otra cuestión planteada durante la negociación del Convenio consistía en determinar si la utilización de "galletitas" ("*cookies*") debía dar lugar a sanciones penales a tenor del Artículo 3[1026]. Los redactores subrayaron que las prácticas comerciales comunes (como los *cookies*) no se consideran interceptaciones sin derecho[1027].

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.

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[1028] se describe un enfoque similar:

> ***Sección 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*

1021 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1022 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.

1023 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1024 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1025 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1026 Cookies are data sent by a server to a browser and the send 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 seqq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

1027 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1028 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

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.

Proyecto de Convenio de Stanford

En el Proyecto de Convenio de Stanford de 1999, de carácter oficioso[1029], no se penaliza explícitamente la interceptación de datos informáticos.

6.1.4 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[1030]. Los ataques a esa información o la obtención de la misma pueden dar lugar a pérdidas financieras[1031]. Además del borrado, la alteración de esa información también puede tener importantes consecuencias[1032]. En algunos casos la legislación en vigor no protege los datos de igual modo que los objetos tangibles, lo que le ha permitido a los delincuentes concebir formas de estafa que no dieran lugar a sanciones penales[1033].

Convenio sobre la Ciberdelincuencia

El Artículo 4 del Convenio sobre la Ciberdelincuencia contiene una disposición que protege la integridad de los datos contra la interferencia no autorizada[1034]. 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[1035].

1029 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: http://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.

1030 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.

1031 The 2007 Computer Economics Malware Report focuses on single of 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: http://www.computereconomics.com/article.cfm?id=1225.

1032 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: Chapter 2.7.1 and below: Chapter: 6.1.16.

1033 Regarding the problems related to those gaps see for example the LOVEBUG case where a designer of a computer worm could not be prosecuted due to missing criminal law provisions related to data interference. See above: Chapter 2.4.d 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", http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1034 A similar approach to Art. 4 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".

1035 Explanatory Report to the Council of Europe Convention on Cybercrime No. 60.

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

- Los términos "dañe" y "deteriore" definen a cualquier acto tendiente a la alteración negativa de la integridad del contenido informativo de datos y programas[1036].
- "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 no hicieron una distinción entre las diversas formas según las cuales se pueden borrar datos[1037]. Si se manda un fichero a la papelera virtual no se elimina este fichero del disco duro[1038]. Incluso el "vaciado" de la papelera virtual no elimina necesariamente el fichero[1039]. Por lo tanto, no está claro si la posibilidad de recuperar un fichero borrado impide la aplicación de la disposición[1040].
- La "supresión" de datos informáticos denota una acción que afecta la disponibilidad de datos para la persona que tiene acceso al medio, y a tenor del cual la información se almacena de una manera negativa[1041]. Se considera particularmente la aplicación de esta disposición en el caso de ataques[1042] de denegación de servicio[1043]. Durante el ataque, los datos del sistema informático víctima ya no están disponibles para el usuario potencial ni para el propietario del sistema informático[1044].

1036 As pointed out in the Explanatory Report the two terms are overlapping. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1037 Regarding the more conventional ways to delete files by Using Windows XP see the Information provided by Microsoft, available at: http://www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

1038 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1039 See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: http://www.cert.org/archive/pdf/05hb003.pdf.

1040 The fact, that the Explanatory Report mentions that the files are unrecognisable 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.

1041 Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1042 With regard to the criminalisation of "Denial-of-Service" attacks see as well below: Chapter 6.1.5.

1043 A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.In 2000 a number of well known US 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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1044 In addition criminalisation of "Denial of Service" attacks is provided by Art. 5 Convention on Cybercrime. See below: Chapter 6.1.5.

- El término "alteración" indica la modificación de los datos existentes, sin reducir forzosamente la disponibilidad de los datos[1045]. Este acto abarca en particular la instalación de software dañinos tales como programas espías, virus o programas publicitarios en el ordenador de la víctima[1046].

Predisposición

Como ocurre con todos los otros delitos definidos en el Convenio 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[1047]. El Convenio no contiene ninguna definición del término "internacionalmente". Los redactores del Informe Explicativo señalaron que la definición de "intencionalmente" debe considerarse a escala nacional[1048].

Sin derechos

Como ocurre con las disposiciones antes examinadas, estos actos deben cometerse "sin derecho"[1049]. Se consideró el derecho a alterar datos, especialmente en el contexto de los "dobles remitentes" ("*remailers*")[1050]. Los dobles remitentes apuntan a modificar ciertos datos con el fin de facilitar las comunicaciones anónimas[1051]. 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[1052].

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 de la Unión Europea

---

1045 Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is likely that the provision could cover unauthorised corrections of faulty information as well.

1046 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://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 recognised functions of malicious software see above: Chapter 2.4.d. Regarding the economic impact of malicious software attacks see above: Chapter 2.9.1.

1047 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1048 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1049 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.

1050 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.

1051 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.

1052 With regard to the possible difficulties to identify offenders that made use of anonymous or encrypted information, the Convention leaves the criminalisation of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

sobre ataques contra sistemas informáticos[1053], que permite a los Estados Miembros limitar la aplicabilidad de la disposición de derecho penal sustantiva a "los casos que no sean menores"[1054].

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[1055] se aplica un enfoque que está en consonancia con el Artículo 4 del Convenio sobre la Ciberdelincuencia.

> ***Sección 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.*

Proyecto de Convenio Stanford

El Proyecto de Convenio Stanford de 1999, de carácter oficioso[1056], 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;*

1053 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1054 For further information, see: *Gercke*, "The EU Framework Decision on Attacks against Information Systems", Computer und Recht 2005, page 468 et seq.

1055 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1056 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: http://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.

Actos contemplados

La principal diferencia entre el Convenio sobre la Ciberdelincuencia y la Ley Modelo de la Commonwealth y el enfoque del Proyecto de Convenio estriba en el hecho de 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 ley 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 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.

6.1.5 Interferencia con el sistema

Las personas o las empresas que ofrecen servicios basados en las TIC dependen del funcionamiento de sus sistemas informáticos[1057]. La indisponibilidad de páginas web que son víctimas de ataques de denegación de servicio (*Denial-of-Service*, DOS)[1058] pone de relieve la gravedad del ataque[1059]. Este tipo de ataques puede provocar importantes pérdidas financieras y afectar incluso a los sistemas más poderosos[1060]. 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[1061].

1057 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1058 A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see above: Chapter 2.4.e and US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://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: http://www.cert.org/archive/pdf/DoS_trends.pdf.

1059 For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, "Inferring Internet Denial-of-Service Activities", page 1, available at: http://www.caida.org/publications/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: http://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: http://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: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1060 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, page 431-448.

1061 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.; Related to Cyberterrorism see above Chapter 2.8.a and *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://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 seqq., available at: http://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 seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://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 seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf. *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

Convenio 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 sobre la Ciberdelincuencia contiene una disposición que penaliza la obstaculización deliberada del uso legal de los sistemas informáticos[1062].

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[1063].

- Por "obstaculización" se entiende cualquier acto que interfiera con el funcionamiento correcto de un sistema informático[1064]. 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.

La lista de actos como consecuencia de los cuales se influye de manera negativa en el funcionamiento de un sistema informático es concluyente[1065].

- El término "introducción" no está definido en el propio Convenio, ni tampoco lo definen los redactores del Convenio. Con respecto al hecho, la transmisión se menciona como un acto adicional en el Artículo 5 y el término "introducción" podría definirse como cualquier acto relacionado con la utilización de interfaces de insumo físicas para transferir información a un sistema informático, mientras que el término "transmisión" se refiere a actos que van de consuno con la introducción de datos a distancia[1066].
- Los términos "provocación de daños" y "deterioro" tienen significados superpuestos y están definidos por los redactores del Convenio 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[1067].
- El término "borrado" también ha sido definido por los redactores del Convenio y en el Informe Explicativo en relación con el Artículo 4, y abarca aquellos actos como consecuencia de los cuales se elimina información de los medios de almacenamiento[1068].
- El término "alteración" se refiere a la modificación de los datos existentes, sin disminuir forzosamente la disponibilidad de los datos[1069].
- La "supresión" de datos informáticos denota una acción que afecta la disponibilidad de los datos para la persona que tiene acceso al medio, en el que la información se almacena de una manera negativa[1070].

1062 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.

1063 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1064 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1065 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1066 Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection.

1067 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: Chapter 6.1.d. Regarding the impact of the different ways to delete 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1068 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1069 Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is therefore likely that the provision could cover unauthorised corrections of faulty information as well.

Además, la aplicación de esta disposición se limita a los casos en los cuales la obstaculización es "grave". Incumbe a las Partes determinar los criterios que se han de cumplir para que la obstaculización se considere grave.[1071] 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[1072].

Aplicación de la disposición en lo que respecta al correo basura

Se consideró si el problema del correo electrónico basura (*spam*)[1073] podía abordarse en el marco del Artículo 5, puesto que el correo basura puede sobrecargar los sistemas informáticos[1074]. 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"[1075]. Los redactores señalaron asimismo que, en función de su propia legislación nacional[1076], las Partes podrían aplicar un enfoque diferente en lo tocante a la obstaculización, por ejemplo tipificar como delitos o actos susceptibles de sanción a los actos de interferencia administrativa[1077].

Predisposición

Como ocurre con todos los otros delitos definidos en el Convenio sobre la Ciberdelincuencia, en el Artículo 5 se impone el requisito de que, para proceder a la penalización, el delincuente cometa sus infracciones intencionalmente[1078]. 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 no contiene ninguna definición del término "internacionalmente". En el Informe Explicativo, los redactores subrayaron que la definición del término "intencionalmente" debía considerarse a escala nacional[1079].

Sin derecho

Es preciso que el acto se efectúe "sin derecho"[1080]. 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

---

1070 Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1071 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.

1072 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://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 of operations resulting from attacks against a computer system can be covered by the provision.

1073 "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: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: Chapter 2.5.g.

1074 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1075 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1076 Regarding legal approaches in the fight against spam see below: Chapter 6.1.l.

1077 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1078 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1079 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

posible penalización de sus trabajos[1081]. Ahora bien, estos profesionales trabajan con el permiso del propietario y por lo tanto actúan legalmente. Además, los redactores del Convenio indicaron explícitamente que el someter a prueba la seguridad de un sistema informático con la autorización del propietario no constituye un acto sin derecho[1082].

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 limitar su aplicación. En la Decisión Marco de la Unión Europea[1083] sobre ataques contra los sistemas informáticos[1084] 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 sobre la Ciberdelincuencia[1085].

> ***Sección 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*

1080 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.

1081 See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

1082 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, authorised 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 criminalised by this article, even if it causes serious hindering."

1083 Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

1084 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*".

1085 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

c) corromper un sistema informático por cualquier medio; y

d) introducir, borrar o alterar datos informáticos;

Las principales diferencias con respecto al Convenio estriban en el hecho de que, a tenor de lo dispuesto en la Sección 7 de la Ley Modelo de la Commonwealth, se penalizan incluso los actos de imprudencia. Al aplicar este enfoque, la Ley Modelo va más allá de los requisitos impuestos en el Convenio sobre la Ciberdelincuencia. Otra diferencia es el hecho de 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 sobre la Ciberdelincuencia.

