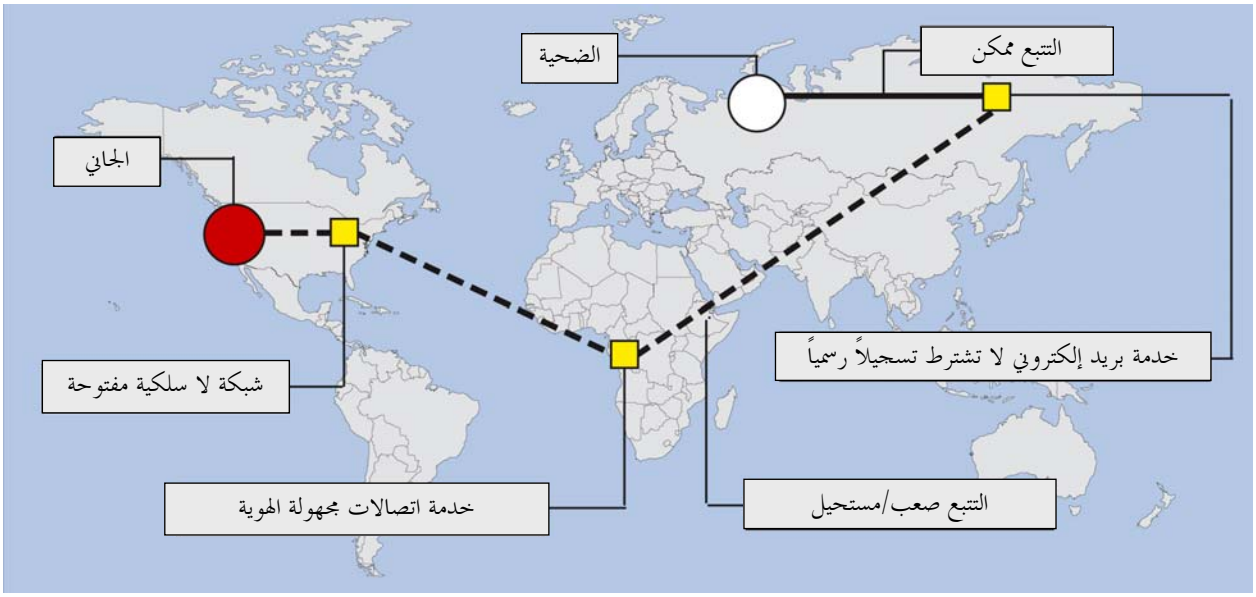
الاتحـــاد الدولـــي للاتصـــالات



فهم الجريمة السيبرانية:
دليـــل للبلـــدان الناميـــة

شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني
دائرة السياسات والاستراتيجيات
قطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات

مشروع أبريل 2009

للمزيد من المعلومات، يرجى الاتصال بشعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، التابعة لقطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات، على العنوان التالي: cybmail@itu.int

الاتحاد الدولي للاتصالات

شكر وتقدير

وُضع هذا التقرير بناء على تكليف من شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، التابعة لقطاع تنمية الاتصالات، بالاتحاد الدولي للاتصالات.

وقد تولى الدكتور ماركو غيرك Dr. Marco Gercke إعداد هذا التقرير الذي يصدر بعنوان "فهم الجريمة السيبرانية: دليل للبلدان النامية". ويود المؤلف أن يشكر الفريق المعني في قطاع تنمية الاتصالات على دعمه وأن يشكر غونهيلد شير Gunhild Scheer على ما أجراه معها من مناقشات مكثفة.

ومنشور الاتحاد الدولي للاتصالات هذا "فهم الجريمة السيبرانية: دليل للبلدان النامية" متاح على الخط في العنوان التالي:

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

وقد صمم إخراج هذه الوثيقة بحيث تطبع على وجهي الصفحة كليهما. وقد صدرت هذه الوثيقة دون تحرير رسمي.

وللحصول على مزيد من المعلومات بشأن هذا المنشور، يرجى الاتصال بالجهة التالية:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland

رقم الهاتف: 5825/6052 730 22 41+

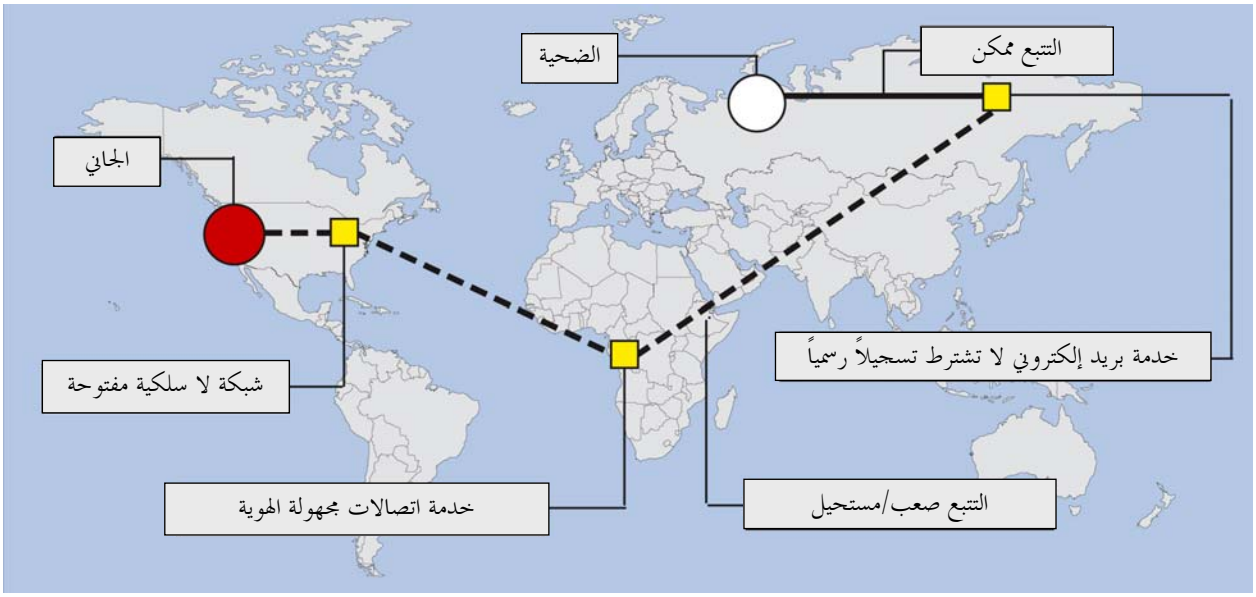
رقم الفاكس: 5484 730 22 41+

البريد الإلكتروني: cybmail@itu.int

الموقع الإلكتروني: www.itu.int/ITU-D/cyb/

يرجى مراعاة البيئة قبل طباعة هذا التقرير.

الاتحـــاد الدولـــي للاتصـــالات



فهم الجريمة السيبرانية:
دليـــل للبلـــدان الناميـــة

شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني
دائرة السياسات والاستراتيجيات
قطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات

مشروع أبريل 2009

للمزيد من المعلومات، يرجى الاتصال بشعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، التابعة لقطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات، على العنوان التالي: cybmail@itu.int

الاتحاد الدولي للاتصالات

المختصرات

ABA	رابطة المحامين الأمريكية *(American Bar Association)*
APEC	منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ *(Asia-Pacific Economic Cooperation Forum)*
APIG	مجموعة الإنترنت لجميع الأحزاب *(All Party Internet Group)*
ASEAN	رابطة أمم جنوب شرق آسيا *(Association of Southeast Asian Nations)*
CFAA	قانون الاحتيال الحاسوبي وإساءة استخدام الأجهزة الحاسوبية (الولايات المتحدة) *((Computer Fraud and Abuse Act (U.S.))*
CMA	قانون إساءة استخدام الأجهزة الحاسوبية (المملكة المتحدة؛ سنغافورة) *((Computer Misuse Act (U.K.) & Computer Misuse Act (Singapore))*
CoE	مجلس أوروبا *(Council of Europe)*
DDoS	نشر هجمات حجب الخطة *(Distributed Denial of Service)*
EC	المفوضية الأوروبية *(European Commission)*
EC Regulations	اللوائح التنظيمية للخصوصية والاتصالات الإلكترونية لعام 2003 (المملكة المتحدة) *((Privacy and Electronic Communications Regulations 2003 (United Kingdom))*
ECPA	قانون خصوصية الاتصالات الإلكترونية *((Electronic Communications Privacy Act (U.S.))*
EU	الاتحاد الأوروبي *(European Union)*
G8	مجموعة البلدان الثمانية *(Group of Eight Nations)*
GCA	البرنامج العالمي للأمن السيبراني *(Global Cybersecurity Agenda)*
IAG	مجموعة المساعدة الدولية (كندا) *((International Assistance Group (Canada))*
ICT	تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*
IRG	قانون المساعدة الدولية في المسائل الجنائية *(Gesetz über die Internationale Rechtshilfe in Strafsachen)*
ITU	الاتحاد الدولي للاتصالات *(International Telecommunication Union)*
OECD	منظمة التعاون والتنمية في الميدان الاقتصادي *(Organization for Economic Cooperation and Development)*
OWig	قانون المخالفات الجنائية (ألمانيا) *((Gesetz über Ordnungswidrigkeiten (Germany))*
PACC	لجنة رابطة المحامين الأمريكية المعنية بالخصوصية والجرائم الحاسوبية *(ABA Privacy & Computer Crime Committee)*
RIPA	قانون تنظيم صلاحيات التحقيق (المملكة المتحدة) *((Regulation of Investigatory Powers Act (United Kingdom))*
StGB	القانون الجنائي الألماني *((German Criminal Code (Strafgesetzbuch))*
StPO	القانون الجنائي الإجرائي الألماني *((German Code of Criminal Procedure (Strafprozessordnung))*
TKG	قانون الاتصالات الألماني *((German Telecommunications Act (Telekommunikationgesetz))*
U.K.	المملكة المتحدة *(United Kingdom)*
UN	الأمم المتحدة *(United Nations)*
UrhG	القانون الألماني لحقوق التأليف والنشر *((German Copyright Act (Urheberrechtsgesecht))*
U.S.	الولايات المتحدة *(United States)*
WSIS	القمة العالمية لمجتمع المعلومات *(World Summit on the Information Society)*

الغرض

الغرض من منشور "**فهم الجريمة السيبرانية: دليل للبلدان النامية**"، الصادر عن الاتحاد الدولي للاتصالات، هو مساعدة البلدان على فهم الجوانب القانونية للأمن السيبراني، ومعاونتها على تحقيق التواؤم بين أطرها القانونية. ومن هذا المنطلق، يرمي الدليل إلى مساعدة البلدان النامية على أن تفهم بشكل أفضل الانعكاسات الوطنية والدولية للتهديدات السيبرانية المتنامية، وإلى تقييم متطلبات الصكوك الوطنية والإقليمية والدولية القائمة، وإلى معاونة البلدان على إرساء أساس قانوني سليم.

ويوفر الدليل لمحة عامة شاملة عن أهم المواضيع المتصلة بالجوانب القانونية للجريمة السيبرانية. ويركز الدليل، في النهج الذي يتوخاه، على مطالب البلدان النامية. وبحكم البعد الدولي للجريمة السيبرانية، تعد الصكوك القانونية متماثلة بالنسبة للبلدان النامية والمتقدمة. غير أن الإحالات التي استخدمت في الدليل قد اختيرت بما يعود بالنفع على البلدان النامية. ويوفر الدليل نخبة واسعة من الموارد التي تتيح إجراء دراسة أكثر تعمقاً للمواضيع المختلفة. واستخدمت، حيثما أمكن، مصادر متوافرة علناً تشمل كثيراً من الإصدارات المجانية للمجلات القانونية المتاحة على الخط.

ويحتوي الدليل على ستة فصول رئيسية. فبعد المقدمة *(الفصل 1)*، يقدم الدليل لمحة عامة عن ظاهرة الجريمة السيبرانية *(الفصل 2)*. ويتضمن هذا الفصل وصفاً لكيفية ارتكاب الجرائم وشرحاً لأكثر الجرائم السيبرانية انتشاراً، مثل القرصنة، وسرقة الهوية، والهجمات الرامية إلى الحرمان من النفاذ إلى الخدمة. ويتضمن الدليل أيضاً لمحة عامة عن التحديات المتعلقة بالتحقيق في الجريمة السيبرانية وملاحقتها قضائياً *(الفصلان 3 و4)*. وبعد إيراد ملخص لبعض الأنشطة التي تقوم بها المنظمات الدولية والإقليمية من أجل مكافحة الجريمة السيبرانية *(الفصل 5)*، يتطرق الدليل إلى تحليل للنُهج القانونية المختلفة المتعلقة بقانون الجريمة السيبرانية، وقانون الإجراءات القضائية، والتعاون الدولي ومسؤولية مقدمي خدمة الإنترنت *(الفصل 6)*، وضُربت في هذا الصدد أمثلة للنهج الدولية، وأمثلة للممارسات الجيدة المستقاة من الحلول الوطنية.

ويتناول منشور **فهم الجريمة السيبرانية: دليل للبلدان النامية** الهدف الأول من الأهداف الاستراتيجية السبعة للبرنامج العالمي للأمن السيبراني للاتحاد الدولي للاتصالات الذي يدعو إلى وضع استراتيجيات لاستحداث تشريع للجريمة السيبرانية يمكن تطبيقه عالمياً ويكون قابلاً للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي، ويتناول المنشور أيضاً النهج الذي تتوخاه لجنة الدراسات المعنية بدراسة المسألة 22/1، التابعة لقطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات، إزاء تنظيم الجهود الوطنية في مجال الأمن السيبراني. ويعد إنشاء الإطار القانوني الملائم عنصراً جوهرياً في الاستراتيجية الوطنية للأمن السيبراني. ويشكل اعتماد جميع البلدان لتشريعات ملائمة ضد إساءة استخدام تكنولوجيا المعلومات والاتصالات في أغراض إجرامية أو في أغراض أخرى، بما فيها الأنشطة الرامية إلى الإضرار بسلامة البنى التحتية الحاسمة للمعلومات، أمراً محورياً لتحقيق الأمن السيبراني العالمي. ولما كانت التهديدات يمكن أن تنشأ في أي مكان حول العالم، فإن التحديات تعد، من الناحية الجوهرية، دولية النطاق وتستوجب تعاوناً دولياً، وتآزراً في إجراء التحقيقات، وأحكاماً موضوعية وإجرائية مشتركة. ولذا، فإن من المهم أن تحقق البلدان التواؤم بين أطرها القانونية الرامية إلى مكافحة الجريمة السيبرانية وتيسير التعاون الدولي.

المحتويات

1 مقدمة

1.1 البنية التحتية والخدمات

تعد الإنترنت أحد المجالات الأسرع نمواً من زاوية تطور البنية التحتية التقنية.[1] واليوم، تنتشر تكنولوجيا المعلومات والاتصالات في كل مكان ويتنامى الاتجاه إلى الرقمنة. وأدى الطلب على الإنترنت والتوصيلية الحاسوبية إلى إدماج تكنولوجيا الحاسوب في منتجات كانت تُشغَّل بدونها عادةً، مثل السيارات والمباني.[2] فالإمداد بالكهرباء، والبنية التحتية للنقل، والخدمات واللوجستيات العسكرية – أي كل الخدمات الحديثة تقريباً – تعتمد على استخدام تكنولوجيا المعلومات والاتصالات.[3]

وعلى الرغم من أن تطور التكنولوجيات الجديدة يركز أساساً على تلبية احتياجات المستهلكين في البلدان الغربية، فإن البلدان النامية يمكنها أن تنتفع هي الأخرى من التكنولوجيات الجديدة.[4] ومع توافر تكنولوجيا الاتصالات اللاسلكية عبر مسافات طويلة مثل تكنولوجيا[5] WiMAX (قابلية التشغيل البيني على الصعيد العالمي فيما يخص النفاذ بالموجات الصِغرية)، وتَيسُّر النظم الحاسوبية التي أصبحت متاحة الآن بأقل من 200 دولار أمريكي،[6] بات بوسع عدد أكبر من الناس في البلدان النامية النفاذ إلى الإنترنت والمنتجات والخدمات ذات الصلة بمزيد من اليسر.[7]

وتأثير تكنولوجيا المعلومات والاتصالات على المجتمع يتعدى إلى حد بعيد إقامة البنية التحتية الأساسية للمعلومات. فتَيسُّر تكنولوجيا المعلومات والاتصالات يشكل ركيزة للتنمية يُستند إليها لدى استحداث الخدمات المعتمدة على الشبكات وإتاحتها واستخدامها.[8] فرسائل البريد الإلكتروني قد حلت محل الرسائل التقليدية؛[9] وأضحت العروض البيانية على شبكة الويب أكثر أهمية اليوم للأنشطة التجارية من المواد الدعائية المطبوعة؛[10] كما تنمو الاتصالات والخدمات الهاتفية المعتمدة على الإنترنت بوتيرة أسرع من وتيرة نمو الاتصالات المعتمدة على الخطوط الأرضية.[11]

---

[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.

[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.

ويتيح تَيسُّر تكنولوجيا المعلومات والاتصالات والخدمات الجديدة المعتمدة على الشبكات عدداً من المزايا للمجتمع بوجه عام، ولا سيما في البلدان النامية.

وتعتبر تطبيقات تكنولوجيا المعلومات والاتصالات، مثل الحكومة الإلكترونية والتجارة الإلكترونية والتعليم الإلكتروني والصحة الإلكترونية والبيئة الإلكترونية، من العناصر التي تساعد على تحقيق التنمية، بحكم أنها توفر قناة فعالة لتنفيذ طائفة واسعة من الخدمات الأساسية في المناطق النائية والريفية. وتستطيع تطبيقات تكنولوجيا المعلومات والاتصالات أن تيسر تحقيق الأهداف الإنمائية للألفية، والحد من الفقر، وتحسين الظروف الصحية والبيئية في البلدان النامية. وبمقدور الاستثمارات الموظفة في تطبيقات وأدوات تكنولوجيا المعلومات والاتصالات – إذا ما اتبع فيها النهج الصحيح، وروعي ملاءمتها للسياق، وطبقت بشأنها السياسات التنفيذية السليمة – أن تسفر عن تحسن الإنتاجية والجودة. وبمقدور تطبيقات تكنولوجيا المعلومات والاتصالات، بدورها، أن تحرر القدرات التقنية والبشرية وتوسع فرص الانتفاع بالخدمات الأساسية. وفي هذا الصدد، تشكل الآن سرقة الهوية على الخط والتقاط بيانات الوثائق الشخصية و/أو المعلومات الشخصية الخاصة بأشخاص آخرين عن طريق الإنترنت بنية إعادة استخدامها بطرق احتيالية في أغراض إجرامية أحد التهديدات الرئيسية التي تحدق بالمضي في تنمية خدمات الحكومة الإلكترونية والأعمال التجارية الإلكترونية.[12]

كما تعد تكاليف الخدمات المتاحة على الإنترنت أقل إلى حد كبير في أحيان كثيرة من تكاليف الخدمات المناظرة المتاحة خارج الشبكة.[13] فخدمات البريد الإلكتروني تتوافر في أحيان كثيرة مجاناً أو بتكلفة ضئيلة للغاية بالقياس إلى الخدمات البريدية التقليدية.[14] وموسوعة ويكيبيديا[15] المتاحة على الخط يمكن استخدامها مجاناً، شأنها شأن المئات من الخدمات التي توفر البيانات على الخط.[16] وانخفاض التكلفة هو من الأهمية بمكان لأنه ييسر الانتفاع بالخدمات لأعداد أكبر من المستخدمين، من بينهم محدودو الدخل. فالإنترنت تُمكِّن كثيراً من الناس في البلدان النامية، بحكم محدودية مواردهم المالية، من استخدام خدمات لم يكن بوسعهم لولا ذلك أن ينتفعوا بها خارج الشبكة.

2.1 المزايا والمخاطر

أفضى تطبيق تكنولوجيا المعلومات والاتصالات في كثير من جوانب الحياة اليومية إلى تبلور مفهوم حديث هو مفهوم مجتمع المعلومات.[17] ويتيح تطور مجتمع المعلومات فرصاً كبيرة.[18] فالنفاذ دون عائق إلى المعلومات بمقدوره أن يدعم الديمقراطية، لأنه ينتزع تدفق المعلومات من سيطرة سلطات الدولة (كما حدث مثلاً في أوروبا الشرقية).[19] وقد حَسَّنت التطورات التقنية الحياة اليومية – وما الصرافة والتسوق على الخط، واستخدام خدمات البيانات المتنقلة، والمهاتفة عن طريق نقل الصوت باستخدام بروتوكول الإنترنت إلا بعض الأمثلة على مدى تغلغل تكنولوجيا المعلومات والاتصالات في حياتنا اليومية.[20]

---

[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.

[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.

غير أن نمو مجتمع المعلومات تصاحبه تهديدات جديدة وخطيرة.[21] فالخدمات الأساسية مثل الإمداد بالماء والكهرباء باتت تعتمد الآن على تكنولوجيا المعلومات والاتصالات.[22] كما تعتمد السيارات، وتنظيم المرور، والمصاعد، وتكييف الهواء، والهواتف على سلاسة أداء تكنولوجيا المعلومات والاتصالات.[23] ولذا، فإن الهجمات التي قد تشن الآن ضد البنية التحتية للمعلومات وخدمات الإنترنت بمقدورها إلحاق الأذى بالمجتمع بطرق جديدة وحرجة.[24]

وقد تعرضت البنية التحتية للمعلومات وتعرضت خدمات الإنترنت للهجمات بالفعل.[25] وما الاحتيال الذي يمارس على الخط، ونشر المواد الإباحية التي يستغل فيها الأطفال، وهجمات القرصنة إلا بعض الأمثلة على الجرائم المتعلقة بالحاسوب التي ترتكب على نطاق واسع كل يوم.[26] ويعد الضرر المالي الذي تسببه الجريمة السيبرانية هائلاً.[27] ففي عام 2003 وحده، سببت البرمجيات الخبيثة أضراراً وصل مقدارها إلى 17 مليار دولار أمريكي.[28] وتشير بعض التقديرات إلى أن الدخول المتأتية من الجريمة السيبرانية قد تخطت 100 مليار دولار أمريكي في عام 2007، متفوقة بذلك للمرة الأولى على التجارة غير المشروعة في المخدرات.[29] ويعتقد نحو 60 في المائة من المؤسسات التجارية في الولايات المتحدة أن الجرائم السيبرانية تُكبِّدها تكلفة أبهظ مما تلحقه بها الجرائم المادية.[30] وتبين هذه التقديرات بوضوح أهمية حماية البنى التحتية للمعلومات.[31]

[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; *Wilshusen*, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: 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.

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

[31] *Wilshusen*, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: http://www.gao.gov/new.items/d08212t.pdf.For more information on the economic impact of Cybercrime see below 2.9.

3.1 الأمن السيبراني والجريمة السيبرانية

يؤدي الأمن السيبراني[32] دوراً هاماً في التنمية الراهنة لتكنولوجيا المعلومات وخدمات الإنترنت.[33] ويعد تعزيز الأمن السيبراني وحماية البنى التحتية الحاسمة للمعلومات عنصرين أساسيين في أمن كل أمة ورفاهها الاقتصادي. وأصبح تعزيز أمان الإنترنت (وحماية مستخدمي الإنترنت) جزءاً لا يتجزأ من تنمية الخدمات الجديدة ومن السياسات الحكومية.[34] ويمثل ردع الجريمة السيبرانية عنصراً جوهرياً في الأمن السيبراني الوطني وفي استراتيجية حماية البنية التحتية الحاسمة للمعلومات. ويشمل هذا على وجه الخصوص اعتماد تشريع ملائم لمكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات في أغراض إجرامية أو في أغراض أخرى، ولمكافحة الأنشطة الرامية إلى النيل من سلامة البنى التحتية الوطنية الحاسمة للمعلومات. ويمثل هذا، على المستوى الوطني، مسؤولية مشتركة تتطلب عملاً منسقاً تضطلع به السلطات الحكومية والقطاع الخاص والمواطنون من أجل درء الحوادث، والتأهب لمواجهتها، والتصدي لها، والتعافي من آثارها. ويستدعي هذا على المستوى الإقليمي والدولي تعاوناً وتنسيقاً مع الشركاء المعنيين. ولذا يقتضي صوغ وتنفيذ إطار واستراتيجية وطنيين للأمن السيبراني اتباع نهج شامل.[35] وتستطيع استراتيجيات الأمن السيبراني – ومنها مثلاً تنمية نظم الحماية التقنية أو توعية المستخدمين لوقايتهم من الوقوع في براثن الجريمة السيبرانية – أن تساعد على الحد من احتمالات حدوث الجريمة السيبرانية.[36] ويمثل وضع ودعم استراتيجيات الأمن السيبراني عنصراً حيوياً في مكافحة الجريمة السيبرانية.[37]

وتعد التحديات القانونية والتقنية والمؤسسية التي تطرحها قضية الجريمة السيبرانية تحديات عالمية النطاق وبعيدة المدى لن تتسنى مواجهتها إلا عن طريق استراتيجية متماسكة تراعي دور مختلف أصحاب المصلحة والمبادرات القائمة، ضمن إطار من التعاون الدولي.[38] وفي هذا الصدد، اعترفت القمة العالمية لمجتمع المعلومات[39] بالمخاطر الحقيقية والهامة الناجمة عن عدم كفاية الأمن السيبراني وعن تفشي الجريمة السيبرانية. وترسم الفقرات من 108 إلى 110 من *برنامج عمل تونس بشأن مجتمع المعلومات*، الصادر عن *القمة العالمية لمجتمع المعلومات*،[40] وكذلك ملحق برنامج العمل هذا، خطة عمل تتيح لأصحاب المصلحة المتعددين أن يُنفّذوا على المستوى الدولي *خطة عمل جنيف للقمة العالمية لمجتمع المعلومات*،[41] وتصف عملية التنفيذ التي سيشارك فيها أصحاب المصلحة المتعددون وفقاً لأحد عشر خط عمل، وتوزع المسؤوليات عن تيسير تنفيذ خطوط العمل

[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.

[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

المختلفة. وفي القمة العالمية لمجتمع المعلومات، أسند قادة وحكومات العالم إلى الاتحاد الدولي للاتصالات مهمة تيسير تنفيذ خط العمل جيم5، المتعلق ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.[42]

وفي هذا الصدد، قام الأمين العام للاتحاد الدولي للاتصالات، في 17 مايو 2007، بإطلاق البرنامج العالمي للأمن السيبراني[43] بحضور شركاء من الحكومات، والصناعة، والمنظمات الإقليمية والدولية، والمؤسسات الأكاديمية والبحثية. وهذا البرنامج هو إطار عالمي للحوار وللتعاون الدولي من أجل تنسيق الاستجابة الدولية للتحديات المتنامية التي يواجهها الأمن السيبراني، وتعزيز الثقة والأمن في مجتمع المعلومات. ويستند البرنامج إلى الأعمال والمبادرات والشراكات القائمة بهدف اقتراح استراتيجيات عالمية تكفل التصدي للتحديات المعاصرة المتعلقة ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات. وعلى صعيد الاتحاد الدولي للاتصالات، يستكمل البرنامج العالمي للأمن السيبراني برامج العمل الحالية للاتحاد الدولي للاتصالات، عن طريق تيسير تنفيذ الأنشطة التي تضطلع بها قطاعات الاتحاد الثلاثة في مجال الأمن السيبراني، ضمن إطار من التعاون الدولي.

والبرنامج العالمي للأمن السيبراني له سبعة أهداف استراتيجية رئيسية، تستند إلى خمسة مجالات عمل هي: (1) التدابير القانونية؛ و(2) التدابير التقنية والإجرائية؛ و(3) الهياكل التنظيمية؛ و(4) بناء القدرات؛ و(5) التعاون الدولي.[44]

وتقتضي مكافحة الجريمة السيبرانية اتباع نهج شامل. ولما كانت التدابير التقنية لا تكفي وحدها للحيلولة دون وقوع أي جريمة، فمما يتسم بأهمية حاسمة أن تُمكَّن الوكالات المعنية بإنفاذ القانون من التحقيق في الجريمة السيبرانية وملاحقتها قضائياً بشكل فعال.[45] وفي إطار مجالات عمل البرنامج العالمي للأمن السيبراني، تركز "التدابير القانونية" على كيفية التصدي بطريقة متوافقة دولياً للتحديات التشريعية التي تطرحها الأنشطة الإجرامية المرتكبة على شبكات تكنولوجيا المعلومات الاتصالات. وتركز "التدابير التقنية والإجرائية" على التدابير الرئيسية الرامية إلى تعزيز اعتماد نُهج معززة لتحسين الأمن وإدارة المخاطر في الفضاء السيبراني، ويشمل ذلك خطط الاعتماد وبروتوكولاته ومعاييره. وتركز "الهياكل التنظيمية" على الوقاية من الهجمات السيبرانية واكتشافها والتصدي لها وإدارة أزماتها، ويشمل ذلك حماية نظم البنية التحتية الحاسمة للمعلومات. ويركز "بناء القدرات" على وضع استراتيجيات لآليات بناء القدرات من أجل رفع مستوى الوعي، ونقل المعارف، ورفع المكانة التي يحتلها الأمن السيبراني في جدول أعمال السياسات الوطنية. وأخيراً يركز "التعاون الدولي" على التعاون والتنسيق والحوار على الصعيد الدولي في التصدي للتهديدات السيبرانية.

ويشكل سن التشريعات المناسبة، والقيام ضمن هذا السياق بإنشاء الإطار القانوني المتعلق بالجريمة السيبرانية، جزءاً جوهرياً من استراتيجية الأمن السيبراني. ويقتضي هذا في المقام الأول أن تُجرِّم الأحكام الموضوعية للقانون الجنائي أعمالاً من قبيل الاحتيال الحاسوبي، والنفاذ غير القانوني، والتدخل في البيانات، وانتهاك حقوق المؤلف، واستغلال الأطفال في المواد الإباحية.[46] ولا يعني وجود أحكام في القانون الجنائي تطبق على أفعال مماثلة ترتكب خارج الشبكة أن بالمقدور تطبيقها أيضاً على الأفعال المرتكبة على الإنترنت.[47] ولذا يعد إجراء تحليل وافٍ للقوانين الوطنية الحالية أمراً حيوياً للوقوف على أي ثغرات محتملة.[48] وإلى جانب الأحكام الموضوعية للقانون الجنائي،[49] تحتاج الوكالات المعنية بإنفاذ القانون إلى الأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية.[50] وهذه التحقيقات تطرح هي ذاتها عدداً من التحديات.[51] فمرتكبو الجرائم يمكن أن يقوموا بأفعالهم من أي مكان في العالم تقريباً، وأن يتخذوا من التدابير ما يسعون به إلى إخفاء هويتهم.[52] والأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية يمكن أن تكون مختلفة بقدر ملموس عن الأدوات والصكوك المستخدمة في التحقيق في الجرائم العادية.[53]

---

[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.

[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

4.1 البعد الدولي للجريمة السيبرانية

تنطوي الجريمة السيبرانية في كثير من الأحيان على بعد دولي.[54] فرسائل البريد الإلكتروني ذات المحتوى غير القانوني تمر في كثير من الأحيان عبر عدد من البلدان أثناء نقلها من الراسل إلى المتلقي، أو يُخزَّن المحتوى غير القانوني خارج البلد.[55] ولدى التحقيق في الجريمة السيبرانية، يعد التعاون الوثيق بين البلدان المعنية أمراً بالغ الأهمية.[56] بيد أن الاتفاقات المتعلقة بتبادل المساعدة القانونية تستند إلى إجراءات رسمية ومعقدة تعد مستنزفة للوقت في كثير من الأحيان.[57] ولذا، فإن مما يتسم بأهمية حاسمة وضع إجراءات تكفل الاستجابة السريعة للحوادث ولطلبات التعاون الدولي.[58]

وتؤسس عدد من البلدان نظامها الخاص بتبادل المساعدة القانونية على مبدأ "الإجرام المزدوج".[59] فتقتصر عادةً التحقيقات المنفذة على المستوى العالمي على الأفعال التي تجرمها البلدان المشاركة جميعاً. وعلى الرغم من أن هناك عدداً من الجرائم يمكن ملاحقته قضائياً في أي مكان في العالم، فإن الفوارق الإقليمية تؤدي دوراً هاماً.[60] والمحتوى غير القانوني هو أحد الأمثلة على ذلك. إذ يتباين تجريم المحتوى غير القانوني في البلدان المختلفة.[61] فالمواد التي يمكن توزيعها بشكل قانوني في بلد ما قد يكون توزيعها غير قانوني ببساطة في بلد آخر.[62]

وتعد التكنولوجيا الحاسوبية المستخدمة حالياً في جميع أنحاء العالم تكنولوجيا واحدة من الناحية الأساسية.[63] فباستثناء المسائل المتعلقة باللغة وبمكيِّفات القدرة، لا يوجد فارق يذكر بين النظم الحاسوبية والهواتف الخلوية التي تباع في آسيا وتلك التي تباع في أوروبا. وتنشأ حالة مماثلة فيما يتعلق بالإنترنت. إذ أدى التقييس إلى جعل البروتوكولات المستخدمة في القارة الإفريقية مماثلة لتلك المستخدمة في الولايات المتحدة.[64] فالتقييس يتيح للمستخدمين في كل أنحاء العالم أن النفاذ إلى الخدمات نفسها عن طريق الإنترنت.[65]

والسؤال المطروح هو ما تأثير تحقيق التواؤم بين المعايير التقنية العالمية على تطور القانون الجنائي الوطني. فمن زاوية المحتوى غير القانوني، يستطيع مستخدمو الإنترنت أن ينفذوا إلى المعلومات من أي مكان في العالم، مما يمكنهم من النفاذ إلى معلومات متاحة بشكل قانوني في الخارج، حتى وإن كانت تعد غير قانونية في بلدانهم.

---

[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.

[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.*

من الناحية النظرية، فإن التطورات الناشئة عن التقييس التقني تتجاوز من بعيد عولمة التكنولوجيا والخدمات ويمكن أن تفضي إلى تحقيق التواؤم بين القوانين الوطنية، وكما أظهرت المفاوضات التي دارت بخصوص البروتوكول الأول لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية،[66] ومع ذلك فإن مبادئ القانون الوطني تتغير بمعدل أبطأ كثيراً من وتيرة التطورات التقنية.[67]

وعلى الرغم من أن الإنترنت قد لا تقيم وزناً للرقابة الحدودية، فإن هناك من الوسائل ما يتيح تقييد النفاذ إلى معلومات معينة.[68] فمقدم خدمة النفاذ يستطيع بوجه عام أن يحجب مواقع معينة على شبكة الويب، ومقدم الخدمة الذي يخزن موقعاً على شبكة الويب يستطيع أن يمنع نفاذ بعض المستخدمين إلى المعلومات استناداً إلى عناوين بروتوكول الإنترنت المرتبطة ببلد معين ("استهداف عناوين بروتوكول الإنترنت").[69] وكلا النوعين من التدابير يمكن التحايل عليه، ولكنه يعد مع ذلك أداة يمكن استخدامها لمواصلة الاحتفاظ بفروق إقليمية في شبكة عالمية.[70] وتفيد تقارير مبادرة الشبكة المفتوحة (OpenNet Initiative)[71] أن هذا النوع من الرقابة يمارس في أكثر من عشرين دولة.[72]

5.1 العواقب بالنسبة للبلدان النامية

يمثل التوصل إلى استراتيجيات تتيح التصدي لتهديد الجريمة السيبرانية تحدياً كبيراً، وخاصة بالنسبة للبلدان النامية. وتتضمن الاستراتيجية الشاملة لمكافحة الجريمة السيبرانية عادةً تدابير للحماية التقنية، علاوة على الصكوك القانونية.[73] وإعداد هذه الصكوك وتنفيذها يستلزم وقتاً. وتعد تدابير الحماية التقنية كثيفة التكاليف بوجه خاص.[74] ويتعين على البلدان النامية أن تدرج تدابير الحماية في عملية نشر الإنترنت منذ البداية، لأن هذا الأمر لئن كان قد يرفع في البداية تكلفة خدمات الإنترنت، فإن ما يحققه من مكاسب طويلة الأجل، تتمثل في تجنب التكاليف والأضرار الناجمة عن الجريمة السيبرانية، يشكل مكاسب كبيرة تتجاوز إلى حد كبير أي نفقات أولية تنفق على تدابير الحماية التقنية وضمانات الشبكة.[75]

والمخاطر المرتبطة بضعف تدابير الحماية يمكن أن يكون تأثيرها أشد وطأة في الواقع على البلدان النامية، لأن ما يطبق فيها من ضمانات ومن تدابير حماية يعد أقل صرامةً.[76] وتشكل القدرة على حماية المستهلكين، بالإضافة إلى الشركات، شرطاً أساسياً لا للشركات العادية فحسب، بل أيضاً للشركات التي تمارس نشاطها على الخط أو تعتمد على الإنترنت. وفي غياب أمن الإنترنت، يمكن أن تواجه البلدان النامية صعوبات جمة في ترويج الأعمال التجارية الإلكترونية والمشاركة في الصناعات التي تقدم الخدمات على الخط.

ويعد وضع تدابير تقنية لتعزيز الأمن السيبراني وسن التشريعات الملائمة بشأن الجريمة السيبرانية أمراً حيوياً للبلدان المتقدمة وللبلدان النامية على السواء. ومن المرجح أن تكون التدابير الأولية التي تتخذ من البداية أقل تكلفة إذا ما قورنت بتكاليف إضافة الضمانات وتدابير الحماية إلى الشبكات الحاسوبية في وقت لاحق. كما يتعين على البلدان النامية أن تجعل استراتيجياتها الخاصة بمكافحة الجريمة السيبرانية متماشية منذ البداية مع التدابير الدولية.[77]

---

[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

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

2 ظاهرة الجريمة السيبرانية

1.2 *تعاريف الجريمة السيبرانية*

تبدأ معظم التقارير والأدلة والمنشورات المتعلقة بالجريمة السيبرانية بتعريف مصطلح "الجريمة السيبرانية".[78] ويصف أحد التعاريف الشائعة الجريمة السيبرانية بأنها أي نشاط تستخدم فيه الحواسيب أو الشبكات كأداة أو هدف أو مكان لممارسة النشاط الإجرامي.[79] ومن الأمثلة على أحد النهج الدولية لتعريف الجريمة السيبرانية المادة 1-1 من مشروع الاتفاقية الدولية لتعزيز الحماية من الجريمة السيبرانية والإرهاب[80] التي تبين أن الجريمة السيبرانية تشير إلى أفعال تتعلق بالنظم السيبرانية.[81] وتحاول بعض التعاريف أن تأخذ المقاصد أو النوايا في الحسبان وتطرح توصيفاً أكثر دقة للجريمة السيبرانية،[82] فتعرفها بأنها "أنشطة معتمدة على الحاسوب تعد إما *غير قانونية أو تعتبر غير مشروعة* من جانب أطراف معينة ويمكن الاضطلاع بها *عن طريق الشبكات الإلكترونية العالمية*".[83]

وهذه التوصيفات الأكثر دقة تستبعد الحالات التي تستخدم فيها الأجهزة المادية لارتكاب جرائم عادية، لكنها قد تستبعد بذلك أيضاً جرائم تدرجها اتفاقات دولية مثل "اتفاقية الجريمة السيبرانية"[84] في باب الجريمة السيبرانية. ومن ذلك مثلاً، أن الشخص الذي ينتج أجهزة USB[85] تحتوي على برمجيات خبيثة تدمر البيانات الموجودة على الحواسيب عند توصيل تلك الأجهزة بها يكون قد ارتكب جريمة بمفهوم المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[86] غير أن الفعل المتمثل في حذف البيانات، باستخدام جهاز مادي لاستنساخ شفرة ضارة، فعل لم يرتكب

---

[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] *Article 1*
Definitions and Use of Terms
For the purposes of this Convention:
1. "cyber crime" means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;
[...]

[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

[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.