Proyecto de Convenio de Stanford

El Proyecto de Convenio de Stanford de 1999, de carácter oficioso[1086], contiene una disposición que penaliza los actos relacionados con la interferencia a los sistemas informáticos.

Disposición

Artículo 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 sobre la Ciberdelincuencia y la Ley Modelo de la Commonwealth y el enfoque aplicado en el Proyecto de Convenio estriba en el hecho de que en este último se abarca cualquier manipulación de los sistemas informáticos, mientras que el Convenio sobre la Ciberdelincuencia y la Ley Modelo de la Commonwealth limitan la penalización a la obstaculización del funcionamiento de un sistema informático.

6.1.6 Material erótico y pornográfico

La penalización del contenido ilícito y sexual explícito, así como la gravedad de la misma, varía según el país[1087]. Las Partes que negociaron el Convenio 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[1088].

1086 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: http://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.

1087 For an overview on hate speech legislation, see for example: For an overview on hate speech legislation see the data base provided at: http://www.legislationline.org. For an overview on other Cybercrime related legislation see the database provided at: http://www.cybercrimelaw.net.

1088 Regarding the challenges of international investigation see above: Chapter 3.2.f 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.

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[1089]. Así pues, la ley tiene por objetivo proteger el desarrollo del menor sin trastornos[1090]. El que la pornografía tenga una incidencia negativa en el desarrollo del menor es un asunto polémico[1091]. 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[1092]. 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[1093].

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[1094].

> ***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,*

1089 For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

1090 *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 5.

1091 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, Marco 2003, page 330 et seq., available at: http://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.

1092 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".

1093 *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 28.

1094 The draft law was not in power by the time this publication was finalised.

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[1095], las investigaciones de alcance internacional respecto a estos enfoques generales se topan con dificultades[1096].

6.1.7 Pornografía infantil

Internet se está convirtiendo en el principal instrumento para el comercio e intercambio de material con pornografía infantil[1097]. 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[1098]. Las fotos que se publican en una página web son accesibles por millones de usuarios del mundo, que pueden descargarlas[1099]. 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[1100]. Lo que sucede es sencillamente que la mayoría de los usuarios desconocen las huellas electrónicas que dejan cuando navegan por Internet[1101].

El Convenio sobre la Ciberdelincuencia del Convenio de Europa

Para mejorar y armonizar la protección del menor contra la explotación sexual[1102], el Convenio incluye un artículo relativo a la pornografía infantil.

El Artículo

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;

1095 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1096 Regarding the challenges of international investigation see above: Chapter 3.2.f and See *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.

1097 *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.

1098 Regarding the methods of distribution, see: *Wortley/Smallbone*, "Child Pornography on the Internet", page 10 et seq., available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication see above: Chapter 3.2.m.

1099 It was reported that some websites containing child pornography experienced 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: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1100 Regarding the challenges related to investigations involving anonymous communication technology see above: Chapter 3.2.l.

1101 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

1102 Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

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[1103]. Por tanto, la Convención no se limita a colmar las lagunas del derecho penal nacional[1104], sino que trata de armonizar las reglamentaciones divergentes[1105]. Existen tres elementos polémicos en el Artículo 9, a saber:

- la edad de la persona implicada;
- la penalización de la posesión de pornografía infantil; y
- la creación o integración de imágenes ficticias[1106].

Límite de la mayoría de edad

Una de las diferencias más importantes entre la legislación nacional 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[1107], a saber, todo ser humano menor de 18 años de edad. Otros países consideran menor a las personas menores de 14 años[1108]. 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[1109] se adopta un planteamiento similar y en el Convenio

---

1103 *Akdeniz* in *Edwards / Waelde*, "Law and the Internet: Regulating Cyberspace"; *Williams* in *Miller*, "Encyclopaedia of Criminology", Page 7. Regarding the extend of criminalisation, see: "Child Pornography: Model Legislation & Global Review", 2006, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalisation 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: http://www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf. *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.

1104 Regarding differences in legislation, see: *Wortley/Smallbone*, "Child Pornography on the Internet", page 26, available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1105 Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

1106 For an overview of the discussion, see: *Gercke*, "The Cybercrime Convention", Multimedia und Recht 2004, page 733.

1107 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.

1108 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) ...".

1109 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.

de 2007 del Consejo de Europa relativo a la protección a los niños contra la explotación y el abuso sexual[1110]. Subrayando la importancia de alcanzar la unanimidad internacional en lo que respecta a la edad, el Convenio define este término con arreglo al Convenio de las Naciones Unidas[1111]. Sin embargo, debido a las grandes diferencias en las legislaciones nacionales existentes, el Convenio permite a las Partes adoptar un límite de edad diferente pero no inferior a los 16 años.

Penalización de la posesión de pornografía infantil

La penalización de la posesión de pornografía infantil también varía según el sistema jurídico nacional[1112]. La demanda de este tipo de material podría fomentar su constante producción[1113]. La posesión de este tipo de material podría fomentar el abuso sexual de menores, razón por la cual los redactores consideran que una forma eficaz de reducir la producción de pornografía infantil es ilegalizar la posesión[1114]. Sin embargo, en el párrafo 4 del Convenio se permite a las Partes no penalizar la mera posesión, es decir, la responsabilidad penal se limita exclusivamente a la producción, oferta y distribución de pornografía infantil[1115].

Creación o integración de imágenes ficticias

Aunque el objetivo de los redactores es aumentar la protección del menor contra la explotación sexual, el alcance jurídico contemplado por el párrafo 2 es más amplio. El apartado a) del párrafo 2 se refiere directamente en la protección del menor contra abuso sexual, mientras que los apartados b) y c) de este mismo párrafo se refieren a imágenes producidas sin infringir los derechos del menor -por ejemplo, imágenes creadas mediante programas de dibujo en 3D[1116]. 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[1117].

Factor psicológico

Al igual que otros delitos definidos en el Convenio sobre la Ciberdelincuencia, en el Artículo 9 se exige que el infractor actúe de una manera deliberada[1118]. En el Informe Explicativo se subraya explícitamente que el Convenio 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.

1110 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http:// http://conventions.coe.int.

1111 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

1112 Regarding the criminalisation 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 criminalisation of child pornography.

1113 See: "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

1114 Explanatory Report to the Council of Europe Convention on Cybercrime No. 98.

1115 *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1116 Based on the National Juvenile Online Victimisation Study, only 3% of the 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

1117 Explanatory Report to the Council of Europe Convention on Cybercrime No. 102.

1118 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

Carencia de derecho

De conformidad con el Artículo 9 del Convenio, sólo pueden penalizarse los actos relacionados con la pornografía infantil que se realizan "sin derecho"[1119]. En el Convenio 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[1120].

El Artículo

> ***Artículo 20 – Delitos relacionados con la pornografía infantil***
>
> *(1) Cada Parte adoptará las medidas legislativas o de otro tipo que resulten necesarias para penalizar la conducta deliberada, cuando se realice sin autorización:*
>
> *a) la producción de pornografía infantil;*
>
> *b) la oferta o puesta a disposición de pornografía infantil;*
>
> *c) la distribución o transmisión de pornografía infantil;*
>
> *d) la adquisición para uno mismo o para otros de pornografía infantil;*
>
> *e) la posesión de pornografía infantil;*
>
> *f) acceder conscientemente, a través de las tecnologías de la información y la comunicación, a pornografía infantil.*
>
> *(2) A los efectos del presente Artículo, se entenderá por "pornografía infantil" todo material que contenga la representación visual de un menor adoptando un comportamiento sexualmente explícito, ya sea real o simulado, o toda imagen que muestre los órganos sexuales de un menor con fines principalmente sexuales.*
>
> *(3) Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados a) y e) del párrafo 1 relativos a la producción y posesión de material pornográfico:*
>
> *– que consista exclusivamente en representaciones simuladas o imágenes realistas de un niño ficticio;*
>
> *– en el que participen menores que hayan alcanzado la edad estipulada en aplicación del párrafo 2 del Artículo 18, siempre que dichas imágenes hayan sido producidas por ellos y estén en su posesión con su consentimiento y con fines exclusivamente privados.*
>
> *(4) Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el apartado f) del párrafo 1.*

Actos contemplados

Esta disposición se basa en el Artículo 9 del Convenio sobre la Ciberdelincuencia y, por tanto, es comparable en gran medida al mismo[1121]. La principal diferencia radica en el hecho de que el Convenio sobre la

---

1119 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.

1120 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

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. Esto permite a las fuerzas de seguridad incriminar a los infractores en los casos en que pueden probar que el infractor a abierto un sitio web con pornografía infantil pero no pueden demostrar que el infractor ha 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[1122]. 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[1123]. En general, al abrir un sitio web se inicia automáticamente un proceso de descarga, a menudo sin el conocimiento del usuario[1124]. 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

En la Sección 10 de la Ley Modelo de la Commonwealth de 2002 se adopta un enfoque similar al del Artículo 9 del Convenio sobre la Ciberdelincuencia[1125].

> ***Sección 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[1126].

1121 *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1122 Regarding the challenges related to the use of encryption technology see above: Chapter 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: http://www.missingkids.com/en_US/publications/NC144.pdf.

1123 See Explantory Report to the Convention on the Protection of Children, No. 140.

1124 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 are 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: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

1125 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1126 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.

(2) Puede esgrimirse contra la acusación de un delito en virtud del párrafo (1) (a) ó (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[1127].

(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 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.

Proyecto de Convenio de Stanford

El Proyecto de Convenio de Stanford[1128] 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[1129]. El Convenio reconoce los distintos enfoques y deja a los Estados que decidan acerca de la penalización de estos aspectos[1130].

6.1.8 Incitación al odio, racismo

No todos los países penalizan la incitación al odio[1131].

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].

1127 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.*

1128 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: http://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.

1129 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1130 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1131 For an overview of hate speech legislation, see the database provided at: http://www.legislationline.org.

Convenio sobre la Ciberdelincuencia

Como las Partes que negociaron el Convenio sobre la Ciberdelincuencia no pudieron llegar a un acuerdo[1132] en lo que respecta a la penalización de este tipo de material, las disposiciones relativas a este asunto se integraron en un Primer Protocolo independiente del Convenio sobre la Ciberdelincuencia[1133].

El Artículo

> ***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.*

1132 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."

1133 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

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. Cualquier 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.

Una de las principales dificultades que entraña la penalización del material xenófobo es lograr un equilibrio entre la libertad de expresión[1134], por una parte, y la violación de los derechos de las personas o grupos, por la otra. Sin entrar en detalles acerca de la negociación del Convenio sobre la Ciberdelincuencia[1135] ni de la situación de las firmas/ratificaciones del Protocolo Adicional[1136], ha quedado demostrado que las diferencias en cuanto al grado de protección de la libertad de expresión dificultan el proceso de armonización[1137]. En lo que respecta especialmente al principio común de doble incriminación[1138], la falta de armonización dificulta la aplicación de la ley en los casos de alcance internacional[1139].

1134 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

1135 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

1136 Regarding the list of states that signed the Additional Protocol see above: Chapter 5.1.4.

1137 Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/Computer Law Review International(2000)27.pdf.

1138 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1139 Regarding the challenges of international investigation see above: Chapter 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.

Proyecto de Convenio de Stanford

El Proyecto de Convenio de Stanford[1140] 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[1141]. El Convenio reconoce los distintos enfoques y deja a los Estados que decidan acerca de la penalización de estos aspectos[1142].

6.1.9 Delitos contra la religión

El grado de protección de las religiones y sus símbolos varía según el país[1143].

Convenio sobre la Ciberdelincuencia

Las negociaciones sobre este tema entre las Partes en el Convenio sobre la Ciberdelincuencia experimentaron las mismas dificultades que en el caso del material xenófobo[1144]. 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 Artículos.

Los Artículos

> ***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.

1140 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: http://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.

1141 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1142 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1143 Regarding the 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: http://www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf.

1144 See above: Chapter 6.1.h as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

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 contiene dos disposiciones que giran en torno a los delitos relacionados con Internet[1145]:

> ***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[1146]. Como se indicó anteriormente, las diferencias en cuanto al grado de protección de la libertad de expresión dificultan el proceso de armonización[1147]. En lo que respecta especialmente al principio común de doble incriminación[1148], la falta de armonización dificulta la aplicación de la ley en los casos de alcance internacional[1149].

1145 The draft law was not in power, at the time this publication was finalised.

1146 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, 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 seqq; 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: http://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: http://www.fas.org/sgp/crs/misc/95-815.pdf.

1147 Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ Computer Law Review International(2000)27.pdf.

1148 Dual criminality exists if the offence is a crime under both the requestor 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 http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1149 Regarding the challenges of international investigation see above: Chapter 3.2.f 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.

6.1.10 Juego ilegal

El creciente número de sitios web que ofrecen juego ilegal es motivo de preocupación[1150], dado que puede utilizarse para burlar la prohibición del juego que aplican algunos países[1151]. 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[1152].

Ejemplo de legislación nacional

El Convenio 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 adición[1153] al juego, para lo cual define los procedimientos para la organización de estos juegos[1154]. Aunque no hace referencia explícita a los juegos de azar por Internet, éstos también quedan comprendidos[1155]. 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[1156]. Esta penalización transciende las consecuencias de la ayuda y la instigación, dado que los infractores pueden ser objeto de sentencias más graves[1157].

1150 The 2005 eGaming data report estimates the total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: http://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: http://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.

1151 For an overview of different national Internet gambling legislation, see: "Internet Gambling – An overview of the Issue", GAO-03-89, page 45 et seqq., available at: http://www.gao.gov/new.items/d0389.pdf.

1152 Regarding the situation in the People's Republic of China, see for example: "Online Gambling challenges China's gambling ban", available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

1153 Regarding the addiction see: *Shaffer*, Internet Gambling & Addiction, 2004 , available at: http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf ; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: https://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: http://www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

1154 See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

1155 See *Thumm*, Strafbarkeit des Anbietens von Internetgluecksspielen gemaess § 284 StGB, 2004.

1156 Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which did not know that their services were abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

1157 For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously the criminalisation is limited to those cases where the offender is intentionally making the equipment available.

Para evitar la investigación penal el operador de sitios web de juego ilegal puede desplazar físicamente sus actividades[1158] a países que no penalizan el juego[1159]. Este desplazamiento supone un problema para las fuerzas de seguridad por cuanto el hecho de que el servidor se encuentre fuera del territorio nacional[1160] no impide, en general, que un usuario acceda al mismo desde dentro del país[1161]. Para que las fuerzas de seguridad tengan mayores posibilidades de luchar contra el juego ilegal, el Gobierno Alemán ha extendido la penalización al usuario[1162]. 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 días de multa.*

Si el infractor utiliza los sitios de juego en línea para lavar activos, la identificación del infractor suele resultar difícil[1163]. Un ejemplo de método[1164] para impedir el juego ilegal y el lavado de activos es la Ley sobre el juego ilegal por Internet de Estados Unidos de 2005[1165].

> ***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.*

1158 This is especially relevant with regard to the location of the server.

1159 Avoiding the creation of those safe havens is a major intention of harmonisation processes. The issue of safe havens was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out 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: http://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*".

1160 With regard to the principle of sovereignty changing the location of a server can have a great impact on the ability of the 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: http://www.law.uga.edu/intl/roth.pdf.

1161 Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene see above: Chapter 3.2.6 and Chapter 3.2.7.

1162 For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

1163 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: http://www.gao.gov/new.items/d0389.pdf.

1164 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 Approache sin the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: http://www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

1165 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: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm. *Shaker*, Americas'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.

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 refuse 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[1166]. 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[1167]. El incumplimiento de esta prohibición puede ser objeto de sanciones penales[1168]. 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 afecta solamente a la persona dedicada al negocio de apuestas y juego de dinero sino en general a toda institución financiera. 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. La incidencia internacional de los posibles conflictos que surjan de este reglamento en relación al Acuerdo General sobre el Comercio de Servicios (AGCS)[1169] se está investigando[1170].

6.1.11 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[1171] y los problemas logísticos que conlleva la inmensa cantidad de información disponible en Internet[1172] son parámetros favorables a este tipo de actos.

La cuestión de si debe penalizarse la difamación es un tema de debate polémico[1173]. 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[1174]. 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:

1166 *Landes*, "Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation", available at: http://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: http://www.gamblingandthelaw.com/columns/2006_act.htm.

1167 *Rose*, "Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed", 2006, available at: http://www.gamblingandthelaw.com/columns/2006_act.htm.

1168 Based on Sec. 5366 the criminalisation is limited to the acceptance of financial instruments for unlawful Internet gambling.

1169 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.

1170 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: http://www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

1171 See above: Chapter 3.2.l.

1172 See above: Chapter 3.2.2.

1173 See for example: Freedom of Expression, Free Media and Information, Statement of Mr. *McNamara*, United States 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: http://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: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://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.

1174 See for example the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE

"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."[1175]

Pese a estas inquietudes, algunos países[1176] 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[1177], mientras que en Alemania las estadísticas penales registran 187 527 delitos de difamación en 2006[1178]. El Convenio sobre la Ciberdelincuencia, la Lay Modelo de la Commonwealth y el Proyecto de Convenio 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[1179].

La disposición

> ***365 Difamación penal***[1180]
>
> *(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 un delito menor. 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:

Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information see: http://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 at the 25th of February 2005.

1175 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: http://www.osce.org/documents/rfm/2004/10/14893_en.pdf. European Convention of Human Rights and the constitutional principle of freedom of expression — the cornerstone of all modern democracies — the European Court of Human Rights, the United States Supreme Court, the UN Rapporteur on Freedom of Opinion and Expression, the OAS Special Rapporteur on Freedom of Expression, the OSCE Representative on Freedom of the Media, constitutional and supreme courts of many countries, and respected international media NGOs have repeatedly stated that criminal defamation laws are not acceptable in modern democracies. These laws threaten free speech and inhibit discussion of important public issues by practically penalising political discourse. The solution that all of them prefer and propose is to transfer the handling of libel and defamation from the criminal domain to the civil law domain".

1176 Regarding various regional approaches regarding the criminalisation of defamation see Greene (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: http://www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf.

1177 For more details see the British Crime Survey 2006/2007 published in 2007, available at: http://www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

1178 See Polizeiliche Kriminalstatistik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

1179 The full version of the Criminal Defamation Amendment Bill 2002 is available at: http://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: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf.

1180 The full text of the Criminal Code of Queensland, Australia is available at: http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

La 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.

6.1.12 Correo basura

Dado que el 75 por ciento[1181] de todos los mensajes de correo electrónico son correo basura[1182], se ha debatido detenidamente acerca de la necesidad de penalizar el envío de este tipo de mensajes[1183]. Las medidas adoptadas en la legislación nacional sobre este particular varían de un país a otro[1184]. 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[1185]. 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[1186]. 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[1187].

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 sobre la Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia no penaliza de manera expresa el correo basura[1188]. Se propone que la penalización de estos actos debe limitarse a los casos en los que hay una clara intención de dificultar la

---

1181 The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see http://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 http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

1182 For a more information on the phenomenon see above: Chapter 2.5.g. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1183 Regarding the development of spam e-mails, see: *Sunner*, "Security Landscape Update 2007", page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1184 See "ITU Survey on Anti-Spam Legislation Worldwide, 2005", available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1185 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: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf

1186 "Spam Issues in Developing Countries", a. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

1187 See "Spam Issues in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

1188 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

comunicación de manera grave y deliberada[1189]. 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 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 de Stanford

El Proyecto de Convenio de Stanford[1190] de 1999 no prevé la penalización del correo basura. Al igual que el Convenio 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.

Ejemplo de legislación nacional

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. Ahora bien, sus efectos sobre la actividad comercial no pueden enjuiciarse, siempre que no afecte al sistema informático. En algunos países se adopta un enfoque distinto. Como ejemplo, puede citarse la legislación de Estados Unidos – 18 U.S.C. § 1037[1191].

> ***§ 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*

1189 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."

1190 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: http://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.

1191 Regarding the United States 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 U.S. conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 et. seq. , available at: http://www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

(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[1192]. La finalidad de esta ley era crear una única norma nacional destinada a controlar el envío de mensajes comerciales de correo electrónico[1193]. 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[1194]. En el 18 U.S.C. § 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[1195]. Además la disposición penaliza el acceso no autorizado a computadores protegidos y el inicio de transmisiones de múltiples mensajes comerciales de correo electrónico.

6.1.13 Abuso de los dispositivos

Otro problema grave es la disponibilidad de software y hardware diseñados para cometer delitos[1196]. 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[1197]. 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[1198].

1192 For more details about the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" – short: CAN-SPAM act 2003 see: http://www.spamlaws.com/f/pdf/pl108-187.pdf.

1193 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)).

1194 For more details see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1195 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.

1196 "Websense Security Trends Report 2004", page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; "Information Security – Computer Controls over Key Treasury Internet Payment System", GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

1197 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.

1198 One example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

Convenio sobre la Ciberdelincuencia

Tomando en consideración otras iniciativas del Consejo de Europa, los redactores del Convenio 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:[1199]

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[1200] diseñados para cometer y promover el ciberdelito como las contraseñas que permiten acceder a un sistema informático.

- El término "dispositivo" incluye tanto a los hardware como a los software concebidos 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[1201].
- "Una contraseña, un código de acceso o datos informáticos similares" son elementos disímiles que no efectúan operaciones sino que facilitan códigos de acceso. En este contexto, se trató de determinar si la

1199 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".

1200 With its 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.

1201 Explanatory Report to the Council of Europe Convention on Cybercrime No 72.

disposición incluía la publicación de las vulnerabilidades del sistema[1202]. A diferencia de las vulnerabilidades clásicas, las de los sistemas de códigos de acceso no permiten forzosamente 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 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. La legislación de la Unión Europea aplica un enfoque similar (limitado en los dispositivos diseñados para eludir disposiciones de orden técnico) en lo tocante a la armonización de los derechos de autor[1203], y en cierto número de países se han adoptado disposiciones similares en la esfera del derecho penal[1204].