عن طريق الشبكات الإلكترونية العالمية ولن يُوصَّف، بموجب التعريف الضيق المبين أعلاه، على أنه جريمة سيبرانية. فهذا الفعل لن يوصف على أنه جريمة سيبرانية إلا بموجب تعريف يستند إلى توصيف أوسع نطاقاً يشمل أفعالاً مثل التدخل غير المشروع في البيانات.

ويبين هذا أن هناك صعوبات كبيرة تكتنف تعريف مصطلح "الجريمة السيبرانية".[87] ويستخدم مصطلح "الجريمة السيبرانية" لوصف طائفة واسعة من الأفعال الإجرامية تشمل الجرائم التقليدية التي يستخدم فيها الحاسوب، بالإضافة إلى الجرائم التي تستخدم فيها الشبكات. ولما كانت هذه الجرائم تتباين من نواح كثيرة، لا يتوافر معيار واحد يمكنه أن يحيط بكل الأفعال التي ورد ذكرها في مشروع اتفاقية ستانفورد واتفاقية الجريمة السيبرانية، مع استبعاده في الوقت نفسه الجرائم التقليدية التي يكون استخدام الأجهزة في ارتكابها أمراً عارضاً. وعدم توافر تعريف واحد "للجريمة السيبرانية" لا ينبغي اعتباره أمراً ذا بال، ما دام هذا المصطلح لا يستخدم كمصطلح قانوني.[88]

2.2 تصنيف الجريمة السيبرانية

يغطي مصطلح "الجريمة السيبرانية" مجموعة واسعة من الجرائم.[89] وتشمل الجرائم التي تم الوقوف عليها طائفة واسعة من الأفعال الإجرامية، الأمر الذي يجعل من الصعب وضع نظام لتصنيف الجريمة السيبرانية.[90] وتتضمن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية نظاماً يستلفت الانتباه.[91] إذ تفرق اتفاقية الجريمة السيبرانية بين أربعة أنواع مختلفة من الجرائم:[92]

- الجرائم التي تستهدف سرية البيانات والنظم الحاسوبية وتكامليتها وتيسُرها؛[93]
- الجرائم المتعلقة بالحاسوب؛[94]
- الجرائم المتعلقة بالمحتوى؛[95]
- الجرائم المتعلقة بحقوق المؤلف.[96]

وهذا التصنيف ليس متسقاً تماماً، لأنه لا يستند إلى معيار وحيد للتفرقة بين الفئات المذكورة. فثلاث من هذه الفئات تركز على موضوع الحماية القانونية، وهذه الفئات هي: "الجرائم التي تستهدف سرية البيانات والنظم الحاسوبية وتكامليتها وتيسُرها"[97]؛ و"الجرائم المتعلقة بالمحتوى"؛[98] و"الجرائم المتعلقة بحقوق المؤلف".[99] أما الفئة الرابعة، وهي "الجرائم المتعلقة بالحاسوب"،[100] فلا تركز على موضوع الحماية القانونية بل على الأسلوب المستخدم في ذلك. ويؤدي عدم الاتساق هذا إلى بعض التداخل بين الفئات.

---

(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.

[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 2.9.2.

[98] See below: Chapter 2.5

[99] See below: Chapter 2.6

[100] See below: Chapter 2.7

وبالإضافة إلى ذلك، تغطي بعض المصطلحات المستخدمة لوصف الأفعال الإجرامية (مثل "الإرهاب السيبراني"[101] أو "التصيد الاحتيالي"[102]) أفعالاً تندرج ضمن عدة فئات. ومع ذلك، فإن الفئات التي تتضمنها اتفاقية الجريمة السيبرانية تشكل أساساً مفيداً لمناقشة ظاهرة الجريمة السيبرانية.

3.2 المؤشرات الإحصائية المتعلقة بالجرائم السيبرانية

من الصعب وضع تقدير كمي لتأثير الجريمة السيبرانية على المجتمع.[103] ومن العسير للغاية تقدير حجم الخسائر المالية الناجمة عن الجريمة السيبرانية، وعدد الأفعال المندرجة في إطارها. وتقدر بعض المصادر الخسائر التي تلحق بالشركات والمؤسسات في الولايات المتحدة[104] من جراء الجريمة السيبرانية بمبلغ ضخم يصل إلى 67 مليار دولار أمريكي؛ ولكن ليس من المؤكد ما إذا كان استقراء نتائج عينة مستقاة من دراسة استقصائية أمراً مسوغاً.[105] ويصدق هذا النقد المنهجي لا على حجم الخسائر فحسب، بل يصدق أيضاً على عدد الجرائم التي تم الوقوف عليها.[106]

ومن الصعب قياس عدد الجرائم السيبرانية، لأن المستهدفين بها لا يُبلِّغون دوماً عن هذه الجرائم.[107] ومع ذلك، تستطيع الدراسات الاستقصائية أن تساعد على فهم تأثير الجريمة السيبرانية. غير أن الأمر الأهم من العدد الدقيق للجرائم السيبرانية التي ترتكب في سنة من السنوات هو الاتجاه الذي ترسمه، وهو اتجاه يمكن تبينه من مقارنة النتائج المسجلة على مدى عدة سنوات.

ومن الأمثلة المتاحة في هذا الصدد الدراسة الاستقصائية للجرائم الحاسوبية والأمن الحاسوبي لعام 2007، الصادرة عن معهد الأمن الحاسوبي في الولايات المتحدة،[108] التي تحلل اتجاهات شتى من بينها عدد ما تم ارتكابه من جرائم متعلقة بالحاسوب.[109] وتستند الدراسة إلى ردود 494 من المشتغلين بأمن الحواسيب في شركات ووكالات حكومية ومؤسسات مالية بالولايات المتحدة.[110] وتوثِّق الدراسة عدد الجرائم التي أبلغ عنها المجيبون المشاركون في الاستقصاء بين عامي 2000 و2007، وتبين أن نسبة المجيبين الذين تعرضوا لهجمات فيروسية أو لعمليات تستهدف النفاذ غير المأذون به إلى المعلومات (أو ولوج النظام) قد انخفضت منذ عام 2001. ولا تشرح الدراسة سبب حدوث هذا الانخفاض. غير أن هذا الانخفاض في عدد الجرائم التي تم الوقوف عليها في الفئات المذكورة أمر تؤيده دراسات استقصائية أجرتها مؤسسات أخرى (خلافاً لما توحي به أحياناً التقارير التي تنشرها وسائل الإعلام).[111] وتُلاحظ تطورات مماثلة لدى تحليل إحصاءات الجرائم – ومن ذلك مثلاً أن الإحصاءات الألمانية للجرائم[112] تبين أن الجرائم المتعلقة بالحاسوب، بعد أن وصلت إلى ذروتها في عام 2004، قد انخفضت إلى مستوى قريب من مستواها في عام 2002.

وليس بمقدور الإحصاءات المتعلقة بالجريمة السيبرانية أن توفر معلومات موثوق بها عن نطاق أو مدى انتشار الجرائم.[113] وعدم التيقن من مدى قيام المستهدفين بالجرائم بالإبلاغ عنها،[114] فضلاً عن عدم توافر تفسير لانخفاض عدد الجرائم السيبرانية، يجعلان هذه الإحصاءات عرضة للتأويلات. ولا تتيسر في الوقت الحاضر أدلة كافية تتيح التنبؤ بالاتجاهات والتطورات التي يحملها المستقبل في طياته.

---

[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.*

[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.

4.2 الجرائم التي تستهدف سرية البيانات والنظم الحاسوبية وتكامليتها وتيسرها

تستهدف جميع الجرائم المندرجة في هذه الفئة واحدة (على الأقل) من المبادئ القانونية الثلاثة المتمثلة في السرية، والتكاملية، والتيسُر. وخلافاً للجرائم التي غطاها القانون الجنائي منذ قرون (مثل السرقة أو القتل)، فإن تَحَوسُب الجرائم أمر حديث نسبياً، لأن النظم والبيانات الحاسوبية لم تستحدث إلا منذ ما يقرب من ستين عاماً.[115] وتقتضي الملاحقة القضائية الفعالة لهذه الأفعال أن تحمي أحكام القانون الجنائي الحالية ليس فقط البنود الملموسة والوثائق المادية من التلاعب، بل أن يجري أيضاً توسيع نطاق تلك الأحكام ليشمل هذه المبادئ القانونية الجديدة.[116] ويقدم هذا الفرع لمحة عامة عن أكثر الجرائم التي تندرج في هذه الفئة شيوعاً.

1.4.2 النفاذ غير القانوني (القرصنة، التسلل)[117]

تشير الجريمة التي توصف بـ "القرصنة" إلى نفاذ غير قانوني إلى نظام حاسوبي،[118] وهي واحدة من أقدم الجرائم المتعلقة بالحاسوب.[119] وفي أعقاب تطور الشبكات الحاسوبية (ولا سيما الإنترنت)، أصبحت هذه الجريمة ظاهرة واسعة النطاق.[120] وتشمل الجهات الشهيرة التي استهدفتها هجمات القرصنة الإدارة الوطنية للملاحة الجوية والفضاء بالولايات المتحدة (ناسا)، والقوات الجوية للولايات المتحدة، والبنتاغون، وياهو، وغوغل، وإيباي (Ebay)، والحكومة الألمانية.[121] وتشمل أمثلة جرائم القرصنة ما يلي:

الشكل 1

يوضح الرسم البياني موقعاً على شبكة الويب تم التسلل إليه بالقرصنة. وقد عدّل مرتكب هذا الفعل الصفحة الأولى ليخبر المستخدمين بنجاح هجومه.

- اختراق كلمة السر الخاصة بمواقع الويب المحمية بكلمة سر؛[122]
- الالتفاف على الحماية المكفولة لكلمة السر على الحاسوب.

وتشمل أمثلة الأفعال التحضيرية لذلك ما يلي:

- استخدام الأجهزة أو البرمجيات بطريقة معيبة من أجل الحصول بطريقة غير قانونية على كلمة السر للدخول إلى نظام حاسوبي؛[123]
- إنشاء مواقع "إيهامية" على شبكة الويب لجعل المستخدمين يفصحون عن كلمات السر الخاصة بهم؛[124]
- تركيب أجهزة وبرمجيات تعتمد على أساليب تسجل كل نقرة تضرب على لوحة المفاتيح – وبالتالي أي كلمة سر تستخدم على الحاسوب و/أو الجهاز.[125]

[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.
[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.

وتتباين دوافع مرتكبي هذه الجرائم. فبعضهم يُقصر أنشطته على الالتفاف على التدابير الأمنية لمجرد إثبات ما يتمتعون به من قدرات (كما يتضح ذلك من الشكل 1).[126] ويتصرف آخرون بوحي من دافع سياسي (يعرف باسم "القرصنة الحركية"[127]) – ومن الأمثلة عليه حادث تعرض له مؤخراً الموقع الرئيسي للأمم المتحدة على شبكة الويب.[128] وفي معظم الحالات، لا يقتصر دافع مرتكبي الجريمة على النفاذ غير المشروع إلى النظام الحاسوبي. فهم يستغلون هذا النفاذ لاقتراف مزيد من الجرائم، مثل التجسس على البيانات، أو التلاعب فيها، أو شن هجمات تستهدف الحرمان من النفاذ إلى الخدمات.[129] وفي معظم الحالات، لا يمثل النفاذ غير المشروع إلى النظام الحاسوبي إلا خطوة أولى حيوية.[130]

ويسلم كثير من المحللين بارتفاع عدد محاولات النفاذ غير المشروع إلى النظم الحاسوبية، إذ سُجل في شهر أغسطس وحده من عام 2007 ما يربو على 250 مليون حادث من هذا النوع.[131] ويعزى تزايد عدد هجمات القرصنة إلى ثلاثة عوامل رئيسية هي:

قصور ونقص الحماية الموفرة للنظم الحاسوبية:

هناك مئات الملايين من الحواسيب موصولة بالإنترنت، ويفتقر كثير من النظم الحاسوبية إلى حماية كافية إزاء النفاذ غير القانوني.[132] ويبين التحليل الذي أجرته جامعة مريلاند أن النظام الحاسوبي غير المحمي الموصول بالإنترنت سيتعرض على الأرجح لإحدى الهجمات خلال أقل من دقيقة واحدة.[133] ويمكن الحد من هذا الخطر بتركيب تدابير توفر الحماية، لكن نجاح الهجمات على نظم حاسوبية تتمتع بحماية جيدة يثبت أن التدابير التقنية وحدها لا تستطيع أن تصد الهجمات بصورة كاملة.[134]

استحداث أدوات برمجياتية تُؤتمت الهجمات:

ما برحت تستخدم في الآونة الأخيرة أدوات برمجياتية تستهدف أتمتة الهجمات.[135] ويستطيع أحد الجناة منفرداً، مستعيناً ببرمجيات وهجمات سابقة التبييت، أن يشن خلال يوم واحد هجمات على آلاف النظم الحاسوبية غير مستخدم في ذلك سوى حاسوب واحد.[136] أما إذا اتيح للجاني النفاذ إلى مزيد من الحواسيب – وذلك مثلاً من خلال شبكة مُسَخَّرة[137] – لأستطاع أن يوسع من نطاق هجماته بقدر أكبر. ولما كانت معظم الأدوات البرمجياتية تستخدم أساليب للهجوم سابقة التهيئة، فإن الهجمات لا تكلل جميعها بالنجاح. والمستخدمون الذين يُحيِّنون نظم التشغيل والتطبيقات البرمجياتية الخاصة بهم على نحو منتظم يقللون من احتمال تعرضهم لهذه الهجمات الواسعة النطاق، لأن الشركات التي تُطور برمجيات الحماية تحلل الأدوات المستخدمة في الهجوم وتستعد لصد هجمات القرصنة المعيارية.

والهجمات التي تجتذب الأنظار تستند في كثير من الأحيان إلى هجمات مصممة بشكل فردي. ولا يعزى نجاح تلك الهجمات في أحيان كثيرة إلى اتباع أساليب فائقة التطور، بل إلى عدد النظم الحاسوبية المتعرضة للهجوم. والأدوات التي تسمح بشن هذه الهجمات المُعيَّرة تتوافر بصورة

---

[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.

[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.

واسعة على شبكة الإنترنت[138] – بعضها مجاناً لكن أشدها كفاءة قد تصل تكلفته بسهولة إلى عدة آلاف من الدولارات الأمريكية.[139] ومن الأمثلة على ذلك أداة قرصنة تسمح للجاني بتحديد مجموعة من عناوين بروتوكول الإنترنت (وذلك مثلاً من 112.2.0.0 إلى 111.9.253.253). وتسمح البرمجيات بمسح المنافذ غير المحمية لجميع الحواسيب التي تستخدم أحد عناوين بروتوكول الإنترنت المحددة.[140]

تنامي دور حواسيب الأفراد في استراتيجيات القراصنة:

لا يشكل النفاذ إلى النظام الحاسوبي في كثير من الأحيان الدافع الرئيسي للهجوم.[141] ولما كانت حواسيب الشركات تتمتع بوجه عام بحماية أفضل من حواسيب الأفراد، فمن الأصعب شن الهجمات على حواسيب الشركات باستخدام أدوات برمجياتية سابقة التشكيل.[142] وخلال السنوات الماضية، ركز الجناة هجماتهم بصورة متزايدة على حواسيب الأفراد، لأن العديد منها لا يتمتع بحماية كافية. كما أن حواسيب الأفراد تحتوي في أحيان كثيرة على معلومات حساسة (مثل البيانات المتعلقة ببطاقات الائتمان والحسابات المصرفية). ويستهدف الجناة أيضاً حواسيب الأفراد لأن الجناة يستطيعون، بعد نجاح هجومهم، أن يدرجوا هذه الحواسيب في الشبكات المُسخّرة الخاضعة لهم فيستخدمون تلك الحواسيب في مزيد من الأنشطة الإجرامية.[143]

ويمكن النظر إلى النفاذ غير القانوني إلى النظام الحاسوبي على أنه يماثل النفاذ غير القانوني إلى مبنى ما، وهو يعتبر فعلاً إجرامياً في بلدان كثيرة.[144] ويبين تحليل النُهج المختلفة إزاء تجريم النفاذ إلى الحواسيب أن الأحكام التي تم سنها تخلط في بعض الأحيان بين النفاذ غير القانوني والجرائم اللاحقة عليه، أو تحاول أن تُقصر تجريم النفاذ غير القانوني على الانتهاكات الخطيرة وحدها. وتجرّم بعض الأحكام النفاذ الأولي، في حين تجعل نُهج أخرى الفعل الإجرامي قاصراً على الحالات التي يكون فيها:

- النظام الذي تم النفاذ إليه محمياً بتدابير أمنية؛[145] و/أو
- لمرتكب الفعل نوايا ضارة؛[146] و/أو
- قد تم الحصول على بيانات أو تعديلها أو إتلافها.

وثمة نظم قانونية أخرى لا تجرم النفاذ في حد ذاته بل تركز على الجرائم اللاحقة عليه.[147]

2.4.2 التجسس على البيانات

تخزن المعلومات الحساسة في النظم الحاسوبية في كثير من الأحيان. وإذا كان النظام الحاسوبي موصولاً بالإنترنت، فإن الجناة يستطيعون أن يسعوا إلى النفاذ إلى هذه المعلومات عن طريق الإنترنت من أي مكان تقريباً في العالم.[148] ويتنامى استخدام الإنترنت للحصول بصورة متزايدة على الأسرار التجارية.[149] وقيمة المعلومات الحساسة، والقدرة على النفاذ إليها عن بعد، يجعلان التجسس على البيانات محط اهتمام كبير. وفي ثمانينات

[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.

[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/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

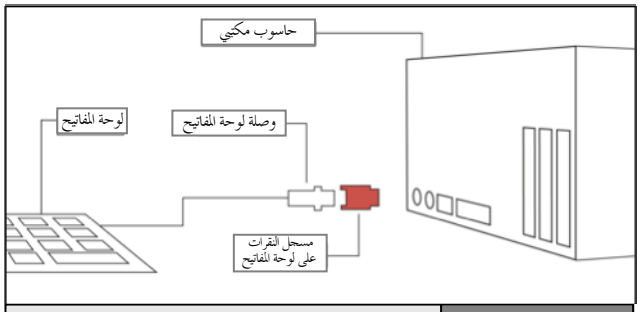
[149] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage — 2003, page 1, available at: http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

القرن الماضي، نجح عدد من القراصنة الألمان في الدخول إلى النظم الحاسوبية الحكومية والعسكرية للولايات المتحدة والحصول على معلومات سرية، وباعوا هذه المعلومات إلى عملاء للاتحاد السوفييتي.[150]

ويستخدم الجناة تقنيات مختلفة للنفاذ إلى حواسيب الضحايا،[151] تشمل ما يلي:

- استخدام برمجيات تمسح المنافذ غير المحمية؛[152]
- استخدام برمجيات تتحايل على تدابير الحماية؛[153]
- "الهندسة الاجتماعية".[154]

والنهج الأخير على وجه الخصوص، أي نهج "الهندسة الاجتماعية"، الذي يشير إلى نوع غير تقني من الاقتحام يعتمد اعتماداً شديداً على التفاعل البشري وينطوي في كثير من الأحيان على خداع الآخرين لاختراق الإجراءات الأمنية العادية، يثير الاهتمام لأنه لا يستند إلى وسائل تقنية.[155] و"الهندسة الاجتماعية" ليست بحال من الأحوال أقل السبل فعالية في شن الهجمات على النظم الحاسوبية المتمتعة بحماية جيدة. وهي تصف كذلك التلاعب بالبشر بغرض النفاذ إلى النظم الحاسوبية.[156] وتعد الهندسة الاجتماعية عادةً ناجحة للغاية، لأن أضعف حلقة في أمن الحاسوب تتمثل أحياناً كثيرة في المستخدمين الذين يقومون بتشغيل النظام الحاسوبي.



الشكل 2

يوضح الرسم البياني كيف تُركب أجهزة تسجيل النقرات على لوحة المفاتيح. فمعظم هذه الأدوات – الشبيهة بمكيف القِدرة – توضع بين واصل لوحة المفاتيح والحاسوب. وبعض الأجهزة الأحدث عهداً تكون مبيتة في لوحة المفاتيح، بحيث يتعذر العثور عليها دون فتح الجهاز. وليس بمقدور برمجيات مكافحة الفيروسات أن تكتشف أجهزة تسجيل النقرات على لوحة المفاتيح متى كانت مركبة في الجهاز.

ومن ذلك مثلاً، أن "التصيد الاحتيالي" قد أصبح مؤخراً من الجرائم الرئيسية التي ترتكب في الفضاء السيبراني،[157] وهو يصف محاولات الحصول بالاحتيال على معلومات حساسة (مثل كلمات السر) عن طريق التخفي – وراء رسالة إلكترونية تبدو كما لو كانت رسالة رسمية – على هيئة شخصية أو شركة (مؤسسة مالية مثلاً) جديرة بالثقة.

وعلى الرغم من أن الضعف البشري للمستخدمين يفتح الباب أمام خطر الخداع، فإن العنصر البشري يوفر الحلول أيضاً. فليس من السهل على الجناة الإيقاع بمستخدمي الحاسوب الواعين. ولذا تشكل توعية المستخدمين جزءاً جوهرياً في أي استراتيجية لمكافحة الجريمة السيبرانية.[158] وتسلط منظمة التعاون والتنمية في الميدان الاقتصادي الضوء على أهمية التجفير بالنسبة للمستخدمين، لأن بمقدوره أن يساعد على تحسين حماية البيانات.[159] وإذا استخدم الشخص أو المنظمة التي تخزن المعلومات تدابير الحماية السليمة، فإن الحماية التي يوفرها التجفير يمكن أن تكون أكثر فعالية من أي حماية مادية.[160] فنجاح الجناة في الحصول على معلومات حساسة يعزى في أحيان كثيرة إلى غياب تدابير الحماية.

---

[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.

[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.

وعلى الرغم من أن الجناة يستهدفون عادةً الأسرار التجارية، فإن البيانات المخزنة في حواسيب الأفراد تُستهدف بدورها على نحو متزايد.[161] فالمستخدمون الأفراد كثيراً ما يخزنون المعلومات المتعلقة بالحسابات المصرفية وبطاقات الائتمان الخاصة بهم على حواسيبهم.[162] ويستطيع الجناة استخدام هذه المعلومات في أغراضهم الخاصة (كاستغلال بيانات الحسابات المصرفية في تحويل أموال) أو بيعها لطرف ثالث.[163] فسجلات بطاقات الائتمان مثلاً تباع بمبلغ يصل إلى 60 دولاراً أمريكياً.[164] وتركيز القراصنة على حواسيب الأفراد أمر لافت للنظر، لأن الأرباح التي يمكن جنيها من الأسرار التجارية تعد عادةً أعلى من الأرباح المحققة من الحصول على معلومات خاصة ببطاقة ائتمان واحدة أو من بيعها. ولكن لما كانت حواسيب الأفراد تتمتع عامةً بقدر أقل من الحماية، فإن التجسس على البيانات المخزنة في حواسيب الأفراد يكون على الأرجح أعلى ربحاً.

وهناك نهجان للحصول على المعلومات:

- عن طريق النفاذ إلى نظام حاسوبي أو جهاز لتخزين البيانات واستخلاص المعلومات؛ أو
- عن طريق اللجوء إلى التلاعب لحمل المستخدمين على الإفصاح عن المعلومات أو شفرات النفاذ التي تمكن الجناة من النفاذ إلى المعلومات ("التصيد الاحتيالي").

ويستخدم الجناة في أحيان كثيرة الأدوات الحاسوبية المركبة في حواسيب الضحايا أو برمجيات خبيثة تُدعى برمجيات التجسس في نقل البيانات إليهم.[165] قد اكتشفت في السنوات الأخيرة أنواع مختلفة من برمجيات التجسس، مثل مسجلات النقرات على لوحة المفاتيح.[166] ومسجلات النقرات على لوحة المفاتيح هذه هي أدوات برمجياتية تسجل كل نقرة تُوقَّع على لوحة مفاتيح حاسوب مصاب.[167] وبعض هذه المسجلات ترسل كل المعلومات المسجلة إلى الجاني، بمجرد توصيل الحاسوب بالإنترنت. وبعضها يُجري فرزاً وتحليلاً أوليين للبيانات المسجلة (مع التركيز مثلاً على المعلومات التي يحتمل أن تخص بطاقات الائتمان[168]) كيلا تنقل إلا أهم البيانات المكتشفة.

وتتوافر أيضاً أجهزة مماثلة في صورة أجهزة عتادية توصَّل بين لوحة المفاتيح والنظام الحاسوبي لتسجيل النقرات الموقَّعة على لوحة المفاتيح (انظر الشكل 4). ومسجلات النقرات العتادية من الصعب تركيبها واكتشافها، لأنها تتطلب النفاذ المادي إلى النظام الحاسوبي.[169] ولذا، فإن أدوات مكافحة برمجيات التجسس والفيروسات تعجز إلى حد كبير عن اكتشافها.[170]

وإلى جانب النفاذ إلى النظم الحاسوبي، يستطيع الجناة أن يحصلوا على المعلومات عن طريق التلاعب بالمستخدم. وقد استحدث الجناة، في الآونة الأخيرة، خدعاً فعالة للحصول على المعلومات السرية (مثل المعلومات المتعلقة بالحسابات المصرفية والبيانات المتعلقة ببطاقات الائتمان) عن طريق التلاعب بالمستخدم بواسطة تقنيات الهندسة الاجتماعية.[171] وقد أصبح "التصيد الاحتيالي" مؤخراً واحدة من أهم الجرائم المتعلقة بالفضاء السيبراني.[172] ويستخدم مصطلح "التصيد الاحتيالي" لوصف نوع من الجرائم يتسم بمحاولة الحصول بالاحتيال على معلومات حساسة، مثل كلمات السر عن طريق التخفي – وراء رسالة إلكترونية تبدو كما لو كانت رسالة رسمية – على هيئة شخصية أو شركة (مؤسسة مالية مثلاً) جديرة بالثقة.[173]

---

[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

[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.

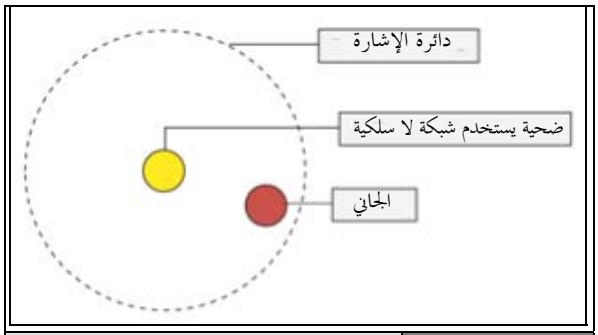
[173] For more information on the phenomenon of phishing see below: Chapter 2.8.4.

والتجسس على البيانات نموذج آخر لجريمة تستهدف ببراعة أضعف حلقة في أمن الحاسوب، ألا وهي المستخدم. وأخذ هذا الأمر بعين الاعتبار يبين بجلاء المخاطر التي تنطوي عليها الخدع الاحتيالية. ولكن ذلك يفتح الباب أيضاً أمام الحلول. فليس من السهل على الجناة الإيقاع بمستخدمي الحاسوب الواعين. ويسلط هذا الضوء على أهمية توعية المستخدمين بوصفها جزءاً جوهرياً في أي استراتيجية لمكافحة الجريمة السيبرانية.[174]

وتخزن المعلومات الحساسة بصورة متزايدة على النظم الحاسوبية. ومن الجوهري تقييم ما إذا كانت التدابير التقنية التي يتخذها المستخدمون تعد كافية، أو ما إذا كان يتعين على المشرعين أن يوفروا حماية إضافية بتجريم التجسس على البيانات.[175]

3.4.2 الاعتراض غير القانوني

يستطيع الجناة أن يعترضوا الاتصالات بين المستخدمين[176] (مثل الرسائل الإلكترونية) أو أن يعترضوا عمليات نقل البيانات (لدى قيام المستخدمين بتحميل البيانات على مُخدّم على الويب، أو النفاذ إلى وسائط للتخزين الخارجي معتمدة على الويب[177]) من أجل تسجيل البيانات التي يجري تبادلها. ويستطيع الجناة أن يستهدفوا أي بنية أساسية للاتصالات (مثل الخطوط الثابتة أو اللاسلكية) وأي خدمة توفر عن طريق الإنترنت (مثل البريد الإلكتروني، أو الدردشة، أو الاتصالات عن طريق نقل الصوت باستخدام بروتوكول الإنترنت[178]).



الشكل 3

يوضح الرسم البياني سيناريو هجوم موجه ضد مستخدم حاسوب يستعمل اتصالاً بشبكة لا سلكية. ويستطيع الجاني الذي يريد اعتراض البيانات المرسلة والمستلَمة أن يقوم بذلك من أي موقع داخل دائرة الإشارة. وتبعاً للمُوجّه اللاسلكي ولموقعه، يمكن اعتراض الإشارات داخل دائرة يصل نصف قطرها إلى 100 متر.

وتتمتع معظم عمليات نقل البيانات بين موفري البنية التحتية للإنترنت أو مقدمي خدمة الإنترنت بحماية جيدة ومن الصعب اعتراضها.[179] غير أن الجناة يبحثون عن النقاط الضعيفة في النظام. وتتمتع التكنولوجيات اللاسلكية بشعبية أكبر، وتبين خبرة الماضي أنها قليلة المنعة.[180] واليوم، توفر الفنادق والمطاعم والحانات لعملائها إمكانية النفاذ إلى الإنترنت عن طريق نقاط نفاذ لا سلكية. بيد أن الإشارات المستخدمة في تبادل البيانات بين الحاسوب ونقطة النفاذ اللاسلكية يمكن استقبالها ضمن حدود دائرة يصل نصف قطرها إلى 100 متر.[181] وبمقدور الجناة الذين يريدون أن يعترضوا عملية لتبادل البيانات أن يقوموا بذلك من أي موقع داخل هذه الدائرة (الشكل 3). وحتى عندما تكون الاتصالات اللاسلكية مجفرة، قد يستطيع الجناة أن يفكوا تجفير البيانات المسجلة.[182]

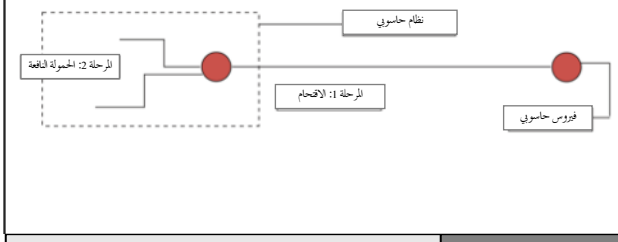
وكيما يتمكن الجناة من النفاذ إلى المعلومات الحساسة، ينشئ بعضهم نقاط نفاذ بالقرب من المواقع التي يوجد بها طلب مرتفع على النفاذ اللاسلكي[183] (بجوار الحانات والفنادق مثلاً). ويُسمى موقع المحطة في كثير من الأحيان بطريقة تسوق المستخدمين الذين يبحثون عن نقطة نفاذ إلى الإنترنت إلى أن يختاروا على الأرجح نقطة النفاذ الاحتيالية المعنية. وإن كان المستخدمون يعتمدون على مقدم خدمة النفاذ في ضمان أمن اتصالاتهم دون تنفيذ تدابير أمنية خاصة بهم، فإن الجناة يستطيعون أن يعترضوا اتصالاتهم بسهولة.

---

[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.
[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.

ولا يحول استخدام الخطوط الثابتة دون الجناة واعتراض الاتصالات.[184] فعمليات نقل البيانات التي تمر عبر السلك تصدر عنها طاقة كهرمغنطيسية.[185] وإن استخدم الجناة المعدات الصحيحة، لكان باستطاعتهم أن يكشفوا ويسجلوا هذه الانبعاثات[186] وربما تمكنوا من تسجيل عمليات نقل البيانات بين حواسيب المستخدمين والشبكة الموصولين بها، وكذلك داخل النظام الحاسوبي.[187]

وقد عمدت معظم البلدان إلى حماية استخدام خدمات الاتصالات بتجريم الاعتراض غير القانوني للمكالمات الهاتفية. ولكن مع تنامي شعبية الخدمات المعتمدة على بروتوكول الإنترنت قد يتعين على المشرعين أن يقيّموا إلى أي مدى تتوافر حماية مماثلة للخدمات المعتمدة على بروتوكول الإنترنت.[188]



الشكل 4

يوضح الرسم البياني أداء فيروس حاسوبي. فبعد إصابة النظام الحاسوبي (المرحلة 1)، يُفعّل الفيروس الحمولة النافعة المبرمجة (المرحلة 2) وقد تتمثل هذه في حذف ملفات معينة أو تخفيرها.

4.4.2 التدخل في البيانات

تتسم البيانات الحاسوبية بأهمية حيوية للمستخدمين الأفراد وللشركات والإدارات لأن هذه الأطراف تعتمد جميعاً على تكاملية البيانات وتيسُرها.[189] والعجز عن النفاذ إلى البيانات يمكن أن يسفر عن ضرر (مالي) كبير. ويستطيع المهاجمون أن ينتهكوا تكاملية البيانات وأن يتدخلوا فيها عن طريق ما يلي:[190]

- حذف البيانات؛ و/أو
- حجب البيانات؛ و/أو
- تحوير البيانات؛ و/أو
- تقييد النفاذ إلى البيانات.

ومن الأمثلة الشائعة لحذف البيانات الفيروس الحاسوبي.[191] ومنذ البدايات الأولى لاستحداث التكنولوجيا الحاسوبية، كانت الفيروسات الحاسوبية تهدد المستخدمين الذين لم يقوموا بتركيب وسائل الحماية السليمة.[192] ومنذ ذلك الحين، ما برح عدد الفيروسات الحاسوبية يتزايد بدرجة ملموسة.[193] ويتمثل تطوران رئيسيان استجدا مؤخراً في:

- الطريقة التي تتوزع بها الفيروسات؛
- والحمولة المؤثرة.[194]

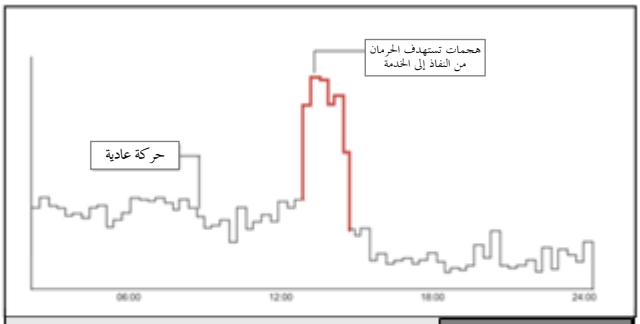
ففي السابق كانت الفيروسات الحاسوبية توزع عن طريق أجهزة تخزين مثل الأقراص المرنة، في حين أن معظم الفيروسات توزع اليوم عن طريق الإنترنت على هيئة مرفقات أو ملفات يقوم المستخدمون بتنزيلها من الإنترنت.[195] وقد سرّعت أساليب التوزيع الفعالة الجديدة هذه على نحو هائل من الإصابة بالفيروسات، وزادت بدرجة ضخمة من عدد النظم الحاسوبية المصابة. وتشير التقديرات إلى أن الدودة الحاسوبية المسماة (SQL Slammer)[196] قد أصابت 90% من النظم الحاسوبية القليلة المنعة في غضون عشرة دقائق من توزيعها.[197] ويقدر الضرر المالي الذي

---

[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.
[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.

تسببت فيه الهجمات الفيروسية في عام 2000 وحده بنحو 17 مليار دولار أمريكي.[198] وظل هذا الضرر كبيراً في عام 2003 إذ بلغ آنذاك ما يربو على 12 مليار دولار أمريكي.[199]

وتقوم معظم الفيروسات الحاسوبية المنتمية إلى الجيل الأول إما بحذف بيانات أو بعرض رسائل (انظر الشكل 4). وقد تنوعت الحمولات المؤثرة في الآونة الأخيرة.[200] فقد أصبحت الفيروسات الحديثة قادرة على تركيب أبواب خلفية تمكن الجناة من التحكم عن بعد في حاسوب الضحية أو من تجفير الملفات مما يحرم الضحايا من النفاذ إلى الملفات الخاصة بهم إلى أن يدفعوا مبلغاً من المال نظير الحصول على المفتاح اللازم لذلك.[201]



الشكل 5

يوضح الرسم البياني عدد طلبات النفاذ إلى موقع ويب أثناء التشغيل العادي (باللون الأسود)، وأثناء هجوم يستهدف الحرمان من النفاذ إلى الخدمة. فإذا لم يتمكن المُحدّم المتعرض للهجوم من مناولة العدد المتزايد من الطلبات، فإن الهجوم يمكن أن يبطئ من سرعة استجابة الموقع أو أن يُخمد الخدمة تماماً.

5.4.2 التدخل في النظام

الشواغل المتعلقة بالهجمات الموجهة ضد البيانات الحاسوبية تصدق هي ذاتها على الهجمات الموجهة ضد النظم الحاسوبية. فقد باتت مزيد من الشركات تدرج في عملياتها الإنتاجية خدمات الإنترنت مما يوفر خدماتها على مدار الأربع والعشرين ساعة ويتيح النفاذ إليها على النطاق العالمي.[202] وإذا نجح الجناة في منع النظم الحاسوبية من العمل بشكل سلس لألحق هذا خسائر مالية ضخمة بالضحايا.[203]

ويمكن شن الهجمات عن طريق القيام بهجمات مادية على النظم الحاسوبية.[204] ولو تمكن الجناة من النفاذ إلى النظام الحاسوبي لأصبح بمقدورهم أن يدمروا المعدات. وبالنسبة لمعظم النظم القانونية، لا تطرح حالات الهجوم المادي عن بعد مشكلات كبرى لأنها تشبه الحالات التقليدية لإتلاف الممتلكات أو تدميرها. أما بالنسبة للشركات التي تمارس التجارة الإلكترونية، فإن الأضرار المالية الناجمة عن الهجمات على النظام الحاسوبي تكون في كثير من الأحيان أكبر بكثير من مجرد تكلفة المعدات الحاسوبية.[205]

وتطرح الخدع الاحتيالية مزيداً من التحديات على النظم القانونية. ومن أمثلة الهجمات المنفذة عن بعد ضد النظم الحاسوبية ما يلي:

- الديدان الحاسوبية؛[206]
- الهجمات الرامية إلى الحرمان من النفاذ إلى الخدمة.[207]

---

[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.

[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.

[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.

والديدان الحاسوبية[208] هي مجموعة فرعية من البرمجيات الخبيثة (مثل الفيروسات الحاسوبية). وهي برامج حاسوبية تتناسخ ذاتياً وتلحق الضرر بالشبكة عن طريق استهلال عمليات متعددة لنقل البيانات. وهي تستطيع أن تؤثر في النظم الحاسوبية عن طريق:

- تبعاً للحمولة المؤثرة للدودة الحاسوبية، يمكن أن تؤدي الإصابة إلى وقف التشغيل السلس للنظام الحاسوبي وإلى استخدام الدودة لموارد النظام من أجل استنساخ ذاتها على الإنترنت؛
- إنتاج حركة على الشبكة يمكن أن تُوقف توافر خدمات معينة (مثل مواقع الويب).

وفي حين تؤثر الديدان الحاسوبية بوجه عام على الشبكة بأسرها دون استهداف نظم حاسوبية محددة، فإن الهجمات الرامية إلى الحرمان من النفاذ إلى الخدمة تستهدف نظماً حاسوبية بعينها. فهذا النوع من الهجمات يجعل الموارد الحاسوبية غير متيسرة للمستخدمين المفترضين لها.[209] فعن طريق استهداف نظام حاسوبي بطلبات تفوق قدرته على مناولتها (انظر الشكل 7)، يستطيع الجناة أن يمنعوا المستخدمين من النفاذ إلى النظام الحاسوبي، أو الاطلاع على رسائل البريد الإلكتروني، أو قراءة الأخبار، أو حجز مكان على رحلة جوية، أو تنزيل الملفات. وفي عام 2000، شُنت في غضون فترة قصيرة هجمات تستهدف الحرمان من النفاذ ضد شركات معروفة مثل السي إن إن وإيباي (Ebay) وأمازون[210] وأسفر ذلك عن عدم تيسر بعض الخدمات لعدة ساعات بل ولعدة أيام.[211]

وتطرح الملاحقة القضائية لهذه الهجمات ولهجمات الديدان الحاسوبية تحديات خطيرة على معظم النظم الحاسوبية، لأن هذه الهجمات قد لا تنطوي على أي تأثير مادي على النظم الحاسوبية. وإلى جانب الحاجة الأساسية إلى تجريم الهجمات المعتمدة على الويب،[212] فإن مسألة ما إذا كانت الوقاية من الهجمات ضد البنية التحتية الحاسمة والملاحقة القضائية لها تحتاج إلى نهج تشريعي منفصل، ما زالت مسألة قيد النقاش.

5.2 الجرائم المتعلقة بالمحتوى

تغطي هذه الفئة المحتوى الذي يعتبر غير قانوني، ويشمل ذلك استغلال الأطفال في المواد الإباحية، والمواد الحاضة على كراهية الأجانب، أو توجيه الإهانات إلى الرموز الدينية.[213] ووضع صكوك قانونية للتعامل مع هذه الفئة يعد أشد تأثراً إلى حد بعيد بالنُهج الوطنية التي يمكن أن تأخذ المبادئ الثقافية والقانونية الأساسية في الاعتبار. ففيما يخص المحتوى غير القانوني، تتباين نظم القيم والنظم القانونية تبايناً واسعاً فيما بين المجتمعات. فنشر المواد الحاضة على كراهية الأجانب أمر غير قانوني في كثير من البلدان الأوروبية،[214] ولكنه يمكن أن يكون مشمولاً بالحماية بموجب مبدأ حرية

[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*.

[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.

التعبير[215] في الولايات المتحدة.[216] كما أن استخدام عبارات مسيئة للنبي أمر مجرم في كثير من البلدان العربية،[217] ولكن ليس في بعض البلدان الأوروبية.

وتعد هذه التحديات القانونية مركبة، لأن المعلومات التي تستخدم في أحد البلدان يمكن النفاذ إليها من أي مكان آخر في العالم تقريباً.[218] وإذا ما قام "الجناة" بإنتاج محتوى غير قانوني في بعض البلدان، لكن ليس في البلد الذي يعملون انطلاقاً منه، فإن الملاحقة القضائية لهم قد تكون صعبة إن لم تكن مستحيلة.[219]

وهناك افتقار واسع إلى الاتفاق بشأن محتوى المواد وبشأن المدى المحدد الذي ينبغي عنده تجريم أفعال معينة. وقد أسهم تباين الآراء الوطنية والصعوبات المصادفة في الملاحقة القضائية للانتهاكات المرتكبة خارج أراضي البلد القائم بالتحقيق في حجب أنواع معينة من المحتوى على الإنترنت. وعندما ينعقد الاتفاق على منع النفاذ إلى مواقع ويب تحتوي على محتوى غير قانوني ويوجد مركزها خارج البلد، تستطيع الدول أن تطبق قوانين صارمة وتحجب مواقع الويب وترشّح المحتوى.[220]

وتتبع نهج متنوعة في ترشيح النظم. ويتطلب أحد الحلول أن يقوم مقدمو خدمة النفاذ بتركيب برامج تحلل مواقع الويب التي تجري زيارتها وبحجب المواقع المدرجة على قائمة سوداء.[221] ويتمثل الحل الآخر في تركيب برمجيات ترشيح على حاسوب المستخدم (وهذا نهج مفيد للآباء الذين يريدون أن يتحكموا في المحتوى الذي يستطيع أولادهم أن يطلعوا عليه، وهو مفيد كذلك للمكتبات والوحدات المطرافية العمومية الموصولة بالإنترنت).[222]

والمحاولات الرامية إلى التحكم في المحتوى المنشور على الإنترنت لا تقتصر على أنواع معينة من المحتوى تتفق الآراء بشكل واسع على أنها غير قانونية. وتستخدم بعض البلدان تكنولوجيا الترشيح لتقييد النفاذ إلى مواقع الويب التي تتناول مسائل سياسية. وتفيد مبادرة الإنترنت المفتوحة (OpenNet Initiative)[223] أن هذا النوع من الرقابة يمارس في الوقت الحاضر في أكثر من عشرين بلداً.[224]

---

[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.*

[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.

1.5.2 المواد المثيرة جنسياً أو المواد الإباحية (باستثناء استغلال الأطفال في المواد الإباحية)

كان المحتوى المتعلق بالجنس من أول أنواع المحتوى التي وزعت تجارياً عن طريق الإنترنت، فهو يوفر لتجار التجزئة في المواد المثيرة جنسياً والمواد الإباحية مزايا تشمل:

- تبادل الوسائط (مثل الصور، والأفلام، والتغطية الحية) دون الحاجة إلى تحمل تكاليف شحن باهظة؛[225]
- النفاذ العالمي،[226] الذي يتيح الوصول إلى عدد من الزبائن أكبر كثيراً من متاجر التجزئة؛
- كثيراً ما ينظر إلى الإنترنت على أنها وسيط مجهول الهوية (بطريقة خاطئة في أحيان كثيرة[227]) – وهذا الجانب يحظى بتقدير مستهلكي المواد الإباحية، بحكم الآراء الاجتماعية السائدة.

الشكل 6

يوضح هذا الرسم البياني أحد النُهج المستخدمة لمنع نفاذ القصر إلى مواقع الويب التي تحتوي على مضمون إباحي. ولما كان هذا الحل لا يتيح التحقق من صحة إجابة المستخدم، فإنه لا يعتبر حلاً مناسباً في عدد من البلدان.

ووقفت بحوث أجريت مؤخراً على أن الإنترنت يتوافر عليها في أي وقت نحو 4,2 ملايين موقع إباحي.[228] وإلى جانب مواقع الويب، يمكن توزيع المواد الإباحية عن طريق:

- التبادل باستخدام نظم تقاسم الملفات؛[229]
- التبادل في حجرات الدردشة المغلقة.

وتجرم البلدان المختلفة المواد المثيرة جنسياً والمواد الإباحية بدرجات متباينة. فبعض البلدان تسمح بتبادل المواد الإباحية بين الكبار وتقصر التجريم على الحالات التي ينفذ فيها القصر إلى هذا النوع من المواد،[230] ساعية بذلك إلى حماية القصر.[231] وتبين الدراسات أن نفاذ الأطفال إلى المواد الإباحية يمكن أن يؤثر تأثيراً سلبياً على تطورهم.[232] وامتثالاً لهذه القوانين، استحدثت "نظم للتحقق من بلوغ السن" (انظر الشكل 6).[233] وتجرم بلدان أخرى أي تبادل للمواد الإباحية حتى بين الكبار،[234] مع التركيز على مجموعات بعينها (مثل القصر).

---

[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.

[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; […]

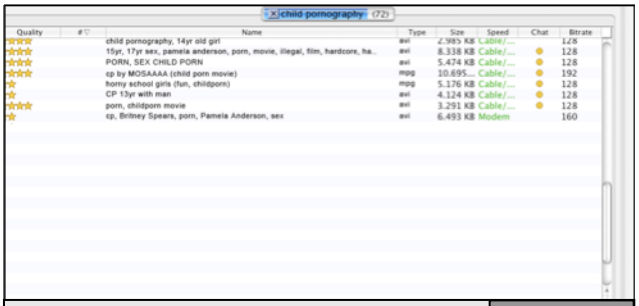
[231] Regarding this aspect see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

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

ويمثل منع النفاذ إلى المواد الإباحية تحدياً أمام البلدان التي تجرم التعامل مع هذه المواد. وخارج الإنترنت تستطيع السلطات في كثير من الأحيان أن تكتشف انتهاكات الحظر المفروض على المواد الإباحية وأن تلاحقها قضائياً. أما على الإنترنت، فإن إنفاذ هذه التدابير يكون صعباً، لأن المواد الإباحية تتوافر بسهولة في أحيان كثيرة على مخدّمات تقع خارج البلد. وحتى إذا تمكنت السلطات من تحديد مواقع الويب التي تحتوي على مواد إباحية، فإنها قد لا تملك الصلاحية التي تمكنها من إلزام مقدمي الخدمة بإزالة المحتوى المشين.



الشكل 7

يوضح هذا الرسم البياني السطح البيني الخاص بالمستخدم في برمجيات اقتسام الملفات. فبعد تقديم طلب يتضمن مصطلح "مواد إباحية تتعلق بالأطفال"، تعرض البرمجيات كل الملفات التي يوفرها مستخدمو نظام اقتسام الملفات التي تحتوي على ذلك المصطلح.

ومبدأ *السيادة الوطنية* لا يسمح بوجه عام لبلد من البلدان بأن يجري تحقيقات داخل أراضي بلد آخر، دون إذن من السلطات المحلية.[235] وحتى عندما تلتمس السلطات دعم البلدان التي تعمل انطلاقاً من مواقع الويب المشينة، فإن نجاح التحقيقات والعقوبات الجنائية قد يعوقه مبدأ "الإجرام المزدوج".[236] وعملاً على منع النفاذ إلى المحتوى الإباحي، فإن البلدان التي تطبق قوانين صارمة بشكل استثنائي لا يبقى أمامها في أحيان كثيرة سوى المنع (وذلك مثلاً باستخدام تكنولوجيا الترشيح[237]) للحد من فرص النفاذ إلى مواقع معينة على الويب.[238]

2.5.2 المواد الإباحية التي يُستغل فيها الأطفال

إذا كانت الآراء تتباين بشأن المواد الإباحية التي تصور الكبار، فإن المواد الإباحية التي يُستغل فيها الأطفال تلقى إدانة واسعة، وينظر على نطاق واسع إلى الأفعال المتعلقة بها على أنها أفعال إجرامية.[239] وتشارك منظمات دولية في مكافحة ما يُنشر على الخط من مواد إباحية يُستغل فيها الأطفال،[240] وطرحت في هذا الصدد عدة مبادرات قانونية دولية تشمل فيما تشمله: اتفاقية الأمم المتحدة لحقوق الطفل لعام 1989؛[241] والمقرر الإطاري لمجلس الاتحاد الأوروبي بشأن مكافحة الاستغلال الجنسي للأطفال واستخدام الأطفال في المواد الإباحية لعام 2003؛[242] واتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي لعام 2007.[243]

---

[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.

[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.

ومن المؤسف أن هذه المبادرات الرامية إلى مكافحة توزيع المواد الإباحية على الشبكة لم توفر رادعاً يُذكر للقائمين بالتوزيع، الذين يستخدمون الإنترنت لنشر وتبادل المواد الإباحية التي يُستغل فيها الأطفال (انظر الشكل 7).[244] وساعدت زيادة عرض النطاق على تبادل محفوظات الأفلام والصور.

وبينت البحوث المتعلقة بسلوك منتجي المواد الإباحية التي يُستغل فيها الأطفال أن 15% ممن أُلقي القبض عليهم بسبب حيازة مواد من هذا النوع منشورة على الإنترنت، قد عثر في حواسيبهم على ما يزيد على 1000 صورة؛ وأن 80% منهم كانوا يحتفظون في حواسيبهم بصور لأطفال تتراوح أعمارهم بين 6 أعوام و12 عاماً؛[245] وأن 19% منهم كان لديهم صور لأطفال تقل أعمارهم عن 3 أعوام؛[246] وأن 21% منهم كانت لديهم صور تُظهر مشاهد عنف.[247]

ويدر بيع المواد الإباحية التي يُستغل فيها الأطفال أرباحاً طائلة؛[248] إذ يكون جامعوها مستعدين لدفع مبالغ كبيرة للحصول على أفلام وصور تعرض مشاهد لأطفال في سياق جنسي.[249] وتعثر محركات البحث على هذه المواد بشكل سريع.[250] ويجري تبادل معظم المواد في منتديات مغلقة محمية بكلمة سر لا يستطيع المستخدمون العاديون ووكالات إنفاذ القانون النفاذ إليها إلا فيما ندر. ولذا تتسم العمليات السرية بأهمية حيوية في مكافحة المواد الإباحية التي يُستغل فيها الأطفال.[251]

وثمة عاملان رئيسيان في استخدام تكنولوجيا المعلومات والاتصال لتبادل المواد الإباحية التي يُستغل فيها الأطفال يطرحان صعوبات أمام التحقيق في هذه الجرائم وهما:

1 استخدام العملات الافتراضية والسداد المجهول الهوية[252]:

يُمكّن السداد النقدي بائعي سلع معينة من إخفاء هويتهم، ولذا يهيمن التعامل النقدي على كثير من الأنشطة الإجرامية. وأدى الطلب على السداد المجهول الهوية إلى استحداث نظم للدفع الافتراضي وللعملات الافتراضية تسمح بالسداد المجهول الهوية.[253] فالعملات الافتراضية قد لا تقتضي تحديد الهوية والتأكد منها، مما يمنع وكالات إنفاذ القانون من تعقب تدفقات الأموال رجوعاً إلى مرتكبي الأفعال الإجرامية. ونجح مؤخراً عدد من التحقيقات بشأن المواد الإباحية التي يُستغل فيها الأطفال في استخدام آثار تخلفت عن عمليات السداد في كشف الجناة.[254] ولكن عندما يُجري الجناة عملية سداد مجهول الهوية يكون من الصعب تعقبهم.

2 استخدام تكنولوجيا التجفير[255]:

يلجأ الجناة على نحو متزايد إلى تجفير رسائلهم. وتلاحظ وكالات إنفاذ القانون أن الجناة يستخدمون هذه التكنولوجيا لحماية المعلومات المخزنة على الأقراص الصلبة الخاصة بهم،[256] مما يعوق التحقيقات الجنائية بصورة خطيرة.[257]

---

[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.

[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.

وبالإضافة إلى التجريم الواسع النطاق للأفعال المتعلقة بالمواد الإباحية التي يُستغل فيها الأطفال، تناقش في الوقت الحاضر نهج أخرى مثل تنفيذ التزامات تستوجب من مقدمي خدمة الإنترنت أن يسجلوا المستخدمين أو أن يحجبوا أو أن يرشحوا النفاذ إلى مواقع الويب التي تتضمن مواد إباحية يُستغل فيها الأطفال.[258]

3.5.2 العنصرية والأقوال الحاضة على الكراهية، وتمجيد العنف

تستخدم الجماعات الراديكالية نظم الاتصالات الجماهيرية مثل الإنترنت لنشر دعايتها (الشكل 8).[259] وقد ارتفع في الآونة الأخيرة عدد مواقع الويب التي تحتوي على مضمون عنصري وأقوال حاضة على الكراهية[260] – إذ أفادت دراسة أجريت في عام 2005 أن عدد صفحات الويب التي تروج للكراهية العنصرية والعنف وكراهية الأجانب قد ارتفع بنسبة 25% بين عامي 2004 و2005.[261] وفي عام 2006، كان يوجد بالإنترنت ما يزيد على 6 000 موقع ويب من هذا النوع.[262]

الشكل 8

يوضح الرسم البياني موقع ويب يخص جماعة راديكالية. وتستخدم مثل هذه الجماعات الإنترنت بكثافة لاطلاع الناس على أهدافهم ولتجنيد أعضاء جدد.

ويوفر التوزيع عن طريق الإنترنت عدة مزايا للجناة، من بينها انخفاض تكاليف التوزيع، واستخدام معدات غير متخصصة، ومخاطبة جمهور عالمي. وتشمل أمثلة مواقع الويب الحاضة على الكراهية مواقع تقدم إرشادات عن كيفية صنع القنابل.[263] وإلى جانب بث المواد الدعائية، تُستخدم الإنترنت لبيع سلع معينة كالمواد ذات المحتوى النازي مثل الأعلام والشعارات والأزياء الرسمية والكتب، التي تتوافر بسهولة في مواقع المزادات والمتاجر المتخصصة المتاحة على الويب.[264] وتُستخدم الإنترنت أيضاً لإرسال رسائل البريد الإلكتروني والنشرات الإخبارية وتوزيع لقطات الفيديو والبرامج التلفزيونية من خلال مواقع محفوظات الفيديو التي تتمتع بالشعبية مثل موقع يوتيوب YouTube.

وهذه الجرائم لا تجرمها البلدان كلها.[265] ففي بعض البلدان، قد يتمتع مثل هذا المحتوى بالحماية بموجب مبادئ حرية التعبير.[266] وتتباين الآراء بشأن كيفية انطباق مبدأ حرية التعبير على موضوعات معينة، مما يعوق في كثير من الأحيان التحقيقات الدولية. ومن الأمثلة على تعارض القوانين في هذا الصدد قضية تتعلق بمقدم الخدمة ياهو Yahoo بحثت في عام 2001، وأمرت فيها محكمة فرنسية شركة ياهو (التي يوجد مقرها في الولايات المتحدة) بسد الطريق أمام نفاذ المستخدمين الفرنسيين إلى المواد ذات المحتوى النازي.[267] غير أن بيع هذه المواد يُعدّ قانونياً بموجب قانون الولايات المتحدة، استناداً إلى التعديل الأول لدستور الولايات المتحدة. وعملاً بهذا التعديل الأول، قررت إحدى المحاكم في الولايات المتحدة أن الأمر الفرنسي لا يمكن إنفاذه ضد ياهو Yahoo في الولايات المتحدة.[268]

---

[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.

[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=21313829894194994194493893493893796151919991.

وتجلت التفاوتات بين البلدان بشأن هذه القضايا أثناء إعداد مشروع اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. وتسعى الاتفاقية إلى تحقيق التوازن بين القوانين المتعلقة بالجريمة السيبرانية لكفالة عدم تعويق التحقيقات الدولية من جراء تعارض القوانين.[269] و لم تتمكن الأطراف المشاركة في المفاوضات من أن تتفق كلها على موقف مشترك إزاء تجريم نشر المواد الحاضة على كراهية الأجانب، ومن ثم استبعد هذا الموضوع برمته من الاتفاقية وعولج، عوضاً عن ذلك، في البروتوكول الأول القائم بذاته.[270] ولولا ذلك لما كان بمقدور بعض البلدان (ومن بينها الولايات المتحدة) أن توقع الاتفاقية.

الشكل 9

يوضح الرسم البياني موقع ويب يوفر محتوى ذا خلفية دينية يمكن أن ينفذ إليه المستخدمون في جميع أنحاء العالم.

4.5.2 إهانة الأديان

يعرض عدد متزايد[271] من مواقع الويب مواد معينة تخضع في بعض البلدان للأحكام المتعلقة بإهانة الأديان، ومن هذه المواد مثلاً الكتابات المعادية للدين.[272] وعلى الرغم من أن بعض المواد توثق وقائع واتجاهات موضوعية (كانخفاض التردد على الكنائس في أوروبا مثلا)، فإن هذه المعلومات قد تعتبر غير قانونية في بعض الولايات القضائية. وتشمل أمثلة أخرى الطعن في الأديان أو نشر رسوم كاريكاتورية (الشكل 9).

وتوفر الإنترنت مزايا للراغبين في مناقشة موضوع ما أو تناوله تناولاً نقدياً – إذ يستطيع الناس أن يدلوا بتعليقات أو أن ينشروا مواد أو أن يكتبوا مقالات دون الاضطرار إلى الإفصاح عن هويتهم. وتستند كثير من مجموعات النقاش إلى مبدأ حرية التعبير.[273] وتُعد حرية التعبير سبباً رئيسياً من نجاح الإنترنت، بما تتضمنه من بوابات تُستخدم تحديداً لنشر محتوى لا يعده إلا المستخدمون.[274] وعلى الرغم من الأهمية الحيوية لحماية هذا المبدأ، فإن تطبيق مبادئ حرية التعبير تحكمها، حتى في أكثر البلدان ليبرالية، شروط وقوانين.

وتباين المعايير القانونية بشأن المحتوى غير القانوني يوضح التحديات المصادفة في مجال تنظيم المحتوى. فحتى إذا كان نشر المحتوى مشمول بالأحكام المتعلقة بحرية التعبير في البلد الذي يتوافر فيه هذا المحتوى، فإن تلك المواد يمكن النفاذ إليها من بلدان تطبق قواعد أكثر صرامة. وقد أظهر "النزاع حول الرسوم الكاريكاتورية" الذي نشب في عام 2005 مواطن الصراع الكامنة. فقد أثار نشر اثني عشر رسماً كاريكاتورياً افتتاحياً في الجريدة الدانماركية ييلاندز–بوستِن Jyllands-Posten احتجاجات واسعة النطاق في جميع أنحاء العالم الإسلامي.[275]

وعلى غرار المحتوى غير القانوني، يُعد توفير معلومات أو مواد معينة فعلاً إجرامياً في بعض البلدان. وتتفاوت الحماية المكفولة للأديان والرموز الدينية المختلفة من بلد لآخر. فبعض البلدان تجرم استخدام عبارات مسيئة للنبي[276] أو تدنيس نسخ القرآن الكريم،[277] في حين تتبع بلدان أخرى نهجاً أكثر ليبرالية وقد لا تجرم هذه الأفعال.

---

[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.
[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.

5.5.2 المقامرة غير القانونية والألعاب المتاحة على الخط

الشكل 10

يوضح الرسم البياني السطح البيني الذي يتعامل معه المستخدم لكازينو قمار متاح على الخط. ويستطيع المستخدم بعد اتمام عملية التسجيل وتحويل الأموال، المشاركة في المقامرة على الخط. ويسمح عدد من كازينوهات القمار المتاحة على الخط باستخدام خدماته دون عملية تسجيل رسمي.

الألعاب والمقامرة على الإنترنت من أسرع المجالات نمواً على هذه الشبكة.[278] وتفيد شركة ليندن لابز Linden Labs، التي ابتكرت لعبة "حياة ثانية" (Second Life) المتاحة على الخط،[279] أن هذه اللعبة قد تُسجل فيها نحو عشرة ملايين حساب.[280] وتبين التقارير أن بعض هذه الألعاب قد استخدمت لارتكاب جرائم من بينها:[281]

- تبادل وعرض المواد الإباحية التي يستغل فيها الأطفال؛[282]
- الاحتيال؛[283]
- المقامرة في كازينوهات القمار المتاحة على الخط؛[284]
- القذف (مثل ترك رسائل بذيئة أو تشهيرية).

وتشير بعض التقديرات إلى أن إيرادات المقامرة على الخط قد ارتفعت من 3,1 مليارات دولار أمريكي في عام 2001 إلى 24 مليار دولار أمريكي في عام 2010 فيما يخص المقامرة على الإنترنت[285] (غير أن هذه التقديرات ما زالت منخفضة نسبياً إذا قورنت بإيرادات المقامرة التقليدية[286]).

ويتباين تنظيم القمار على الإنترنت وخارجها بين البلدان[287] – وهذه الثغرة قد استغلها الجناة وكذلك الشركات القانونية وكازينوهات القمار. وتوضح حالة ماكاو تأثير الاختلاف بين الأنظمة. فبعد أن قامت البرتغال بردّ ماكاو إلى الصين في عام 1999، أصبحت ماكاو من بين أكبر مقاصد القمار في العالم. إذ تفيد التقديرات أن عائدات القمار السنوية قد بلغت فيها 6,8 مليارات دولار أمريكي في عام 2006، لتنتزع ماكاو بذلك مكان الصدارة من لاس فيغاس (6,6 مليارات دولار أمريكي).[288] ويعزى نجاح ماكاو إلى أن القمار يعتبر غير قانوني في الصين[289] ولذا يسافر آلاف المقامرين من أرض الصين القارية إلى ماكاو للعب القمار فيها.

وتسمح الإنترنت للناس بالالتفاف على القيود المفروضة على القمار.[290] وتنتشر كازينوهات القمار المتاحة على الخط على نطاق واسع (انظر الشكل 10)، وتوجد مراكز معظمها في بلدان تطبق قوانين ليبرالية، أو لا تطبق أي أنظمة، فيما يتعلق بالمقامرة على الإنترنت. فيستطيع

---

[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/.

[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;

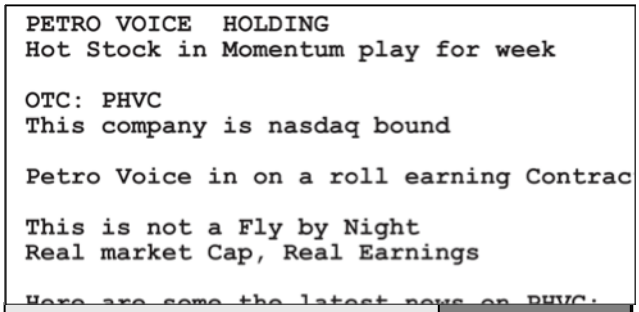
[287] See, for example, GAO, "Internet Gambling - An Overview of the Issues", available at: http://www.gao.gov/new.items/d0389.pdf; Regarding the WTO Proceedings, "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; 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.

المستخدمون فتح حسابات على الخط وتحويل الأموال والمشاركة في ألعاب الحظ.[291] كما يمكن استخدام كازينوهات القمار المتاحة على الخط في غسل الأموال وفي أنشطة تموّل الإرهاب.[292] وإذا استخدم الجناة كازينوهات القمار المتاحة على الخط ضمن حدود مرحلة الرهان التي لا يُحتفظ فيها بسجلات، أو التي توجد مواقعها في بلدان لا تطبق فيها تشريعات لمكافحة غسل الأموال، كان من العسير على وكالات إنفاذ القانون أن تحدد مصدر الأموال.



الشكل 11

تمثل رسائل البريد الإلكتروني الاقتحامية مشكلة خطيرة. وتغطي هذه الرسائل طائفة واسعة من المواضيع. وتروج هذه الرسائل لمنتجات شتى، كما يتمتع توفيرها لمعلومات عن السندات والأسهم بشعبية عالية.

ومن الصعب على البلدان التي تفرض قيوداً على القمار أن تراقب استخدام كازينوهات القمار المتاحة على الخط أو أنشطتها. وتقوض الإنترنت القيود القانونية التي تفرضها بعض البلدان على نفاذ مواطنيها إلى المقامرة على الخط.[293] وقد بذلت عدة محاولات تشريعية لمنع المشاركة في المقامرة على الخط:[294] وعلى وجه الخصوص، يسعى قانون الولايات المتحدة بشأن إنفاذ حظر المقامرة على الإنترنت لعام 2006 إلى الحد من المقامرة غير القانونية على الخط عن طريق مقاضاة مقدمي الخدمات المالية إذا ما قاموا بتسوية المعاملات المرتبطة بالمقامرة غير القانونية.[295]

6.5.2 القذف والمعلومات الزائفة

يمكن استخدام الإنترنت بغرض التضليل بنفس السهولة التي تستخدم بها للإعلام.[296] فمواقع الويب يمكن أن تعرض معلومات زائفة أو تشهيرية، ولا سيما في المنتديات وحجرات الدردشة، حيث يستطيع المستخدمون نشر رسائل لا تخضع لتحقق المشرفين.[297] ويستخدم القصر على نحو متزايد منتديات الويب ومواقع العلاقات الاجتماعية، حيث يمكن كذلك نشر هذا النوع من المعلومات.[298] ويمكن أن يشمل السلوك الإجرامي[299] (على سبيل المثال) نشر صوراً فوتوغرافية حميمة أو معلومات زائفة عن السلوك الجنسي.[300]

وفي معظم الحالات، يستفيد الجناة من أن مقدمي الخدمة الذين يتيحون النشر المجاني أو الرخيص الثمن لا يشترطون عادة تحديد هوية أصحاب المواد المنشورة أو قد لا يتحققون من البيانات الدالة على هوياتهم.[301] وهذا أمر يعقد تحديد هوية الجناة. وعلاوة على ذلك، قد لا يفرض المشرفون على المنتدى أي تنظيم على الإطلاق أو قد يفرضون تنظيماً محدوداً للغاية (الشكل 11). وهذه المزايا لم تَحُل دون استحداث مشروعات قيمة مثل موسوعة ويكيبديا،[302] التي يُعِدّ محتواها المستخدمون على الخط والتي تطبق إجراءات صارمة لضبط المحتوى. غير أن هذه التكنولوجيا نفسها يمكن أن يستخدمها الجناة من أجل:

---

[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.

[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

- نشر معلومات زائفة (عن المنافسين مثلاً)؛[303]
- التشهير (كترك رسائل بذيئة أو تشهيرية)؛[304]
- كشف معلومات سرية (كنشر أسرار حكومية أو معلومات تجارية حساسة).

ومما يتسم بأهمية حيوية تسليط الضوء على تزايد الخطر الذي تمثله المعلومات الزائفة أو المضللة. وهذا القذف يمكن أن ينال على نحو خطير من سمعة وكرامة الضحايا بدرجة كبيرة، لأن البيانات المنشورة على الخط يمكن أن ينفذ إليها جمهور عالمي. ففي اللحظة التي تنشر فيها المعلومات على الإنترنت يفقد صاحبها (أصحابها) في كثير من الأحيان أي قدرة على التحكم فيها. وحتى لو جرى تصويب المعلومات أو حذفها بعد نشرها بفترة وجيزة، فربما يكون قد جرى بالفعل استنساخها ("نقل صورتها") وإتاحتها على أيدي أناس غير مستعدين لإلغائها أو حذفها. وفي هذه الحالة، قد تظل المعلومات متاحة على الإنترنت، حتى ولو كان مصدرها الأصلي قد قام بإزالتها أو تصويبها.[305] وتشمل الأمثلة على ذلك حالات "رسائل البريد الإلكتروني التشهيرية"، حيث يتلقى ملايين الأشخاص رسائل إلكترونية بذيئة أو مضللة أو زائفة عن أشخاص أو منظمات قد لا يتسنى أبداً إصلاح الضرر الذي طال سمعتهم، بصرف النظر عن صحة الرسالة الأصلية أو عدم صحتها. ولذا، فإن حرية التعبير[306] يتعين موازنتها بحماية ضحايا القذف المحتملين.[307]

الشكل 12

منتديات الإنترنت التي يستطيع أي شخص أن يترك عليها رسائل دون تسجيل رسمي أماكن يجري الإقبال عليها لترك رسائل تتضمن معلومات زائفة.

7.5.2 الرسائل الاقتحامية وما يتعلق بها من تهديدات

تعني عبارة "الرسائل الاقتحامية" توجيه أعداد ضخمة من الرسائل الطفيلية (الشكل 12).[308] وعلى الرغم من أن هناك خدعاً احتيالية متنوعة، فإن أكثرها شيوعاً هي الرسائل الاقتحامية الموجهة عن طريق البريد الإلكتروني. فالجناة يرسلون إلى المستخدمين ملايين من رسائل البريد الإلكتروني التي تحتوي في كثير من الأحيان على دعايات لمنتجات وخدمات، ولكنها تحتوي أيضاً في مرات عديدة على برمجيات خبيثة. ومنذ إرسال الرسالة الاقتحامية الإلكترونية الأولى في عام 1978،[309] اكتسبت موجة رسائل البريد الإلكتروني الاقتحامية أبعاداً هائلة.[310] واليوم، تفيد منظمات مقدمي خدمة البريد الإلكتروني أن الرسائل الاقتحامية تشكل نسبة تتراوح بين 85 و90 في المائة من جميع رسائل البريد الإلكتروني.[311] وكانت المصادر الرئيسية لهذه الرسائل الاقتحامية في عام 2007 هي: الولايات المتحدة (19,6% من المجموع المسجل)؛ وجمهورية الصين الشعبية (8,4%)؛ وجمهورية كوريا (6,5%).[312]

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

وتصدى معظم مقدمي خدمة البريد الإلكتروني لتزايد مستويات الرسائل الاقتحامية الإلكترونية عن طريق تركيب تكنولوجيا ترشيح لمكافحة هذا النوع من الرسائل. وتتعرف هذه التكنولوجيا على الرسائل الاقتحامية باستخدام مرشحات تعتمد على كلمات مفتاحية أو قوائم سوداء لعناوين بروتوكول الإنترنت الخاصة بمن يرسلون هذه الرسائل.[313] وعلى الرغم من أن تكنولوجيا الترشيح تواصل تطورها، فإن مرسلي الرسائل الاقتحامية يجدون سبلاً للالتفاف عليها – وذلك مثلا بتجنب الكلمات المفتاحية. وقد نجح مرسلو هذه الرسائل في العثور على طرق كثيرة لوصف "الفياغرا"، وهي أحد المنتجات الأعلى شعبية التي تروج لها الرسائل الاقتحامية، دون الاضطرار إلى استخدام الاسم التجاري لها.[314]

ويعتمد مدى النجاح في كشف رسائل البريد الإلكتروني الاقتحامية على ما يطرأ من تغيرات في طريقة توزيعها. فبدلاً من إرسال الرسائل إلى مخدم بريدي واحد (يعد التعرف عليه أسهل من الناحية التقنية بالنسبة لمقدمي الخدمة، بسبب محدودية عدد المصادر[315])، فإن كثيراً من الجناة يستخدمون الشبكات المُسخّرة[316] لتوزيع البريد الإلكتروني الطفيلي. فعن طريق استخدام الشبكات المُسخّرة المعتمدة على الآلاف من النظم الحاسوبية،[317] يمكن الاكتفاء بأن يرسل كل حاسوب مئات قليلة من رسائل البريد الإلكتروني. ويزيد هذا من الصعوبة التي يواجهها مقدمو خدمة البريد الإلكتروني في كشف الرسائل الاقتحامية عن طريق تحليل المعلومات الخاصة بالمرسلين، ومن الصعوبة التي تواجهها وكالات إنفاذ القانون في تعقب الجناة.

وتحقق رسائل البريد الإلكتروني الاقتحامية أرباحاً ضخمة لأن تكلفة إرسال مليارات الرسائل تكلفة منخفضة – ويتزايد انخفاضها عند استخدام الشبكات المُسخّرة.[318] ويرى بعض الخبراء أن الحل الحقيقي الوحيد لمكافحة الرسائل الاقتحامية هو زيادة تكاليف الإرسال التي يتحملها الراسلون.[319] وقد حلل تقرير نُشر في عام 2007 تكاليف الرسائل الاقتحامية وأرباحها. وأوضحت نتائج التحليل أن تكاليف إرسال 20 مليون رسالة إلكترونية تبلغ نحو 500 دولار أمريكي.[320] ولما كانت تكاليف إرسال الرسائل الاقتحامية منخفضة بالنسبة للجناة، فإنهم يجنون من ورائها أرباحاً طائلة، خاصة إذا تمكنوا من إرسال مليارات الرسائل. وقد أفاد شخص هولندي أنه حقق ربحاً يبلغ قرابة 000 50 دولار أمريكي عن طريق إرسال ما لا يقل عن 9 مليارات رسالة اقتحامية.[321]

وفي عام 2005، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي تقريراً حلل تأثير الرسائل الاقتحامية على البلدان النامية.[322] وتقول البلدان النامية في كثير من الأحيان إن مستخدمي الإنترنت فيها يعانون من تأثير الرسائل الاقتحامية وإساءة استخدام الإنترنت. إذ تمثل الرسائل الاقتحامية مشكلة خطيرة في البلدان النامية، حيث يكون عرض النطاق وفرص النفاذ إلى الإنترنت أكثر محدودية وأعلى تكلفة عنهما في البلدان الصناعية.[323] وتستهلك الرسائل الاقتحامية وقتاً قيماً وموارد ثمينة في البلدان التي تعد فيها موارد الإنترنت أكثر ندرة وأعلى تكلفة.

---

[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%20perspective%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

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

8.5.2 الأشكال الأخرى للمحتوى غير القانوني

تستخدم الإنترنت لا من أجل شن هجمات مباشرة فحسب بل أيضاً كمنتدى من أجل:

- الإغواء بارتكاب الجرائم، وتقديم عروض لارتكابها، والتحريض على ارتكابها؛[324]
- البيع غير القانوني للمنتجات؛
- تقديم معلومات وإرشادات بشأن أعمال غير قانونية (مثل كيفية صنع المتفجرات).

وقد وضعت كثير من البلدان أنظمة للتجارة في منتجات معينة. وتطبق البلدان المختلفة أنظمة وقيوداً تجارية وطنية مختلفة على منتجات شتى مثل المعدات العسكرية.[325] ويصدق الأمر نفسه على الأدوية – فالأدوية التي تتوافر بلا قيود في بعض البلدان قد تستوجب تذكرة طبية في بلدان أخرى.[326] وقد تجعل التجارة عبر الحدود من الصعب التأكد من أن النفاذ إلى منتجات معينة يبقى قاصراً على الأراضي المعنية.[327] وقد تفاقمت هذه المشكلة من جراء شعبية الإنترنت. فمتاجر الويب التي تعمل انطلاقاً من بلدان لا تُفرض فيها قيود تستطيع أن تبيع منتجات معينة لزبائن في بلدان أخرى تفرض قيوداً عليها، مما يقوض مفعول قيودها هذه.

وقبل ظهور الإنترنت، كان من الصعب على معظم الناس النفاذ إلى إرشادات تبين كيفية صنع الأسلحة. لقد كانت المعلومات اللازمة متيسرة (وذلك مثلاً في الكتب التي تتناول الجوانب الكيميائية للمتفجرات)، لكن العثور عليها كان يتطلب وقتاً طويلاً. أما اليوم، فإن المعلومات المتعلقة بكيفية صنع المتفجرات تتوافر على الإنترنت،[328] وسهولة النفاذ إلى هذه المعلومات يزيد من احتمال وقوع الهجمات.

الشكل 13

يوضح الرسم البياني أداء الجيل الثاني من نظم اقتسام الملفات. إذ كان الجيل الأول من هذه النظم يستند إلى مخدمات مركزية تستضيف قوائم بالوثائق المتاحة. أما الجيل الثاني منها فيفوض وظيفة المخدم إلى المستخدمين، مما يزيد من صعوبة تفكيك الشبكة ومنع انتهاكات حقوق المؤلف.

6.2 الجرائم المتعلقة بحقوق المؤلف والعلامات التجارية

تتمثل إحدى الوظائف الحيوية للإنترنت في نشر المعلومات. وتستخدم الشركات الإنترنت لتوزيع المعلومات عن منتجاتها وخدماتها. ومن زاوية القرصنة، فإن الشركات الناجحة قد تواجه على الإنترنت مشكلات تماثل المشكلات التي تواجهها خارج الشبكة. فقد تستخدم صورتها التجارية وتصميم شعارها لتسويق منتجات مزيفة، حيث يقوم المزيفون باستنساخ الشعارات والمنتجات ويحاولون تسجيل الميدان الخاص بتلك الشركة المحددة. ويمكن أن تتعرض الشركات التي توزع المنتجات مباشرة على الإنترنت[329] لمشكلات قانونية تتصل بانتهاكات حقوق المؤلف. إذ قد يجري تنزيل منتجاتها واستنساخها وتوزيعها.

1.6.2 الجرائم المتعلقة بحقوق المؤلف

مع التحول من التكنولوجيا التماثلية إلى التكنولوجيا الرقمية،[330] أتاحت الرقمنة[331] لصناعة الترفيه أن تضيف سمات وخدمات إضافية للأفلام المسجلة على أقراص DVD، تشمل اللغات، وترجمة الحوار، والإعلانات عن الأفلام، ومواد إضافية مجانية. وأثبتت أقراص CD وDVD أنها أطول عمراً من الشرائط الصوتية وشرائط الفيديو.[332]

---

[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: *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.
[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.

وقد فتحت الرقمنة الباب أمام انتهاكات جديدة لحقوق المؤلف. والأساس الذي تستند إليه الانتهاكات الراهنة لحقوق المؤلف هو الاستنساخ السريع والدقيق. فقبل ظهور الرقمنة، كان نسخ شريط صوتي أو شريط فيديو يسفر دوماً عن فقدان قدر معين من الجودة. أما اليوم، فقد بات من الممكن استنساخ مصادر رقمية دون فقدان الجودة، وأتاح ذلك بالتالي إنتاج نسخ إضافية من أي نسخة متاحة. وتشمل أكثر انتهاكات حقوق المؤلف شيوعاً ما يلي:

- تبادل الأغاني والملفات والبرمجيات المحمية بحقوق المؤلف في نظم اقتسام الملفات؛[333]
- الالتفاف على نظم إدارة الحقوق الرقمية.[334]

ونظم اقتسام الملفات هي خدمات شبكية تقوم على الاتصال بين النظراء[335] وتتيح للمستخدمين تقاسم الملفات،[336] مع ملايين المستخدمين الآخرين في كثير من الأحيان.[337] وبعد تركيب برمجيات اقتسام الملفات، يستطيع المستخدمون أن يختاروا الملفات التي يريدون تقاسمها ويستعملون البرمجيات للبحث عن ملفات أخرى يوفرها آخرون لتنزيلها من مئات المصادر. وقبل أن تُستحدث نظم اقتسام الملفات، كان الناس يستنسخون الشرائط الصوتية وشرائط الفيديو ويتبادلونها، لكن نظم اقتسام الملفات تسمح بتبادل النسخ من جانب أعداد أكبر كثيراً من المستخدمين.