- Por "distribución" se entiende el acto deliberado de transmitir dispositivos o contraseñas a otros[1205].
- "Venta" incluye las actividades inherentes a la venta de dispositivos y contraseñas a cambio de dinero o alguna otra forma de compensación.

1202 See in this context *Biancuzzi*, The Law of Full Disclosure, 2008, available at: http://www.securityfocus.com/print/columnists/466.

1203 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation 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.

1204 See for example one approach in the United States legislation:

18 U.S.C. § 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. […]

1205 Explanatory Report to the Council of Europe Convention on Cybercrime No 72.

- "Obtención para su utilización" se refiere al acto de obtener activamente contraseñas y dispositivos[1206]. 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" de utilizarlos con objeto de cometer cualquiera de los delitos consignados en los Artículos 2 a 5.

La importación implica el acto de obtener dispositivos y códigos de acceso procedentes de países extranjeros[1207]. 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 cabe poner en tela de juicio la conveniencia de que la adquisición de dichos instrumentos sólo se penalice si puede vincularse a la utilización de los mismos, en el Artículo 6 del Convenio sobre la Ciberdelincuencia sólo se contempla la 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[1208]. 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[1209].

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[1210], esta disposición no sólo se aplica a los dispositivos diseñados exclusivamente para facilitar la comisión de un ciberdelito, sino que el Convenio 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[1211].

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 se abordan estos aspectos de tres maneras distintas[1212]:

1206 This approach could lead to a broad criminalization. Therefore Art. 6, Subparagraph 3 Convention on Cybercrime enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.

1207 Art. 6, Subparagraph 3 Convention on Cybercrime enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.

1208 Explanatory Report to the Council of Europe Convention on Cybercrime No 72.

1209 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".*

1210 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

1211 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.

1212 Regarding the United States approach to address the issue see for example 18 U.S.C. § 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.

- A tenor de lo dispuesto en el párrafo 1 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[1213]. 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"[1214].
- 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 b) se amplía aún más el alcance de la reglamentación consignada en el párrafo 1 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[1215]. 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[1216]. El Convenio 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 sobre la Ciberdelincuencia, en el Artículo 6 se exige que el delincuente cometa el delito deliberadamente[1217]. 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[1218].

1213 *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1214 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'."

1215 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 731.

1216 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: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

1217 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1218 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

Sin derecho

De manera similar a las disposiciones antes examinadas, los actos deben cometerse "sin derecho"[1219]. 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"[1220].

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 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 a); entre éstas figura por ejemplo la producción de dichos dispositivos[1221].

Ley Modelo de la Commonwealth

En la Sección 9 de la Ley Modelo de la Commonwealth de 2002[1222] se aplica un enfoque que está en consonancia con el Artículo 6 del Convenio sobre la Ciberdelincuencia:

> ***Sección 9***
>
> *1. Una persona comete un delito si:*
>
> *a) deliberada o imprudentemente, sin una excusa o justificación legal, 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.*

1219 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.

1220 Explanatory Report to the Council of Europe Convention on Cybercrime No 77.

1221 For more information see: Explanatory Report to the Council of Europe Convention on Cybercrime No 78.

1222 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

La principal diferencia con el Convenio sobre la Ciberdelincuencia estriba en el hecho de que la Ley Modelo de la Commonwealth penaliza los actos de imprudencia. Durante las negociaciones entabladas en torno a la Ley Modelo de la Commonwealth, se consideraron nuevas enmiendas a la disposición que penaliza 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[1223]. Canadá propuso que se aplicase un enfoque similar, sin definir previamente el número de artículos que justificarían la penalización[1224].

Proyecto de Convenio de Stanford

El Proyecto de Convenio de Stanford de 1999[1225], 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[1226]. La única excepción está relacionada con los dispositivos ilegales[1227]. 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[1228].

6.1.14 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,

---

1223 Expert Groups suggest 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: S*ubsection 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.*

1224 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: S*ubsection 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.*

1225 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: http://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.

1226 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1227 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1228 "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: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

debido a la digitalización, la situación está cambiando[1229]. 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*")[1230].

Convenio sobre la ciberdelincuencia

En la mayoría de los sistemas de derecho penal se penaliza la falsificación de documentos tangibles[1231]. Los redactores del Convenio señalaron que la estructura dogmática de los enfoques jurídicos varía según el país[1232]. Mientras un concepto se basa en la autenticidad del autor del documento, 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[1233].

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.*

1229 See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

1230 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.

1231 See for example 18 U.S.C. § 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.

1232 See Explanatory Report to the Council of Europe Convention on Cybercrime No 82.

1233 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."

Objetos contemplados

El objetivo de una falsificación informática son los datos, independientemente del hecho de que éstos sean legibles y/o inteligibles directamente. En el Convenio se definen los datos informáticos[1234] 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[1235]; en la disposición no se contempla la falsificación de datos que no puedan utilizarse con fines jurídicos.

1) Los actos contemplados son los siguientes:

- La "introducción" de datos[1236] debe corresponderse con la producción de un documento falso tangible[1237].
- El término "alteración" se refiere a la modificación de los datos existentes.[1238] En el Informe Explicativo se subrayan particularmente las variaciones y los cambios parciales[1239].
- El término "supresión" de datos informáticos describe una acción que afecta la disponibilidad de datos[1240]. En el Informe Explicativo los redactores se referían en particular a la retención o el ocultamiento de datos[1241]. 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[1242]. El Informe Explicativo se refiere únicamente a la eliminación de datos de un medio de datos[1243], 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[1244].

Predisposición

Al igual que todos los otros delitos definidos en el Convenio sobre la Ciberdelincuencia, en el Artículo 3 se exige para penalizar que el delincuente lleve a cabo los actos delictivos intencionalmente[1245]. El Convenio no contiene una definición del término "internacionalmente". Los redactores del Informe Explicativo señalaron que el término "intencionalmente" debía considerarse a nivel nacional[1246].

1234 See Art. 1 (b) Convention on Cybercrime.

1235 Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

1236 For example by filling in a form or adding data to an existing document.

1237 See Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

1238 With regard the definition of "alteration" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

1239 See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.

1240 With regard the definition of "suppression" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1241 See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.

1242 With regard the definition of "deletion" see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1243 See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.

1244 If only part of a document is deleted the act might also be covered by the term "alteration".

1245 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1246 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

Sin derecho

Los actos de falsificación sólo pueden penalizarse a tenor del Artículo 7 del Convenio siempre que éstos se realicen "sin derecho"[1247].

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[1248].

Ley Modelo de la Commonwealth

La Ley Modelo de la Commonwealth de 2002 no contiene ninguna disposición que penalice la falsificación informática[1249].

Proyecto de Convenio de Stanford

El Proyecto de Convenio de Stanford de 1999, de carácter oficioso[1250], 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 sobre la Ciberdelincuencia estriba en el hecho de 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 sobre la Ciberdelincuencia

---

1247 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.

1248 See Explanatory Report to the Council of Europe Convention on Cybercrime No 85.

1249 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1250 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: http://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.

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.

6.1.15 Usurpación de identidad

Tomando en consideración la cobertura media[1251], los resultados de los estudios efectuados recientemente[1252], así como las numerosas publicaciones jurídicas y técnicas[1253] en este ámbito, es apropiado considerar la usurpación de identidades como un fenómeno de masas[1254]. 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[1255]. 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[1256].

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[1257]. 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[1258]:

- 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 disposición que penaliza 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).

Ejemplo de un método con una disposición única

Los ejemplos más conocidos de métodos con una disposición única son los consignados en 18 U.S.C. § 1028(a)(7) y 18 U.S.C. 1028A(a)(1). Las disposiciones abarcan una amplia gama de delitos relacionados con

---

1251 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*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

1252 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.

1253 See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://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: http://www.privacyrights.org/ar/id_theft.htm.

1254 Regarding the phenomenon of identity theft see above: Chapter 2.7.3.

1255 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.

1256 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.

1257 *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.

1258 *Gercke*, Internet-related Identity Theft, 2007, available at: http://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.

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[1259]. 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

1259 This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data see above *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, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

muy amplia[1260]. 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[1261]. En otras palabras, las disposiciones 8 U.S.C. § 1028(a)(7) y 18 U.S.C. 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[1262]. No se tipifica como delito la posesión de datos relacionados con la identidad sin intención de utilizarlos[1263].

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 U.S.C. § 1028(a)(7) no está relacionada con un delito específico (como el fraude).

Ejemplo de un enfoque con múltiples disposiciones

La principal diferencia entre el Convenio 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 no se define un ciberdelito separado de la utilización ilegal de información relacionada con la identidad[1264]. Análogamente a lo que ocurre con respecto a la penalización de la obtención de información relacionada con la identidad, el Convenio no contempla todos los actos posibles relacionados con la utilización ilegal de información personal.

Fase 1

El Convenio sobre la Ciberdelincuencia[1265] 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)[1266]

1260 The reason for the success is the fact that the provisions are focussing on the most relevant aspect of phase 1: the transfer of the information from the victim to the offender.

1261 Examples for acts that are not covered is the illegal access to a computer system in order to obtain identity related information.

1262 One of the most common ways the obtained information are used are linked to fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1263 Further more it is uncertain if the provisions criminalise the possession if the offender does not intent to use them but sell them. The prosecution could in this case in general be based on fact that 18 U.S.C. § 1028 does not only criminalise the possession with the intent to use it to commit a crime but also to aid or abet any unlawful activity.

1264 See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.

1265 Similar provisions are included in the Commonwealth Model Law and the Draft Stanford 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: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Draft Stanford 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: http://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.

1266 See above: Chapter 6.1.1.

- Interceptación ilícita (Artículo 3)[1267]
- Interferencia de los datos (Artículo 4)[1268].

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 sobre la Ciberdelincuencia es el espionaje de datos.

Fase 2

El Convenio 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.

Fase 3

En el Convenio 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[1269]. 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[1270]. 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 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. No es posible, en particular, entablar un juicio por utilización de información relacionada con la identidad con la intención de ocultar la identidad.

6.1.16 Fraude informático

El fraude es un delito muy propagado en el ciberespacio[1271]. Se trata asimismo de un problema común más allá de Internet, por lo cual la mayoría de las leyes nacionales contienen disposiciones que penalizan este tipo de delito[1272]. 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[1273]. 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[1274].

1267 See above: Chapter 6.1.3.

1268 See above: Chapter 6.1.4.

1269 *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1270 See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1271 See above: Chapter 2.7.1.

1272 Regarding the criminlisation of computer-related fraud in the UK see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 et seq.

1273 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.

1274 A national approach that is explicitly address computer-related fraud is 18 U.S.C. § 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,

Convenio sobre la Ciberdelincuencia

El Convenio 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 relacionado con el fraude informático, a saber[1275]:

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[1276].