وتؤدي تكنولوجيا الاتصال بين النظراء دوراً حيوياً في الإنترنت. ففي الوقت الحاضر تولّد شبكات الاتصال بين النظراء ما يزيد على 50% من حركة المستهلكين على الإنترنت.[338] ولا يبرح عدد المستخدمين يتنامى طول الوقت – ويقدر تقرير نشرته منظمة التعاون والتنمية في الميدان الاقتصادي أن نحو 30% من مستخدمي الإنترنت الفرنسيين قد قاموا بتنزيل مواد موسيقية أو ملفات بواسطة نظم تقاسم الملفات،[339] وتسجل اتجاهات مماثلة في سائر بلدان المنظمة.[340] ويمكن استخدام نظم تقاسم الملفات لتبادل أي نوع من البيانات الحاسوبية، بما في ذلك الموسيقى والأفلام والبرمجيات.[341] ومن الزاوية التاريخية، كانت نظم تقاسم الملفات تستخدم أساساً لتبادل الموسيقى، لكن تبادل مواد الفيديو تتزايد أهميته أكثر فأكثر.[342]

والتكنولوجيا المستخدمة في خدمات تقاسم الملفات فائقة التطور وتتيح تبادل ملفات كبيرة في غضون فترات زمنية قصيرة.[343] وكان الجيل الأول من نظم تقاسم الملفات يعتمد على مخدم مركزي، مما كان يتيح لوكالات إنفاذ القانون أن تتصدى للتقاسم غير القانوني للملفات في إطار شبكة

[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.

[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.

نابستر Napster.[344] وخلافاً للجيل الأول من نظم إنتاج الملفات (ولا سيما مخدم نابستر الشهير)، فإن الجيل الثاني من نظم تقاسم الملفات لم يعد يستند إلى مخدم مركزي يوفر قائمة بالملفات المتاحة بين المستخدمين.[345] فالمفهوم اللامركزي للجيل الثاني من شبكة تقاسم الملفات (انظر الشكل 13) يجعل من الأصعب منعها من العمل. ولكن يمكن، بفضل الاتصالات المباشرة، تعقب مستخدمي إحدى الشبكات عن طريق عنوان بروتوكول الإنترنت الخاص بهم.[346] وقد حققت وكالات إنفاذ القانون قدراً من النجاح في التحقيق في انتهاكات حقوق المؤلف في إطار نظم تقاسم الملفات. غير أن نظم تقاسم الملفات الأحدث عهداً تتيح أشكالاً من الاتصال المجهول الهوية وستزيد من صعوبة إجراء التحقيقات.[347]

وتكنولوجيا تقاسم الملفات يستخدمها لا الأشخاص العاديون والمجرمون وحدهم بل تستخدمها أيضاً الشركات التجارية العادية.[348] والملفات التي يتم تبادلها بنظم تقاسم الملفات لا تنتهك كلها حقوق المؤلف. إذ تشمل أمثلة استخدامها المشروع ما يؤذن بتبادله في إطار الملك العام من نسخ ومصنفات فنية.[349]

ومع ذلك، فإن استخدام نظم تقاسم الملفات يطرح تحديات على صناعة الترفيه.[350] ومن غير الواضح إلى أي مدى يعزى الانخفاض في مبيعات الأقراص CD/DVD وتذاكر السينما إلى تبادل الملفات في إطار نظم تقاسم الملفات. وقد كشف البحث عن وجود الملايين من مستخدمي تقاسم الملفات[351] وعن وجود مليارات الملفات التي تم تنزيلها.[352] وظهرت في نظم تقاسم الملفات أفلام يتم تبادلها قبل عرضها في دور العرض رسمياً[353] مما ألحق خسائر بأصحاب حقوق المؤلف. ومن شأن استحداث نظم تقاسم الملفات المجهولة الهوية في الآونة الأخيرة أن يزيد من صعوبة عمل أصحاب حقوق المؤلف وعمل وكالات إنفاذ القانون.[354]

وقد ردت صناعة الترفيه على ذلك بتطبيق تكنولوجيا ترمي إلى منع المستخدمين من استنساخ أقراص CD وDVD مثل نظم تخليط المحتوى،[355] وهي تكنولوجيا تجفير تمنع استنساخ المحتوى على أقراص DVD.[356] وتعد هذه التكنولوجيا عنصراً حيوياً بالنسبة للنماذج التجارية الجديدة الساعية إلى توخي مزيد من الدقة في إسناد حقوق النفاذ إلى المستخدمين. ويصف مصطلح "إدارة الحقوق الرقمية"[357] تطبيق تكنولوجيات تسمح لأصحاب حقوق المؤلف بتقييد استخدام الوسائط الرقمية، حيث يشتري الزبائن حقوقاً محدودة فقط (مثل الحق في بث أغنية واحدة أثناء حفل واحد). وتسمح إدارة الحقوق الرقمية بتنفيذ نماذج تجارية جديدة تعبر عن مصالح أصحاب حقوق المؤلف والمستخدمين بمزيد من الدقة ويمكن أن تعكس اتجاه الانخفاض في الأرباح.

---

[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.

[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.

ومن أكبر الصعوبات التي تصادفها هذه التكنولوجيات إمكانية الالتفاف على تكنولوجيا حماية حقوق المؤلف.[358] فقد استحدث الجناة أدوات برمجياتية تُمكّن المستخدمين من أن يتيحوا على الإنترنت ملفات محمية بحقوق المؤلف[359] مجاناً أو بأسعار زهيدة. فما أن يجري إزالة الحماية التي تكفلها إدارة الحقوق الرقمية من ملف، يمكن إنتاج نسخ منها وبثها بلا حدود.

والجهود الرامية إلى حماية المحتوى لا تقتصر على الأغاني والأفلام. فبعض محطات التلفزيون (ولا سيما قنوات التلفزيون التي تشاهد نظير ثمن معلوم) تقوم بتجفير البرامج لتضمن ألا يتلقاها إلا الزبائن الذين سددوا الثمن المطلوب. وعلى الرغم من تقدم تكنولوجيات الحماية، فقد نجح الجناة في تزييف الأجهزة المستخدمة لمكافحة النفاذ، أو في اختراق التجفير باستخدام أدوات برمجياتية.[360]

وبغير أدوات برمجياتية، يصبح المستخدمون العاديون أقل قدرة على ارتكاب الجرائم. والمناقشات المتعلقة بتجريم انتهاكات حقوق المؤلف تركز لا على نظم تقاسم الملفات والالتفاف حول الحماية القانونية فحسب، بل تركز أيضاً على إنتاج وبيع وحيازة "أجهزة غير قانونية" أو أدوات ترمي إلى تمكين المستخدمين من انتهاك حقوق المؤلف.[361]

● بنك NPW™

عميلنا العزيز،

نود أن نخبركم بأننا نحتاج إلى التحقق من حسابكم. لقد تلقينا في الأسابيع الماضية عدداً من الشكاوى تتعلق برسائل التصيد الاحتيالي. وتجنباً للمشاكل، نرجوكم أن تزوروا موقع الويب التالي:

www.npwbank-online.com/security-chech/

إن لم تنفذوا هذا الإجراء في غضون 24 ساعة سنضطر آسفين إلى إقفال حسابكم.

ونشكركم جزيل الشكر على تعاونكم.

الشكل 14

تبين الصورة رسالة اصطياد. وتصمم الرسائل التصيد الاحتيالية بحيث تشبه الرسائل الواردة من الشركات المشروعة. ويستخدم الجناة في كثير من الأحيان الشعارات الأصلية المحمية بالعلامة التجارية.

2.6.2 الجرائم المتعلقة بالعلامات التجارية

انتهاكات العلامات التجارية تماثل انتهاكات حقوق المؤلف، وهذا جانب معروف جيداً من جوانب التجارة العالمية. وقد انتقلت الانتهاكات المتعلقة بالعلامات التجارية إلى الفضاء السيبراني، وهي تخضع للتجريم بدرجات متباينة بموجب القوانين الجنائية الوطنية المختلفة.[362] وتشمل أخطر هذه الجرائم ما يلي:

- استخدام العلامات التجارية في أنشطة إجرامية بغرض تضليل الأطراف المستهدفة (الأهداف)؛
- الجرائم المتعلقة بالميدان أو الاسم.

وترتبط السمعة الطيبة لشركة من الشركات في كثير من الأحيان ارتباطاً مباشراً بعلاماتها التجارية. ويستخدم الجناة الأسماء والعلامات التجارية بطرق احتيالية في عدد من الأنشطة، من بينها التصيد الاحتيالي (انظر الشكل 14)،[363] حيث ترسل إلى مستخدمي الإنترنت ملايين الرسائل الإلكترونية الشبيهة بالرسائل الصادرة عن الشركات المشروعة، تتضمن، على سبيل المثال، العلامات التجارية.[364]

ومن القضايا الأخرى المتصلة بانتهاكات العلامات التجارية الجرائم المتعلقة بالميدان[365] مثل الاستقطان السيبراني،[366] الذي يعني عملية غير قانونية لتسجيل اسم ميدان مطابق أو مماثل للعلامة التجارية لمنتج أو لشركة.[367] ويسعى الجناة، في معظم هذه الحالات، إلى بيع الميدان بسعر مرتفع إلى

[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.

[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.

الشركة[368] أو يستخدمونه لبيع منتجات أو خدمات تضلل المستخدمين من خلال ارتباطها المفترض بالعلامة التجارية.[369] ومن الأمثلة الأخرى على الجرائم المتصلة بالميدان "اختطاف الميدان" أو تسجيل أسماء الميدان التي انقضت مدتها عرضاً.[370]

7.2 الجرائم المتعلقة بالحاسوب

تغطي هذه الفئة عدداً من الجرائم التي يستلزم ارتكابها نظاماً حاسوبياً. وخلافاً للفئات السابقة، فإن هذه الفئة الواسعة من الجرائم لا تعد، في كثير من الأحيان، صارمة بنفس القدر من زاوية الحماية التي تكفلها المبادئ القانونية، وهي تشمل:

- الاحتيال الحاسوبي؛
- التزييف والتصيد الاحتيالي وسرقة الهوية باستخدام الحاسوب؛
- إساءة استخدام الأجهزة.

1.7.2 الاحتيال والاحتيال الحاسوبي

الاحتيال الحاسوبي من أكثر الجرائم شيوعاً على الإنترنت،[371] لأنه يمكن الجناة من استخدام الأتمتة[372] وأدوات برمجياتية لإخفاء هويتهم.

وتُمكّن الأتمتة الجناة من جني أرباح طائلة من عدد من الأفعال الصغيرة.[373] وتتمثل إحدى الاستراتيجيات التي يستخدمها الجناة في ضمان أن تظل الخسارة المالية التي يتحملها كل ضحية أدنى من حد معين. فعندما تكون الخسارة "صغيرة" تقل احتمالات قيام الضحايا بإنفاق الوقت والجهد للإبلاغ عن هذه الجرائم والمطالبة بالتحقيق فيها.[374] ومن أمثلة هذا النوع من الخدع الاحتيالية ما يعرف باسم الخدعة النيجيرية ويقصد بها الاحتيال لتحصيل مبلغ من المال بزعم تقديم خدمة لاحقة وهمية (انظر الشكل 15).[375]

صديقي العزيز،

اسمح لي بادئ ذي بدء بأن أقدم نفسي إليك. اسمي هو مبوتو بوتاليا. وأنا زوجة رئيس جمهورية تاليا السابق. لقد توفي زوجي الحبيب مؤخراً في حادث طائرة. وأثناء ترتيب أوراقه، وجدت أن زوجي يحتفظ بمبلغ 10 000 000 دولار أمريكي في حساب سري. وأنا أعتزم تحويل هذا المبلغ إلى أسرتي التي تعيش في الولايات المتحدة. غير أنني لا أستطيع أن أحول الأموال إليهم مباشرة. ولذا سألتمس مساعدتك الكريمة.

وأود أن أحول إلى حسابكم مبلغ الـ 10 000 000 دولار أمريكي هذا راجية منكم أن تحولوا منه إلى أسرتي مبلغ 9 000 000 دولار أمريكي. أما مبلغ الـ 1 000 000 دولار أمريكي المتبقي فستحتفظون به لنفسكم. فإن وافقتم على ذلك، أرجو منكم أن تحولوا إلى حسابي أولاً مبلغ 10 دولارات أمريكية كي أتمكن من التحقق من المعلومات الخاصة بحسابكم المصرفي.

الشكل 15

يوضح الرسم البياني رسالة تقليدية تستند إلى خدعة احتيالية لتحصيل مبلغ من المال بزعم تقديم خدمة لاحقة وهمية. ولكي يستطيع متلقو الرسالة الحصول على الربح المفترض يُطلب منهم أن يحولوا مبلغاً معيناً من المال مقدماً. وهذه خدعة شائعة للغاية ولكنها لا تعتبر جريمة متعلقة بالحاسوب نظراً لعدم استغلال نظام حاسوبي فيها.

وعلى الرغم من أن هذه الجرائم ترتكب باستخدام تكنولوجيا الحاسوب، فإن معظم نظم القانون الجنائي تصنفها لا كجرائم متعلقة بالحاسوب، بل كحالات احتيال عادي.[376] والتفرقة الرئيسية بين الاحتيال الحاسوبي والاحتيال التقليدي هو الضحية المستهدفة بالاحتيال. فإذا حاول الجناة التأثير على شخص من الأشخاص، تعتبر الجريمة بوجه عام ضرباً من الاحتيال. أما إذا استهدف الجناة نظماً حاسوبية أو نظماً لمعالجة البيانات، فإن الجرائم تصنف في كثير من الأحيان على أنها احتيال حاسوبي. ويظل بمقدور نظم القانون الجنائي التي تغطي الاحتيال، ولكنها لا تتضمن بعد استغلال النظم الحاسوبية في أغراض احتيالية، أن تلاحق الجرائم المذكورة أعلاه قضائياً في كثير من الأحيان.

[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.

وتشمل أهم الخدع الاحتيالية ما يلي:

1 الاحتيال عن طريق المزادات المتاحة على الخط[377]

تعد المزادات العامة المتاحة على الخط من أكثر خدمات التجارة الإلكترونية شعبية. ففي عام 2006، بيعت على موقع إيباي eBay، وهو أكبر سوق للمزادات المتاحة على الخط في العالم، سلع تزيد قيمتها على 20 مليار دولار أمريكي.[378] وتتيح هذه المزادات للمشترين النفاذ إلى سلع متنوعة أو إلى سلع مخصوصة من كل أنحاء العالم. كما تتيح للبائعين عرض سلعهم على جمهور عالمي، مما ينشط الطلب ويرفع الأسعار.

ويستطيع الجناة الذي يرتكبون الجرائم في هذه المزادات أن يستغلوا غياب الاتصال وجهاً لوجه بين البائع والمشتري.[379] والصعوبة في التمييز بين البائعين الحقيقيين والجناة، جعلت من الاحتيال عن طريق المزادات واحدة من أكثر الجرائم السيبرانية انتشاراً.[380] وأوسع حيلتين انتشاراً هما:[381]

- عرض سلع غير موجودة للبيع، ومطالبة المشترين بدفع ثمنها قبل تسليمها؛[382]
- شراء السلع والمطالبة بتسليمها، دون وجود نية الدفع.

ورداً على ذلك، استحدث مقدمو خدمة المزادات نظماً للحماية، مثل نظام استقاء الآراء/التعليقات عن المعاملات المنفذة. فبعد كل معاملة، يدون المشترون والبائعون آراءهم كي يستنير بها المستخدمون الآخرون[383] بوصفها معلومات محايدة عن مدى جدارة البائعين/المشترين بالثقة. وفي هذه الحالة تصبح "السمعة هي كل شيء"، وبدون عدد كاف من التعليقات الإيجابية، يصبح من الأصعب على الجناة أن يقنعوا الأطراف المستهدفة (الأهداف) إما بالدفع نظير سلع غير موجودة، وإما بإرسال السلع دون تلقي ثمنها أولاً.

غير أن المجرمين قد ردوا على ذلك بالالتفاف على تلك الحماية عن طريق استخدام حسابات أطراف ثالثة.[384] وبموجب هذه الخدعة المسماة "الاستيلاء على الحسابات"[385] يحاول الجناة الاستيلاء على ما يخص مستخدمين شرعيين من أسماء وكلمات السر بغية شراء أو بيع السلع غشاً واحتيالاً، مما يزيد من صعوبة الكشف عن هويتهم.

2 الاحتيال لتحصيل مبلغ من المال بزعم تقديم خدمة لاحقة وهمية[386]

في هذه الحالة، يرسل الجناة رسائل إلكترونية يلتمسون فيها مساعدة المرسل إليهم في تحويل كميات كبيرة من المال إلى أطراف ثالثة واعدين إياهم بنسبة معلومة، إن هم وافقوا على إجراء التحويل باستخدام حساباتهم الشخصية[387] وبعد ذلك يطلب منهم الجناة أن يحولوا إليهم مبلغاً بسيطاً للتحقق من بيانات حساباتهم المصرفية (معتمدين في ذلك على تصور أشبه بالتصور الذي يقوم عليه اليانصيب – فالمشاركون قد يكونوا مستعدين لتحمل خسارة صغيرة حتى وإن كانت مؤكدة على أمل أن يكسبوا ربحاً كبيراً حتى وإن كان غير مؤكد) أو أن يرسلوا إليهم بيانات حساباتهم المصرفية مباشرة. وما أن يقوم المشاركون بتحويل الأموال، لن يتصل الجناة بهم مرة أخرى إلى الأبد. أما إذا قام المشاركون بإرسال

---

[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/Faloutsos*, 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.

[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.

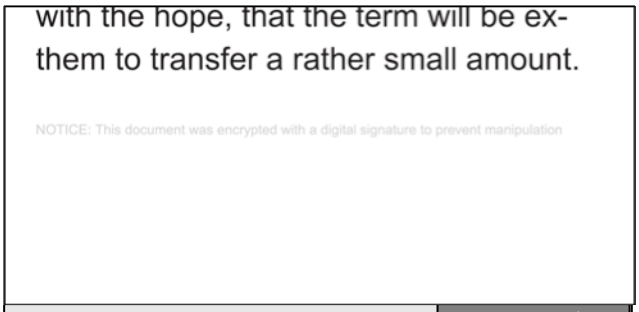
[387] Advance Fee Fraud, Foreign & Commonwealth Office, available at: http://www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.

بيانات حساباتهم المصرفية، فإن الجناة قد يستخدمونها في أنشطة احتيالية. وتوحي الأدلة بأن مثل هذه الرسائل الإلكترونية يرد عليها آلاف الضحايا[388] وتبين البحوث الراهنة أنه على الرغم من الحملات والمبادرات الإعلامية المختلفة، فإن الاحتيال لتحصيل مبلغ من المال بزعم تقديم خدمة لاحقة وهمية ما زال يتزايد، وذلك فيما يخص عدد الضحايا وحجم الخسائر الإجمالية سواء بسواء.[389]

2.7.2 التزييف الحاسوبي

يعني التزييف الحاسوبي التلاعب في الوثائق الرقمية[390] وذلك مثلاً عن طريق:

- إنشاء وثيقة تبدو كما لو كانت صادرة عن مؤسسة موثوق بها؛
- التلاعب في الصور الإلكترونية (ومن ذلك مثلا الصور المستخدمة كدليل في المحاكم)؛
- تحوير الوثائق النصية.



الشكل 16

يمكن التلاعب في البيانات الإلكترونية بسهولة بالمقارنة مع تزوير الوثائق التقليدية. وثمة حلول تقنية، مثل التوقيعات الرقمية، بمقدورها أن تمنع التلاعب الخفي.

ويشمل تزوير الرسائل الإلكترونية خدعة "التصيد الاحتيالي" الذي يشكل تحدياً خطيراً لوكالات إنفاذ القانون في جميع أنحاء العالم[391] ذلك أن "التصيد الاحتيالي" يسعى إلى جعل الأهداف يفصحون عن معلومات شخصية/سرية[392] فيرسل الجناة في كثير من الأحيان رسائل إلكترونية شبيهة بالرسائل الصادرة عن مؤسسات مالية مشروعة يتعامل معها الهدف[393] وتصمم هذه الرسائل الإلكترونية بطريقة تجعل من الصعب على الأهداف أن يكتشفوا زيفها[394] وتطلب هذه الرسائل من المرسل إليه أن يفصح عن معلومات حساسة معينة و/أو أن يتحقق منها. ويستجيب كثير من الضحايا لهذا الطلب فيفصحون عن معلومات تمكن الجناة من إجراء تحويلات على الخط، وما إلى ذلك.[395]

وكانت الملاحقة القضائية للتزييف الحاسوبي نادرة في الماضي، لأن معظم الوثائق القانونية كانت وثائق ملموسة. غير أن الوثائق الرقمية باتت تؤدي دوراً متزايد الأهمية وتستخدم أكثر فأكثر. والاستعاضة عن الوثائق التقليدية بالوثائق الرقمية أمر تدعمه وسائل قانونية تتيح استخدامها مثل اعتراف التشريع بالتوقيعات الرقمية (انظر الشكل 16).

وقد حاول المجرمون دوماً التلاعب في الوثائق. ومع استحداث التزييف الرقمي، بات بالمقدور الآن استنساخ الوثائق الرقمية دون فقدان الجودة وبات بالمقدور التلاعب فيها بسهولة. ومن الصعب على خبراء الأدلة الجنائية أن يثبتوا حدوث التلاعب الرقمي ما لم تكن الحماية التقنية[396] قد استخدمت من أجل حماية الوثيقة من التزييف.[397]

---

[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.
[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.

3.7.2 سرقة الهوية

يصف مصطلح سرقة الهوية – الذي لا يُعرّف ولا يستخدم بطريقة متسقة – فعلاً إجرامياً يتمثل في الاحتيال لانتحال هوية شخص آخر واستخدامها.[398] ويمكن القيام بهذه الأفعال دون الاستعانة بوسائل تقنية[399] كما يمكن ارتكابها على الخط باستخدام تكنولوجيا الإنترنت.[400]

وتشمل الجريمة التي توصف بأنها سرقة هوية ثلاث مراحل مختلفة بوجه عام:[401]

- في المرحلة الأولى يحصل الجاني على معلومات متعلقة بالهوية. ويمكن القيام بهذا الجزء من الجريمة عن طريق استخدام برمجيات خبيثة أو هجمات التصيد الاحتيالي على سبيل المثال؛
- والمرحلة الثانية تتسم بالتفاعل مع المعلومات المتعلقة بالهوية قبل استخدامها في ارتكاب أفعال إجرامية.[402] ومن الأمثلة على ذلك بيع المعلومات المتعلقة بالهوية.[403] فسجلات بطاقات الائتمان تباع مثلاً بمبلغ يصل إلى 60 دولاراً أمريكياً؛[404]
- والمرحلة الثالثة هي استخدام المعلومات المتعلقة بالهوية في فعل إجرامي. وفي معظم الحالات، فإن النفاذ إلى البيانات المتعلقة بالهوية يُمكّن الجاني من ارتكاب المزيد من الجرائم.[405] ولذا لا يركّز الجناة على مجموعة البيانات ذاتها بل على القدرة على استخدامها في أنشطة إجرامية. ومن أمثلة هذه الجرائم تزييف وثائق الهوية أو الاحتيال ببطاقات الائتمان.[406]

[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.

[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.

وتغطي الأساليب المستخدمة للحصول على البيانات في المرحلة الأولى طائفة واسعة من الأفعال. إذ يستطيع الجاني أن يستخدم أساليب مادية وأن يسرق مثلاً أجهزة تخزين حاسوبية تحتوي على البيانات المتعلقة بالهوية، أو أن يبحث في القمامة (فيما يُدعى "الغوص في المهملات"[407])، أو أن يسرق البريد.[408] كما يستطيع الجناة استخدام محركات البحث للعثور على بيانات متعلقة بالهوية. ويصف مصطلحا "القرصنة على غوغل" (Googlehacking) و"المنقبون في غوغل" (Googledorks) تسخير محركات بحث معقدة في الإجابة عن استفسارات معينة ثم ترشيح الكميات الكبيرة من نتائج البحث وصولا إلى معلومات تتعلق بقضايا أمن الحاسوب وإلى معلومات شخصية يمكن استغلالها في الخدع الخاصة بسرقة الهوية. وقد يتمثل هدف الجاني مثلاً في البحث عن نظم لا تكفل حماية مأمونة لكلمة السر لاستقاء البيانات منها.[409] وتسلط التقارير الضوء على المخاطر التي قد تصاحب الاستخدام القانوني لمحركات البحث في أغراض غير قانونية.[410] وتشير التقارير إلى مشكلات مماثلة تتعلق بنظم تقاسم الملفات.

وقد ناقش كونغرس الولايات المتحدة مؤخراً إمكانية استخدام نظم تقاسم الملفات للحصول على معلومات شخصية يمكن استغلالها في سرقة الهوية.[411] وإلى جانب هذا، يستطيع الجناة الحصول على تلك المعلومات من خلال الاستعانة بأطراف داخلية تتيسر لها فرصة النفاذ إلى المعلومات المخزنة المتعلقة بالهوية. وتبين الدراسة الاستقصائية للجريمة الحاسوبية والأمن الحاسوبي لعام 2007، الصادرة عن معهد الأمن الحاسوبي،[412] أن أكثر من 35% من المجيبين يُعزون إلى الأطراف الداخلية نسبة تزيد على 20% من خسائر منظمتهم. ويستطيع الجناة أخيراً أن يستخدموا تقنية الهندسة الاجتماعية لإقناع الضحايا بالإفصاح عن معلومات شخصية. وقد ابتكر الجناة في السنوات الأخيرة خدعاً فعالة للحصول على المعلومات السرية (مثل المعلومات المتعلقة بالحسابات المصرفية والبيانات المتعلقة ببطاقات الائتمان) عن طريق التلاعب بالمستخدمين من خلال تقنيات الهندسة الاجتماعية (انظر الشكل 17).[413]

● **بنك NPW™**

عميلنا العزيز،

نود أن نخبركم بأننا نحتاج إلى التحقق من حسابكم. لقد تلقينا في الأسابيع الماضية عدداً من الشكاوى تتعلق برسائل التصيد الاحتيالي. وتجنباً للمشكلات، نرجوكم أن تزوروا موقع الويب التالي:

WWW.npwbank-online.com/security-chech/

إن لم تنفذوا هذا الإجراء في غضون 24 ساعة سنضطر آسفين إلى إقفال حسابكم.

ونشكركم جزيل الشكر على تعاونكم.

الشكل 17

تستخدم رسائل التصيد الاحتيالي للحصول من الأهداف على معلومات سرية (مثل المعلومات المتعلقة بالحسابات وكلمة السر وأرقام المعاملات). ويستطيع الجناة استخدام هذه المعلومات في ارتكاب الجرائم.

ويتباين نوع البيانات التي يستهدفها الجناة.[414] وتتمثل أهم هذه البيانات فيما يلي:

- **رقم الضمان الاجتماعي أو رقم جواز السفر** – رقم الضمان الاجتماعي الذي يستخدم مثلا في الولايات المتحدة نموذج تقليدي لإحدى بيانات الهوية التي يستهدفها الجناة. وعلى الرغم من أن رقم الضمان الاجتماعي قد استحدث للاحتفاظ بسجل دقيق للإيرادات، فإنه يستخدم في الوقت الحاضر على نطاق واسع في أغراض إثبات الهوية.[415] ويستطيع الجناة استخدام هذا الرقم، بالإضافة إلى ما يحصلون عليه من معلومات عن جوازات السفر، لفتح حسابات مالية، أو الاستيلاء على الحسابات المالية القائمة، أو إنشاء ائتمانات، أو أخذ قروض.[416]

[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/.

[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.

- **تاريخ الميلاد، العنوان، أرقام الهاتف** – وهذه البيانات لا يمكن استخدامها بوجه عام لارتكاب سرقات الهوية إلا إذا تم الجمع بينها وبين معلومات أخرى (مثل رقم الضمان الاجتماعي).[417] فالنفاذ إلى معلومات إضافية كتاريخ الميلاد والعنوان يمكن أن يساعد الجاني على الالتفاف على عمليات التحقق. ومن أشد المخاطر التي تحدق بتلك المعلومات أنها تتوافر في الوقت الحاضر على نطاق واسع على الإنترنت – إما بأن تنشر طوعاً في أحد المنتديات التي تستوجب الإفصاح عن الهوية[418] وإما بأن تنشر نزولا على متطلبات قانونية وذلك مثلاً لدى تسجيل العلامات على مواقع الويب.[419]

- **كلمة السر للحسابات غير المالية** – النفاذ إلى كلمات السر الخاصة بالحسابات يتيح للجناة أن يغيروا بيانات تهيئة الحساب وأن يستخدمونه في الأغراض الخاصة بهم.[420] فيستطيعون مثلاً الاستيلاء على حساب للبريد الإلكتروني ويستخدمونه لإرسال رسائل ذات محتوى غير قانوني أو للاستيلاء على حساب يخص مستخدماً لموقع مزادات فيستغلون حسابه هذا في بيع سلع مسروقة.[421]

- **كلمة السر الخاصة بالحسابات المالية** – تعد المعلومات المتعلقة بالحسابات المالية هدفاً مفضلاً لهجمات سرقة الهوية شأنها شأن أرقام الضمان الاجتماعي. وهذا يشمل الحسابات الجارية وحسابات الادخار، وبطاقات الائتمان وبطاقات الخصم، والمعلومات المتعلقة بالتخطيط المالي. وتعد هذه المعلومات مصدراً هاماً لسرقة الهوية من أجل ارتكاب جرائم مالية سيبرانية.

وسرقة الهوية مشكلة خطيرة ومتنامية.[422] وتبين أرقام حديثة أن 3% من الأسر في الولايات المتحدة قد وقعت، خلال النصف الأول من عام 2004، ضحية لسرقة الهوية.[423] وفي المملكة المتحدة، تشير الحسابات إلى أن التكلفة التي تُحملها سرقة الهوية للاقتصاد البريطاني تصل إلى 1,3 مليار جنيه أسترليني كل عام.[424] وتتراوح تقديرات الخسائر الناجمة عن سرقة الهوية في أستراليا بين ما يقل عن مليار دولار أمريكي وأكثر من 3 مليارات دولار أمريكي كل عام.[425] وتقدر الدراسة الاستقصائية لانتحال الهوية لعام 2006 خسائر الولايات المتحدة في عام 2005 بمقدار 56,6 مليار دولار أمريكي.[426] وقد لا تكون الخسائر مالية فحسب، بل هي تشمل أيضاً الإضرار بالسمعة.[427] والواقع أن كثيراً من الضحايا لا يبلغون عن هذه الجرائم، كما أن المؤسسات المالية لا تود في أحيان كثيرة الإعلان عن تجارب عملائها السيئة. ومن المرجح أن يفوق الانتشار الفعلي لسرقة الهوية من بعيد عدد الحالات المبلغ عنها.[428]

وتستند سرقة الهوية إلى قلة الأدوات المستخدمة للتحقق من هوية المستخدمين على الإنترنت. فمن الأسهل تحديد هوية الأفراد في العالم الحقيقي، لكن معظم أشكال التحقق من الهوية على الخط تعد أكثر تعقيداً. وتعد الأدوات المتطورة للتحقق من الهوية (مثل استخدام معلومات القياسات الحيوية (المعلومات البيومترية)) مكلفة وغير مستخدمة على نطاق واسع. ونظراً لقلة القيود المفروضة على الأنشطة التي تمارس على الخط، فإن سرقة الهوية تصبح سهلة ومربحة.[429]

---

[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.

[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.

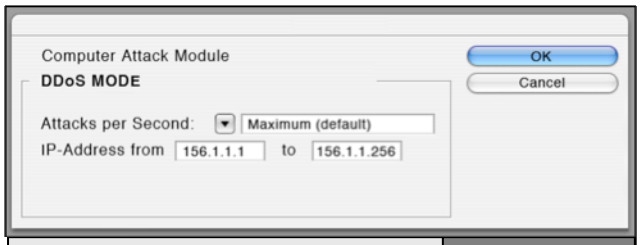
4.7.2 إساءة استخدام الأجهزة

يمكن ارتكاب الجريمة السيبرانية بغير أن تستخدم في ذلك إلا معدات أساسية نسبياً.[430] فارتكاب جرائم مثل القذف أو الاحتيال على الخط لا يستلزم أكثر من حاسوب وإمكانية النفاذ إلى الإنترنت، ويمكن القيام به من مقهى إنترنت عمومي. أما الجرائم الأكثر تطوراً، فترتكب باستخدام أدوات برمجياتية متخصصة.

والأدوات اللازمة لارتكاب جرائم معقدة تتوافر بشكل واسع على الإنترنت،[431] ومجاناً في كثير من الأحيان. أما الأدوات الأكثر تطوراً، فتكلف عدة آلاف من الدولارات.[432] ويستطيع الجناة، باستخدام هذه الأدوات البرمجياتية، مهاجمة نظم حاسوبية أخرى بمجرد الضغط على أحد الأزرار (انظر الشكل 18). وقد باتت الهجمات المعيارية أقل كفاءة الآن، لأن الشركات التي تنتج برمجيات الحماية أصبحت تحلل الأدوات المتاحة في الوقت الحاضر وتتهيأ لهجمات القرصنة المعيارية. وكثيراً ما تكون الهجمات التي تجتذب الأنظار مصممة تصميماً فردياً يتوجه لأهداف بعينها.[433]

وتتوافر أدوات برمجياتية تتيح[434]:

- شن هجمات تستهدف الحرمان من النفاذ إلى الخدمة؛[435]
- تصميم فيروسات حاسوبية؛
- فك تجفير الرسائل المجفرة؛
- النفاذ إلى النظم الحاسوبية بطريقة غير قانونية.



الشكل 18

يتوافر عدد من الأدوات التي تمكن الجناة من شن هجمات مؤتمتة ضد جميع النظم الحاسوبية باستخدام عناوين بروتوكول الإنترنت، ضمن نطاق محدد سلفاً لهذه العناوين. ويمكن بمساعدة هذه البرمجيات شن الهجمات على مئات من النظم الحاسوبية في غضون ساعات قليلة.

وقد نجح الآن جيل ثان من الأدوات البرمجياتية في أتمتة كثير من الحيل السيبرانية فأصبح يتيح للجناة شن هجمات متعددة في غضون فترة قصيرة. كما تسمح الأدوات البرمجياتية بتبسيط الهجمات، مما يتيح لمستخدمي الحاسوب الأقل خبرة ارتكاب الجريمة السيبرانية. وتتوافر "صناديق أدوات لإعداد الرسائل الاقتحامية" تُمكّن أي فرد تقريباً من أن يبعث برسائل اقتحامية.[436] كما تتوافر الآن أدوات برمجياتية يمكن استخدامها لتحميل وتنزيل الملفات من نظم تقاسم الملفات. ومع تزايد تيسّر الأدوات البرمجياتية المصممة لأغراض خاصة محددة، شهد عدد الجناة المحتملين ارتفاعاً مثيراً. وتتخذ في الوقت الحاضر مبادرات تشريعية وطنية ودولية مختلفة من أجل التصدي للأدوات البرمجياتية المستخدمة في الخدع السيبرانية – وذلك مثلاً بتجريم إنتاجها وبيعها وحيازتها.[437]

8.2 *الجرائم المشتركة*

يستخدم عدد من المصطلحات لوصف الخدع المعقدة التي تغطي عدداً من الجرائم المختلفة. ومن أمثلة ذلك:

- الإرهاب السيبراني؛
- غسل الأموال السيبراني؛
- التصيد الاحتيالي.

[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.

[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.

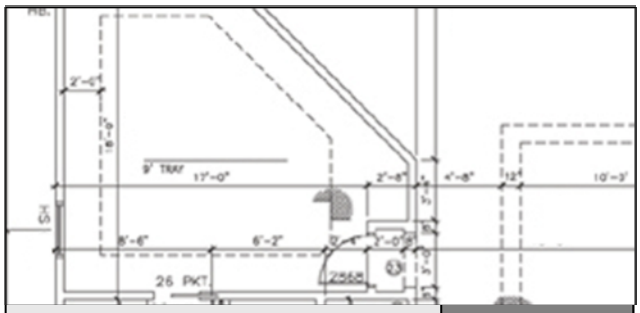
[435] DoS is an acronym for Denial-of-Service attack. For more information, see above : Chapter 2.4.e.

[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.

1.8.2 الإرهاب السيبراني

كان النقاش الدائر في تسعينات القرن الماضي حول استخدام الشبكة من قبل المنظمات الإرهابية يركّز على الهجمات المعتمدة على الشبكة والموجهة ضد بنى تحتية حاسمة مثل النقل وإمدادات الطاقة ("الإرهاب السيبراني")، كما كان يركز على استخدام تكنولوجيا المعلومات في الصراعات المسلحة ("الحرب السيبرانية").[438] وقد أوضح نجاح الهجمات التي تستخدم فيها الفيروسات والشبكات المُسخّرة، على نحو جلي، أوجه الضعف في أمن الشبكة. وقيام الإرهابيين بشن هجمات ناجحة بالاعتماد على الإنترنت أمر ممكن،[439] لكن من الصعب تقييم دلالة التهديدات،[440] وكانت درجة التوصيل البيني آنذاك محدودة بالقياس إلى الوضع الراهن، ومن المرجح للغاية أن يكون هذا الأمر – إلى جانب حرص الدول على تكتم المعلومات عن الهجمات الناجحة – من الأسباب الرئيسية لعدم الإبلاغ إلا عن عدد قليل جداً من الحوادث. وعليه، كان سقوط الأشجار يشكل، في الماضي على الأقل، خطراً أكبر على إمدادات الطاقة من نجاح هجمات القرصنة.[441]



الشكل 19

الإنترنت مصدر هام للمعلومات، ويشمل ذلك المعلومات (مثل الرسومات المعمارية) المتعلقة بأهداف محتملة (مثل المباني العمومية). وهي معلومات يمكن العثور عليها مثلاً في موقع الويب الخاص بالمهندس المعماري الذي صممها، وما إلى ذلك.

غير أن هذه الحالة قد تبدلت بعد هجمات الحادي عشر من سبتمبر. فبدأت مناقشة مكثفة بشأن استخدام الإرهابيين لتكنولوجيا المعلومات والاتصالات.[442] ومما سهل هذه المناقشة التقارير[443] التي أفادت أن الجناة قد استخدموا الإنترنت في التحضير للهجوم.[444] وعلى الرغم من أن الهجمات لم تكن هجمات سيبرانية، لأن الجماعة التي شنت هجوم الحادي عشر من سبتمبر لم تقم بهجوم معتمد على الإنترنت، فإن الإنترنت قد أدت دوراً في التحضير للاعتداء.[445] وضمن هذا السياق، اكتُشفت طرق مختلفة تستخدم بها المنظمات الإرهابية الإنترنت.[446] ومن المعروف اليوم أن الإرهابيين يستخدمون تكنولوجيا المعلومات والاتصالات والإنترنت من أجل:

- الدعاية؛
- جمع المعلومات؛
- التحضير للهجمات في العالم الحقيقي؛
- نشر المواد التدريبية؛
- الاتصال؛

[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.*;

- تمويل الإرهاب؛
- شن الهجمات ضد البنى التحتية الحاسمة.

وكان لهذا التحول في موطن تركيز النقاش تأثير إيجابي على البحوث المتعلقة بالإرهاب السيبراني لأنه سلط الضوء على مجالات لأنشطة إرهابية تكاد تكون غير معروفة من قبل. ولكن على الرغم من أهمية اتباع نهج شامل، فإن تهديد الهجمات المعتمدة على الإنترنت والموجهة ضد بنى تحتية حاسمة ينبغي ألا يخرج من دائرة النقاش. فقلة المنعة وتنامي الاعتماد[447] على تكنولوجيا المعلومات يجعلان من الضروري مراعاة الهجمات المعتمدة على الإنترنت والموجهة ضد البنى التحتية الحاسمة في الاستراتيجيات الرامية إلى منع الإرهاب السيبراني ومكافحته.