- Por "introducción" de datos informáticos se entiende todo tipo de manipulación de insumos, como por ejemplo alimentar al computador con datos incorrectos, así como manipulaciones de programas informáticos y demás interferencias con el procesamiento de datos[1277].
- El término "alteración" se refiere a la modificación de los datos existentes[1278].
- El término "supresión" de datos informáticos indica una acción que afecta la disponibilidad de datos[1279].
- El término "borrado" se corresponde con la definición que figura en el Artículo 4 y abarca actos como resultados de los cuales se elimina información[1280].

---

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 U.S.C. 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.

1275 Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

1276 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.

1277 Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

1278 With regard the definition of "alteration" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

1279 With regard the definition of "suppression" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

1280 With regard the definition of "deletion" see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

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[1281].

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[1282].

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 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[1283].

Predisposición

Como ocurre con los otros delitos enumerados, en el Artículo 8 del Convenio 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[1284]. 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[1285].

Sin derecho

El fraude informático sólo puede penalizarse a tenor del Artículo 8 del Convenio si tiene lugar "sin derecho"[1286]. Esto incluye el requisito de que el beneficio económico debe ser obtenido sin derecho. Los redactores del Convenio subrayaron que los actos efectuados en el marco de un contrato válido entre las personas afectadas no son considerados actos sin derecho[1287].

1281 As a result, not only data- related offences, but also hardware manipulations, are covered by the provision.

1282 Explanatory Report to the Council of Europe Convention on Cybercrime No 87.

1283 Explanatory Report to the Council of Europe Convention on Cybercrime No 88.

1284 "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."

1285 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.

1286 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.

1287 Explanatory Report to the Council of Europe Convention on Cybercrime No 90.

Ley Modelo de la Commonwealth

La Ley Modelo de la Commonwealth de 2002 no contiene disposición alguna que penalice el fraude informático[1288].

Proyecto de Convenio Stanford

El Proyecto de Convenio Stanford de 1999, de carácter oficioso[1289], no contiene disposición alguna que penalice el fraude informático.

6.1.17 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[1290]. 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[1291].

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[1292], pero hasta la fecha se ha esquivado el efecto de estas medidas muy poco tiempo después de su introducción[1293]. 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[1294].

1288 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1289 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: http://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.

1290 Regarding the ongoing transition process, see: "OECD Information Technology Outlook 2006", Highlights, page 10, available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.

1291 For more information on the effects of the digitalisation for the entertainment industry see above: Chapter 2.6.a.

1292 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 the copy protection that 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: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

1293 Regarding the technical approach of copyright protection see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: http://www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

1294 For details see above: Chapter 2.6.1.

Convenio sobre la Ciberdelincuencia

Por consiguiente, en el Convenio se ha incluido una disposición para penalizar estas infracciones de la propiedad intelectual, con la cual se intenta armonizar las diversas reglamentaciones consignadas en las leyes nacionales:

> ***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[1295] y se abordan en cierto número de tratados internacionales[1296]. En el Convenio se estipulan los principios fundamentales que

---

1295 Examples are 17 U.S.C. § 506 and 18 U.S.C. § 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) oftitle 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.

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[1297].

Referencia a acuerdos internacionales

A diferencia de lo que ocurre con otros instrumentos jurídicos, en el Convenio no se designan explícitamente los actos que se han de penalizar, sino que se hace referencia a cierto número de acuerdos internacionales[1298]. 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 obliga o no a los Estados signatarios a firmar los acuerdos mencionados en el Artículo 10. Los redactores del Convenio señalaron que en el Convenio sobre la Ciberdelincuencia no se incluiría ninguna obligación de ese tipo.[1299]. Así pues, los Estados que no hayan firmado los acuerdos internacionales mencionados no 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 limita la penalización a aquellos actos que hayan sido cometidos por conducto de un sistema informático[1300]. 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

---

(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: http://www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

1296 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: http://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: http://www.unctad.org/en/docs/iteipc200610_en.pdf; Regarding international approaches of anti-circumvention laws see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: http://www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

1297 Explanatory Report to the Council of Europe Convention on Cybercrime No. 109.

1298 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."

1299 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."

1300 Explanatory Report to the Council of Europe Convention on Cybercrime No. 16 and 108.

(ADPIC)[1301], que gobierna la obligación de penalizar las infracciones relacionadas con la propiedad intelectual[1302].

Escala comercial

La limitación de la penalización a actos que se cometen a escala comercial también tiene en cuenta el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio (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 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[1303].

Sin derecho

Por lo general, en las disposiciones fundamentales de derecho penal definidas en el Convenio sobre la Ciberdelincuencia se impone el requisito de que el acto sea realizado "sin derecho"[1304]. Los redactores del Convenio subrayaron que el término "infracción" ya implica la realización de un acto sin autorización[1305].

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 Stanford

El Proyecto de Convenio Stanford de 1999, de carácter oficioso[1306], 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

---

1301 *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.

1302 Explanatory Report to the Council of Europe Convention on Cybercrime No. 113.

1303 Explanatory Report to the Council of Europe Convention on Cybercrime No. 114.

1304 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.

1305 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.

1306 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: http://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.

hubiera resultado difícil[1307]. En su lugar éstos hacen referencia directamente a los acuerdos internacionales en vigor[1308].

6.2 Derecho procesal

6.2.1 Introducción

Según se explica en los puntos anteriores, la lucha contra la ciberdelincuencia exige que el derecho procesal contenga disposiciones fundamentales apropiadas[1309]. 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[1310]. 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[1311]. 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[1312].

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[1313]. Si el infractor se encuentra en otro país[1314], 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[1315].

Las autoridades de varios países ya disponen de instrumentos que les permiten investigar ciberdelitos y otros delitos tradicionales analizando datos informáticos[1316]. 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

---

1307 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1308 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1309 See above: Chapter 4.4.1 and Chapter 6.1.

1310 This was as well highlighted by the drafters of the Council of Europe Convention on Cybercrime that 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: Chapter 6.1.

1311 Regarding the elements of a Anti-Cybercrime strategy see above: xxx. Regarding user-based approaches in the fight against Cybercrime see: *Görling*, The Myth Of User Education, 2006 at http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See as well the comment made by *Jean-Pieree 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."

1312 Due to the protocols used in Internet communication and the 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: Chapter 3.2.7.

1313 Regarding the challenges of fighting Cybercrime see above: Chapter 3.2.

1314 The pure fact that the offender is acting from a different country can go along with additional challenges for the law enforcement agencies as the investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases the investigation never the less requires an international cooperation of the authorities in both countries that in general is more time consuming compared to investigations concentrating on a single country.

1315 See in this context as well: Explanatory Report to the Council of Europe Convention on Cybercrime No. 134.

1316 For an overview about 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: http://www.coe.int/cybercrime/.

los ciberdelitos[1317]. 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.

6.2.2 Investigaciones sobre equipos informáticos e Internet (Criminología informática)

Existen varias definiciones de la "criminología informática"[1318]. Puede definirse como "examen de equipos y sistemas informáticos para obtener información en investigaciones penales o civiles"[1319]. Los delincuentes, tanto tradicionales como informáticos, suelen dejar rastros[1320]. 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[1321]. 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[1322] y plantean dificultades particulares[1323].

Por lo general, ambos aspectos de las investigaciones cibercriminológicas están estrechamente relacionados y reciben a menudo el calificativo general de "criminología informática", o compilación y análisis de pruebas[1324]. Como hemos dicho, la expresión criminología informática significa utilización de técnicas informáticas de investigación y análisis para estudiar posibles pruebas, que pueden consistir en análisis generales tales como la búsqueda de pornografía infantil en discos duros informáticos[1325], o investigaciones específicas tales como

---

1317 See Art. 15 – 21 Council of Europe Convention on Cybercrime.

1318 *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: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://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.

1319 *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

1320 For an overview on different kind 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: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

1321 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

1322 For an overview about 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: https://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: http://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: https://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

1323 *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

1324 See in this context ABA International Guide to Combating Cybercrime, 128 et seq.

1325 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.

estudios criminológicos de iPod[1326] y acceso a archivos cifrados[1327]. Expertos en criminología informática ayudan en sus investigaciones a funcionarios de policía y fiscales especializados. En las investigaciones sobre Internet, los expertos en criminología informática pueden prestar asistencia, por ejemplo, en las situaciones siguientes[1328]:

- buscar posibles rastros digitales (especialmente la posible ubicación de datos de tráfico)[1329];
- ayudar a proveedores de servicios Internet a identificar la información que pueden proporcionar para facilitar las investigaciones;
- proteger los datos compilados y garantizar su custodia[1330].

Una vez identificadas las pruebas potenciales, los expertos también pueden ayudar, por ejemplo, en las situaciones siguientes:

- proteger el sistema informático estudiado contra posibles alteraciones o deterioraciones de los datos durante el análisis[1331];
- descubrir todos los ficheros pertinentes en el sistema informático o el medio de almacenamiento estudiado[1332];
- descifrar los archivos cifrados[1333];
- recuperar ficheros suprimidos;
- identificar la utilización del sistema informático cuando más de una persona tiene acceso al aparato o dispositivo[1334];
- desvelar el contenido de los ficheros temporales utilizados por aplicaciones y el sistema operativo;
- analizar las pruebas reunidas[1335];
- documentar el análisis[1336];

1326 *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2.

1327 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

1328 Regarding the models of Forensic Investigations see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.

1329 *Gercke*, Cybercrime Training for Judges, 2009, page 56, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

1330 This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.

1331 This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.

1332 This includes stored files as well as deleted files that have not yet been completely removed from the hard disk. In addition experts might be able to identify temporary, hidden or encrypted files. *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.

1333 Regarding legal approaches related to the use of encryption technology see below: Chapter 6.2.9.

1334 *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1.

1335 *Gercke*, Cybercrime Training for Judges, 2009, page 55, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1336 Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at: http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

- facilitar pruebas para investigaciones más detalladas;
- proporcionar opiniones y testimonios en calidad de expertos.

La participación de peritos judiciales en la protección de la integridad de las pruebas demuestra en particular que su labor aúna aspectos técnicos y jurídicos. Una de las mayores dificultades en estos casos es garantizar la integridad de los datos originales y tener en cuenta las grandes exigencias de la labor práctica de los peritos judiciales[1337].

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.

6.2.3 Salvaguardias

Durante los últimos años, las autoridades competentes de todo el mundo han destacado la urgente necesidad de instrumentos de investigación apropiados[1338] 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[1339], 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[1340]. 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[1341]. 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[1342]. 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[1343]. Por consiguiente, los redactores decidieron no incorporar

---

1337 Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at: http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

1338 See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801 for further reference.

1339 *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 Finacial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at http://www.ccc.de.

1340 See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 et seqq.

1341 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.

1342 See above: Chapter 5.1.4.

1343 "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

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[1344].

> ***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[1345]. 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[1346], en el Convenio sobre la Ciberdelincuencia se definen las normas mínimas haciendo referencia a marcos fundamentales tales como los siguientes:

- 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;
- 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[1347], 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.

---

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.

1344 "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.

1345 For the transformation of safeguards to 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.

1346 This is especially relevant with regard to the protection of the suspect of an investigation.

1347 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.