ولكن مكافحة الإرهاب السيبراني تبقى عسيرة على الرغم من تزايد كثافة ما يضطلع به من بحوث. وتبين المقارنة بين مختلف النُهج الوطنية العديد من أوجه التماثل في الاستراتيجيات.[448] ومن أسباب هذا التطور أن المجتمعات الدولية قد أقرت بأن تهديدات الإرهاب الدولي تستوجب حلولاً عالمية.[449] ولكن من غير المعروف على وجه اليقين في الوقت الحاضر ما إذا كان هذا النهج يعد ناجحاً أو ما إذا كانت النظم القانونية والخلفيات الثقافية المتباينة تستوجب حلولاً متباينة. وتقييم هذه القضية يحمل في طياته تحديات فريدة، لأنه باستثناء التقارير عن الحوادث الكبرى لا تتوافر إلا معلومات ضئيلة للغاية يمكن الاستعانة بها في التحليل العلمي. وتنشأ هذه الصعوبات نفسها لدى تحديد مستوى التهديد المتعلق باستخدام تكنولوجيا المعلومات من قبل المنظمات الإرهابية. فالمعلومات المتعلقة بهذه المسألة تعد في كثير من الأحيان معلومات سرية ولذا لا تتوافر إلا لقطاع الاستخبارات،[450] وإلى الآن لم تتوافق الآراء حتى على المقصود بمصطلح "الإرهاب".[451] ومن ذلك مثلاً أن تقريراً صادراً عن دائرة البحوث بكونغرس الولايات المتحدة يقول إن استخدام أحد الإرهابيين الإنترنت في حجز بطاقة طائرة إلى الولايات المتحدة دليلٌ على أن الإرهابيين يستخدمون الإنترنت في التحضير لهجماتهم.[452] وتبدو هذه حجة ملتبسة، لأن حجز بطاقة طائرة لا يصبح نشاطاً إرهابياً لمجرد أن الذي قام به أحد الإرهابيين.

الدعاية

في عام 1998 كانت 12 منظمة إرهابية فقط، من المنظمات الإرهابية الأجنبية الثلاثين التي قامت بحصرها وزارة الخارجية في الولايات المتحدة، هي التي تحتفظ بمواقع على الويب لإعلام الجمهور عن أنشطتها.[453] وفي عام 2004 أفاد معهد السلام في الولايات المتحدة أن كل المنظمات الإرهابية تقريباً قد أنشأت مواقع ويب – ومن بينها حماس، وحزب الله، وحزب العمال الكردستاني، وتنظيم القاعدة.[454] كما بدأ الإرهابيون في استخدام جمهور مواقع الفيديو (مثل يوتيوب YouTube) لتوزيع رسائل ومواد دعائية عن طريق الفيديو.[455] واستخدام مواقع الويب والمنتديات الأخرى دليل على أن الجماعات المخربة باتت تركز على العلاقات العامة بطريقة ذات طابع مهني أوضح.[456] فتستخدم مواقع الويب والوسائط الأخرى لنشر المواد الدعائية،[457] ولوصف أنشطتها وتبريرها،[458] ولتجنيد أعضاء ومانحين جدد[459] والاتصال بالحاليين منهم.[460] وقد استخدمت مواقع الويب مؤخراً في توزيع لقطات فيديو عن عمليات إعدام.[461]

---

[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.

[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.

جمع المعلومات

تتوافر على الإنترنت معلومات كثيرة عن الأهداف المحتملة.[462] ومن ذلك مثلاً، أن المهندسين المشاركين في بناء المباني العمومية كثيراً ما ينشرون الرسومات الهندسية لتلك المباني على مواقع الويب الخاصة بهم (انظر الشكل 21). كما تتوافر اليوم مجاناً صور ساتلية عالية الاستبانة من خلال خدمات شتى متاحة على الإنترنت، وهي صور لم تكن تتوافر قبل عدة سنوات مضت إلا لقلة من المؤسسات العسكرية في العالم.[463] وعلاوة على ذلك، تم الوقوف على إرشادات تبين كيفية صنع القنابل، بل وحتى على مخيمات تدريب افتراضية تقدم إرشادات عن كيفية استخدام الأسلحة بنهج التعلّم الإلكتروني.[464] وتم الوقوف أيضاً على معلومات حساسة لا توفر لها روبوتات البحث حماية كافية، ويمكن النفاذ إليها عن طريق محركات البحث.[465] وفي عام 2003، أُبلغت وزارة الدفاع في الولايات المتحدة بأن ثمة دليلاً تدريبياً منسوباً إلى تنظيم القاعدة يحتوي على معلومات تفيد أن المصادر العمومية يمكن استخدامها للعثور على بيانات تتعلق بأهداف محتملة.[466] وفي عام 2006، أفادت جريدة النيويورك تايمز أن موقع ويب حكومياً قد نشر، في إطار سوقه لأدلة على النُهج التي يتبعها العراق لاستحداث أسلحة نووية، معلومات أساسية تتعلق بصنع الأسلحة النووية.[467] وأُبلغ عن حادثة مماثلة في أستراليا حيث نُشرت على مواقع ويب حكومية معلومات عن أهداف محتملة للهجمات الإرهابية.[468] وفي عام 2005، أفادت الصحافة الألمانية أن محققين قد وجدوا أن أدلة تتعلق بصنع المتفجرات قد تم تنزيلها من الإنترنت إلى حاسوب شخصين مشتبه فيهما حاولا مهاجمة مرافق النقل العمومي بقنابل ذاتية الصنع.[469]

التحضير لهجمات تنفذ في العالم الحقيقي

هناك طرق مختلفة يمكن أن يستخدم الإرهابيون بها تكنولوجيا المعلومات في التحضير لهجومهم. ومن الأمثلة التي ستناقش في سياق موضوع "الاتصالات" الوارد أدناه، توجيه الرسائل الإلكترونية أو استخدام المنتديات لترك الرسائل.[470] وتناقش في الوقت الحاضر طرق ذات طابع مباشر أوضح تستعمل في التحضير للهجمات على الخط. وقد نُشرت تقارير تشير إلى أن الإرهابيين يستخدمون الألعاب المتاحة على الخط في التحضير لهجماتهم.[471] إذ تتوافر على الخط ألعاب مختلفة تحاكي العالم الحقيقي. ويستطيع مستخدم هذه الألعاب أن يحرك الشخصيات الإلكترونية لهذه الألعاب لتأتي بأعمال معينة في هذا العالم الافتراضي. ويمكن من الناحية النظرية استخدام هذه الألعاب المتاحة على الخط لمحاكاة الهجمات، لكن ليس من المعروف على وجه اليقين حتى الآن إلى أي مدى تستخدم بالفعل الألعاب المتاحة على الخط في ذلك النشاط التحضيري.[472]

نشر المواد التدريبية

يمكن استخدام الإنترنت لنشر مواد تدريبية مثل الإرشادات المتعلقة بكيفية استخدام الأسلحة وكيفية اختيار الأهداف. وهذه المواد متاحة على نطاق واسع من مصادر موجودة على الخط.[473] وفي عام 2008، اكتشفت دوائر غربية مخدماً على الإنترنت يوفر قاعدة لتبادل مواد تدريبية وتيسير الاتصالات.[474] وأُبلغ عن مواقع ويب مختلفة تشغلها منظمات إرهابية لتنسيق أنشطتها.[475]

---

[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.
[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* in 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.

الاتصالات

لا يقتصر استخدام المنظمات الإرهابية لتكنولوجيا المعلومات على تشغيل مواقع الويب والبحث في قواعد البيانات. فقد أفادت التقارير، في سياق التحقيقات التي جرت في أعقاب هجمات الحادي عشر من سبتمبر، أن الإرهابيين قد استخدموا الاتصالات بالبريد الإلكتروني في إطار التنسيق لهجماتهم.[476] ونقلت الصحافة أخباراً عن استخدام البريد الإلكتروني في تبادل إرشادات تفصيلية عن الأهداف وعدد المهاجمين.[477] وعن طريق استخدام تكنولوجيا التجفير ووسائل الاتصالات المجهولة الهوية، يستطيع الشريك في الاتصالات أن يوجد مزيداً من الصعوبات أمام تحديد هويته ورصد الاتصالات الإرهابية.

تمويل الإرهاب

تعتمد معظم المنظمات الإرهابية على الموارد المالية التي تتلقاها من أطراف ثالثة. وقد أصبح تتبع هذه المعاملات المالية من النُهج الرئيسية المتبعة في مكافحة الإرهاب بعد هجمات الحادي عشر من سبتمبر. ومن أهم الصعوبات المصادفة في هذا الصدد أن الموارد المالية المطلوبة لشن الهجمات لا تعد مرتفعة بالضرورة.[478] وثمة عدة طرق يمكن أن تستخدم بها خدمات الإنترنت من أجل تمويل الإرهاب. فالمنظمات الإرهابية تستطيع أن تستخدم نظم الدفع الإلكتروني في الحصول على تبرعات على الخط.[479] وبمقدورها أن تستخدم مواقع الويب لنشر معلومات عن كيفية التبرع، ومن هذه المعلومات مثلاً الحساب المصرفي الذي ينبغي استخدامه لإجراء المعاملات. ومن أمثلة هذا النهج ما تتبعه منظمة "حزب التحرير" التي تنشر معلومات عن حساب مصرفي يستخدمه المتبرعون المحتملون.[480] ويتمثل نهج آخر في تحصيل التبرعات على الخط عن طريق بطاقات الائتمان. وكان الجيش الجمهوري الآيرلندي من أولى المنظمات الإرهابية التي أتاحت فرصة التبرع عن طريق بطاقات الائتمان.[481] ويجازف كلا النهجين باحتمال أن تكتشف المعلومات المنشورة وأن يستعان بها لتتبع المعاملات المالية. ولذا، فإن من المرجح أن تصبح نظم الدفع الإلكتروني المجهول الهوية أكثر انتشاراً. وتحاول المنظمات الإرهابية، تجنباً لاكتشافها، أن تخفي أنشطتها بإشراك لاعبين لا يشتبه فيهم مثل المنظمات الخيرية. ويتمثل نهج آخر (يعتمد على الإنترنت) في تشغيل متاجر ويب زائفة. فمن السهل نسبياً إنشاء متجر على الإنترنت. ومن أضخم مزايا الشبكة أن الشركات التجارية يمكن أن تمارس نشاطها على نطاق عالمي. وإثبات أن المعاملات المالية التي تجري على هذه المواقع ليس عمليات شراء عادية بل تبرعات أمر بالغ الصعوبة. وسيكون من الضروري التحقيق في كل معاملة، وهو أمر قد يكون صعباً إذا كان المتجر الموجود على الخط يعمل في ولاية قضائية مختلفة أو يستخدم نظماً للدفع المجهول الهوية.[482]

الهجمات ضد البنى التحتية الحاسمة

بالإضافة إلى الجرائم الحاسوبية العادية مثل الاحتيال وسرقة الهوية، يمكن أن تصبح الهجمات ضد البنى التحتية الحاسمة للمعلومات هدفاً للإرهابيين. وتنامي الاعتماد على تكنولوجيا المعلومات يجعل البنى التحتية الحاسمة أكثر عرضة للهجمات.[483] ويصدق هذا بوجه خاص على الهجمات الموجهة ضد النظم الموصولة بينياً عن طريق شبكات الحواسيب والاتصالات.[484] وفي تلك الحالات يتجاوز الخلل الذي يسببه هجوم معتمد على الشبكة مجرد تعطل نظام واحد. فحتى الانقطاعات القصيرة في الخدمات يمكن أن تلحق أضراراً مالية ضخمة بالأعمال التجارية الإلكترونية – ولا يصدق هذا على الخدمات المدنية وحدها بل ويصدق أيضاً على البنى التحتية والخدمات العسكرية.[485] ويطرح التحقيق في تلك

[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.
[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

الهجمات أو حتى الوقاية منها تحديات فريدة.[486] فخلافاً للهجمات المادية، لا يتعين على الجناة أن يكونوا موجودين في مكان وقوع الهجوم.[487] ويستطيع الجناة، إبان قيامهم بالهجوم، استخدام وسائل الاتصال المجهول الهوية وتكنولوجيا التجفير لإخفاء هويتهم.[488] وكما سلفت الإشارة، يقتضي التحقيق في هذه الهجمات صكوكاً إجرائية خاصة، والتكنولوجيا اللازمة للتحقيق، والموظفين المدربين.[489]

ومن المعترف به على نطاق واسع أن البنى التحتية الحاسمة تشكل هدفاً محتملاً لهجوم إرهابي، لأنها تعد بحكم التعريف ذات أهمية حيوية لاستدامة دولة من الدول واستقرارها.[490] وتعتبر البنية التحتية حاسمة إذا كان من شأن تعطيلها أو تدميرها أن يضعف الأمن الدفاعي أو الاقتصادي للدولة.[491] وهذه البنى التحتية هي على وجه الخصوص: نظم الطاقة الكهربائية، ونظم الاتصالات، ومرافق التخزين ونقل الغاز والنفط، والصرافة والمالية، والنقل، ونظم إمدادات المياه، وخدمات الطوارئ. وتُبرز درجة الخلل المدني الذي نجم عن اضطراب الخدمات من جراء إعصار كاترينا الذي أصاب الولايات المتحدة مدى اعتماد المجتمع على تيسّر تلك الخدمات.[492]

ويمكن إيضاح مظاهر قلة منعة البنى التحتية الحاسمة إزاء الهجمات المعتمة على الشبكات بتسليط الضوء على بعض الحوادث المتعلقة بالنقل الجوي.

- تستند بالفعل نظم التسجيل للسفر في معظم مطارات العالم إلى نظم حاسوبية موصولة بينياً.[493] وفي عام 2004 أصابت دودة ساسر (Sasser) الحاسوبية[494] ملايين الحواسيب حول العالم، ومن بينها النظم الحاسوبية للخطوط الجوية الكبرى، مما فرض إلغاء الرحلات.[495]
- واليوم يُشترى عدد كبير من بطاقات السفر على الخط. وتستخدم الخطوط الجوية تكنولوجيا المعلومات في عمليات متنوعة. وتسمح جميع الخطوط الجوية الكبرى لزبائنها بشراء البطاقات على الخط. ومثلما يستهدف الجناة أنشطة التجارة الإلكترونية الأخرى، فإن بوسعهم أن يستهدفوا أيضاً تلك الخدمات المتاحة على الخط. ومن التقنيات الشائعة المستخدمة للهجوم على الخدمات المعتمدة على الويب الهجمات الرامية إلى الحرمان من النفاذ إلى الخدمة.[496] وفي عام 2000، شُنت عدة هجمات من هذا النوع، في غضون فترة وجيزة، ضد شركات شهيرة مثل الـ سي إن إن وإيباي وأمازون.[497] وأسفر ذلك عن عدم توافر بعض الخدمات لعدة ساعات بل ولعدة أيام.[498] كما تضررت الخطوط الجوية بدورها من تلك الهجمات. وفي عام 2001 كان موقع لوفتهانزا على الويب هدفاً لإحدى الهجمات.[499]

[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* in 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.
[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.

- ونظم المراقبة الجوية من الأهداف المحتملة الأخرى للهجمات المعتمدة على الإنترنت والموجهة ضد البنى التحتية للنقل الجوي التي تتسم بأهمية حاسمة. وقد تجلت قلة منعة نظم المراقبة الجوية الحاسوبية إبان هجوم قرصنة تعرض له مطار وورسستر في الولايات المتحدة في عام 1997[500] ففي أثناء هذا الهجوم، عطل الجناة الخدمات الهاتفية الداخلة إلى برج المراقبة وأغلقوا نظام المراقبة الذي يدير إضاءة مهابط الطائرات.[501]

2.8.2 الحرب السيبرانية

يقصد بالحرب السيبرانية استخدام تكنولوجيا المعلومات والاتصالات في إدارة الحرب باستخدام الإنترنت. وتشترك الحرب السيبرانية في عدد من السمات مع الإرهاب السيبراني.[502] وقد ركّزت المناقشات في البداية على الاستعاضة عن الحرب التقليدية بهجمات تشن بواسطة الحاسوب أو تعتمد عليه.[503] وتعد الهجمات المعتمدة على الشبكة أزهد تكلفة بوجه عام من العمليات العسكرية التقليدية[504] ويمكن أن تقوم بها حتى الدول الصغيرة.

خطأ

لا تتوافر هذه الخدمة بسبب العمليات العسكرية الجارية.

الشكل 20

أصبحت الإنترنت في السنوات الأخيرة وسيطاً هاماً لتبادل المعلومات والدعاية أثناء الصراعات المسلحة. وكثيراً ما يُناقش إلى أي مدى يمكن و/أو يستصوب تعطيل بعض خدمات الإنترنت أثناء المراحل الرئيسية لتصاعد الصراع.

وتوفير الحماية إزاء الهجوم السيبراني أمر صعب. وحتى الآن، لا تتوافر إلا تقارير محدودة بشأن مسألة الاستعاضة عن الصراعات المسلحة بالهجمات المعتمدة على الإنترنت.[505] وتركز المناقشات الراهنة على الهجمات ضد البنى التحتية الحاسمة وعلى التحكم في المعلومات أثناء الصراع (انظر الشكل 20).

وفيما يتعلق بكل من الاتصالات المدنية والعسكرية، تشكل البنى التحتية للمعلومات هدفاً رئيسياً في الصراعات المسلحة. ولكن ليس من المعروف على وجه اليقين ما إذا كانت هذه الهجمات ستشن عن طريق الإنترنت. ولقد رُبطت الهجمات ضد النظم الحاسوبية في إستونيا[506] والولايات المتحدة[507] بالحرب السيبرانية. غير أنه لما كان من المتعذر تتبع الهجمات وصولاً، بأي قدر من اليقين، إلى منظمات حكومية رسمية، فمن الصعب تصنيف تلك الهجمات على أنها تدخل في باب الحرب السيبرانية. كما أن الهجمات المنفذة مادياً ضد البنى التحتية – وذلك مثلاً عن طريق الأسلحة والمتفجرات – من الصعب تصنيفها هي الأخرى على أنها حرب سيبرانية.[508]

وكان التحكم في المعلومات من القضايا الهامة دوماً في الصراعات المسلحة، لأن المعلومات يمكن استخدامها للتأثير في الجمهور وكذلك في أفراد القوات المسلحة المعادية. وسيصبح التحكم في المعلومات على الإنترنت وسيلة تأثير تتزايد أهميتها أثناء الصراعات المسلحة.

3.8.2 غسل الأموال السيبراني

بدلت الإنترنت عملية غسل الأموال. وإذا كانت التقنيات التقليدية لغسل الأموال ما زالت توفر عدداً من المزايا فيما يخص المبالغ الكبيرة، فإن الإنترنت توفر من جهتها مزايا جمة. فالخدمات المالية المتاحة على الخط تتيح إجراء معاملات مالية متعددة على النطاق العالمي بسرعة بالغة. وأسهمت الإنترنت في التغلب على الاعتماد على المعاملات النقدية المادية. وحلت التحويلات السلكية محل نقل المبالغ النقدية، لتكون هذه هي الخطوة المبتكرة الأولى في القضاء على الاعتماد المادي على الأموال، لكن تطبيق أنظمة أكثر صرامة للكشف عن التحويلات السلكية المشتبه فيها أجبر الجناة على ابتكار تقنيات جديدة. ويستند كشف المعاملات المشتبه فيها في إطار مكافحة غسل الأموال إلى التزامات المؤسسات المالية المشاركة في عملية التحويل.[509]

---

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

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

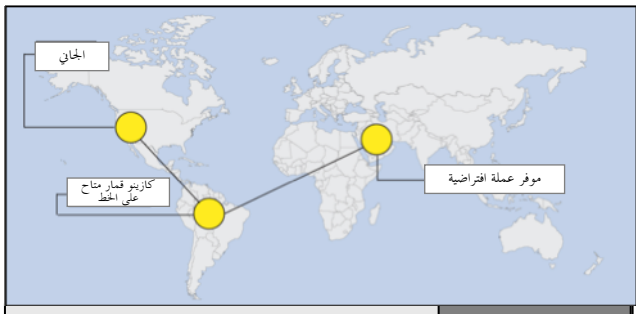
وينقسم غسل الأموال بوجه عام إلى ثلاث مراحل هي:

1 الاستثمار؛

2 الترقيد؛

3 الإدماج.

فيما يتعلق باستثمار كميات كبيرة من النقد قد لا يوفر استخدام الإنترنت مزايا ملموسة جمة.[510] غير أن الإنترنت تعد مفيدة بوجه خاص للجناة في مرحلة الترقيد (أو الإخفاء). وفي هذا السياق، يعد تقصي غسل الأموال صعباً بوجه خاص عندما يلجأ غاسلو الأموال إلى كازينوهات القمار المتاحة على الخط لترقيد أموالهم (انظر الشكل 21).[511]



الشكل 21

يوضح هذا الرسم البياني مسألة الجمع بين كازينوهات القمار المتاحة على الخط والعملات الافتراضية في حيل غسل الأموال المعتمدة على الإنترنت. إذ يستطيع الجناة، عن طريق استخدام هذه الخدمات، أن يجعلوا من الصعب على وكالات إنفاذ القانون تتبع عمليات التحويل وتحديد هوية الجناة.

ويعد تنظيم عمليات تحويل الأموال محدوداً في الوقت الحاضر، وتتيح الإنترنت للجناة إمكانية إجراء عمليات رخيصة ومعفاة من الضرائب لتحويل الأموال عبر الحدود. وتعزى الصعوبات الراهنة في التحقيق في تقنيات غسل الأموال المعتمدة على الإنترنت، في كثير من الأحيان، إلى استخدام العملات الافتراضية وكازينوهات القمار المتاحة على الخط.

1 استخدام العملات الافتراضية:

كان من الدوافع الرئيسية وراء استحداث العملات الافتراضية الحاجة إلى دفع مبالغ بالغة الصغر (وذلك مثلاً نظير تنزيل مقالات على الخط بتكلفة تبلغ 10 سنتات أمريكية أو أقل)، حيث يكون من الصعب استخدام بطاقات الائتمان. ومع تنامي الطلب على المدفوعات البالغة الصغر، ابتكرت العملات الافتراضية، بما فيها "العملات الذهبية الافتراضية". وهذه العملات الذهبية الافتراضية هي نظم دفع مستندة إلى حسابات تعتمد القيمة فيها على ودائع ذهبية. ويستطيع المستخدمون فتح حسابات ذهبية إلكترونية على الخط، وذلك دون تسجيل في كثير من الأحيان. بل أن بعض موفري هذه الحسابات يتيحون التحويل المباشر بين النظراء (من شخص لآخر) أو سحب مبالغ نقدية.[512] ويستطيع الجناة أن يفتحوا حسابات ذهبية إلكترونية في بلدان مختلفة وأن يجمعوا بينها، مما يعقد سبل استخدام الأدوات المالية في غسل الأموال وتمويل الإرهاب. وقد يستخدم أيضاً أصحاب الحسابات معلومات غير دقيقة أثناء التسجيل لإخفاء هويتهم.[513]

2 استخدام كازينوهات القمار المتاحة على الخط:

خلافاً لكازينوهات القمار الحقيقية، لا يقتضي الأمر توظيف استثمارات مالية كبيرة لإنشاء كازينوهات القمار على الخط.[514] وبالإضافة إلى ذلك، فإن الأنظمة المتعلقة بكازينوهات القمار المتاحة على الخط وخارج الخط تتفاوت في كثير من الأحيان فيما بين البلدان.[515] ولن يتسنى تعقب تحويلات الأموال وإثبات أن الأموال لا تتأتى من فوز بجوائز بل تم غسلها، إلا إذا احتفظت كازينوهات القمار بسجلات ووفرتها لوكالات إنفاذ القانون.

والأنظمة القانونية الراهنة التي تحكم الخدمات المالية المعتمدة على الإنترنت ليست في صرامة الأنظمة المالية التقليدية. وإلى جانب الثغرات التشريعية، تنبع الصعوبات الناشئة عن الأنظمة مما يلي:

- الصعوبات المصادفة في التحقق من الزبائن: قد يكون من الصعب إجراء تحقق دقيق إذا كان مقدم الخدمة المالية والزبون لا يلتقيان أبداً؛[516]
- بسبب الافتقار إلى اتصال شخصي يكون من الصعب تطبيق الإجراءات التقليدية القاضية بالتعرف على الزبون؛
- كثيراً ما تنطوي تحويلات الإنترنت على مشاركة من مقدمي الخدمة في بلدان مختلفة عبر الحدود؛
- يسبب غياب القانون/القانون الجنائي اللازم لرصد أدوات معينة وضعاً صعباً بوجه خاص، عندما يسمح مقدمو الخدمة للزبائن بنقل القيمة وفقاً لنموذج التعامل بين النظراء.

[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] The costs of setting up an online casino are not significantly larger than other e-commerce businesses.
[516] See: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000 – 2001", 2001, page 2.

4.8.2 التصيد الاحتيالي

استحدث الجناة تقنيات تتيح لهم الحصول على معلومات شخصية من المستخدمين، تتراوح من برمجيات التجسس[517] إلى هجمات "التصيد الاحتيالي".[518] ويقصد بمصطلح "التصيد الاحتيالي" أفعالاً تنفذ لجعل الضحايا يفصحون عن معلومات شخصية/سرية.[519] وهناك أنواع مختلفة من برمجيات التصيد الاحتيالي[520] لكن هجمات التصيد الاحتيالي المعتمدة على الرسائل الإلكترونية تتضمن ثلاث مراحل رئيسية. في المرحلة الأولى، يحدد الجناة شركة مشروعة توفر خدمات على الخط ويتصلون إلكترونياً بزبائن يستطيعون استهدافهم، مثل المؤسسات المالية. ويصمم الجناة مواقع ويب تشبه مواقع الويب المشروعة ("مواقع إيهامية") تتطلب من الضحايا القيام بإجراءات الدخول العادية، مما يمكن الجناة من الحصول على معلومات شخصية (مثل أرقام الحسابات وكلمات السر الخاصة بالصرافة على الخط).

وبغية توجيه المستخدمين إلى المواقع الإيهامية، يبعث الجناة برسائل إلكترونية تشبه الرسائل الصادرة عن الشركة المشروعة (انظر الشكل 22)[521] مما يسفر في كثير من الأحيان عن انتهاكات للعلامات التجارية.[522] وتطلب الرسائل المزيفة من متلقيها تسجيل بيانات الدخول من أجل إجراء عمليات تحيين أو عمليات للتحقق الأمني، وقد تلجأ إلى التهديد (بإقفال الحساب مثلا) في حالة عدم تعاون المستخدمين. وتحتوي الرسائل المزيفة عادة على وصلة ينبغي أن يتبعها الضحية تقوده إلى الموقع الإيهامي، كيلا يدخل المستخدمون يدوياً إلى عنوان الويب الصحيح للبنك المشروع. وقد استحدث الجناة تقنيات متقدمة تمنع المستخدمين من تبين أنهم ليسوا في موقع الويب الحقيقي.[523]

وبمجرد الإفصاح عن المعلومات السرية، يدخل الجناة إلى حسابات الضحايا ويرتكبون جرائم مثل تحويل الأموال، وطلب الحصول على جوازات السفر، أو فتح حسابات جديدة، وما إلى ذلك. ويثبت ارتفاع عدد الهجمات الناجحة الإمكانات التي ينطوي عليها التصيد الاحتيالي.[524] ففي أبريل 2007، أُبلغ فريق العمل المعني بمكافحة التصيد الاحتيالي[525] بأكثر من 55 000 موقع اصطياد قائم بذاته.[526] ولا تقتصر تقنيات التصيد الاحتيالي على النفاذ إلى كلمة السر للقيام بعمليات مصرفية على الخط. فقد يسعى الجناة أيضاً إلى الحصول على شفرات النفاذ إلى الحواسيب، ومنصات المزادات، وكذلك إلى أرقام الضمان الاجتماعي التي تعد هامة بوجه خاص في الولايات المتحدة ويمكن استخدامها في ارتكاب جرائم "سرقة الهوية".[527]

بنك NPW™

عميلنا العزيز،

نود أن نخبركم بأننا نحتاج إلى التحقق من حسابكم. لقد تلقينا في الأسابيع الماضية عدداً من الشكاوى تتعلق برسائل التصيد الاحتيالي. وتجنباً للمشكلات، نرجوكم أن تزوروا موقع الويب التالي:

www.npwbank-online.com/security-chech/

إن لم تنفذوا هذا الإجراء في غضون 24 ساعة سنضطر آسفين إلى إقفال حسابكم.

ونشكركم جزيل الشكر على تعاونكم.

الشكل 22

تصمم رسائل التصيد الاحتيالي الإلكترونية بحيث تشبه رسالة إلكترونية واردة من شركة مشروعة لجعل الضحية يفصح عن معلومات سرية. ويستهدف الجناة في أحيان كثيرة للغاية زبائن المؤسسات المالية.

[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.
[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.

9.2 التأثير الاقتصادي للجريمة السيبرانية

مما لا شك فيه أن الضرر المالي الذي تتسبب فيه جرائم الحواسيب والإنترنت ضرر كبير. وقد نشرت مؤخراً دراسات استقصائية متنوعة تحلل التأثير الاقتصادي للجريمة السيبرانية،[528] فأبرزت ضخامة تأثيرها. وتثور شواغل عامة بشأن مدى دقة إحصاءات الجرائم، وهذه الشواغل نفسها تنطبق أيضاً على التقديرات الخاصة بالضرر المالي – فمن غير المعروف على وجه اليقين إلى أي مدى توفر الدراسات الاستقصائية أرقاماً وإحصاءات دقيقة، لأن كثيراً من الضحايا قد لا يبلغون عما يتعرضون له من جرائم.[529]

1.9.2 لمحة عامة عن نتائج نخبة من الدراسات الاستقصائية

حللت الدراسة الاستقصائية للجريمة الحاسوبية والأمن الحاسوبي لعام 2007، الصادرة عن معهد الأمن الحاسوبي، التأثير الاقتصادي للجريمة السيبرانية،[530] استناداً إلى ردود 494 مشتغلاً بالأمن الحاسوبي في شركات ووكالات حكومية ومؤسسات مالية في الولايات المتحدة. وتنطبق هذه الدراسة أساساً على الولايات المتحدة.[531]

وتفيد الدراسة، التي أخذت الدورة الاقتصادية في حسبانها، أن التأثير المالي للجريمة السيبرانية، بعد أن ظل يرتفع حتى عام 2002، أخذ ينخفض خلال السنوات التالية. وترى الدراسة أن هذه نتيجة خلافية، فمن غير الواضح لماذا قلّ عدد جرائم المبلغ عنها ولماذا انخفضت الخسارة المتوسطة التي لحقت بالضحايا. وفي عام 2006، أخذ حجم الخسائر يتصاعد مرة أخرى. ولا تفسر الدراسة انخفاض الخسائر في عام 2002 ولا ارتفاعها في عام 2006. ومن بين 21 فئة من فئات الجرائم وقفت عليها الدراسة، كانت أعلى الخسائر المالية تتعلق بالتزوير المالي، والفيروسات، ودخول أطراف خارجية إلى النظام، وسرقة البيانات السرية. ووصلت الخسائر الإجمالية لعام 2006 التي أبلغ عنها جميع المجيبين إلى نحو 66,9 مليون دولار أمريكي.

وبعد انقضاء عدد من السنوات انخفضت فيها الخسائر المتوسطة لكل مجيب، بدا أن هناك تحولاً آخذاً في الحدوث. ففي عام 2006، كانت الخسائر المتوسطة تبلغ 345 000 دولار أمريكي. وفي عام 2001، كانت الخسائر المتوسطة أعلى بنحو عشرة أمثال (3,1 مليون دولار أمريكي). وتعتمد الخسارة المتوسطة لكل مجيب اعتماداً قوياً على تكوين المجيبين – فإذا كانت الشركات الصغيرة والمتوسطة الحجم هي التي تجيب أساساً في إحدى السنوات ثم يستعاض عنها بالشركات الكبرى في السنة التالية، فإن تغير المشاركين يؤثر تأثيراً قوياً في النتائج الإحصائية.

وتتبع الدراسة الاستقصائية للجريمة الحاسوبية لعام 2005 الصادرة عن مكتب التحقيقات الفيدرالي (FBI)[532] نهجاً مماثلاً للدراسة الخاصة بمعهد الأمن الحاسوبي، ولكنها تتسم بتغطية أكثر شمولاً وأوسع نطاقاً[533] وتقدر دراسة مكتب التحقيقات الفيدرالي تكلفة الحوادث الأمنية الناجمة عن الجرائم الحاسوبية وجرائم الإنترنت بما يصل إلى 21,7 مليون دولار أمريكي.[534] وكانت أكثر الجرائم انتشاراً التي كشفت عنها المنظمات المجيبة هي الهجمات الفيروسية، وبرمجيات التجسس، ومسح المنافذ، وتخريب البيانات أو الشبكات.[535] وتتضمن الدراسة الاستقصائية للجرائم الحاسوبية لعام 2005 الصادرة عن مكتب التحقيقات الفيدرالي تقديراً للخسائر الكلية الواقعة على اقتصاد الولايات المتحدة.[536] فاستناداً إلى الخسائر المتوسطة[537] وبافتراض أن نحو 20% من المنظمات في الولايات المتحدة تتضرر من الجرائم الحاسوبية، قُدرت الخسائر الإجمالية بمبلغ 67 مليار دولار أمريكي.[538] ولكن تثور الشواغل إزاء مدى اتصاف هذه التقديرات بالصفة التمثيلية، ومدى اتساق المشاركين سنة بعد أخرى.[539]

---

[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/.

[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/

ويركز "تقرير الاقتصاديات الحاسوبية للبرمجيات الضارة لعام 2007"[540] على استبانة تأثير البرمجيات الضارة في الاقتصاد العالمي، وذلك عن طريق تجميع إجمالي الخسائر المقدرة[541] التي تتسبب فيها الهجمات. ومن النتائج الرئيسية للتقرير أن الجناة الذين يصممون البرمجيات الخبيثة آخذون في التحول من أعمال التخريب إلى التركيز على جني الأرباح المالية. ووجد التقرير أن الخسائر المالية التي تتسبب فيها هجمات البرمجيات الضارة قد وصلت إلى ذروتها في عام 2000 (17,1 مليار دولار أمريكي) وعام 2004 (17,5 مليار دولار أمريكي)، غير أنها أخذت تنخفض منذ عام 2004 لتصل إلى 13,3 مليار دولار أمريكي في عام 2006. ولكن على غرار نتائج الدراسة الاستقصائية، من غير المعروف على وجه اليقين إلى أي مدى تعد الإحصاءات المتعلقة بتأثير البرمجيات الضارة إحصاءات واقعية. فهناك تفاوتات كبيرة بين الخسائر المبلغ عنها والأضرار المؤكدة – وخذ مثلاً حالة دودة ساسر (Sasser). فقد تم الإبلاغ عن إصابة الملايين من النظم الحاسوبية.[542] ولكن في الدعوى المدنية المقامة ضد مصمم البرمجيات، لم تستجب إلا قلة قليلة من الشركات والأفراد للطلب الداعي إلى إثبات خسائرهم والانضمام إلى الدعوى. وانتهت القضية إلى تسوية تقضي بأن يدفع مصمم الفيروس تعويضاً يقل عن عشرة آلاف دولار أمريكي.[543]

2.9.2 الصعوبات المتعلقة بإحصاءات الجرائم السيبرانية

من غير الواضح إلى أي مدى تتصف الإحصاءات المتعلقة بالتأثير الاقتصادي للجريمة السيبرانية بالصفة التمثيلية، ومن غير الواضح ما إذا كانت توفر معلومات موثوق بها عن حجم الخسائر.[544] ومن غير المعروف على وجه اليقين إلى أي مدى يجري الإبلاغ عن الجريمة السيبرانية، لا في إطار الدراسات الاستقصائية وحدها، بل أيضاً إلى وكالات إنفاذ القانون. وتشجع السلطات المُشاركة في مكافحة الجرائم السيبرانية ضحايا هذه الجرائم على الإبلاغ عنها.[545] ومن شأن النفاذ إلى معلومات أكثر دقة عن الحجم الحقيقي للجرائم السيبرانية أن يمكن وكالات إنفاذ القانون من تحسين الملاحقة القضائية للجناة، وردع الهجمات المحتملة، وسن تشريعات أكثر ملاءمة وفعالية.

وقد حاولت عدة منظمات تابعة للقطاعين العام والخاص أن تضع تقديراً كمياً للتكاليف المباشرة وغير المباشرة للبرمجيات الضارة. ولئن كان من الصعب تقدير هذه التكلفة بالنسبة للشركات، فمن الأصعب تقدير الخسائر المالية التي تلحقها البرمجيات الضارة والبرمجيات المماثلة بالمستهلكين الأفراد، على الرغم من وجود أدلة متفرقة على أن هذه الأضرار قد تكون كبيرة للغاية.[546] غير أن هذه التكاليف تتألف من عناصر مختلفة. فهذه البرمجيات قد تسفر عن أضرار مباشرة تلحق بالمعدات والبرمجيات وكذلك عن خسائر مالية وأضرار أخرى تعزى إلى سرقة الهوية أو خطط احتيالية أخرى. ولئن تباين نطاق هذه التقديرات، فإن الصورة العامة التي تتبدى معالمها تعد متماسكة إلى حد كبير.

أما الشركات التجارية فقد تتجنب، من جهة أخرى، الإبلاغ عن الجرائم السيبرانية لعدة أسباب:

فقد تخشى هذه الشركات من أن تضر الدعاية السلبية بسمعتها.[547] فإذا ما أعلنت إحدى الشركات أن القراصنة قد نفذوا إلى مخدمها، فإن زبائنها قد يفقدون ثقتهم بها. وقد تكون الخسائر والعواقب الكلية أكبر حجماً من الخسائر التي تسبب فيها هجوم القراصنة. ولكن إذا لم يتم الإبلاغ عن الجناة وملاحقتهم قضائياً فقد يمضون في اقتراف جرائم جديدة.

[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.
[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

وقد لا يؤمن الأهداف بأن وكالات إنفاذ القانون ستكون قادرة على تحديد هوية الجناة.[548] فعند مقارنة العدد الكبير من الجرائم السيبرانية بالعدد الضئيل للتحقيقات الناجحة، قد لا يرى الأهداف فائدة تُرجى من الإبلاغ عما تعرضوا له من جرائم.[549]

كذلك تعني الأتمتة أن مرتكبي الجرائم السيبرانية يتبعون استراتيجية تتمثل في جني أرباح طائلة من شن هجمات عديدة تستهدف مبالغ صغيرة (كما يحدث مثلاً في الاحتيال لتحصيل مبلغ من المال بزعم تقديم خدمة لاحقة وهمية[550]). فعندما لا يتعلق الأمر إلا بمبالغ صغيرة، قد يفضل الضحايا ألا يمروا بإجراءات الإبلاغ المستنزفة للوقت. وتتعلق الحالات المبلغ عنها في كثير من الأحيان بمبالغ بالغة الارتفاع[551] وباستهداف المبالغ الصغيرة فقط، يصمم الجناة خدعاً لن يجري تعقبها في كثير من الأحيان.

[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.

[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.

3 تحديات مكافحة الجريمة السيبرانية

أسفرت التطورات التي استجدت مؤخراً في مجال تكنولوجيا المعلومات والاتصالات لا عن جرائم سيبرانية جديدة وأساليب إجرامية جديدة فحسب، بل أيضاً عن أساليب جديدة للتحقيق في الجريمة السيبرانية. فالتقدم الذي شهدته تكنولوجيا المعلومات والاتصالات قد زاد بدرجة هائلة من قدرات وكالات إنفاذ القانون. وفي المقابل، قد يستخدم الجناة بدورهم أدوات جديدة للحيلولة دون التعرف عليهم ولتعويق التحقيقات. ويركز هذا الفصل على التحديات المصادفة في مكافحة الجريمة السيبرانية.