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 ingerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta ingerencia 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[1348]. La jurisprudencia tiene particularmente en cuenta la gravedad de la ingerencia de la investigación[1349], su objeto[1350] y su proporcionalidad[1351]. Los principios fundamentales que se pueden extraer de la jurisprudencia son los siguientes:

- los instrumentos de investigación necesitan una base jurídica suficiente[1352];
- la base jurídica debe ser clara con respecto al objeto[1353];
- las competencias de las autoridades competentes deben ser previsibles[1354];
- la intervención de las comunicaciones sólo puede justificarse cuando se trata de delitos graves[1355].

Por otra parte, en el Artículo 15 del Convenio sobre la Ciberdelincuencia se tiene en cuenta el principio de proporcionalidad[1356]. Esta disposición es particularmente pertinente para los Estados signatarios que no son

---

1348 ABA International Guide to Combating Cybercrime, page 139.

1349 "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.

1350 "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.

1351 "Powers of secret surveillance of citizens, characterising 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.

1352 "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.

1353 "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.

1354 "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.

1355 "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, characterising 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.

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[1357], 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[1358].

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:

- Distinción entre la interceptación de datos relativos al contenido (Artículo 21)[1359] y la obtención de datos relativos al tráfico (Artículo 20)[1360]. A diferencia de la obtención de datos relativos al tráfico, la interceptación de datos relativos al contenido se limita a los delitos graves[1361].
- Distinción entre la orden de conservación rápida de datos informáticos almacenados (Artículo 16)[1362] y la de presentación de datos informáticos almacenados en cumplimiento de una orden de presentación (Artículo 18)[1363]. El Artículo 16 sólo permite que las autoridades competentes ordenen la conservación de los datos, pero no su revelación[1364].

1356 "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.

1357 The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 146.

1358 "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.

1359 See below 6.2.9.

1360 See below 6.2.10.

1361 "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.

1362 See below 6.2.4.

1363 See below 6.2.7.

1364 As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorise the law enforcement agencies to prevent the deletion of the relevant data. The advantage of a 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.

- Distinción en el Artículo 18[1365] entre la obligación de comunicar "datos relativos a los abonados"[1366] y "datos informáticos"[1367].

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.

6.2.4 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[1368]. En particular, la dirección IP utilizada por el infractor puede ayudar a las autoridades competentes a seguir su rastro. 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[1369].

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)[1370].

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[1371].

> ***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

---

1365 As described more in detail below the differentiation between "computer data" and "subscriber information" the Art. 18 Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.

1366 A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 Convention on Cybercrime.

1367 A definition of the term "computer data" is provided in Art. 1 Convention on Cybercrime.

1368 "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, 577 et seq.

1369 *Gercke*, Preservation of User Data, DUD 2002, 578.

1370 The cost issue was especially raised within the discussion about 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: http://www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

1371 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.

datos pertinentes durante el proceso de investigación, que puede ser bastante largo. A este respecto, se estudian actualmente dos planteamientos diferentes[1372]:

- conservación de datos;
- 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[1373]. En los sistemas legislativos más recientes se han de conservar los registros durante 6 a 24 meses[1374]. De este modo, las autoridades competentes pueden consultar los datos necesarios para identificar a los infractores incluso varios meses después del delito[1375]. El Parlamento de la Unión Europea adoptó recientemente una obligación de conservación de datos[1376], obligación que también se está examinando actualmente en Estados Unidos[1377]. 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[1378]. 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[1379]. Los redactores del Convenio sobre la Ciberdelincuencia prefirieron

---

1372 The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantaged 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. 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.

1373 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.

1374 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.

1375 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."

1376 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.

1377 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 StoppingAdults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: http://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.

1378 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

1379 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.

centrarse en la "conservación de los datos" en lugar de la "retención de datos"[1380]. 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[1381]. 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[1382]. 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[1383], 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[1384]. 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[1385]. De este

---

1380 Gercke, Cybercrime Training for Judges, 2009, page 63, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1381 See Gercke, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

1382 '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.

1383 Explanatory Report No 152.

1384 Regarding the advantages of a system of graded safeguards see above: Chapter 6.2.3.

1385 "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.

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[1386].

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[1387]. 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

---

1386 The drafters of the Convention on Cybercrime tried to approach the problems related to the need of immediate action from law enforcement agencies on the one hand side and the importance of ensuring safeguards on the other hand side 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."

1387 *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

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[1388] 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[1389].

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[1390]. 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[1391]. 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[1392].

La disposición:

> ***Sección 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*

1388 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 does only enable 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.

1389 If the offender is using services that do not require a registration or the subscriber information provided by the user are 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).

1390 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

1391 "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.

1392 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

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;

(c)[1393] *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.*

Sección 16[1394]

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;

(b) el trayecto por el cual se ha transmitido la comunicación.

Sección 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;

(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.

6.2.5 Conservación de datos

La obligación de conservación de datos fuerza al proveedor de servicios Internet a salvaguardar datos de tráfico durante cierto tiempo[1395]. 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. La Directiva de la Unión Europea sobre la conservación de datos[1396] es un ejemplo de ese tipo de planteamiento.

1393 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.*

1394 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.

1395 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.

1396 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.

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[1397], lo cual podría a su vez provocar una revisión de la Directiva y de su aplicación en tribunales constitucionales[1398]. Además, en su conclusión en el caso Productores de Música de España (Promusicae) contra Telefónica de España[1399], Juliane Kokott, Abogada General ante el Tribunal Europeo de Justicia, señaló que le parecía poco probable que se pudiera aplicar la obligación de conservación de datos sin violar derechos fundamentales[1400]. En 2001 el G8 ya señaló dificultades con respecto a la aplicación de ese tipo de reglamentaciones[1401].

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[1402];
- la utilización de servicios de comunicación anónimos explotados (al menos parcialmente) en países en los cuales no es obligatorio conservar los datos[1403].

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[1404].

1397 See for example: Briefing for the Members of the European Parliament on Data Retention, available at: http://www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf; Regarding the concerns related to a 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.

1398 See: Heise News, 13,000 determined to file suit against data retention legislation, 17.11.2007, available at: http://www.heise.de/english/newsticker/news/99161/from/rss09.

1399 Case C-275/06.

1400 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 does usually but not invariably follow the advisors conclusion.

1401 In a G8 Meeting in Tokyo experts discussed the advantaged 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.

1402 Regarding the challenges for law enforcement agencies related to the use of means of anonymous communication see above: Chapter 3.2.12.

1403 Regarding the technical discussion about traceability and anonymity see: CERT Research 2006 Annual Report, page 7 et seq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

1404 An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation.

Los infractores pueden eludir además la obligación de conservación de datos utilizando servidores de comunicación anónimos[1405]. 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[1406].

En lo que respecta al hecho de 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[1407] o la prohibición de la utilización de tecnologías de comunicación anónimas[1408].

6.2.6 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[1409]. 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[1410].

Algunos países europeos y Estados Unidos están contemplando la posibilidad de sustituir o enmendar el procedimiento de registro y confiscación [1411]. 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[1412]. 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

---

In addition he is obliged to request an identification of his customers prior to the use of this 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1405 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.

1406 Regarding the impact of use of anonymous communication technology on the work of law enforcement agencies see above: Chapter 3.2.12.

1407 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1408 Regarding the protection of the use of anonymous mean of communication by the United States constitution *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.

1409 A detailed overview about 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 seqq.; *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 seqq. 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: http://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.

1410 Regarding the involvement of computer forensic experts in the investigations see above: Chapter 6.2.2.

1411 Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security , available at: http://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: http://www.news.com/8301-10784_3-9769886-7.html.

1412 See below: Chapter 6.2.12.

físico al equipo permite utilizar técnicas de investigación más eficaces[1413]. Esto subraya la importancia de los procedimientos de registro y confiscación en la investigación en Internet.

Convenio sobre la Ciberdelincuencia

La mayoría de las legislaciones procesales penales nacionales contienen disposiciones que autorizan a los organismos competentes a registrar y confiscar objetos[1414]. 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[1415]. Algunos países, por ejemplo, limitan la aplicación de los procedimientos de confiscación a los objetos físicos[1416]. 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[1417].

El punto 1 del Artículo 19 del Convenio 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[1418].

> ***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[1419]. Una de las principales es que los mandatos judiciales suelen estar limitados a determinados lugares (por ejemplo, el hogar del sospechoso)[1420]. En lo que respecta al registro de datos informáticos, la investigación puede revelar que el sospechoso no los almacenó en

---

1413 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 it is the only way to ensure that the files on the suspects 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: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

1414 See Explanatory Report to the Convention on Cybercrime, No. 184.

1415 "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.

1416 Explanatory Report No. 184.

1417 Regarding the difficulties of online-search procedures see below: Chapter 6.2.12.

1418 "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.

1419 *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1420 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

discos duros locales, sino en un servidor externo al cual accedió por Internet[1421]. 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[1422]. El Convenio 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[1423]. Los instrumentos necesarios no se limitan a copiar los datos pertinentes[1424], ya que se necesitan 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[1425]. 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[1426]. 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[1427] (por ejemplo, pornografía infantil) en particular, los investigadores no podrán dejar los

---

1421 The importance of being able to extend the search to connected computer systems was already addressed by the Council of Europe Recommendation No. R (95) 13 of he 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: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf.

1422 In this context it is important to keep in mind the principle of National Sovereignty. If the information are 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 as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1423 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: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1424 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 seqq.

1425 "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.

1426 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.

1427 See above: Chapter 2.5.

datos en el servidor y, por lo tanto, necesitarán un instrumento que les permita suprimirlos o, al menos, garantizar que ya no sean accesibles[1428]. 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[1429], que entonces plantean dificultades particulares porque adquieren una dimensión internacional que exige, a su vez, una cooperación internacional en las investigaciones[1430]. 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[1431], 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

---

1428 One possibility to prevent access to the information without deleting them is the use encryption technology.

1429 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

1430 The fact, that the law enforcement agencies are able to access certain data, that are stored outside the country through a computer system in their territory does not automatically legalise 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 trans-border 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.

1431 "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.

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[1432]. 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*"[1433].

> ***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[1434].

> ***Sección 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.*

Sección 12[1435]

> *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.*

1432 "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.

1433 Explanatory Report to the Convention on Cybercrime, No. 202.

1434 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1435 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.*

Sección 13[1436]

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.

6.2.7 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[1437].

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[1438].

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

1436 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 ist constitutional or common law protections against self -incrimination.*

1437 Regarding the motivation of the drafters see Explanatory Report to the Convention on Cybercrime, No. 171.

1438 "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.

los que se encuentra la información especificada[1439]. La aplicación de la disposición se extiende con la expresión "bajo su control". Los datos se encuentran bajo el control de una persona si ésta no tiene acceso físico a la información, pero la gestiona, por ejemplo, cuando un sospechoso almacena datos en un sistema de almacenamiento en línea a distancia. En el Informe Explicativo los redactores del Convenio señalan no obstante que la simple capacidad técnica de acceder a distancia a datos almacenados no constituye necesariamente el control de los mismos[1440]. 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[1441]. 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[1442]. A este respecto, es importante subrayar que el Artículo 18 del Convenio sobre la Ciberdelincuencia no contempla una obligación de conservación de datos[1443] ni una obligación de que los proveedores de servicio registren información sobre los abonados[1444]. El apartado 1b) permite que los investigadores ordenen al proveedor que someta esta información.