1.3 الفرص

بمقدور وكالات إنفاذ القانون أن تستخدم الآن القوة المتزايدة للنظم الحاسوبية وبرمجيات الأدلة الجنائية المعقدة للإسراع بالتحقيقات ولأتمتة إجراءات البحث.[552]

وقد يتبين أن من الصعب أتمتة عمليات التحقيق. ففي حين أنه يمكن بسهولة البحث عن المحتوى غير القانوني اعتماداً على كلمة مفتاحية، فإن اكتشاف الصور غير القانونية قد يكون أمراً أشد صعوبة. ولا تكون النُهج المعتمدة على قيمة الفرم ناجحة إلا إذا كانت الصور قد سبق تصنيفها، وكانت قيمة الفرم قد خزنت في قاعدة بيانات، و لم تكن الصورة التي حللت قد تم تعديلها.[553]

الشكل 23

في المثل الوارد أعلاه تمكن خبراء الأدلة الجنائية الحاسوبية من تفكيك التعديلات التي أدخلت على الصورة وإعادة بناء وجه المشتبه فيه.

وتتسم برمجيات الأدلة الجنائية بالقدرة على البحث آلياً عن صور المواد الإباحية التي يستغل فيها الأطفال وذلك عن طريق مقارنة الملفات الموجودة في الأقراص الصلبة للمشتبه فيهم مع المعلومات عن الصور المعروفة. ومن ذلك مثلا، أن السلطات قد عثرت، في أواخر عام 2007، على عدد من الصور عن الاعتداء الجنسي على الأطفال. وقام الجاني، من أجل الحيلولة دون الكشف عن هويته باستخدام تقنية رقمية، لتعديل ذلك الجزء من الصور الذي يظهر فيه وجهه قبل نشر الصور على الإنترنت (انظر الشكل 23). وتمكن خبراء الأدلة الجنائية الحاسوبية من تفكيك التعديلات وإعادة بناء وجه المشتبه فيه.[554] وعلى الرغم من أن نجاح هذا التحقيق قد أظهر بوضوح إمكانات الأدلة الجنائية الحاسوبية، فإن هذه الحالة ليست دليلاً على تحقيق تقدم حاسم في التحقيق في المواد الإباحية التي يستغل فيها الأطفال. فلو كان الجاني قد غطى ببساطة وجهه بنقطة بيضاء لكان اكتشاف هويته أمراً مستحيلاً.

2.3 التحديات العامة

1.2.3 الاعتماد على تكنولوجيا المعلومات والاتصالات

تعتمد الاتصالات اليومية على تكنولوجيا المعلومات والاتصالات وعلى الخدمات المستندة إلى الإنترنت، بما في ذلك المكالمات بتقنية نقل الصوت باستخدام بروتوكول الإنترنت والاتصالات بالبريد الإلكتروني.[555] وتعد تكنولوجيا المعلومات والاتصالات مسؤولة الآن عن مراقبة وإدارة

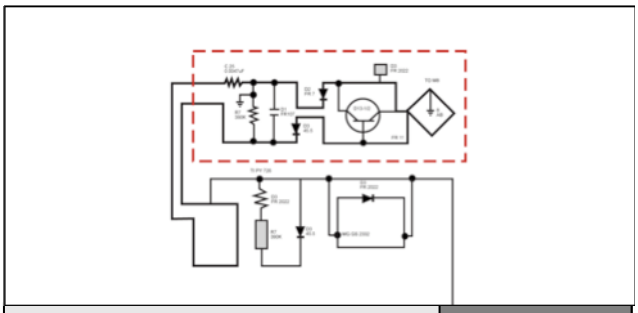
[552] See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf; *Reith*, An Examination of Digital 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

[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.

الوظائف في المباني،[556] والسيارات، وخدمات الطيران (انظر الشكل 24).[557] كما تعتمد إمدادات الطاقة والمياه ومرافق الاتصالات على تكنولوجيا المعلومات والاتصالات. ومن المرجح أن يستمر تغلغل هذه التكنولوجيا بقدر أكبر في الحياة اليومية.[558]



الشكل 24

تحل تكنولوجيا المعلومات بصورة متزايدة محل الوظائف اليدوية.

وتزايد الاعتماد على تكنولوجيا المعلومات والاتصال يجعل النظم والخدمات أكثر عرضة للهجمات الموجهة ضد البنى التحتية الحاسمة.[559] فحتى الانقطاعات القصيرة في الخدمات يمكن أن تسبب أضراراً مالية ضخمة لشركات التجارة الإلكترونية[560] – فالهجمات ليس بمقدورها أن تعطل الاتصالات المدنية وحدها؛ ذلك أن الاعتماد على تكنولوجيا المعلومات والاتصالات يشكل خطراً كبيراً على الاتصالات العسكرية أيضاً.[561]

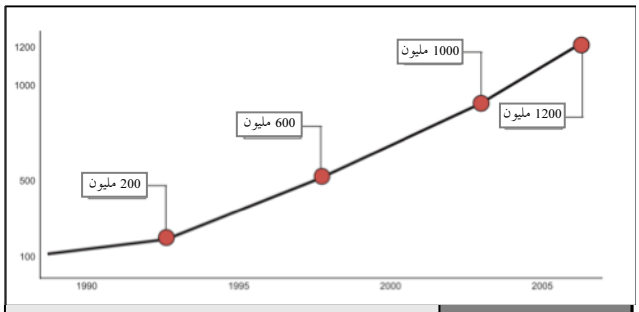
وتعاني البنى التحتية التقنية القائمة من عدد من أوجه الضعف، مثل شيوع ثقافة واحدة فيما يخص نظم التشغيل أو هيمنة نظم بعينها. إذ يستعمل كثير من المستخدمين الأفراد ومن الشركات المتوسطة والصغيرة نظام التشغيل ميكروسوفت،[562] ولذا فإن الجناة يستطيعون أن يصمموا هجمات ناجعة بالتركيز على هذا الهدف الواحد.[563]

واعتماد المجتمع على تكنولوجيا المعلومات والاتصالات لا يقتصر على البلدان الغربية[564] – فالبلدان النامية تواجه أيضاً تحديات فيما يتعلق بدرء الهجمات الموجهة ضد بناها التحتية وضد المستخدمين الموجودين بها.[565] واستحداث بنى تحتية تكنولوجية أزهد تكلفة مثل واي ماكس WiMAX[566] (قابلية التشغيل على الصعيد العالمي فيما يخص النفاذ بالموجات الصغرية) قد يُمكّن البلدان النامية من توفير خدمات الإنترنت لعدد أكبر من الناس. وتستطيع البلدان النامية أن تتجنب أخطاء بعض البلدان الأوروبية التي ركزت أساساً على تعظيم فرص النفاذ دون توظيف

[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.
[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".

استثمارات ذات شأن في مجال الحماية. وأوضح خبراء من الولايات المتحدة أن الهجمات الناجحة ضد موقع الويب الرسمي للمنظمات الحكومية في إستونيا[567] لم يكن ليحدث لولا عدم كفاية تدابير الحماية[568] وتملك البلدان النامية فرصة فريدة لإدماج التدابير الأمنية في وقت مبكر. وقد يقتضي هذا التوظيف استثمارات أولية أكبر، لكن دمج التدابير الأمنية في مرحلة لاحقة قد يكون أعلى تكلفة على المدى الطويل.[569]

ويجب وضع استراتيجيات لدرء هذه الهجمات ولاستحداث تدابير مضادة، تشمل استنباط وتعزيز السبل التقنية للحماية، بالإضافة إلى وضع قوانين مناسبة وكافية تمكن وكالات إنفاذ القانون من مكافحة الجريمة السيبرانية على نحو فعال.[570]



الشكل 25

يصل عدد مستخدمي الإنترنت في الوقت الحاضر إلى أكثر من مليار مستخدم.

2.2.3 عدد المستخدمين

تنمو شعبية الإنترنت وخدماتها نمواً سريعاً، إذ يزيد عدد مستخدميها على مليار نسمة على الصعيد العالمي (انظر الشكل 25).[571] وتركز شركات الحاسوب ومقدمو خدمة الإنترنت على البلدان النامية التي توجد بها أعظم الإمكانات للنمو الإضافي.[572] وفي عام 2005، تجاوز عدد مستخدمي الإنترنت في البلدان النامية عددهم في البلدان الصناعية،[573] في حين سيُمكّن استحداث الأجهزة الرخيصة وتنمية فرص النفاذ اللاسلكي مزيداً من الناس من النفاذ إلى الإنترنت.[574]

ومع تنامي عدد الأشخاص الموصولين بالإنترنت، يتزايد عدد الأهداف وعدد الجناة.[575] ومن الصعب تقدير عدد من يستخدمون الإنترنت في أنشطة إجرامية. فحتى لو لم تزد نسبة من يرتكبون الجرائم على 0,1 في المائة من المستخدمين، فإن العدد الكلي للجناة سيربو بذلك على المليون. وعلى الرغم من أن معدلات استخدام الإنترنت تعد أكثر انخفاضاً في البلدان النامية، فإن تعزيز الأمن السيبراني ليس أكثر سهولة فيها، لأن الجناة يستطيعون ارتكاب جرائمهم من أي مكان في العالم.[576]

ويسبب تزايد عدد مستخدمي الإنترنت صعوبات لوكالات إنفاذ القانون، لأنه من الصعب نسبياً أتمتة عمليات التحقيق. ففي حين يكون البحث عن المحتوى القانوني باستخدام كلمات مفتاحية من السهولة بمكان، فإن الكشف عن هوية أصحاب الصور غير القانونية قد يكون أمراً أشد صعوبة. فالنُهج المعتمدة على قيمة الفرم مثلاً لا تكون ناجحة إلا إذا كانت الصور قد سبق تصنيفها، وكانت قيمة الفرم قد خزنت في قاعدة بيانات، و لم تكن الصورة التي حللت قد تم تعديلها.[577]

---

[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.

[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.

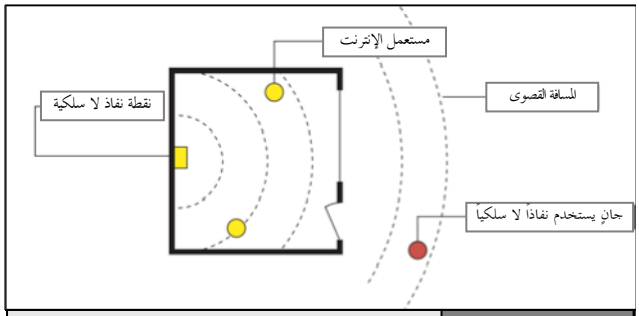
[576] The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: "Phishing Activity Trends", Report for the Month of April 2007, available 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.

3.2.3 توافر الأجهزة وفرص النفاذ

لا يلزم توافر إلا معدات أساسية لارتكاب الجرائم الحاسوبية، فهي لا تتطلب بوجه عام إلا العناصر التالية:

- المعدات؛
- البرمجيات؛
- النفاذ إلى الإنترنت.



الشكل 26

يشكل النفاذ إلى الإنترنت دون ترك أي آثار أولوية عالية لكثير من الجناة. ويوضح الرسم البياني كيف يستطيع أحد الجناة استخدام إشارة شبكة لا سلكية مفتوحة ليتمكن من النفاذ عن بعد. ومن المستحيل تقريباً كشف هذا الجاني.

وفيما يتعلق بالمعدات، تتنامى قوة الحواسيب باطراد.[578] وهناك عدد من المبادرات التي تُمكّن الناس في البلدان النامية من استخدام تكنولوجيا المعلومات والاتصالات على نطاق واسع.[579] ويستطيع المجرمون أن يرتكبوا جرائم حاسوبية خطيرة غير مستخدمين في ذلك سوى تكنولوجيا حاسوبية رخيصة أو مستعملة – فالمعرفة تهم في هذا الصدد أكثر كثيراً من تكنولوجيا المعدات الحاسوبية. ولا تؤثر حداثة التكنولوجيا الحاسوبية المتاحة تأثيراً يذكر على استخدام تلك المعدات لارتكاب الجرائم السيبرانية.

وبمقدور الأدوات البرمجاتية المتخصصة أن تجعل ارتكاب الجريمة السيبرانية أكثر سهولة. ويستطيع الجناة أن يقوموا بتنزيل أدوات برمجياتية[580] مصممة كي تُعين موضع المنافذ المفتوحة أو كي تخترق حماية كلمة السر.[581] ومن الصعب تقييد الانتشار الواسع لهذا النوع من الأجهزة بسبب تقنيات المحاكاة والتبادل بين النظراء.[582]

والعنصر الحيوي الأخير هو النفاذ إلى الإنترنت. وعلى الرغم من أن تكلفة النفاذ إلى الإنترنت[583] تعد أعلى في معظم البلدان النامية عن نظيرتها في البلدان الصناعية، فإن عدد مستخدمي الإنترنت في البلدان النامية يتزايد بسرعة.[584] ولن يجنح الجناة بوجه عام إلى الاشتراك في خدمة الإنترنت، كي يقللوا من احتمالات اكتشافهم، فهم يفضلون الخدمات التي يستطيعون استخدامها دون تسجيل (خاضع للتحقق). ومن السبل النموذجية للنفاذ إلى الشبكات ما يسمى بـ "التجول الحربي" ويقصد بهذا المصطلح التجول بحثاً عن شبكات لا سلكية يمكن النفاذ إليها.[585] وأكثر السبل انتشاراً لنفاذ الجناة إلى التوصيلات الشبكية هي:

- الوحدات المطرافية العمومية للإنترنت؛
- الشبكات (اللاسلكية المفتوحة) (انظر الشكل 26)؛[586]
- الشبكات التي أخضعتها القرصنة؛
- الخدمات المدفوعة الثمن مقدماً دون تطبيق متطلبات تسجيل.

---

[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.

[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.

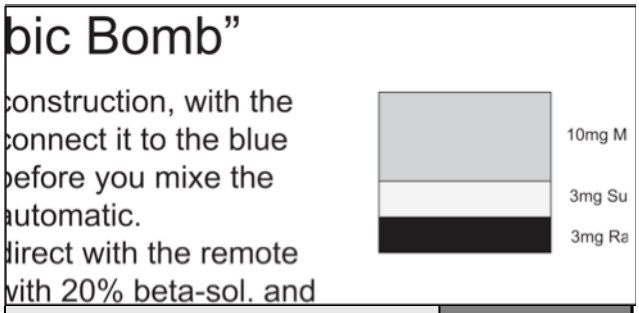
[582] In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime. See below: Chapter 6.1.13.

[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.



الشكل 27

تتوافر الإرشادات المتعلقة بكيفية صنع الأسلحة والمتفجرات على نطاق واسع على الإنترنت. ويُظهر الرسم البياني شرحاً لكيفية صنع قنبلة دون أن تستخدم في ذلك إلا مكونات متاحة في الصيدليات.

وتتخذ وكالات إنفاذ القانون إجراءات لتقييد النفاذ بلا ضوابط إلى خدمات الإنترنت تجنباً لاستخدام هذه الخدمات في ارتكاب الجرائم. ففي إيطاليا والصين، على سبيل المثال، يتطلب استخدام الوحدات المطرافية للإنترنت تعريف المستخدمين لأنفسهم.[587] غير أن هناك حججاً تعارض تطبيق متطلبات التعريف هذه.[588] فعلى الرغم من أن تقييد النفاذ يمكنه أن يمنع ارتكاب الجرائم وييسر التحقيقات التي تجريها وكالات إنفاذ القانون، فإن هذه التشريعات يمكن أن تعوق نمو مجتمع المعلومات وتنمية التجارة الإلكترونية.[589] وقد أشير إلى أن تقييد النفاذ إلى الإنترنت على هذا النحو يمكن أن يشكل انتهاكاً لحقوق الإنسان.[590] فالمحكمة الأوروبية مثلاً قد حكمت في عدد من القضايا المتعلقة بالبث بأن الحق في حرية التعبير ينطبق لا على محتوى المعلومات فحسب بل ينطبق أيضاً على وسيلة نقلها أو استقبالها. ففي القضية المرفوعة من أوترونيك (Autronic) ضد سويسرا،[591] رأت المحكمة أن الأخذ بالتفسير الواسع النطاق أمر ضروري، لأن أي تقييد يُفرض على الوسائل يتعارض مع الحق في تلقي المعلومات ونشرها. ولو طبقت هذه المبادئ على التقييدات المحتمل فرضها على النفاذ إلى الإنترنت لكانت هذه النهج التشريعية تنطوي على انتهاك لحقوق الإنسان.

4.2.3 توافر المعلومات

تضم الإنترنت الملايين من صفحات الويب[592] التي تحتوي على أحدث المعلومات. ويمكن أن يشارك في ذلك أي شخص ينشر أو يتعهد صفحة ويب. ومن الأمثلة على نجاح المواقع التي يُعدّها المستخدمون موسوعة ويكيبديا،[593] المتاحة على الخط والتي يستطيع أي إنسان أن ينشر فيها.[594]

كما يعتمد نجاح الإنترنت أيضاً على محركات بحث قوية تمكن المستخدمين من البحث في ثوان معدودة في الملايين من صفحات الويب. ويمكن استخدام هذه التكنولوجيا في أغراض مشروعة وأغراض إجرامية سواء بسواء. ويعني مصطلح "القرصنة على غوغل" أو مصطلح "المنقبون في غوغل" استخدام محركات البحث للإجابة عن استفسارات معينة ثم ترشيح نتائج البحث الكثيرة وصولاً إلى معلومات عن مسائل تتصل بأمن الحاسوب. ومن ذلك مثلاً، أن الجناة قد يستهدفون البحث عن كلمات سر غير مؤمنة لنظم الحماية.[595] وقد سلطت التقارير الضوء على احتمال استخدام محركات البحث في أغراض غير قانونية.[596] فالجاني الذي يخطط لشن الهجمات يمكنه أن يجد على الإنترنت معلومات تفصيلية تشرح له كيف يصنع قنبلة غير مستخدم في ذلك إلا المواد الكيميائية المتوافرة في المتاجر العادية (انظر الشكل 27).[597] وعلى الرغم من أن مثل هذه المعلومات كانت متاحة قبل استحداث الإنترنت، فإن النفاذ إليها كان أشد صعوبة. أما اليوم فقد أصبح باستطاعة أي مستخدم للإنترنت أن ينفذ إلى هذه المعلومات.

---

[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

[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.

كما يستطيع المجرمون استخدام محركات البحث لتحليل الأهداف.[598] وقد وُجد أثناء التحقيقات مع أعضاء جماعة إرهابية دليل تدريبي يثبت مدى فائدة الإنترنت في جمع المعلومات عن الأهداف المحتملة.[599] إذ يستطيع الجناة، باستخدام محركات البحث، أن يجمعوا المعلومات المتاحة علناً (مثل الرسوم الهندسية للمباني العمومية) التي تعينهم في استعدادهم. وتفيد التقارير أن المتمردين الذين هاجموا القوات البريطانية في أفغانستان قد استخدموا صوراً ساتلية مأخوذة من موقع غوغل إيرث (Google Earth).[600]

5.2.3 نقص آليات التحكم

تحتاج جميع شبكات الاتصالات الجماهيرية – من الشبكات الهاتفية المستخدمة في المكالمات الهاتفية الصوتية إلى الإنترنت – إلى إدارة مركزية ومعايير تقنية لضمان تشغيلها. وتبين المناقشات الدائرة حالياً بشأن حوكمة الإنترنت أن الإنترنت لا تختلف عن البنى التحتية للاتصالات الوطنية بل وحتى عبر الوطنية.[601] ويتعين أيضاً أن تخضع الإنترنت لحكم القانون والمشرعين، وقد بدأت وكالات إنفاذ القانون في وضع معايير تستلزم درجة معينة من التحكم المركزي.

وقد صممت الإنترنت في الأصل كشبكة عسكرية[602] تستند إلى معمار الشبكة اللامركزية، وهو معمار يسعى إلى الحفاظ على التشغيل الأساسي سليماً ومستمراً حتى لو تعرضت بعض مكونات الشبكة للهجوم. ونتيجة لذلك، تقاوم البنية التحتية للإنترنت محاولات التحكم الخارجي. فهي لم تصمم أصلاً لتيسير التحقيقات الجنائية أو لمنع هجوم آت من داخل الشبكة.

واليوم، تُستخدم الإنترنت بشكل متزايد في الخدمات المدنية. ومع الانتقال من الخدمات العسكرية إلى الخدمات المدنية، تغيرت طبيعة الطلب على أدوات التحكم. فلما كانت الشبكة تعتمد على بروتوكولات مصممة لأغراض عسكرية، فقد غابت عنها أدوات التحكم المركزي هذه، ومن الصعب إضافتها الآن بأثر رجعي دون إعادة تصميم الشبكة بدرجة كبيرة. وغياب أدوات التحكم يجعل التحقيقات في الجريمة السيبرانية أمراً بالغ الصعوبة.[603]

الشكل 28

يوضح الرسم البياني إمكانية الالتفاف على آليات التحكم المركزية التي يركبها مقدمو الخدمة. فإذا ركب مقدم الخدمة تكنولوجيا ترشيح معينة، سيتم حجب طلبات المستخدم. ويمكن التحايل على نهج الحجب هذا إذا استعمل المستخدم مخدمات اتصال مجهولة تُحفر الطلبات. وفي هذه الحالة مثلاً لا يستطيع مقدم الخدمة النفاذ إلى الطلبات المرسلة إلى مخدم اتصالات مجهول ولا يستطيع حجب مواقع الويب.

[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.

[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.

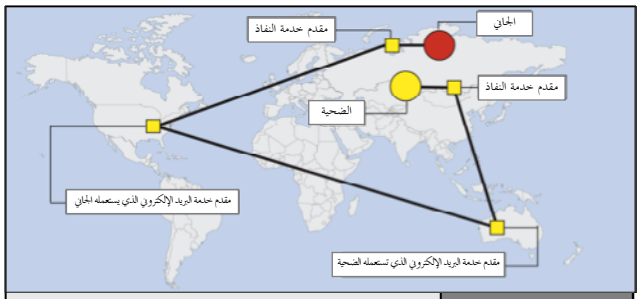
[600] See Telegraph.co.uk, news from January the 13th 2007.

[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".

ومن أمثلة المشكلات الناجمة عن غياب أدوات التحكم أن المستخدمين يستطيعون الالتفاف على تكنولوجيا الترشيح[604] باستخدام مخدمات اتصالات مجهولة مجفرة.[605] فإذا حجب مقدمو الخدمة مواقع ويب معينة ذات محتوى غير قانوني (مثل المواد الإباحية التي يستغل فيها الأطفال)، يصبح الزبائن عاجزين بوجه عام عن النفاذ إلى مواقع الويب تلك. ولكن حجب المحتوى غير القانوني يمكن تجنبه إذا استخدم الزبائن مخدم اتصالات مجهولاً يجفر الاتصالات بينه وبين المخدم المركزي. وفي هذه الحالة قد لا يستطيع مقدم الخدمة أن يحجب الطلبات، لأن الطلبات المرسلة على هيئة رسائل مجفرة لا يستطيع مقدمو خدمة النفاذ إلى الإنترنت فتحها (الشكل 28).



الشكل 29

يوضح الرسم البياني أنه حتى في حالة وجود الجناة والضحايا في نفس البلد، فإن إرسال رسالة إلكترونية ذات محتوى غير قانوني قد يمر بعدة بلدان مختلفة. وحتى إن لم تكن هذه هي الحالة، فإن عملية نقل البيانات قد توجه إلى خارج البلد قبل أن يعاد توجيهها إليه مرة أخرى.

6.2.3 الأبعاد الدولية

تطال كثير من عمليات نقل البيانات أكثر من بلد واحد.[606] وتستند البروتوكولات المستخدمة لنقل البيانات على الإنترنت إلى مسار أمثل، في حال سد الوصلات المباشرة بصفة مؤقتة.[607] وحتى عندما تكون عمليات النقل المحلي داخل بلد المصدر محدودة، فإن البيانات يمكن أن تغادر هذا البلد فتنقل عبر مسارات خارج أراضيه ثم يعاد توجيهها إليه نحو مقصدها النهائي فيه.[608] وعلاوة على ذلك، فإن كثيراً من خدمات الإنترنت تستند إلى خدمات من الخارج،[609] فقد يؤجر مقدم الخدمة المضيف مساحة على الويب في أحد البلدان بالاعتماد على معدات موجودة في بلد آخر.[610]

وإذا كان الجناة والأهداف موجودين في بلدان مختلفة، ستحتاج التحقيقات في الجريمة السيبرانية إلى تعاون وكالات إنفاذ القانون في

[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.

[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".

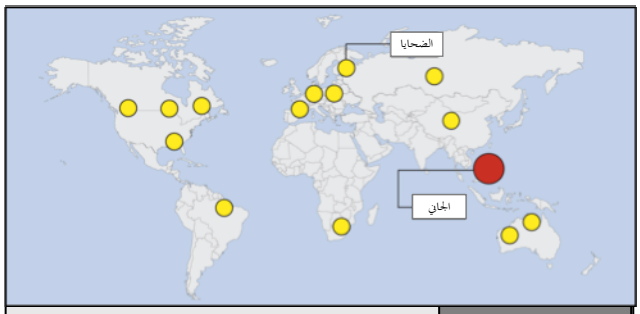
[608] See *Kahn/Lukasik*, "Fighting Cyber Crime and Terrorism: The Role of Technology," presentation at the Stanford Conference, December 1999, page 6 *et seqq.*; *Sofaer/Goodman*," Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime 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.

كل البلدان المتضررة.[611] ولا تسمح السيادة الوطنية بإجراء تحقيقات داخل أراضي بلدان مختلفة دون إذن من السلطات المحلية.[612] وتحتاج التحقيقات في الجريمة السيبرانية إلى دعم ومشاركة سلطات جميع البلدان المعنية.

ومن الصعب تأسيس التعاون في مجال الجريمة السيبرانية على المبادئ المتصلة بتبادل المساعدة القانونية التقليدية. فالمتطلبات الرسمية والوقت اللازم للتعاون مع وكالات إنفاذ القانون الأجنبية يعوقان التحقيقات في كثير من الأحيان.[613] إذ تنفذ التحقيقات في كثير من الأحيان ضمن أطر زمنية قصيرة للغاية.[614] والبيانات الحيوية لتعقب الجرائم كثيراً ما تحذف بعد فترة قصيرة فقط. ويمثل قصر هذه الفترة مشكلة للتحقيق، لأن نظام تبادل المساعدة القانونية التقليدية يستلزم في كثير من الأحيان وقتاً لتنظيمه.[615] كما يطرح مبدأ الإجرام المزدوج[616] صعوبات إذا كان الفعل المعني غير مُجرّم في أحد البلدان المشاركة في التحقيق.[617] وقد يدرج الجناة عن عمد بلداناً ثالثة في هجماتهم لجعل التحقيق أكثر صعوبة.[618]



الشكل 30

يستطيع الجناة النفاذ إلى الإنترنت لارتكاب الجرائم من أي مكان تقريباً في العالم. وتشمل المسائل التي يأخذها الجناة المحتملون في الاعتبار عندما يقررون المكان الذي يتخذونه مقراً لهم: حالة التشريعات المتعلقة بالجريمة السيبرانية، وفعالية وكالات إنفاذ القانون، وتوافر النفاذ إلى الإنترنت دون الإفصاح عن الهوية.

وقد يختار المجرمون عن عمد أهدافاً تقع خارج بلدهم، ويأتون بأفعالهم انطلاقاً من بلدان تعاني من عدم كفاية التشريعات المتعلقة بالجريمة السيبرانية (الشكل 29).[619] وتحقيق التواؤم بين القوانين المتعلقة بالجريمة السيبرانية والتعاون الدولي أمران من شأنهما أن يساعدا في هذا الصدد. وثمة نهجان يرميان إلى التعجيل بالتعاون الدولي في التحقيقات المتعلقة بالجريمة السيبرانية هما شبكة 7/24 التابعة للدول الثماني الكبرى،[620] والأحكام المتعلقة بالتعاون الدولي الواردة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[621]

7.2.3 استقلالية الموضع والوجود في مكان الجريمة

لا يحتاج المجرمون لأن يكونوا موجودين في نفس الموضع الذي يوجد فيه الهدف. ولما كان الموضع الذي يوجد فيه المجرم قد يكون مختلفاً اختلافاً كاملاً عن موقع الجريمة، فإن كثيراً من الجرائم السيبرانية تعد جرائم عبر وطنية. وتتطلب الجرائم السيبرانية الدولية كثيراً من الجهد والوقت. ويسعى مرتكبو هذه الجرائم إلى تجنب البلدان التي تُطبّق فيها تشريعات قوية لمكافحة الجريمة السيبرانية (الشكل 30).[622]

---

[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.

[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.

ويعد منع "الملاذات الآمنة" من التحديات الرئيسية المصادفة في مجال مكافحة الجريمة السيبرانية.[623] فما دامت هناك "ملاذات آمنة"، فإن الجناة سيستخدمونها لتعويق التحقيق. والبلدان النامية التي لم تنفذ بعد تشريعات تتعلق بالجريمة السيبرانية قد تصبح معرضة لها، لأن المجرمين قد يختارون أن يتخذوها مقراً لنشاطهم لتجنب الملاحقة. وقد يكون من الصعب وقف الجرائم الخطيرة التي تطال ضحايا منتشرين في شتى أنحاء العالم بسبب نقص التشريعات في البلد الذي يوجد به الجناة. وقد يؤدي هذا إلى الضغط على بلدان محددة لسن التشريعات اللازمة. ومن الأمثلة على ذلك الدودة الحاسوبية المسماة "لف بغ" (Love Bug) التي استنبطها شخص مشتبه فيه بالفلبين في عام 2000،[624] والتي أصابت ملايين الحواسيب في جميع أنحاء العالم.[625] وكان مما أعاق التحقيقات المحلية أن استحداث ونشر برمجيات خبيثة لم يكن مجرماً في ذلك الوقت بصورة كافية في الفلبين.[626] ومن الأمثلة الأخرى نيجيريا التي تعرضت لضغوط لاتخاذ إجراء ضد خدع الاحتيال المالي الموزعة عن طريق البريد الإلكتروني.

8.2.3 الأتمتة

من أكبر مزايا تكنولوجيا المعلومات والاتصالات قدرتها على أتمتة عمليات معينة. والأتمتة لها عدة نتائج كبرى هي:

- أنها تزيد من سرعة العمليات؛
- أنها تزيد من نطاق وتأثير العمليات؛
- أنها تحد من التدخل البشري.

وتقلل الأتمتة من الحاجة إلى أيدي عاملة كثيفة التكلفة، مما يتيح لمقدمي الخدمات أن يوفروها بأسعار أقل.[627] ويستطيع الجناة أن يستخدموا الأتمتة لتعظيم نطاق أنشطتهم – إذ يمكنهم إرسال ملايين عديدة من الرسائل الاقتحامية جملة واحدة[628] عن طريق الأتمتة[629] (انظر الشكل 31). وباتت هجمات القرصنة مؤتمتة الآن هي الأخرى،[630] إذ يصل عدد ما يشن من هجماتها كل يوم إلى 80 مليون هجوم[631] بسبب استخدام أدوات برمجياتية[632] تستطيع أن تهاجم آلاف النظم الحاسوبية في غضون ساعات.[633] ويستطيع الجناة، عن طريق أتمتة العمليات، جني أرباح طائلة بتصميم خدع احتيالية تستند إلى عدد كبير من الأفعال الإجرامية التي تُلحق بكل ضحية خسارة منخفضة نسبياً.[634] وكلما انخفضت الخسارة الواحدة زاد احتمال عدم إبلاغ الضحية عن الجريمة.

```
PETRO VOICE  HOLDING
Hot Stock in Momentum play for week

OTC: PHVC
This company is nasdaq bound

Petro Voice in on a roll earning Contrac

This is not a Fly by Night
Real market Cap, Real Earnings

Here are some the latest news on PHVC:
```

الشكل 31

من أمثلة عمليات الأتمتة نشر الرسائل الاقتحامية. إذ يمكن إرسال ملايين الرسائل الإلكترونية في غضون فترة قصيرة من الزمن.

[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.

[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.

وتؤثر أتمتة الهجمات على البلدان النامية بوجه خاص. فلما كانت موارد البلدان النامية محدودة، فإن الرسائل الاقتحامية قد تطرح عليها مشكلة أكثر خطراً مما تطرحها على البلدان الصناعية.[635] وتمثل الأعداد الكبيرة من الجرائم التي يمكن ارتكابها من خلال الأتمتة تحديات لوكالات إنفاذ القانون في كل أنحاء العالم، إذ يصبح عليها أن تكون مستعدة لوقوع مزيد من الضحايا ضمن حدود ولاياتها القضائية.

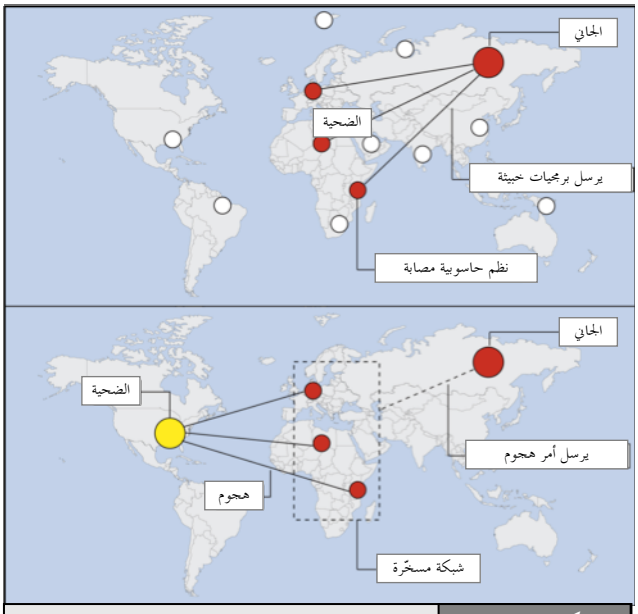
9.2.3 الموارد

تعد النظم الحاسوبية الحديثة المتداولة الآن في السوق نظماً قوية ويمكن استخدامها لتوسيع نطاق الأنشطة الإجرامية. لكن تزايد قوة[636] الحواسيب الخاصة بآحاد المستخدمين ليس هو وحده الذي يطرح المشكلات أمام التحقيقات. فتزايد قدرات الشبكات يُعدّ أمراً رئيسياً بدوره.

ومن الأمثلة على ذلك الهجمات التي شنت مؤخراً على المواقع الحكومية في إستونيا.[637] إذ يوحي تحليل الهجمات بأنها ارتكبت من قبل آلاف الحواسيب المنضوية ضمن "شبكة مُسخّرة"،[638] أو من قبل مجموعة من الحواسيب المُستغلة التي تُشغل برامج معينة عن طريق التحكم الخارجي.[639] وفي معظم الحالات، تصاب الحواسيب ببرمجيات خبيثة تُركّب فيها أدوات تسمح بسيطرة الجناة عليها (انظر الشكل 32). وتستخدم الشبكات المُسخّرة لجمع معلومات عن الأهداف أو للقيام بهجمات عالية المستوى.[640]

وخلال السنوات الأخيرة، أصبحت الشبكات المُسخّرة تشكل خطراً جسيماً على الأمن السيبراني.[641] ويتفاوت حجم الشبكة المُسخّرة، من عدة حواسيب إلى أكثر من مليون حاسوب.[642] ويفيد التحليل الراهن أن نسبة تصل إلى ربع كل الحواسيب الموصولة بالإنترنت يمكن أن تصيبها برمجيات تجعلها جزءاً من شبكة مُسخّرة.[643] ويمكن استخدام الشبكات المُسخّرة في أنشطة جنائية مختلفة تشمل:

- الهجمات التي تستهدف الحرمان من النفاذ إلى الخدمات؛[644]
- إرسال الرسائل الاقتحامية؛[645]
- القيام بهجمات القرصنة؛
- شبكات تقاسم الملفات.



الشكل 32

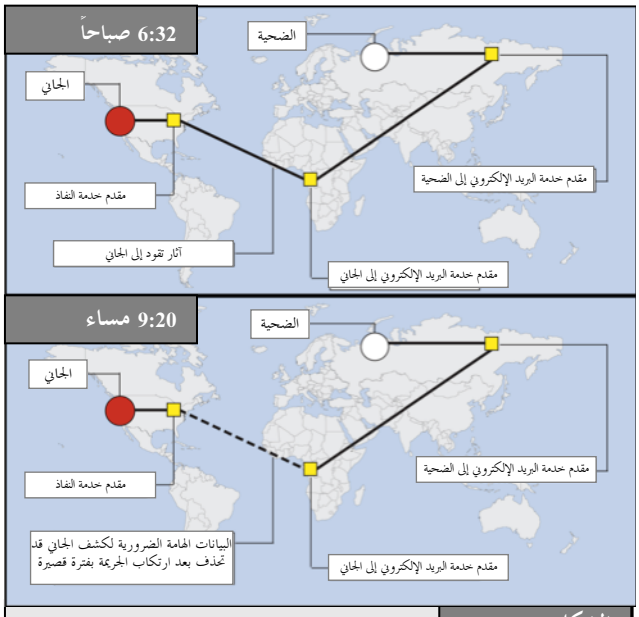
من أمثلة عمليات الأتمتة نشر الرسائل الاقتحامية. إذ يمكن إرسال ملايين من الرسائل الإلكترونية في غضون فترة زمنية قصيرة.

[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".
[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.

وتوفر الشبكات المُسخّرة عدداً من المزايا للجناة. فهي تزيد قدرتهم الحاسوبية وقدرتهم الشبكية على حد سواء. ويستطيع المجرمون، باستخدام آلاف النظم الحاسوبية، شن هجوم على نظم حاسوبية سيتعطل الاتصال بها دون أن تستخدم في ذلك سوى عدة حواسيب تقود الهجوم[646] كما تزيد الشبكات المُسخّرة من صعوبة تتبع الجاني الأصلي، لأن الآثار الأولية لن تقود إلا إلى عضو في الشبكات المُسخّرة. ومع تحكم المجرمين في نظم حاسوبية وشبكات أكثر قوة، تتعاظم الفجوة بين قدرات سلطات التحقيق والقدرات التي يتحكم فيها المجرمون.

10.2.3 سرعة عمليات تبادل البيانات

لا يستغرق نقل رسالة إلكترونية بين البلدان إلا ثوانٍ قليلة. وقصر هذه الفترة الزمنية هو أحد أسباب نجاح الإنترنت، لأن الرسائل الإلكترونية قد ألغت الزمن اللازم للنقل المادي للرسالة. غير أن هذا النقل السريع لا يترك لوكالات إنفاذ القانون وقتاً يذكر للتحقيق أو لجمع الأدلة. فالتحقيقات التقليدية تستغرق وقتاً أطول بكثير.[647]



الشكل 33

يوضح الرسم البياني أهمية الاستجابة الفورية لدى إجراء التحقيقات بشأن الجريمة السيبرانية. فالبيانات الهامة التي تُولّد أثناء عملية إرسال الرسالة الإلكترونية والتي يمكن أن تتيح كشف الجاني تحذف في كثير من الأحيان بعد إرسال الرسالة الإلكترونية بفترة قصيرة. وبغير النفاذ إلى هذه المعلومات يكون الكشف عن الجاني مستحيلاً في أحيان كثيرة.

ومن الأمثلة على ذلك تبادل المواد الإباحية التي يستغل فيها الأطفال. ففي الماضي كانت مواد الفيديو الإباحية تسلم إلى البائعين أو تنقل إليهم. وكان كل من التسليم والنقل يعطيان لوكالات إنفاذ القانون الفرصة للتحقيق. والفارق الرئيسي بين تبادل المواد الإباحية التي يستغل فيها الأطفال على الإنترنت وخارج الإنترنت هو عملية النقل. فعندما يستخدم الجناة الإنترنت يمكن تبادل الأفلام في ثوان قليلة.

كما تبين الرسائل الإلكترونية أهمية أدوات الاستجابة الفورية التي يمكن استخدامها في التو (انظر الشكل 33). فكي يتسنى للمحققين تتبع المشتبه فيهم وكشفهم، يتعين عليهم في كثير من الأحيان النفاذ إلى بيانات قد تحذف بعد النقل بفترة قصيرة.[648] ولذا، فإن قدرة سلطات التحقيق على الاستجابة خلال فترة قصيرة للغاية تعد في كثير من الأحيان حيوية لنجاح التحقيق. وبدون تشريعات وأدوات كافية تسمح للمحققين بالتصرف على الفور ومنع حذف البيانات، قد لا يتسنى مكافحة الجريمة السيبرانية بطريقة فعالة.[649]

وتعد "إجراءات التجميد السريع"[650] ومراكز شبكة 7/24[651] من أمثلة الأدوات التي يمكن أن تعجل بالتحقيقات. كما تستهدف التشريعات المتعلقة باحتجاز البيانات زيادة الوقت المتاح لوكالات إنفاذ القانون لإجراء التحقيقات. فلو تسنى حفظ البيانات اللازمة لتتبع الجناة لفترة معقولة، لأتيح لوكالات إنفاذ القانون فرصة أفضل للنجاح في كشف المشتبه فيهم.

11.2.3 سرعة التطور

تشهد الإنترنت تطوراً مستمراً. وكان ابتكار السطح البيني البياني الخاص بالمستخدم (WWW[652]) هو بداية ما طرأ عليها من توسع مثير، إذ كان استعمال المخدمات السابقة المعتمدة على الأوامر أقل يسراً وسهولة. وأتاح إنشاء الشبكة العالمية تطبيقات جديدة، مثلما أتاح كذلك ارتكاب جرائم جديدة[653] – وتكافح وكالات إنفاذ القانون في سبيل مواكبة التطورات. وتستجد بصفة مستمرة تطورات أخرى، ولا سيما من خلال:

- الألعاب المتاحة على الخط؛
- الاتصالات عن طريق نقل الصوت باستخدام بروتوكول الإنترنت.

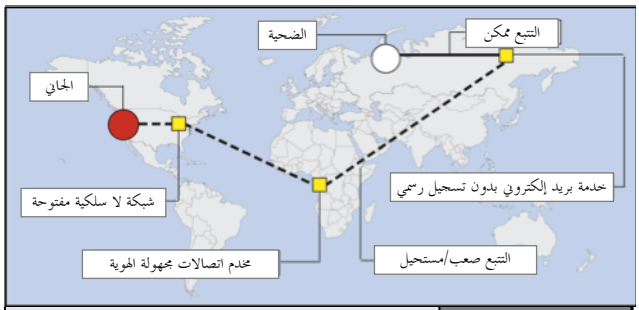
---

[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.
[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.

تتزايد باطراد شعبية الألعاب المتاحة على الخط، ولكن من غير الواضح ما إذا كانت وكالات إنفاذ القانون تستطيع أن تحقق في الجرائم المرتكبة في هذا العالم الافتراضي وأن تلاحقها قضائياً بنجاح.[654]

كما يطرح الانتقال من المكالمات الصوتية التقليدية إلى المهاتفة عبر الإنترنت تحديات جديدة على وكالات إنفاذ القانون. فالتقنيات والأساليب التي وضعتها وكالات إنفاذ القانون لاعتراض المكالمات الهاتفية التقليدية لا تنطبق بوجه عام على الاتصالات من خلال نقل الصوت باستخدام بروتوكول الإنترنت. فاعتراض المكالمات الصوتية التقليدية ينفذ عادة عن طريق مقدمي خدمة الاتصالات الهاتفية. وتطبيق نفس المبدأ على الاتصالات عن طريق نقل الصوت باستخدام بروتوكول الإنترنت، يعني أن تعمل وكالات إنفاذ القانون من خلال مقدمي خدمة الإنترنت ومن خلال مقدمي الخدمة الذين يتيحون خدمات الاتصالات عن طريق نقل الصوت باستخدام بروتوكول الإنترنت. ولكن إذا كانت الخدمة تستند إلى تكنولوجيا الاتصال بين النظراء، فإن مقدمي الخدمة قد لا يكونون بوجه عام قادرين على اعتراض الاتصالات، لأن البيانات ذات الصلة تنقل مباشرة بين الطرفين القائمين بالاتصال.[655] ولذا يستلزم الأمر تقنيات جديدة.[656]

كما تشهد المعدات الحاسوبية الجديدة وتكنولوجيا الشبكات تطوراً سريعاً. وتحول أحدث نظم الترفيه المنزلي أجهزة التلفزيون إلى نقاط للنفاذ إلى الإنترنت، في حين تقوم الهواتف المحمولة الأحدث عهداً بتخزين البيانات وبالاتصال بالإنترنت عن طريق الشبكات اللاسلكية.[657] وأدمجت في الساعات والأقلام ومدى الجيب أجهزة ذاكرة مزودة بناقل متسلسل عام (Universal Serial Bus) تزيد قدرتها على 1 GB. ويتعين على وكالات إنفاذ القانون أن تراعي هذه التطورات في عملها – ومن الجوهري توعية الضباط المشاركين في التحقيقات المتعلقة بالجريمة السيبرانية بصفة متواصلة حتى يكونوا ملمين بأحدث التكنولوجيات ويستطيعوا تحديد المعدات ذات الصلة والأجهزة المحددة التي يتعين مصادرتها.



الشكل 34

يوضح الرسم البياني كيف يستطيع الجناة إخفاء هويتهم عن طريق الجمع بين نُهج مختلفة. فاستخدام الشبكات اللاسلكية المفتوحة يجعل من المستحيل تقريبا كشف هوية الجناة. ويستطيع الجناة، عن طريق استخدام مخدمات اتصالات مجهولة الهوية وخدمات بريد إلكتروني لا تتحقق من معلومات التسجيل، أن يقللوا من احتمالات النجاح في كشف هويتهم.

ويتمثل تحد آخر في استخدام نقاط النفاذ اللاسلكية. ويشكل التوسع في النفاذ اللاسلكي إلى الإنترنت في البلدان النامية فرصة سانحة، كما يشكل تحدياً لوكالات إنفاذ القانون.[658] فإذا استخدم الجناة نقاط نفاذ لا سلكية لا تتطلب تسجيلاً، يصبح من الأصعب على وكالات إنفاذ القانون أن تتبع الجناة لأن التحقيقات لن تقود إلا إلى نقاط النفاذ هذه.

12.2.3 الاتصالات المجهولة الهوية

تجعل بعض خدمات الإنترنت من الصعب كشف الجناة.[659] وإمكانية إجراء اتصالات مجهولة الهوية هي إما نتيجة فرعية لخدمة ما، أو أنها تُوفر بنية تجنيب المستخدم بعض المعوقات. ومن أمثلة هذه الخدمات – التي يمكن حتى الجمع بينها (انظر الشكلين 34 و35) – ما يلي:

- الوحدات المطرافية العمومية للإنترنت (مثل الوحدات المطرافية في المطارات أو مقاهي الإنترنت)؛[660]
- الشبكات اللاسلكية؛[661]
- الخدمات المتنقلة المدفوعة الثمن مقدماً التي لا تتطلب تسجيلاً؛

[654] For more information see above: Chapter 2.5.5.
[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.

- قدرات التخزين لصفحات الاستقبال الموفرة دون تسجيل؛
- مخدمات الاتصالات المجهولة الهوية؛[662]
- المواقع المجهولة الهوية التي تعيد إرسال البريد الإلكتروني.[663]

ويستطيع الجناة إخفاء هوياتهم بأن يستخدموا مثلا عناوين زائفة للبريد الإلكتروني.[664] ويوفر كثير من مقدمي الخدمات عناوين بريد إلكترونية مجانية. وحتى إذا كان ينبغي إدخال معلومات شخصية، فإن هذه المعلومات قد لا يجري التحقق من صحتها مما يتيح للمستخدمين أن يسجلوا عناوين بريد إلكتروني دون كشف هويتهم. وعناوين البريد الإلكتروني المجهولة الهوية يمكن أن تكون مفيدة مثلا إذا ما أراد المستخدمون الانضمام إلى جماعات النقاش السياسي دون كشف هويتهم. وقد تؤدي الاتصالات المجهولة الهوية إلى شيوع سلوك الاجتماعي، ولكنها يمكن أن تسمح أيضاً للمستخدمين بالتصرف بحرية أكبر.[665]

والاهتمام بمسألة أن المستخدمين يتركون وراءهم آثاراً تدل عليهم يوضح ضرورة وضع أدوات لوقاية المستخدمين من الأنشطة التي تستهدف تصنيفهم على أساس خصائصهم.[666] ولذا تؤيد دول ومنظمات شتى مبدأ الاستخدام المجهول الهوية لخدمات البريد الإلكتروني عن طريق الإنترنت، ومن ذلك مثلا أن هذا المبدأ يرد في توجيه الاتحاد الأوروبي المتعلق بالخصوصية والاتصالات الإلكترونية.[667] كما يمكن العثور على نموذج للنهج القانوني الرامي إلى حماية خصوصية المستخدمين في المادة 37 من لائحة الاتحاد الأوروبي المتعلقة بحماية البيانات.[668] غير أن بعض البلدان تتصدى لتحديات الاتصالات المجهولة الهوية بتطبيق قيود قانونية[669] – ومن هذه البلدان إيطاليا التي تلزم مقدمي خدمة النفاذ العمومي إلى الإنترنت بالتعرف على هوية المستخدمين، قبل أن يبدأوا في استخدام الخدمة.[670]

الشكل 35

يوضح الرسم البياني كيفية إخفاء المعلومات في صورة. وتدرج برمجيات التجفير المعلومات عن طريق تغيير معلومات اللون الخاصة ببعض البكسيلات. وإذا كانت الصورة كبيرة بدرجة كافية، تعذر التعرف على التغييرات دون النفاذ إلى الصورة الأصلية وكذلك إلى الصورة المعدلة. ويستطيع الجناة، باستخدام هذه التكنولوجيا، إخفاء قيامهم بتبادل معلومات إضافية.

وتستهدف هذه التدابير مساعدة وكالات إنفاذ القانون على كشف هويات المشتبه فيهم، غير أنه من السهل تجنبها – فقد يستخدم المجرمون شبكات لا سلكية خاصة غير محمية أو شرائح SIM من بلدان لا تستوجب التسجيل. ومن غير الواضح ما إذا كان تقييد الاتصالات المجهولة والنفاذ المجهول الهوية إلى الإنترنت ينبغي أن يؤدي دوراً أكثر أهمية في استراتيجيات الأمن السيبراني.[671]

---

[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.

[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.

13.2.3 تكنولوجيا التجفير

من العوامل الأخرى التي يمكن أن تعقد التحقيق في الجريمة السيبرانية تكنولوجيا التجفير،[672] التي تحمي المعلومات من أن ينفذ إليها أشخاص غير مأذون لهم والتي تعد حلاً تقنياً رئيسياً في مكافحة الجريمة السيبرانية.[673] وعلى غرار عدم الإفصاح عن الهوية، لا يعد التجفير أمراً جديداً،[674] لكن التكنولوجيا الحاسوبية قد بدلت هذا الميدان تبديلاً. فقد بات من الممكن الآن تجفير بيانات الحاسوب بمجرد النقر على الفأرة، مما يجعل من الصعب على وكالات إنفاذ القانون أن تخترق التجفير وتنفذ إلى البيانات.[675] ومن غير المعروف على وجه اليقين أي مدى يستخدم الجناة بالفعل تكنولوجيا التجفير لإخفاء أنشطتهم – فقد أفادت التقارير، على سبيل المثال، أن الإرهابيين يستخدمون تكنولوجيا التجفير.[676] وتفيد دراسة استقصائية عن المواد الإباحية التي يستغل فيها الأطفال أن 6% فقط من حائزي هذه المواد الذين تم القبض عليهم يستخدمون تكنولوجيا التجفير،[677] لكن الخبراء يسلطون الضوء على التهديد المتمثل في تزايد استخدام تكنولوجيا التجفير في قضايا الجريمة السيبرانية.[678]

وتتوافر أدوات تسمح باختراق التجفير.[679] كما تتوافر منتجات برمجياتية متنوعة تمكن المستخدمين من حماية الملفات ضد النفاذ غير المأذون به.[680] واختراق التجفير أمر ممكن، غير أنه صعب وبطئ – وإذا أتيح للمحققين النفاذ إلى البرمجيات المستخدمة في تجفير الملفات فربما كان باستطاعتهم فك التجفير.[681] وربما كان باستطاعتهم، كحل بديل، اختراق التجفير من خلال هجوم "بالقوة الغاشمة" على سبيل المثال.[682]

وتبعاً لتقنيات التجفير وحجم المفتاح قد يستغرق الأمر عقوداً لاختراق التجفير.[683] ومن ذلك مثلا أنه إذا استخدم أحد الجناة برمجيات تجفير لها قدرة تجفير تبلغ 20 بت، فإن حجم مساحة المفتاح تناهز المليون. وباستخدام حاسوب حالي يعالج مليون عملية في الثانية يمكن اختراق هذا التجفير في أقل من ثانية واحدة. ولكن إذا استخدم الجناة قدرة تجفير تبلغ 40 بت، فإن المدة اللازمة لاختراق التجفير قد تصل إلى أسبوعين.[684] وباستخدام قدرة تجفير تبلغ 56 بت، سيحتاج الحاسوب الواحد إلى 852 2 سنة لاختراق التجفير. أما إذا استخدم الجناة قدرة تجفير تبلغ 128 بت، فإن مليار نظام حاسوبي تعمل حصراً على فك التجفير قد تأخذ آلافاً من مليارات السنين لاختراقه.[685] ويلاحظ أن أحدث نسخة من برمجيات التجفير الشائعة بي جي بي (PGP) تسمح بتجفير قدرته 1024 بت.

---

[672] Regarding the impact on computer forensic and criminal investigations, 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.

[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.

وتتجاوز قدرة برمجيات التجفير الحالية مجرد تجفير آحاد الملفات. فأحدث نسخة من نظم تشغيل ميكروسوفت، على سبيل المثال، تسمح بتجفير قرص صلب برمته.[686] ويستطيع المستخدمون أن يركبوا بسهولة برمجيات التجفير. وعلى الرغم من أن بعض خبراء الأدلة الجنائية الحاسوبية يعتقدون أن هذه الوظيفة لا تهددهم،[687] فإن تيسّر هذه التكنولوجيا على نطاق واسع لأي مستخدم يمكن أن تؤدي إلى التوسع في استخدام التجفير. وتتوافر أيضاً أدوات لتجفير الاتصالات – ومن ذلك مثلا أن رسائل البريد الإلكتروني والمكالمات الهاتفية[688] يمكن إرسالها عن طريق نقل الصوت باستخدام بروتوكول الإنترنت.[689] ويستطيع الجناة، عن طريق تكنولوجيا مجفرة لنقل الصورة باستخدام بروتوكول الإنترنت، حماية المحادثات الصوتية من محاولات اعتراضها.[690]

كما يمكن الجمع بين التقنيات المختلفة. فيستطيع الجناة، باستخدام أدوات برمجياتية معينة، تجفير الرسائل وتبادلها في لوح أو صور – وتسمى هذه التكنولوجيا الكتابة الخفية (steganography).[691] ومن الصعب على سلطات التحقيق أن تميز بين التبادل البريء لصور العطل والإجازات، وتبادل صور تحتوي على رسائل خفية مجفرة.[692]

ويمثل توافر تكنولوجيات التجفير واستخدامها من قبل المجرمين تحدياً لوكالات إنفاذ القانون. وتناقش في الوقت الحاضر نهج قانونية متنوعة لمعالجة المشكلة،[693] تشمل: احتمال فرض التزامات على مطوري البرمجيات تقضي بتركيب باب خلفي لوكالات إنفاذ القانون؛ وفرض حدود على قوة المفاتيح؛ وفرض التزامات بالإفصاح عن المفاتيح، في حالة التحقيقات الجنائية.[694] لكن تكنولوجيا التجفير لا يستخدمها المجرمون وحدهم – فثمة سبل شتى تستخدم فيها هذه التكنولوجيا لأغراض قانونية. وبغير النفاذ الكافي إلى تكنولوجيا التجفير قد يكون من الصعب حماية المعلومات الحساسة. وبالنظر إلى تنامي عدد الهجمات،[695] تعد الحماية الذاتية عنصراً هاماً في الأمن السيبراني.

14.2.3 الملخص

يطرح التحقيق في الجريمة السيبرانية وملاحقتها قضائياً عدداً من التحديات على وكالات إنفاذ القانون. ومما يتسم بأهمية حيوية ليس فقط توعية الأشخاص المشاركين في مكافحة الجريمة السيبرانية، بل أيضاً وضع تشريعات وافية وفعالة. وقد استعرض هذا الفرع التحديات الرئيسية أمام تعزيز الأمن السيبراني والمجالات التي قد يتبين فيها أن الأدوات الحالية غير كافية والتي قد يلزم فيها تطبيق أدوات خاصة.

---

[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.

[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 التحديات القانونية

1.3.3 التحديات المصادفة لدى إعداد القوانين الجنائية الوطنية

التشريع السليم هو الأساس الذي يستند إليه لدى التحقيق في الجريمة السيبرانية وملاحقتها قضائياً. ولكن يجب على المشرعين أن يستجيبوا بصفة مستمرة لتطورات الإنترنت وأن يرصدوا فعالية الأحكام القائمة، وخاصة بالنظر إلى سرعة التطورات في مجال تكنولوجيا الشبكات.

ومن المنظور التاريخي، أدى تطبيق الخدمات الحاسوبية أو تكنولوجيات الإنترنت إلى ظهور أشكال جديدة من الجريمة بعد استحداث هذه التكنولوجيا بفترة وجيزة. ومن الأمثلة على ذلك أن أول نفاذ غير مأذون به إلى الشبكات الحاسوبية قد وقع بعد إنشاء تلك الشبكات في سبعينات القرن الماضي بفترة قصيرة.[696] وبالمثل، ظهرت أول جرائم تتعلق بالبرمجيات بعد استحداث الحواسيب الشخصية في ثمانينات القرن الماضي بفترة قصيرة، حيث استخدمت هذه النظم آنذاك لاستنساخ المنتجات البرمجياتية.

وتحيين القانون الجنائي الوطني من أجل الملاحقة القضائية للأشكال الجديدة من الجريمة السيبرانية التي ترتكب على الخط أمر يستغرق وقتاً – وبعض البلدان لم تفرغ بعد من عمليات التكيف هذه. ويتعين استعراض وتحديث الأفعال التي يجرمها القانون الجنائي الوطني – ومن ذلك مثلا أن المعلومات الرقمية يجب أن تتمتع بمركز مكافئ لمركز التوقيعات والمستخرجات التقليدية.[697] فبغير إدراج الأفعال المتعلقة بالجريمة السيبرانية، لن يتسنى ملاحقة الانتهاكات قضائياً.

ويتمثل التحدي الرئيسي الذي يواجه النظم القانونية الجنائية الوطنية في التأخر الزمني الذي يفصل بين الاعتراف بصور إساءة الاستخدام المحتملة للتكنولوجيات الجديدة، والتعديلات التي يلزم إدخالها على القانون الجنائي الوطني. ويظل هذا التحدي هاماً وآنياً أكثر من أي وقت مضى، بحكم السرعة التي يطرد بها تجدد الشبكات. وتسعى بلدان كثيرة بصورة جادة إلى اللحاق بعمليات التكيف التشريعي.[698] وتنطوي عملية التكيف، بوجه عام، على ثلاث خطوات:

يجب أن يبدأ تكيف القانون الوطني بالاعتراف بإساءة استخدام التكنولوجيا الجديدة. ويتعين أن تضم وكالات إنفاذ القانون الوطنية إدارات محددة مؤهلة للتحقيق في الجرائم السيبرانية المحتملة. وقد تحسنت الحالة بفضل إنشاء أفرقة الاستجابة للطوارئ الحاسوبية، [699] وأفرقة الاستجابة للحوادث الحاسوبية، وأفرقة الاستجابة لحوادث الأمن الحاسوبي، ومرافق بحثية أخرى.

وتتمثل الخطوة الثانية في تحديد الثغرات الموجودة في القانون الجنائي. ومن الضروري لإرساء أسس تشريعية فعالة مقارنة حالة الأحكام القانونية الجنائية للقانون الوطني مع المتطلبات الناشئة عن الأنواع الجديدة للأفعال الإجرامية. وقد تكون القوانين القائمة قادرة، في حالات كثيرة، على تغطية الأنواع الجديدة للجرائم الراهنة (ومن ذلك مثلا أن القوانين التي تتناول التزييف يمكن أن تنطبق بنفس القدر من السهولة على الوثائق الإلكترونية). فتقتصر الحاجة إلى التعديلات التشريعية عندئذ على الجرائم التي أغفلها القانون الوطني أو لم يغطها بصورة كافية.

وتتمثل الخطوة الثالثة في إعداد التشريع الجديد. وقد يكون من الصعب على السلطات الوطنية، كما تبين الخبرة، أن تقوم بعملية إعداد تشريعات الجريمة السيبرانية دون تعاون دولي، بسبب التطور السريع لتكنولوجيات الشبكات ولتعقد بناها.[700] وقد يؤدي صوغ تشريعات الجريمة السيبرانية بصورة مستقلة إلى ازدواجية كبيرة وإلى تبديد الموارد، ومن الضروري أيضاً رصد تطور المعايير والاستراتيجيات الدولية. وبغير تحقيق التواؤم الدولي بين الأحكام القانونية الجنائية الوطنية، فإن مكافحة الجريمة السيبرانية عبر الوطنية ستواجه صعوبات خطيرة بسبب عدم اتساق التشريعات الوطنية أو عدم توافقها. ومن ثم، تتسم المحاولات الرامية إلى تحقيق التواؤم بين القوانين الجنائية الوطنية المختلفة بأهمية متزايدة.[701] وتستطيع القوانين الوطنية أن تنتفع بدرجة كبيرة من خبرة البلدان ومن المشورة القانونية الدولية المتخصصة.

2.3.3 الجرائم الجديدة

لا تعد الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات، في معظم الحالات، جرائم جديدة، بل تُعدّ خدعاً احتيالية طُورت كي تمارس على الخط. والاحتيال هو أحد الأمثلة على ذلك – إذ لا يوجد فارق كبير بين شخص يبعث رسالة بنية تضليل شخص آخر وبين شخص يبعث رسالة إلكترونية مضمراً النية نفسها.[702] فإذا كان الاحتيال يشكل بالفعل عملاً إجرامياً، فقد لا يستلزم الأمر تعديل القانون الوطني لملاحقة هذه الأعمال قضائياً.

ولكن الحالة تختلف إذا لم تكن القوانين القائمة تتناول الأفعال المرتكبة. وكانت بعض البلدان تطبق في الماضي أحكاماً مناسبة تتعلق بالاحتيال العادي، ولكنها لا تستطيع أن تتصدى للجرائم التي تطال نظاماً حاسوبياً لا كائناً بشرياً. ويتعين على هذه البلدان أن تعتمد قوانين جديدة تجرم الاحتيال الحاسوبي، بالإضافة إلى الاحتيال العادي. وهناك أمثلة متنوعة تبين أن التوسع في تفسير الأحكام القائمة لا يمكن أن يغني عن اعتماد قوانين جديدة.

---

[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.

[701] See below: Chapter 5.

[702] See above: Chapter 2.7.1.

وإلى جانب التكيف اللازم للتصدي للخدع الاحتيالية المعروفة جيداً، يجب على المشرعين أن يحللوا بصفة مستمرة الأنواع الجديدة والناشئة من الجريمة السيبرانية لضمان تجريمها تجريماً فعلياً. ومن الأمثلة على جريمة سيبرانية لم تجرم بعد في البلدان كلها السرقة والاحتيال في الألعاب الحاسوبية والألعاب التي تنظم على الخط.[703] وقد ركزت المناقشات بشأن الألعاب المنظمة على الخط، لفترة طويلة، على قضايا حماية الشباب (مثل اشتراط التحقق من بلوغ السن) والمحتوى غير القانوني (مثل النفاذ إلى مواد إباحية يستغل فيها الأطفال في اللعبة المسماة "حياة ثانية" (Second Life) المتاحة على الخط).[704] وتُكتشف بصفة مستمرة أنشطة إجرامية جديدة – فقد "تسرق" عملات افتراضية في ألعاب على الخط ويتم تداولها في مواقع المزادات.[705] وتنطوي بعض العملات الافتراضية على قيمة منسوبة إلى العملات الحقيقية (استناداً إلى سعر صرف معلوم)، مما يعطي الجريمة بعداً "حقيقياً".[706] وقد لا يتسنى ملاحقة هذه الجرائم قضائياً في البلدان جميعاً. وعملاً على الحيلولة دون توفير ملاذات آمنة للجناة، من الحيوي رصد التطورات المستجدة على النطاق العالمي.

3.3.3 تزايد استخدام تكنولوجيا المعلومات والاتصالات والحاجة إلى أدوات جديدة للتحقيقات

يستخدم الجناة تكنولوجيا المعلومات والاتصالات بطرق شتى في التحضير لجرائمهم وتنفيذها.[707] وتحتاج وكالات إنفاذ القانون إلى أدوات كافية للتحقيق في الأعمال الإجرامية المحتملة. وبعض هذه الأدوات (مثل احتجاز البيانات[708]) يمكن أن يتعارض مع حقوق مستخدمي الإنترنت الأبرياء.[709] وإذا كانت خطورة الفعل الإجرامي لا تتناسب مع شدة التدخل، فإن استخدام أدوات التحقيق قد لا تكون مبررة أو قانونية. وهذا ما جعل بعض الأدوات التي يمكنها أن تحسن التحقيق لم تطبق بعد في عدد من البلدان.

وتطبيق أدوات التحقيق هو دوماً نتيجة للمفاضلة بين توفير المزايا لوكالات إنفاذ القانون، من جهة، والتدخل في حقوق مستخدمي الإنترنت الأبرياء، من جهة أخرى. ومن الجوهري رصد الأنشطة الإجرامية الجارية من أجل التقييم ما إذا كان التهديد المحدق يسوغ التغيير المطلوب. وكان الأخذ بأدوات جديدة يُبرر، في كثير من الأحيان، على أساس "مكافحة الإرهاب"، ولكن هذا يعتبر دافعاً بعيد المدى، لا مبرراً محدداً في حد ذاته.

4.3.3 وضع إجراءات للأدلة الرقمية

أدى انخفاض تكاليف تخزين الوثائق الرقمية على وجه الخصوص،[710] بالقياس إلى تكاليف تخزين الوثائق المادية، إلى تزايد مطرد في عدد الوثائق الرقمية.[711] وكان للرقمنة والاستخدام الناشئ لتكنولوجيا المعلومات والاتصالات تأثير كبير على الإجراءات المتعلقة بجمع الأدلة واستخدامها في المحكمة.[712] ونتيجة لهذا التطور جرى الأخذ بالدليل الرقمي كمصدر جديد من مصادر الأدلة.[713] وهو يُعرّف بأنه أي بيانات تخزن أو تنقل باستخدام تكنولوجيا حاسوبية تؤيد النظرية الخاصة بكيفية حدوث جريمة ما.[714] وتقترن مناولة الدليل الرقمي بتحديات فريدة وتتطلب إجراءات خاصة.[715] ومن أصعب الجوانب في هذا الصدد الحفاظ على تكاملية الدليل الرقمي.[716] فالبيانات الرقمية بالغة الهشاشة ويمكن بسهولة حذفها[717]

---

[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.

[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.

أو تعديلها. ويصدق هذا بوجه خاص على المعلومات المخزنة في ذاكرة النظام RAM التي تحذف آلياً عند إقفال النظام[718] ولذا تتطلب تقنيات حفظ خاصة.[719] وبالإضافة إلى ذلك، قد يكون للتطورات الجديدة تأثير كبير على التعامل مع الدليل الرقمي. ومن الأمثلة على ذلك معالجة المعلومات عن طريق الإنترنت (التي تعرف باسم معالجة المعلومات في السحاب cloud-computing). وكان المحققون يستطيعون في الماضي التركيز على مقار المشتبه فيهم لدى بحثهم عن البيانات الحاسوبية. أما اليوم فعليهم أن يأخذوا في اعتبارهم أن المعلومات الرقمية قد تخزن في الخارج ويمكن النفاذ إليها عن بعد، عند الضرورة.[720]

ويؤدي الدليل الرقمي دوراً هاماً في شتى مراحل التحقيقات بشأن الجريمة السيبرانية ومن الممكن بوجه عام التمييز بين أربع مراحل هي:[721]

- تعيين الأدلة ذات الصلة؛[722]
- جمع الأدلة وصونها؛[723]
- تحليل التكنولوجيا الحاسوبية والأدلة الرقمية؛
- تقديم الأدلة في المحكمة.

وبالإضافة إلى الإجراءات المتعلقة بعرض الأدلة الجنائية في المحكمة، فإن طرق جمع الأدلة الرقمية تتطلب عناية خاصة. فجمع الأدلة الرقمية يدخل في باب جمع الأدلة الجنائية الحاسوبية. ويقصد بمصطلح "الأدلة الجنائية الحاسوبية" التحليل المنهجي لمعدات تكنولوجيات المعلومات بغرض البحث عن أدلة رقمية.[724] ويسلط التزايد المطرد لحجم البيانات المخزنة في صورة رقمية الضوء على التحديات اللوجستية التي تنطوي عليها هذه التحقيقات.[725] ولذا، فإن النهج الرامية إلى أتمتة إجراءات الأدلة الجنائية، باللجوء مثلا إلى استخدام عمليات البحث عن صور المواد الإباحية التي يستغل فيها الأطفال بالاعتماد على قيمة الفرم[726] أو باستخدام الكلمات المفتاحية،[727] تؤدي دوراً هاماً بالإضافة إلى التحقيقات اليدوية.[728]

وتبعاً لمتطلبات التحقيق المعني، يمكن أن تشمل الأدلة الجنائية الحاسوبية، على سبيل المثال، ما يلي:

- تحليل المعدات والبرمجيات التي يستخدمها المشتبه فيه؛[729]
- دعم المحققين في تعيين الأدلة ذات الصلة؛[730]
- استرجاع الملفات المحذوفة؛[731]
- تجفير الملفات؛[732]
- الكشف عن هوية مستخدمي الإنترنت عن طريق تحليل بيانات الحركة.[733]

---

[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

[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.*

4 استراتيجيات مكافحة الجريمة السيبرانية

يعني تزايد عدد الجرائم السيبرانية التي تم الوقوف عليها وعدد الأدوات التقنية المستخدمة في أتمتة الجرائم السيبرانية (التي تشمل نظم تقاسم الملفات المجهولة الهوية[734] والمنتجات البرمجياتية المصممة لاستحداث فيروسات حاسوبية[735]) أن مكافحة الجريمة السيبرانية قد أصبحت عنصراً جوهرياً في أنشطة وكالات إنفاذ القانون على الصعيد العالمي. وتشكل الجريمة السيبرانية تحدياً لوكالات إنفاذ القانون في البلدان المتقدمة والبلدان النامية على حد سواء. ولما كانت تكنولوجيا المعلومات والاتصالات تتطور بسرعة بالغة، وخاصة في البلدان النامية، فمن الجوهري وضع وتنفيذ استراتيجية فعالة لمكافحة الجريمة السيبرانية بوصفها جزءاً من الاستراتيجية الوطنية للأمن السيبراني.

1.4 تشريعات الجريمة السيبرانية بوصفها جزءاً لا يتجزأ من استراتيجية الأمن السيبراني

يؤدي الأمن السيبراني،[736] كما سلفت الإشارة، دوراً هاماً في التطور الجاري لتكنولوجيا المعلومات ولخدمات الإنترنت.[737] وأصبح تعزيز أمان الإنترنت (وحماية مستخدمي الإنترنت) أمراً جوهرياً لاستحداث الخدمات الجديدة ولوضع السياسات الحكومية.[738] وبمقدور استراتيجيات. الأمن السيبراني – ومن أمثلتها إنشاء نظم للحماية التقنية وتوعية المستخدمين للحيلولة دون وقوعهم في براثن الجريمة السيبرانية – أن تساعد على الحد من خطر الجريمة السيبرانية.[739]

وينبغي أن تكون استراتيجية مكافحة الجريمة السيبرانية عنصراً جوهرياً في استراتيجية الأمن السيبراني. والبرنامج العالمي للأمن السيبراني،[740] بوصفه إطاراً عالمياً للحوار وللتعاون الدولي من أجل تنسيق الاستجابة الدولية للتحديات المتنامية التي تواجه الأمن السيبراني، وتعزيز الثقة والأمن في مجتمع المعلومات، يرتكز على الأعمال والمبادرات والشراكات القائمة بهدف اقتراح استراتيجيات عالمية للتصدي لهذه التحديات المترابطة. وتتسم كل التدابير المطلوبة الواردة في الركائز الخمس للبرنامج العالمي للأمن السيبراني بالأهمية لأي استراتيجية للأمن السيبراني. وعلاوة على ذلك، فإن القدرة على المكافحة الفعالة للجريمة السيبرانية تقتضي اتخاذ تدابير في إطار الركائز الخمس جميعاً.[741]

2.4 تنفيذ الاستراتيجيات القائمة

يتمثل أحد البدائل في إمكان أن تطبق في البلدان النامية استراتيجيات مكافحة الجريمة السيبرانية التي وضعت في البلدان الصناعية، مما يحقق ميزتي تقليل تكلفة استحداث تلك الاستراتيجيات واختصار الوقت اللازم لذلك. ومن شأن تنفيذ الاستراتيجيات القائمة أن يمكن البلدان النامية من الانتفاع من الآراء والخبرات القائمة.

---

[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.

ومع ذلك، فإن تنفيذ استراتيجية قائمة لمكافحة الجريمة السيبرانية يطرح عدداً من الصعوبات. فعلى الرغم من أن كلاً من البلدان النامية والمتقدمة يواجه تحديات مماثلة، فإن الحلول المثلى التي قد يتعين اعتمادها تعتمد على موارد كل بلد وقدراته. وقد تكون البلدان الصناعية قادرة على تعزيز الأمن السيبراني بطرق مختلفة وأكثر مرونة – وذلك مثلا بالتركيز على مسائل الحماية التقنية التي تعد كثيفة التكلفة بقدر أكبر.

وثمة عدة مسائل أخرى يتعين أن تراعيها البلدان النامية التي تعتمد الاستراتيجيات القائمة لمكافحة الجريمة السيبرانية، من بينها:

- مدى توافق النظم القانونية المختلفة؛
- حالة المبادرات المساندة (مثل توعية المجتمع)؛
- نطاق تدابير الحماية الذاتية المطبقة؛
- نطاق الدعم المقدم من القطاع الخاص (وذلك مثلا من خلال الشراكات بين القطاعين العام والخاص).

3.4 الاختلافات الإقليمية

بالنظر إلى الطبيعة الدولية للجريمة السيبرانية، يعد تحقيق التواؤم بين القوانين والتقنيات الوطنية أمراً حيوياً في مكافحة الجريمة السيبرانية. غير أن تحقيق التواؤم يجب أن يراعي الطلب والقدرات الموجودين على الصعيد الإقليمي. ومما يؤكد أهمية الجوانب الإقليمية في تنفيذ استراتيجيات مكافحة الجريمة السيبرانية أن كثيراً من المعايير القانونية والتقنية قد تم الاتفاق عليها بين البلدان الصناعية وأنها لا تتضمن جوانب متنوعة لها أهميتها للبلدان النامية.[742] ولذا يتعين إدراج العوامل والاختلافات الإقليمية لدى تنفيذ هذه الاستراتيجيات في أماكن أخرى.

4.4 أهمية مسائل الجريمة السيبرانية في إطار ركائز الأمن السيبراني

يتوخى البرنامج العالمي للأمن السيبراني سبعة أهداف استراتيجية ترتكز على خمسة مجالات عمل هي: (1) التدابير القانونية؛ (2) التدابير التقنية والإجرائية؛ (3) البنى التنظيمية؛ (4) بناء القدرات؛ (5) التعاون الدولي. وتؤدي المسائل المتعلقة بالجريمة السيبرانية، كما سلفت الإشارة، دوراً هاماً في الركائز الخمس جميعاً للبرنامج العالمي للأمن السيبراني. ومن بين مجالات العمل هذه، يركز مجال العمل المتعلق بالتدابير القانونية على كيفية معالجة التحديات التشريعية التي تطرحها الأنشطة الإجرامية المرتكبة على شبكات تكنولوجيا المعلومات والاتصالات بطريقة متوافقة دولياً.

1.4.4 التدابير القانونية

لعل التدابير القانونية هي، من بين الركائز الخمس، أهم التدابير لاستراتيجية مكافحة الجريمة السيبرانية. وهذا يتطلب أولاً أن تجرم كل أحكام القانون الجنائي الموضوعية اللازمة أعمالاً مثل الاحتيال الحاسوبي، والنفاذ غير القانوني، والتدخل في البيانات، وانتهاك حقوق المؤلف، واستغلال الأطفال في المواد الإباحية.[743] ووجود أحكام في القانون الجنائي تنطبق على أعمال مماثلة ترتكب خارج شبكة لا يعني أنها يمكن أن تنطبق على الأعمال المرتكبة على الإنترنت أيضاً.[744] ولذا، فإن من الحيوي إجراء تحليل شامل للقوانين الوطنية الراهنة للوقوف على أي ثغرات محتملة.[745] وإلى جانب الأحكام المضمونة للقانون الجنائي،[746] تحتاج وكالات إنفاذ القانون إلى الأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية.[747] وتطرح هذه التحقيقات نفسها عدداً من التحديات.[748] فالجناة يستطيعون أن يقوموا بعملهم من أي مكان تقريباً في العالم وأن يتخذوا تدابير

[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.*
[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.

لإخفاء هويتهم.[749] وقد تكون الأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية مختلفة إلى حد كبير عن تلك المستخدمة للتحقيق في الجرائم العادية.[750] وبالنظر إلى البعد الدولي[751] للجريمة السيبرانية، فمن الضروري، بالإضافة إلى ذلك، تطوير الإطار القانوني الوطني ليكون قادراً على التعاون مع وكالات إنفاذ القانون في الخارج.[752]

2.4.4 التدابير التقنية والإجرائية

تنطوي التحقيقات المتعلقة بالجريمة السيبرانية، في كثير من الأحيان، على مكون تقني قوي.[753] وبالإضافة إلى ذلك، يقتضي الشرط المتمثل في الحفاظ على تكاملية الأدلة أثناء التحقيق اتباع إجراءات دقيقة. ولذا يعد تطوير القدرات اللازمة ووضع الإجراءات الضرورية شرطين لا غنى عنهما لمكافحة الجريمة السيبرانية.

وتتمثل مسألة أخرى في تنمية نظم الحماية التقنية. فمن الأصعب مهاجمة النظم الحاسوبية المتمتعة بحماية جيدة. وتتمثل خطوة أولى هامة في تحسين الحماية التقنية عن طريق تنفيذ المعايير الأمنية السليمة. ومن ذلك مثلاً أن التغييرات التي أدخلت على النظام المصرفي المتاح على الخط (مثلا بالانتقال من نظام تان TAN[754] إلى النظام آيتان ITAN[755]) قد أزال كثيراً من المخاطر الناشئة عن هجمات "التصيد الاحتيالي" الراهنة، مما يبين الأهمية الحيوية للحلول التقنية.[756] وينبغي أن تتضمن تدابير الحماية التقنية كل عناصر البنية التحتية التقنية – أي البنية التحتية الأساسية للشبكة، بالإضافة إلى الحواسيب العديدة الموصولة بشكل فردي على النطاق العالمي. وثمة مجموعتان من الأهداف المحتملة يمكن تحديدهما لأغراض حماية مستخدمي الإنترنت والشركات التجارية وهما:

- المستخدمون النهائيون والشركات التجارية (النهج المباشر)؛
- مقدمو الخدمات وشركات البرمجيات.