La distinción entre "datos informáticos" del apartado 1 a) 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[1445].

> ***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;*

1439 Explanatory Report to the Convention on Cybercrime, No. 173.

1440 "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.

1441 Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication see above: Chapter 3.2.12.

1442 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.

1443 See above: Chapter 6.2.5.

1444 Explanatory Report to the Convention on Cybercrime, No. 172.

1445 These can for example be information that were provided on a classic registration form and kept by the provider as paper records.

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[1446]. Se pueden, por ejemplo, aplicar exigencias más estrictas[1447] 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[1448]. La distinción entre la obtención en tiempo real de datos relativos al tráfico (Artículo 20)[1449] y la obtención en tiempo real de datos relativos al contenido (Artículo 21)[1450] 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[1451]. 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[1452].

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[1453].

Sección 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;

1446 The Explanatory Report does even point 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".

1447 For example the requirement of a court order.

1448 The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 20) shows that the drafters of the Convention realised that the instruments are.

1449 See below: Chapter 6.2.9.

1450 See below: Chapter 6.2.10.

1451 Art. 21 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"). Unlike this Art. 20 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.

1452 Regarding the advantages of a graded system of safeguards see above: Chapter 6.2.3.

1453 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(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)[1454] *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.*

6.2.8 Obtención de datos en tiempo real

Las escuchas telefónicas se utilizan en muchos países en investigaciones de delitos de sangre[1455]. 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[1456].

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)[1457]. 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[1458].

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[1459] 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[1460]. Habida cuenta de ello, el Convenio

---

1454 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.

1455 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: http://www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

1456 In these cases other technical solutions for the 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 seqq.

1457 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 http://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.

1458 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: http://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 http://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.

1459 Especially the missing technical preparation of Internet Providers to collect the relevant data in real-time.

1460 Explanatory Report to the Convention on Cybercrime, No. 205.

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[1461].

6.2.9 Obtención de datos relativos al tráfico

Convenio 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[1462], 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[1463].

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[1464]. 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*

1461 ABA International Guide to Combating Cybercrime, page 125.

1462 ABA International Guide to Combating Cybercrime, page 125.

1463 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.

1464 "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 as well: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 et seq.

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[1465].

- 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[1466].
- 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[1467].

En el Convenio 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[1468]. 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[1469], los delincuentes pueden utilizar servicios de comunicación anónima por Internet. Si el infractor utiliza un servicio de comunicación anónima como el software TOR[1470], en la mayoría de los casos los investigadores son

---

1465 "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.

1466 The Convention does not define technical standards regarding the design of such interface. Explanatory Report to the Convention on Cybercrime, No. 220.

1467 Explanatory Report to the Convention on Cybercrime, No. 223.

1468 "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.

1469 See above: Chapter 3.2.12.

1470 Tor is a software that enables users to protect against traffic analysis. For more information about the software see http://tor.eff.org/.

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[1471].

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[1472], 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[1473] de informar a los usuarios[1474].

El Convenio sobre la Ciberdelincuencia se concibió para mejorar y armonizar las legislaciones sobre todo lo relacionado con la ciberdelincuencia[1475]. 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[1476].

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[1477].

> *(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.*

1471 An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1472 This advantage is also relevant for remote forensic investigations. See below: Chapter 6.2.12.

1473 Such obligation might be legal or contractual.

1474 Explanatory Report to the Convention on Cybercrime, No. 226.

1475 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."

1476 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.

1477 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

(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.

6.2.10 Interceptación de datos relativos al contenido

Convenio 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[1478], 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.

1478 One possibility to prevent law enforcement agencies to analyse 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: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

Una de las mayores dificultades que plantean las investigaciones sobre la base del Artículo 21 es la utilización de tecnologías de cifrado[1479]. 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[1480].

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[1481].

> ***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.*

6.2.11 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[1482]. 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[1483].

La utilización de tecnologías de cifrado por los infractores plantea dificultades a las autoridades competentes[1484]. Existen varios planteamientos nacionales e internacionales[1485] para abordar el problema[1486].

1479 Regarding the impact of encryption technology on computer forensic and criminal investigations see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge see below: Chapter 6.2.11.

1480 *Schneier*, Applied Cryptography, Page 185.

1481 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://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: http://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: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1482 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1483 *Schneier*, Applied Cryptography, Page 185.

1484 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:

1485 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. "

1486 For more information see Koops, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

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:

- En las investigaciones judiciales, las autoridades competentes deben poder romper las claves en caso necesario[1487]. 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[1488].
- Reglamentaciones que limitan el rendimiento de los programas de cifrado limitando la longitud de las contraseñas[1489]. 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[1490]. 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[1491]. 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[1492]. 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.
- Otra posibilidad es la orden de presentación[1493], que significa 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[1494]. Varios países han llevado a efecto esas obligaciones[1495]. La Sección 69 de la Ley de 2000

1487 The need for such authorisation if for example mentioned 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."

1488 This topic was discussed in the decision of the United States 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 the law enforcement agencies to make use of a software to record the key strokes on the suspects computer (key logger) 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 http://www.epic.org/crypto/scarfo/opinion.html.

1489 Export limitations for encryption software that is able process 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.

1490 The limitation of the import of such powerful software is even characterised 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: http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm

1491 See: *Lewis*, Encryption Again, available at: http://www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

1492 The key escrow system was promoted by the United States Government and implemented in France for a period of in 1996. For more information see Cryptography and Liberty 2000 – An International Survey of Encryption Policy. Available at: http://www2.epic.org/reports/crypto2000/overview.html#Heading9.

1493 See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 et seq.

1494 "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.", http://www.g7.utoronto.ca/summit/1997denver/formin.htm.

sobre Tecnologías de la Información de la India es un ejemplo de aplicación nacional[1496]. La Sección 49 de la Ley del Reino Unido de 2000 sobre la Reglamentación de los Derechos de los Investigadores[1497] es otro ejemplo de esa obligación:

> ***Sección 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,*

1495 See for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: http://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, Artikel 37, available at: http://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: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: http://www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: http://www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: http://www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative a l'echange electronique de donnees 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 http://www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: http://www.info.gov.za/gazette/acts/2002/a70-02.pdf;Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: http://www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

1496 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.

1497 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: http://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.

(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.

Sección 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 2006 sobre la Reglamentación de los Derechos de los Investigadores obliga al sospechoso de un delito a facilitar la labor de las autoridades competentes. Esta reglamentación es motivo de tres inquietudes principales:

- Una inquietud que la obligación puede conducir a un posible conflicto con los derechos fundamentales del sospechoso contra la autoincriminación[1498]. 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.
- 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[1499].
- 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"[1500].

6.2.12 Software judicial 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[1501], lo cual podría incitarlo a cambiar de

---

1498 Regarding the discussion about the protection against self-incrimination under the 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, Issue1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: http://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: http://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: http://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: http://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: http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe about self-incrimination, in particular with regard to the European Convention on Human Right (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.

1499 In this context see as well: Walker, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: http://www.bileta.ac.uk/01papers/walker.html.

1500 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.

1501 A detailed overview about the elements of search procedures as well as the challenges of carrying them ot 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 seqq.; *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 seqq.

comportamiento [1502]. 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[1503]. 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[1504]. 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[1505]. 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[1506]. Los Informes se referían a una orden de allanamiento cuando era preciso utilizar[1507] una herramienta llamada CIPAV[1508]. 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,

---

1502 Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an on going investigation based on Art. 20 confidential see above: Chapter 6.2.9.

1503 There are disadvantages related to remote investigations. 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 it is the only way to ensure that the files on the suspects 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: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

1504 Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: http://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: http://www.news.com/8301-10784_3-9769886-7.html.

1505 See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: https://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: http://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: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: http://www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; Abreu, FBI confirms "Magic Lantern" project exists, 2001, available at: http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

1506 See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: http://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: http://www.heise-security.co.uk/news/92950.

1507 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: http://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: http://www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV fort he first time, Heise Security News, 19.07.2007, available at: http://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: http://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: http://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.

1508 Computer and Internet Protocol Address Verifier.

comenzó un debate sobre la necesidad de enmendar la legislación vigente en esta materia[1509]. En el curso del debate se divulgó que las autoridades de investigación habían utilizado ilegalmente software judicial a distancia en un par de investigaciones[1510].

Se han estudiado varios conceptos de "software judicial a distancia" y, especialmente, sus posibles funciones[1511], que, teóricamente, podrían ser las siguientes:

- Función de registro – Esta función permitiría que los organismos competentes registraran contenidos ilegales y compilaran información sobre los ficheros almacenados en el ordenador[1512].
- 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[1513]. El software judicial a distancia podría grabar los datos procesados y conservarlos para que los pudieran consultar los investigadores.
- Registrador de teclas – Si el software judicial 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[1514].
- Identificación – Con esta función los investigadores podrían 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[1515].
- Activación de periféricos – El software se podría utilizar a distancia para activar una webcam o el micrófono para observar el recinto[1516].

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

---

1509 Regarding the discussion in Germany see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: http://www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: http://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: http://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: http://www.spiegel.de/international/germany/0,1518,502955,00.html.

1510 See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: http://www.tagesspiegel.de/politik/;art771,1989104.

1511 For an overview see *Gercke*, Secret Online Search, Computer und Recht 2007, page246 et seq.

1512 The search function was in 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: http://www.edri.org/edrigram/number5.3/online-searches.

1513 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 http://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.

1514 This 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: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1515 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.

1516 Regarding this functions see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 et seq.

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[1517]. 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[1518].

- 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[1519] y, por otra parte, es difícil mantener la integridad del sistema informático del sospechoso[1520]. En lo que respecta a estas últimas consideraciones, por lo general el software judicial a distancia no puede reemplazar el examen físico del sistema informático del sospechoso.

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[1521]. 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.

6.2.13 Obligación de autorización

El infractor puede tomar varias medidas para complicar las investigaciones. Además de utilizar software de comunicación anónima[1522], 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[1523] del Decreto 144[1524] italiano, que tomó carácter de ley en 2005 (Legge Nº 155/2005)[1525]. En esta disposición se

---

1517 Regarding the possible ways for an infection of a computer system by a spyware see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: http://www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

1518 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 a detection of the remote forensic software this could go along with serious risks for the computer security. For more information see *Gercke*, Computer und Recht 2007, page 249.

1519 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 do just have access to the computer system via a remote forensic software.

1520 With regard to the importance of maintaining the 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: https://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: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

1521 National Sovereignity is a fundamental principle in International Law. See Roth, State Sovereignity, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

1522 See above: Chapter 3.2.12.

1523 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 licensce by 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.

1524 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 http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

1525 For more details see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 et seq.

obliga a todo el que proyecte ofrecer acceso Internet público (por ejemplo, cafés Internet o universidades[1526]) 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[1527].

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. 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[1528]. 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.

6.3 Cooperación internacional

6.3.1 Introducción

Cada vez más, los ciberdelitos adquieren dimensión internacional[1529]. 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[1530]. Por este motivo, tampoco necesitan estar presentes en el lugar en que se localiza a la víctima. En general, en las investigaciones sobre ciberdelitos es imprescindible la cooperación internacional[1531]. 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[1532]. 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[1533]. En sus Artículos 23 a 35, el Convenio sobre la Ciberdelincuencia tiene en cuenta la importancia creciente de la cooperación internacional. Puede hallarse otro enfoque al respecto en el Proyecto de Convenio de Stanford[1534].

6.3.2 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.

1526 *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

1527 Regarding the related challenges see: *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" in Cybercrime & Security, IIA-2, page 6 et seq.

1528 *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: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

1529 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: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf.

1530 See above: Chapter 3.2.7.

1531 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: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

1532 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

1533 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."

1534 See below: Chapter 6.3.9.

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 de alojamiento de datos[1535]. 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[1536].

6.3.3 Extradición

La extradición de nacionales sigue siendo uno de los aspectos más difíciles de la cooperación internacional[1537]. Los pedidos 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[1538]). 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[1539].

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.

1535 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).

1536 If for example two countries involved in a cybercrime investigation already do have bilateral agreements in place that contain the relevant instruments, this agreement will remain a valid basis for the international cooperation.

1537 Regarding the difficulties related to the dual criminality principle see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 et seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

1538 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.

1539 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 seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

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.

6.3.4 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[1540]. 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[1541]. 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[1542].

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.

1540 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."

1541 See above: Chapter 3.2.10.

1542 See Explanatory Report to the Convention on Cybercrime, No. 256.

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[1543]. 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[1544].

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.

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.

6.3.5 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

1543 This information often leads to successful international investigations. For an overview about 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: http://www.ecpat.se/upl/files/279.pdf

1544 Similar instruments can be found in other Council of Europe Convention. 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. The Council of Europe Conventions are available at: http://www.coe.int.

régimen autónomo de asistencia jurídica mutua obligatoria[1545]. 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, entre otros, los siguientes:

- obligación de establecer un punto de contacto disponible para las solicitudes de asistencia jurídica mutua[1546];
- comunicación directa entre puntos de contacto para evitar procedimientos excesivamente prolongados[1547]; y
- 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; y/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[1548]. 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[1549]. 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[1550].

6.3.6 Asistencia mutua en materia de medidas provisionales

Los Artículo 28 a 33 contemplan los instrumentos de procedimiento del Convenio sobre la Ciberdelincuencia[1551]. 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[1552]. En lo que concierne al principio de soberanía nacional[1553], dichos instrumentos sólo podrán ser aplicados en el ámbito nacional[1554].

1545 See Explanatory Report to the Convention on Cybercrime, No. 262.

1546 Regarding the 24/7 network points of contact see below: Chapter 6.3.8.

1547 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."

1548 See Explanatory Report to the Convention on Cybercrime, No. 268.

1549 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."

1550 See Explanatory Report to the Convention on Cybercrime, No. 269.

1551 See above: Chapter 6.2.

1552 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).

1553 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

1554 An exemption is Art. 32 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

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[1555]	Artículo 29
Artículo 17 – Conservación y revelación parcial rápidas de datos sobre el tráfico[1556]	Artículo 30
Artículo 18 – Orden de presentación[1557]	
Artículo 19 – Registro y confiscación de datos informáticos almacenados[1558]	Artículo 31
Artículo 20 – Obtención en tiempo real de datos sobre el tráfico[1559]	Artículo 33
Artículo 21 – Interceptación de datos sobre el contenido[1560]	Artículo 34

6.3.7 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[1561]. No se pudieron concertar nuevos acuerdos[1562] e incluso los Estados Miembros del Consejo de Europa siguen poniendo en tela de juicio la solución alcanzada[1563].

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*

---

gained from the use of this Article).

1555 See above: Chapter 6.2.4.

1556 See above: Chapter 6.2.4.

1557 See above: Chapter 6.2.7.

1558 See above: Chapter 6.2.6.

1559 See above: Chapter 6.2.9.

1560 See above: Chapter 6.2.410.

1561 See Explanatory Report to the Convention on Cybercrime, No. 293.

1562 "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.

1563 See below in this chapter.

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[1564].

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[1565]. Hay sólidos argumentos contra este tipo de disposición, siendo el más importante el que sostiene que al establecer la segunda exención, los redactores del Convenio están violando la estructura dogmática del régimen de asistencia jurídica mutua. Mediante el Artículo 28, los redactores facultaban a los investigadores a ordenar la presentación de datos. Este 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[1566].

6.3.8 Red de contactos 24/7

Las investigaciones sobre ciberdelitos exigen habitualmente una reacción inmediata[1567]. 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[1568]. 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[1569]. Los redactores del Convenio recordaron que esta disposición es uno de los instrumentos más importantes del Convenio sobre la Ciberdelincuencia[1570].

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

1564 See Explanatory Report to the Convention on Cybercrime, No. 293.

1565 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

1566 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 the foreign law enforcement agency to order the submission of the relevant data. It can only seek for permission.

1567 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."

1568 See above: Chapter 6.2.4.

1569 The availability 24 hours a day and 7 days a week is especially important with regard to 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: Chapter 3.2.6.

1570 See Explanatory Report to the Convention on Cybercrime, No. 298.

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[1571]. 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[1572] y que adquieren dimensión internacional[1573]. 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 las siguientes:

- 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[1574] y un punto de contacto en

---

1571 Regarding the activities of the G8 in the fight against Cybercrime see above: Chapter 5.1.1 . For more information on the 24/7 Network see: 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: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

1572 See above: Chapter 3.2.10.

1573 See above: Chapter 3.2.6.

1574 Regarding the question which authorities should be authorised to order the preservation of data see above: Chapter 6.2.4.

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[1575].

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[1576].

6.3.9 Cooperación internacional en el Proyecto de Convenio de Stanford

Los redactores del Proyecto de Convenio de Stanford[1577] 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[1578]. 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[1579].

6.4 Responsabilidad de los proveedores de Internet

6.4.1 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[1580]. Además del proveedor de correo electrónico, en la transmisión participan proveedores de acceso y encaminadores que envían el correo al destinatario. Con la teledescarga de películas que contienen imágenes de pornografía infantil, ocurre algo similar. En el procedimiento de teledescarga 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

---

1575 Explanatory Report to the Convention on Cybercrime, No. 301.

1576 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

1577 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: http://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.

1578 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1579 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1580 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.

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[1581]. 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[1582].

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[1583]. 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.

6.4.2 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[1584]. Puede hallarse un ejemplo de este enfoque legislativo en los § 517(a) y (b) del 17 U.S.C. (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*

1581 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: http://www.okjolt.org/pdf/2004okjoltrev8a.pdf.

1582 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

1583 For an introduction into 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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf

1584 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 the DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

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[1585]. 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[1586]. En este contexto, es importante en primer lugar poner de relieve que no todos los proveedores están abarcados en la limitación[1587]. Las limitaciones de responsabilidad se aplican únicamente a proveedores de servicio[1588] y proveedores de sistemas de almacenamiento especial[1589]. 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;

1585 Regarding the History of the DMCA and the 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: http://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.

1586 Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq., available at: http://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 http://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.

1587 Regarding the application of the 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: http://www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

1588 17 U.S.C. § 512(a)

1589 17 U.S.C. § 512(b)

- 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[1590] puede consultarse en el § 230(c) del 47 U.S.C.:

> ***§ 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 § 517(a) del 17 U.S.C. y del § 230(c) del 47 U.S.C., 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.

6.4.3 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[1591]. 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[1592]. 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[1593]. Las limitaciones están relacionadas con las diferentes categorías de servicios prestados por el proveedor[1594]. 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

---

1590 Regarding the Communication 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 seqq., available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf.

1591 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 U.S. & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol 31, 2003, pae 325 et seqq., available at: http://www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

1592 See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

1593 Art. 12 – Art. 15 EU E-Commerce Directive.

1594 With the number of different services covered the E-Commerce Directive aims for a broader regulation than 17 U.S.C. § 517(a). Regarding 17 U.S.C. § 517(a) see above.

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.

6.4.4 Responsabilidad del proveedor de acceso (Directiva de la Unión Europea)

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[1595].

> ***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 § 517(a) del 17 U.S.C.[1596]. 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.

6.4.5 Responsabilidad por la memoria tampón (Directiva de la Unión Europea)

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[1597]. Una

---

1595 See Art. 12 paragraph 3 E-Commerce Directive.

1596 The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq., available at: http://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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

1597 With regard to the traditional caching as well as active caching see: Naumenko, Benefits of Active Caching in the WWW, available at: http://lcawww.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

técnica utilizada para reducir la anchura de banda es la instalación de servidores intermediarios[1598]. 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 § 517(b) del 17 U.S.C.[1599]. 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[1600], 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.

6.4.6 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

---

1598 For more information on Proxy Servers see: *Luotonen*, Web Proxy Servers, 1997.

1599 The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider 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: http://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 seqq. , available at: http://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 http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

1600 See above: Chapter 6.4.4.

puede arrendar a esos proveedores capacidad de almacenamiento para su página web. Algunos proveedores ofrecen incluso, en forma gratuita, espacio web con auspicio publicitario[1601].

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[1602]. La ausencia de una reacción inmediata dará lugar a la imputación de responsabilidad del proveedor de alojamiento de datos[1603].

> ***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[1604].

6.4.7 Exclusión de la obligación de supervisión (Directiva de la Unión Europea)

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*

1601 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.

1602 This procedure is called "notice and takedown".

1603 The hosting provider is quite often in a difficult situation. On the one hand side he needs to react immediately to avoid liability – on the other hand side he has certain obligations with regard to his customers. If he removes legal information that was just on first sight illegal, this could lead to claims for indemnity.

1604 By enabling their customers to offer products they provide the necessary storage capacity for the required information.

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.

6.4.8 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[1605]. 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[1606]. 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[1607]. Algunos países de la Unión Europea han decidido contemplar la responsabilidad de los proveedores de hiperenlaces en una disposición especial[1608]. 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[1609]. 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 (Austria)[1610]:

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

---

1605 *Spindler*, Multimedia und Recht 1999, page 204.

1606 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.

1607 *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

1608 Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

1609 See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

1610 § 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.

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.

6.4.9 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"[1611].

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[1612]. A diferencia de lo que ocurre con los hiperenlaces, no todos los países se han basado en los mismos principios[1613]. España[1614] 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[1615], 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

1611 *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, Page 5. Available at: http://www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

1612 Austria, Spain and Portugal. See report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

1613 See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

1614 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 conteni-dos 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.

1615 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.

3. no seleccione ni modifique la información contenida en la transmisión.

7 Referencias de carácter jurídico

Convenio sobre la Ciberdelincuencia del Consejo de Europa[1616]

Ley Modelo de la Commonwealth sobre Delitos Informáticos y relacionados con la Informática[1617]

Proyecto de Convenio de Stanford[1618]

1616 Council of Europe Convention on Cybercrime, available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

1617 Commonwealth Model Law on Computer and Computer Related Crime, available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

1618 Draft Stanford Convention, available at: http://www.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf.

Impreso en Suiza
Ginebra, 2009