وقد يكون من الأسهل، من الناحية اللوجستية، التركيز على حماية البنى التحتية الأساسية (مثل الشبكات الرئيسية، والطرق، والخدمات الأساسية)، بدلا من إدراج ملايين المستخدمين في استراتيجية مكافحة الجريمة السيبرانية. ويمكن توفير الحماية للمستخدمين بطريقة غير مباشرة، وذلك عن طريق تأمين الخدمات التي يستخدمها المستهلكون – مثل الصرافة على الخط. وبمقدور هذا النهج غير المباشر لحماية مستخدمي الإنترنت أن يحد من عدد الأشخاص والمؤسسات الذين يتعين إدراجهم في الخطوات الرامية إلى تعزيز الحماية التقنية.

وعلى الرغم من أن وضع حد لعدد الناس الذين يتعين إدراجهم في الحماية التقنية قد يبدو أمراً مستصوباً، فإن مستخدمي الحواسيب والإنترنت يكونون في كثير من الأحيان هم الحلقة الأضعف والهدف الرئيسي للمجرمين. فمن الأسهل في أحيان كثيرة مهاجمة حواسيب الأفراد للحصول على معلومات حساسة، بدلا من مهاجمة نظم حاسوبية جيدة الحماية تخص مؤسسة مالية. وعلى الرغم من هذه المشكلات اللوجستية، فإن حماية البنية التحتية للمستخدمين النهائيين تعد أمراً حيوياً للحماية التقنية للشبكة بأسرها.

---

[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.

[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.

ويؤدي مقدمو خدمة الإنترنت وبائعو المنتجات (مثل شركات البرمجيات) دوراً حيوياً في دعم استراتيجيات مكافحة الجريمة السيبرانية. فهم يستطيعون، بحكم صلتهم المباشرة بالزبائن، أن يعملوا كضامن للأنشطة الأمنية (مثل توزيع أدوات الحماية وتوفير معلومات عن أحدث ما استجد من خدع احتيالية).[757]

3.4.4 الهياكل التنظيمية

تقتضي المكافحة الفعالة للجريمة السيبرانية هياكل تنظيمية عالية التطور. فبغير إنشاء هياكل سليمة تتفادى التداخل وتستند إلى اختصاصات واضحة سيتعذر إجراء تحقيقات معقدة تتطلب مساعدة من خبراء قانونيين وتقنيين مختلفين.

4.4.4 بناء الثقة وتوعية المستخدمين

الجريمة السيبرانية ظاهرة عالمية. وكي يتسنى التحقيق على نحو فعال في الجرائم، يتعين تحقيق التواؤم بين القوانين وتنمية وسائل التعاون الدولي. وعملاً على ضمان اتباع معايير عالمية في البلدان المتقدمة. والبلدان النامية على حد سواء يستلزم الأمر بناء القدرات.[758]

وبالإضافة إلى بناء القدرات يقتضي الأمر توعية المستخدمين.[759] وبعض الجرائم السيبرانية – وخاصة الجرائم المتعلقة بالاحتيال، مثل "التصيد الاحتيالي" و"الإيهام" – لا تعتمد بوجه عام على نقص الحماية التقنية، بل تعتمد بالأحرى على نقص وعي الضحايا.[760] وهناك برمجيات متنوعة يمكن أن تكشف آلياً عن مواقع الويب الاحتيالية،[761] لكن هذه البرمجيات لا تستطيع حتى الآن الكشف عن جميع مواقع الويب المشبوهة. واستراتيجية حماية المستخدمين بالاعتماد على البرمجيات وحدها تكون ذات قدرة محدودة على توفير الحماية لهم.[762] وعلى الرغم من أن تدابير الحماية التقنية يتواصل تطورها وأن البرمجيات المتاحة تحدث بصفة منتظمة، فإن هذه البرمجيات لا تستطيع أن تحل بعد محل النهج الأخرى.

ولذا، فإن توعية المستخدمين هي من أهم العناصر في منع الجريمة السيبرانية.[763] فإذا كان المستخدمون مثلا يدركون أن مؤسساتهم المالية لن تتصل بهم أبداً عن طريق البريد الإلكتروني لتطلب منهم كلمات السر أو بيانات حساباتهم المصرفية، فإنهم لن يقعوا ضحايا التصيد الاحتيالي أو الهجمات الاحتيالية التي تستهدف كشف هويتهم. وتقلل توعية مستخدمي الإنترنت من عدد الأهداف المحتملة. ويمكن توعية المستخدمين عن طريق:

- الحملات العامة؛
- الدروس المنظمة في المدارس، والمكتبات، ومراكز تكنولوجيا المعلومات، والجامعات؛
- الشراكات بين القطاعين العام والخاص.

ومن المتطلبات الهامة لأي استراتيجية توعية وإعلام فعالة الإبلاغ الصريح عن أحدث تهديدات الجريمة السيبرانية. وترفض بعض الدول و/أو الشركات الخاصة التنويه بأن مواطنيها وزبائنها، على هذا التوالي، يتأثرون بتهديدات الجريمة السيبرانية، تجنباً لفقدان ثقتهم بخدمات الاتصالات المتاحة على الخط. وقد

---

[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-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect." Regarding user education approaches in the fight against Phishing, see: "Anti-Phishing Best Practices for ISPs and Mailbox Providers", 2006, page 6, available at: 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.

[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-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

طلب مكتب التحقيقات الفيدرالي بالولايات المتحدة صراحة من الشركات أن تتغلب على نفورها من الدعاية السلبية وأن تبلغ عن الجريمة السيبرانية.[764] وعملاً على تحديد مستويات التهديد، وإعلام المستخدمين، من الحيوي تحسين جمع المعلومات ذات الصلة ونشرها.[765]

5.4.4 التعاون الدولي

تمر عمليات نقل البيانات على الإنترنت، في عدد كبير من الحالات، بأكثر من بلد واحد.[766] ويعزى هذا إلى تصميم الشبكة وكذلك إلى البروتوكولات التي تضمن إمكانية إجراء عمليات النقل بنجاح، حتى إذا كانت الخطوط المباشرة مسدودة بصفة مؤقتة.[767] وبالإضافة إلى ذلك، فإن عدداً كبيراً من خدمات الإنترنت (ومنها مثلا خدمات الاستضافة) توفره شركات تقع مقارها في الخارج.[768]

وفي الحالات التي لا يكون الجاني موجوداً فيها بنفس بلد الضحية، يقتضي التحقيق التعاون بين وكالات إنفاذ القانون في جميع البلدان المتضررة.[769] ومن الصعب إجراء تحقيقات دولية وعبر وطنية دون موافقة السلطات المختصة في البلدان المعنية إعمالاً لمبدأ السيادة الوطنية. فهذا المبدأ لا يسمح بوجه عام لأحد البلدان بأن يجري تحقيقات في أراضي بلد آخر دون إذن من السلطات المحلية.[770] ولذا يتعين إجراء التحقيقات بمساندة سلطات جميع البلدان المعنية. وفيما يتعلق بأنه لا تتاح في معظم الحالات إلا مهلة زمنية قصيرة للغاية يمكن إجراء التحقيقات الناجحة إبانها، يلاحظ أن تطبيق نظم تبادل المساعدة القانونية التقليدية ينطوي على صعوبات واضحة عندما يتصل الأمر بالتحقيقات في الجريمة السيبرانية. ويعزى هذا إلى أن تبادل المساعدة القانونية يقتضي بوجه عام إجراءات رسمية تستغرق وقتاً طويلاً. ولذا، فإن تحسين التعاون الدولي بقدر أكبر يؤدي دوراً هاماً وحاسماً في وضع وتنفيذ استراتيجيات الأمن السيبراني واستراتيجيات مكافحة الجريمة السيبرانية.

---

[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.

[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.

5 لمحة عامة عن النهج التشريعية الدولية

يقدم الفصل التالي لمحة عامة عن النهج التشريعية الدولية[771] وعلاقتها بالنهج الوطنية.

1.5 *النهج الدولية*

يعكف عدد من المنظمات الدولية بصفة مستمرة على تحليل أحدث ما يستجد من تطورات في مجال الجريمة السيبرانية، وقد أنشأت هذه المنظمات أفرقة عمل لوضع استراتيجيات لمكافحة تلك الجرائم.

1.1.5 مجموعة الثمانية[772]

في عام 1997، أنشأت مجموعة الثمانية "اللجنة الفرعية[773] المعنية بجرائم التكنولوجيا الراقية" التي تهتم بمكافحة الجريمة السيبرانية.[774] واعتمد وزراء العدل والداخلية في مجموعة الثمانية، إبان اجتماعهم في مدينة واشنطن بالولايات المتحدة، عشرة مبادئ وخطة عمل مؤلفة من عشر نقاط لمكافحة جرائم التكنولوجيا الراقية.[775] وأيد رؤساء مجموعة الثمانية في وقت لاحق هذه المبادئ التي جاء فيه أنه:

- يجب ألا تكون هناك ملاذات آمنة لمن يسيئون استخدام تكنولوجيا المعلومات.
- يجب أن تنسق التحقيقات والملاحقات القضائية المتعلقة بجرائم التكنولوجيا الراقية الدولية بين جميع الدول المعنية، بصرف النظر عن مكان وقوع الضرر.
- يجب تدريب موظفي إنفاذ القانون وتجهيزهم للتعامل مع جرائم التكنولوجيا الراقية.

وفي عام 1999، حددت مجموعة الثمانية خططها المتعلقة بمكافحة جرائم التكنولوجيا الراقية في مؤتمر وزاري معني بمكافحة الجرائم المنظمة عبر الوطنية، عقد في موسكو بالاتحاد الروسي.[776] وأعربت بلدان مجموعة الثمانية عن شواغلها إزاء بعض الجرائم (مثل استغلال الأطفال في المواد الإباحية)، وكذلك إزاء إمكانية تتبع المعاملات والنفاذ عبر الحدود إلى البيانات المخزنة. وتضمن بيانها عدداً من المبادئ تتعلق بمكافحة الجريمة السيبرانية، وهي مبادئ ترد اليوم في عدد من الاستراتيجيات الدولية.[777]

---

[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.

[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.

وكان من الإنجازات العملية التي أسفر عنها عمل فريق الخبراء إنشاء شبكة دولية لجهات الاتصال تُدعى شبكة 7/24، التي تستلزم من البلدان المشاركة أن تعين جهات اتصال للتحقيقات عبر الوطنية يمكن النفاذ إليها 24 ساعة في اليوم و7 أيام في الأسبوع.[778]

وتناولت مجموعة الثمانية، في المؤتمر الذي عقدته في باريس بفرنسا في عام 2000، موضوع الجريمة السيبرانية ودعت إلى منع الملاذات الرقمية غير الخاضعة للقانون. وكانت مجموعة الثمانية، قد ربطت منذ ذلك الوقت، محاولاتها الرامية إلى إيجاد حلول دولية باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[779] وفي عام 2001، ناقشت مجموعة الثمانية الأدوات الإجرائية لمكافحة الجريمة السيبرانية في ورشة عمل عقدت في طوكيو،[780] ركزت على ما إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات أو ما إذا كان حفظ البيانات يعد حلاً بديلاً.[781]

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes - including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions - so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.

[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-Pierre 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."

وفي عام 2004، أصدر وزراء العدل والداخلية في مجموعة الثمانية بياناً تناولوا فيه ضرورة إنشاء قدرات عالمية في مجال مكافحة الاستخدامات الإجرامية للإنترنت.[782] وأحاطت مجموعة الثمانية، مرة أخرى، علماً باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[783]

وناقش وزراء العدل والداخلية في مجموعة الثمانية، إبان اجتماعهم في موسكو عام 2006، القضايا المتعلقة بمكافحة الجريمة السيبرانية وقضايا الفضاء السيبراني، وخاصة ضرورة تحسين فعالية التدابير المضادة.[784] وفي أعقاب اجتماع وزراء العدل والداخلية في مجموعة الثمانية، عُقدت في موسكو قمة مجموعة الثمانية حيث كانت قضية الإرهاب السيبراني[785] محل نقاش.[786]

وأثناء الاجتماع الذي عقده وزراء العدل والداخلية في مجموعة الثمانية في ميونيخ بألمانيا في عام 2007 خضعت قضية استخدام الإرهابيين للإنترنت لمزيد من النقاش، واتفق المشاركون على تجريم إساءة استخدام الجماعات الإرهابية للإنترنت.[787] ولم يشر هذا الاتفاق إلى أفعال محددة ينبغي أن تجرمها الدول.

2.1.5 الأمم المتحدة[788]

في المؤتمر الثامن المعني بمنع الجريمة ومعاملة المجرمين (الذي عقد في هافانا بكوبا في الفترة من 27 أغسطس إلى 7 سبتمبر 1990)، اعتمدت الجمعية العامة للأمم المتحدة قراراً يتناول التشريعات المتعلقة بالجرائم الحاسوبية.[789] وفي عام 1994 نشرت الأمم المتحدة، بناء على قرار الجمعية العامة 45/121 (1990)، دليلاً بشأن منع ومكافحة الجريمة المتعلقة بالحاسوب.[790]

وفي عام 2000، اعتمدت الجمعية العامة قراراً بشأن إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية يتضمن عدداً من أوجه التماثل مع خطة العمل المؤلفة من عشر نقاط التي اعتمدتها مجموعة الثمانية في عام 1997.[791] وحددت الجمعية العامة، في قرارها، عدداً من التدابير الرامية إلى منع إساءة استعمال التكنولوجيا من بينها أنه:

ينبغي للدول أن تكفل عدم توفير قوانينها وممارساتها ملاذاً آمناً للذين يسيئون استعمال تكنولوجيات المعلومات لأغراض إجرامية؛

---

[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.”
[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: *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.

ينبغي أن تنسق جميع الدول المعنية التعاون في مجال إنفاذ القانون لدى التحقيق والمقاضاة في القضايا الدولية المتعلقة بإساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية؛

ينبغي تدريب العاملين في مجال إنفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

وفي عام 2002، اعتمدت الجمعية العامة قراراً آخر بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.[792] ويشير القرار إلى النهج الدولية القائمة في مكافحة الجريمة السيبرانية ويسلط الضوء على حلول متنوعة.

وإذ تلاحظ العمل الذي تضطلع به المنظمات الدولية والإقليمية في مجال مكافحة الجريمة المتصلة بالتكنولوجيا الرفيعة، بما في ذلك ما يضطلع به مجلس أوروبا من أعمال لوضع اتفاقية بشأن جرائم الفضاء الحاسوبي، فضلاً عن عمل هذه المنظمات فيما يتعلق بتشجيع الحوار بين الحكومات والقطاع الخاص بشأن السلامة والثقة في الفضاء الحاسوبي،

1 تدعو الدول الأعضاء لدى وضع قوانين وسياسات وممارسات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، إلى أن تأخذ في اعتبارها، حسب الاقتضاء، أعمال وإنجازات لجنة منع الجريمة والعدالة الجنائية، والمنظمات الدولية والإقليمية الأخرى؛

2 تحيط علماً بأهمية التدابير الواردة في قرارها 63/55، وتدعو الدول الأعضاء من جديد إلى مراعاتها عند بذل جهودها الرامية إلى مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية؛

3 تقرر إرجاء النظر في هذا الموضوع ريثما تنجز الأعمال المتوخاة في خطة عمل لجنة منع الجريمة والعدالة الجنائية بشأن مكافحة الجريمة المتصلة بالتكنولوجيات الرفيعة والتطبيقات الحاسوبية.

وفي عام 2004، أنشأت الأمم المتحدة فريقاً عاملاً يعنى بالرسائل الاقتحامية والجريمة السيبرانية والموضوعات الأخرى المتعلقة بالإنترنت، مما أكد اهتمام الأمم المتحدة بالمشاركة في المناقشات الدولية الجارية بشأن تهديدات الجريمة السيبرانية.[793]

وفي مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، الذي عُقد في بانكوك بتايلاند في عام 2005، اعتمد إعلان يسلط الضوء على ضرورة تحقيق التواؤم لدى مكافحة الجريمة السيبرانية.[794] وكان مما جاء فيه القضايا التالية:

نؤكد مجدداً الأهمية الأساسية التي يكتسيها تنفيذ الصكوك الراهنة والمضي في وضع تدابير وطنية وتطوير التعاون الدولي في المسائل الجنائية، ومن ذلك النظر في تعزيز وزيادة التدابير، وخصوصاً تدابير مكافحة الجريمة السيبرانية وغسل الأموال والاتجار بالممتلكات الثقافية، وكذلك التدابير المتعلقة بتسليم المطلوبين للعدالة وتبادل المساعدة القانونية ومصادرة عائدات الجريمة واستردادها وإرجاعها.

نلاحظ أن تكنولوجيا المعلومات وسرعة تطور نظم الاتصالات والشبكات الحاسوبية الجديدة، في فترة العولمة الراهنة، صاحبتهما إساءة استعمال لتلك التكنولوجيات لأغراض إجرامية. ومن ثم، نرحب بالجهود المبذولة لتعزيز واستكمال التعاون القائم لمنع جرائم التكنولوجيا الراقية والجرائم الحاسوبية والتحقيق فيها وملاحقتها قضائياً، بوسائل منها إقامة شراكات مع القطاع الخاص. ونسلم بأهمية إسهام الأمم المتحدة في المحافل الإقليمية وسائر المحافل الدولية في مجال مكافحة الجريمة السيبرانية وندعو لجنة منع الجريمة والعدالة الجنائية إلى أن تدرس إمكانية توفير مزيد من المساعدة في ذلك المجال تحت رعاية الأمم المتحدة وفي إطار شراكة مع منظمات أخرى لها مجال تركيز مشابه، واضعة في اعتبارها تلك التجربة.

وبالإضافة إلى ذلك، يتناول عدد من مقررات منظومة الأمم المتحدة وقراراتها وتوصياتها قضايا تتعلق بالجريمة السيبرانية. ومن أهمها ما يلي:

- اعتمدت لجنة منع الجريمة والعدالة الجنائية،[795] التابعة لمكتب الأمم المتحدة للمخدرات والجريمة، قراراً بشأن المنع الفعال للجريمة واستجابات العدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال.[796]
- وفي عام 2004، اعتمد المجلس الاقتصادي والاجتماعي للأمم المتحدة[797] قراراً بشأن التعاون الدولي على منع جرائم الاحتيال وسوء استعمال الهوية وتزييفها لأغراض إجرامية وما يتصل بها من جرائم والتحري عن تلك الجرائم وملاحقة مرتكبيها ومعاقبتهم.[798]

---

[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.

[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

وفي عام 2007، اعتمد المجلس قراراً بشأن التعاون الدولي على منع جرائم الاحتيال الاقتصادي والجرائم ذات الصلة بالهوية والتحري عنها وملاحقة مرتكبيها قضائياً ومعاقبتهم.[799] ولا يتناول كلا القرارين صراحة التحديات المتعلقة بجرائم الإنترنت[800] ولكنهما ينطبقان على هذه الجرائم أيضاً.

- وفي عام 2004، اعتمد المجلس قراراً بشأن بيع المخدرات المشروعة عن طريق الإنترنت الذي تناول صراحة ظاهرة تتعلق بجريمة حاسوبية.[801]

3.1.5 الاتحاد الدولي للاتصالات[802]

يؤدي الاتحاد الدولي للاتصالات، بوصفه وكالة متخصصة داخل منظومة الأمم المتحدة، دوراً ريادياً بشأن تقييس وتنمية الاتصالات وكذلك بشأن قضايا الأمن السيبراني. واضطلع الاتحاد الدولي للاتصالات، من بين أنشطته الأخرى، بدور الوكالة الرائدة للقمة العالمية لمجتمع المعلومات التي عقدت على مرحلتين في جنيف بسويسرا (2003) وفي تونس العاصمة بتونس (2005). وتبادلت الحكومات وراسمو السياسات والخبراء من جميع أنحاء العالم الأفكار والخبرات بشأن خير سبيل لمعالجة القضايا الناشئة المرتبطة بظهور مجتمع معلومات عالمي، بما في ذلك إعداد معايير وقوانين متوافقة. وترد نواتج القمة في إعلان مبادئ جنيف وخطة عمل جنيف؛ والتزام تونس، وخطة عمل تونس لمجتمع المعلومات.

وتسلط خطة عمل جنيف الضوء على أهمية التدابير الرامية إلى مكافحة الجريمة السيبرانية:[803]

جيم5 – بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات

12 – الثقة والأمن ركيزتان من الركائز الأساسية لمجتمع المعلومات

ب) ينبغي أن تعمل الحكومات، بالتعاون مع القطاع الخاص، على منع واكتشاف ومواجهة الجرائم السيبرانية وإساءة استعمال تكنولوجيا المعلومات والاتصالات عن طريق: وضع خطوط توجيهية تأخذ في الاعتبار الجهود الجارية في هذه المجالات؛ والنظر في تطبيق تشريعات تسمح بالتحقيق الفعال في حالات إساءة الاستعمال ومقاضاتها؛ وتشجيع الجهود الفعالة في مجال المساعدات المتبادلة، وتعزيز الدعم المؤسسي على المستوى الدولي لمنع مثل هذه الجرائم واكتشافها وإصلاح ما يترتب عليها؛ وتشجيع التعليم والنهوض بالوعي العام.

كما عولجت قضية الجريمة السيبرانية في المرحلة الثانية من القمة العالمية لمجتمع المعلومات التي عقدت في تونس في عام 2005. ويسلط برنامج عمل تونس لمجتمع المعلومات[804] الضوء على ضرورة التعاون الدولي في مكافحة الجريمة السيبرانية ويشير إلى النهج التشريعية الراهنة مثل قراري الجمعية العامة للأمم المتحدة واتفاقية مجلس أوروبا بشأن الجريمة السيبرانية:

40 *نحن نؤكد على أهمية ملاحقة الجرائم السيبرانية قضائياً، بما فيها الجرائم السيبرانية التي ترتكب ضمن ولاية قانونية ولكنها تؤثر على ولايات قانونية أخرى. وندعو الحكومات بالتعاون مع أصحاب المصلحة الآخرين إلى وضع التشريعات اللازمة للتحقيق في الجرائم السيبرانية وملاحقتها قضائياً، مع الاستفادة من الأطر القائمة، ومنها، على سبيل المثال، قرار الجمعية العامة للأمم المتحدة 55/63 وقرارها 56/121 بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية" واتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.*

وكان من نتائج القمة العالمية لمجتمع المعلومات، أن اختير الاتحاد الدولي للاتصالات الميسر الوحيد لخط العمل جيم5 المكرس لبناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.[805] وفي اجتماع التيسير الثاني لخط العمل جيم5 للقمة العالمية لمجتمع المعلومات، الذي عُقد في عام 2007، سلط الأمين العام للاتحاد الدولي للاتصالات الضوء على أهمية التعاون الدولي في مكافحة الجريمة السيبرانية وأعلن استهلال *البرنامج العالمي للأمن السيبراني*[806] ويتوخى البرنامج العالمي للأمن السيبراني سبعة أهداف رئيسية،[807] ويستند إلى خمس ركائز استراتيجية،[808] بما في ذلك وضع استراتيجيات وإعداد تشريعات نموذجية بشأن الجريمة السيبرانية. وهذه الأهداف السبعة هي:

---

[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.
[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.

1 وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة السيبرانية يمكن تطبيقه عالمياً وقابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.

2 وضع استراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة الملائمة على الصعيدين الوطني والإقليمي بشأن الجريمة السيبرانية.

3 وضع استراتيجية لصوغ معايير أمنية دنيا وخطط اعتماد للأجهزة الحاسوبية ولتطبيقات البرمجيات والأنظمة تكون مقبولة عالمياً.

4 وضع استراتيجيات لإيجاد إطار عالمي للرصد والإنذار والاستجابة للحوادث لضمان التنسيق عبر الحدود بين المبادرات الجديدة والقائمة.

5 وضع استراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمي عام عالمي، والهياكل التنظيمية اللازمة لضمان الاعتراف بوثائق التفويض الرقمية عبر الحدود الجغرافية.

6 وضع استراتيجية عالمية لتيسير بناء القدرات البشرية والمؤسسية من أجل تعزيز المعارف والمهارات عبر القطاعات وفي المجالات الآنفة الذكر.

7 وضع مقترحات بشأن إطار لاستراتيجية عالمية لأصحاب المصلحة المتعددين لتحقيق الحوار والتنسيق على الصعيد الدولي في جميع المجالات الآنفة الذكر.

وأنشئ فريق خبراء ليضع الاستراتيجيات المتعلقة بالبرنامج العالمي للأمن السيبراني.[809]

4.1.5 مجلس أوروبا[810]

في عام 1976، سلط مجلس أوروبا الضوء على الطبيعة الدولية للجرائم المتعلقة بالحاسوب وناقش هذا الموضوع في مؤتمر تناول الجوانب المتصلة بالجرائم الاقتصادية. وظل هذا الموضوع مدرجة على جدول أعمال مجلس أوروبا منذ ذلك الحين.[811] وفي عام 1985 عيّن مجلس أوروبا لجنة خبراء[812] لمناقشة الجوانب القانونية للجرائم الحاسوبية.[813] وفي عام 1989، اعتمدت اللجنة الأوروبية لمشكلات الجرائم "تقرير الخبراء بشأن الجريمة المتعلقة بالحاسوب"،[814] الذي حلل الأحكام القانونية الجنائية الموضوعية اللازمة لمكافحة الأشكال الجديدة للجرائم الإلكترونية، بما فيها الاحتيال والتزييف الحاسوبيين. واعتمدت لجنة الوزراء في عام 1989 توصية[815] سلطت الضوء تحديداً على الطبيعة الدولية للجريمة الحاسوبية:

إن لجنة الوزراء، بموجب أحكام المادة 15 – ب من النظام الأساسي لمجلس أوروبا، إذ ترى أن هدف مجلس أوروبا هو تحقيق وحدة أكبر بين أعضائه؛

وإذ تعترف بأهمية الاستجابة الوافية والسريعة للتحدي الجديد الذي تمثله الجريمة المتعلقة بالحاسوب؛ وإذ ترى أن الجريمة المتعلقة بالحاسوب تتسم في أحيان كثيرة بطابع عابر للحدود؛ وإدراكاً منها لما يترتب على ذلك من ضرورة المضي في تحقيق التواؤم بين القوانين والممارسات، وتحسين التعاون القانوني الدولي، توصي حكومات الدول الأعضاء بما يلي:

1 أن تأخذ في الاعتبار، لدى استعراض تشريعاتها أو سن تشريعات جديدة، التقرير الخاص بالجريمة المتعلقة بالحاسوب الذي أعدته اللجنة الأوروبية لمشكلات الجرائم، وبوجه خاص المبادئ التوجيهية المقدمة إلى المشرعين الوطنيين؛

2 أن توافي الأمين العام لمجلس أوروبا أثناء عام 1993 بأي تطورات تطرأ على تشريعاتها وممارساتها القضائية وخبراتها المتعلقة بالتعاون القانوني الدولي بشأن الجريمة المتعلقة بالحاسوب.

---

[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.

وفي عام 1995، اعتمدت لجنة الوزراء توصية أخرى تتناول المشكلات الناشئة عن الجرائم الحاسوبية عبر الوطنية.[816] وتضمنت التوصية تذييلاً يلخص المبادئ التوجيهية لصوغ التشريعات المناسبة.[817]

وقررت اللجنة الأوروبية لمشكلات الجرائم في عام 1996 أن تنشئ لجنة خبراء لمعالجة الجريمة السيبرانية.[818] وكانت الفكرة المتمثلة في المضي إلى ما هو أبعد من مجرد وضع مبادئ تتضمنها توصية أخرى، والتوجه بدلاً من ذلك إلى إعداد اتفاقية، فكرة ماثلة في الأذهان وقت إنشاء لجنة الخبراء.[819] وخلال الفترة الممتدة بين عامي 1997 و2000، عقدت اللجنة عشرة اجتماعات بكامل هيئتها وخمسة عشر اجتماعاً لفريق الصياغة المفتوح العضوية التابع لها. واعتمدت الجمعية مشروع الاتفاقية في الجزء الثاني في جلستها العامة المعقودة في أبريل 2001.[820] وقُدم مشروع الاتفاقية، الموضوع في صيغته النهائية، إلى اللجنة الأوروبية لمشكلات الجريمة للموافقة عليه، ثم قُدم نص مشروع الاتفاقية بعد ذلك إلى لجنة الوزراء لاعتماده وفتح باب التوقيع على الاتفاقية. وفتح باب التوقيع على الاتفاقية في حفل توقيع عُقد في بودابست في 23 نوفمبر 2001، وقع خلاله 30 بلداً على الاتفاقية (من بينها أربعة بلدان غير أعضاء في مجلس أوروبا شاركت في المفاوضات هي كندا والولايات المتحدة الأمريكية واليابان وجنوب إفريقيا). وبحلول أبريل 2009، كانت 46 دولة[821] قد وقعت على اتفاقية الجريمة السيبرانية وكانت 25 دولة[822] قد صدقت عليها.[823] وقامت بلدان مثل الأرجنتين،[824] وباكستان،[825] والفلبين،[826] ومصر،[827] وبوتسوانا،[828] ونيجيريا،[829] بصوغ أجزاء من تشريعاتها وفقاً للاتفاقية. وعلى الرغم من أن تلك البلدان لم توقع بعد على الاتفاقية، فإنها تؤيد عملية تحقيق التواؤم والتقييس التي توخاها واضعو الاتفاقية. واليوم يُعترف بالاتفاقية بوصفها أداة دولية هامة في مكافحة الجريمة السيبرانية وتحظى بدعم منظمات دولية مختلفة.[830]

---

[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.

[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.

[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

وفي إثر الاتفاقية، وضع البروتوكول الإضافي الأول للاتفاقية بشأن الجريمة السيبرانية.[831] فخلال المفاوضات حول نص الاتفاقية، تبين أن تجريم العنصرية وتوزيع المواد الحاضة على كراهية الأجانب يعد مسألة خلافية بوجه خاص.[832] إذ أعربت بعض البلدان التي تكفل حماية قوية لمبدأ حرية التعبير[833] عن خشيتها من ألا تستطيع، في حالة تضمين الاتفاقية أحكاماً تنتهك حرية التعبير، من التوقيع على الاتفاقية.[834] ولذا، فإن هذه القضايا قد أدرجت في بروتوكول منفصل. وبحلول أكتوبر 2008، كانت 20 دولة[835] قد وقعت على البروتوكول الإضافي وكانت 13 دولة[836] قد صدقت عليه.

واستحدث مجلس أوروبا، في إطار نهجه الرامي إلى تحسين حماية القصر من الاستغلال الجنسي، اتفاقية جديدة في عام 2007.[837] وفي اليوم الأول لفتح باب التوقيع على اتفاقية حماية الأطفال وقعت عليها 23 دولة.[838] ويتمثل أحد الأهداف الرئيسية للاتفاقية في تحقيق التواؤم بين أحكام القانون الجنائي الرامية إلى حماية الأطفال من الاستغلال الجنسي.[839] وتحقيقاً لهذا الهدف، تتضمن الاتفاقية مجموعة من أحكام القانون الجنائي. وإلى جانب تجريم الاستغلال الجنسي للأطفال (المادة 18)، تتضمن الاتفاقية حكماً يتناول تبادل المواد الإباحية التي يستغل فيها الأطفال (المادة 20) وإغواء الأطفال لأغراض جنسية (المادة 23).

2.5 النهج الإقليمية

بالإضافة إلى المنظمات الدولية التي تضطلع بدور نشط على الصعيد العالمي، مضى عدد من المنظمات الدولية التي تركز في عملها على مناطق محددة قدماً في تنفيذ أنشطة تتناول قضايا تتعلق بالجريمة السيبرانية.

1.2.5 الاتحاد الأوروبي[840]

لا يملك الاتحاد الأوروبي إلا صلاحيات محدودة فيما يتعلق بالتشريع في مجال القانون الجنائي.[841] ولا يملك الاتحاد القدرة على تحقيق تواؤم بين القوانين الجنائية الوطنية إلا في مجالات خاصة مثل حماية المصالح المالية للاتحاد الأوروبي والجريمة السيبرانية.[842]

وفي عام 1999، أطلق الاتحاد الأوروبي مبادرة "أوروبا الإلكترونية"، باعتماده بيان المفوضية الأوروبية المعنون "أوروبا الإلكترونية – مجتمع معلومات للجميع".[843] وفي عام 2000، اعتمد مجلس أوروبا "خطة عمل أوروبا الإلكترونية"، وهي خطة عمل شاملة، ودعا إلى تنفيذها قبل نهاية عام 2002.

---

[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.

[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 - Europe - An information society for all – COM 1999, 687.

وفي عام 2001، أصدرت المفوضية الأوروبية بياناً معنوناً "إنشاء مجتمع معلومات أكثر سلامة عن طريق تحسين أمن البنى التحتية للمعلومات ومكافحة الجريمة المتعلقة بالحاسوب".[844] وفي هذا البيان، حللت اللجنة وعالجت مشكلة الجريمة السيبرانية وأشارت إلى ضرورة الاضطلاع بعمل فعال للتصدي للتحديات المحدقة بتكاملية نظم وشبكات المعلومات وتيسرها وإمكانية الاعتماد عليها.

أصبحت البنى التحتية للمعلومات والاتصالات جزءاً حاسماً في اقتصاداتنا. وللأسف، فإن لهذه البنى التحتية أوجه ضعفها وهي تتيح فرصاً جديدة للسلوك الإجرامي. وقد تتخذ هذه الأنشطة الإجرامية طائفة واسعة من الأشكال وقد تعبر حدوداً كثيرة. وعلى الرغم من أنه لا تتوافر، لعدد من الأسباب، إحصاءات موثوق بها، لا يكاد يثور شك في أن هذه الجرائم تشكل تهديداً لاستثمارات الصناعة وأصولها، ولسلامة مجتمع المعلومات والثقة به. فقد أفادت التقارير أن بعض الأمثلة الأخيرة للهجمات الرامية إلى الحرمان من النفاذ إلى الخدمة والهجمات الفيروسية قد سببت أضراراً مالية كبيرة.

وثمة مجال متاح للعمل على منع النشاط الإجرامي عن طريق تعزيز أمن البنى للمعلومات وكذلك عن طريق تزويد سلطات إنفاذ القانون بوسائل العمل الملائمة، إلى جانب احترام الحقوق الأساسية للأفراد بصورة كاملة في الوقت نفسه.[845]

وتعترف المفوضية، التي شاركت في كل من مناقشات مجلس أوروبا ومجموعة الثمانية، بما تنطوي عليه قضايا القانون الإجرائي من تعقيد وصعوبات. لكن التعاون الفعال في إطار الاتحاد الأوروبي على مكافحة الجريمة السيبرانية يشكل عنصراً أساسياً لإقامة مجتمع معلومات أكثر سلامة ولإنشاء منطقة تسودها الحرية والأمن والعدالة.[846]

وستطرح المفوضية مقترحات تشريعية بموجب الباب السادس من معاهدة الاتحاد الأوروبي:

[...] من أجل المضي في تقريب القانون الجنائي المضموني في مجال الجريمة المتعلقة بالتكنولوجيا الراقية. وتشمل هذه الجريمة أفعالاً تتعلق بهجمات القرصنة والهجمات التي تستهدف الحرمان من النفاذ إلى الخدمة. وستدرس المفوضية أيضاً نطاق العمل المناهض للعنصرية وكراهية الأجانب على الإنترنت بغية طرح مقرر إطاري بموجب الباب السادس من معاهدة الاتحاد الأوروبي يغطي النشاط العنصري والمنطوي على كراهية الأجانب الذي يمارس على الإنترنت وخارجها سواء بسواء.[847]

وستواصل المفوضية القيام بدورها كاملاً في ضمان التنسيق بين الدول الأعضاء في محافل دولية أخرى تناقش فيها الجريمة السيبرانية مثل مجلس أوروبا ومجموعة الثمانية. وستأخذ المبادرات التي تضطلع بها المفوضية على مستوى الاتحاد الأوروبي في حسبانها على الوجه الأكمل التقدم المحرز في محافل دولية أخرى، إلى جانب السعي في الوقت نفسه إلى تحقيق التقارب داخل الاتحاد الأوروبي.[848]

وبالإضافة إلى ذلك، نشرت المفوضية بياناً بشأن "أمن الشبكات والمعلومات"[849] في عام 2001 حلل المشكلات المتصلة بأمن الشبكات ووضع مخطط استراتيجية عمل في هذا المجال.

وأكد بيانا المفوضية كلاهما على ضرورة تحقيق التقارب بين القوانين الجنائية الموضوعية داخل الاتحاد الأوروبي – وخاصة فيما يتعلق بالهجمات ضد نظم المعلومات. وسلما بأن تحقيق التواؤم بين القوانين الجنائية الموضوعية داخل الاتحاد الأوروبي في إطار مكافحة الجريمة السيبرانية يشكل عنصراً أساسياً في جميع المبادرات المضطلع بها على مستوى الاتحاد الأوروبي.[850] وعملاً بهذه الاستراتيجية، قدمت المفوضية في عام 2002[851] اقتراحاً بشأن "مقرر إطاري بشأن الهجمات ضد نظم المعلومات". وقام المجلس بتعديل اقتراح المفوضية جزئياً واعتمده في نهاية المطاف.[852]

[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.

[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.

ويحيط المقرر الإطاري علماً باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية[853] ولكنه يركز على تحقيق التواؤم بين أحكام القانون الجنائي الموضوعية الرامية إلى حماية عناصر البنية التحتية.

المادة 2 – النفاذ غير القانوني إلى نظم المعلومات

1 تتخذ كل دولة عضو التدابير اللازمة لضمان معاقبة النفاذ العمدي دون وجه حق إلى أي نظام للمعلومات، كله أو أي جزء منه، بوصفه عملاً إجرامياً، على الأقل في الحالات التي لا تكون طفيفة.

2 يجوز لكل دولة عضو أن تقرر ألا تجرم السلوك المشار إليه في الفقرة 1 إلا حيثما يرتكب الجرم عن طريق خرق تدبير أمني، يعاقب عليه بعقوبات جنائية فعالة وتناسبية ورادعة.

المادة 3 – التدخل غير القانوني في النظم

تتخذ كل دولة عضو التدابير اللازمة لضمان معاقبة التعويق أو التعطيل الخطير العمدي لتشغيل أي نظام للمعلومات عن طريق إدخال بيانات حاسوبية، أو نقلها، أو إتلافها، أو حذفها، أو إعطابها، أو تحويرها، أو حجبها، أو منع النفاذ إليها، بوصفه عملاً إجرامياً عندما يرتكب دون وجه حق، على الأقل في الحالات التي لا تكون طفيفة.

المادة 4 – التدخل غير المشروع في البيانات

تتخذ كل دولة التدابير اللازمة لضمان معاقبة القيام عمداً بحذف بيانات حاسوبية في نظام للمعلومات أو إتلافها، أو إعطابها، أو تحويرها، أو حجبها، أو منع النفاذ إليها، بوصفه عملاً إجرامياً عندما يرتكب دون حق، على الأقل في الحالات التي لا تكون طفيفة.

وفي عام 2005، أعلنت محكمة العدل للجماعات الأوروبية أن المقرر الإطاري المتعلق بحماية البيئة عن طريق القانون الجنائي،[854] الذي اتخذه المجلس، يُعدّ غير قانوني.[855] وبهذا المقرر، تكون المحكمة قد أوضحت توزيع السلطات بين الركيزتين الأولى والثالثة فيما يتعلق بأحكام القانون الجنائي. فقد قررت أن المقرر الإطاري المتعلق بحماية البيئة عن طريق القانون الجنائي يخالف، بحكم أنه غير قابل للتجزئة، المادة 47 للاتحاد الأوروبي لأنه يتعدى على السلطات التي تخولها المادة 175 من معاهدة مجلس أوروبا إلى المفوضية.[856] وقالت المفوضية في بيان أصدرته بشأن مقرر المحكمة:[857]

"من حيث فحوى المسألة، فإن حجة المحكمة، بالإضافة إلى سريانها على مسألة حماية البيئة، تنطبق من ثم على جميع سياسات المفوضية وعلى الحريات التي تتوافر بشأنها تشريعات ملزمة ينبغي أن تقترن بعقوبات جنائية تضمن فعاليتها."

وقالت المفوضية إنه بناء على حكم المحكمة يكون عدد من المقررات الإطارية التي تتناول القانون الجنائي غير صحيحة كلياً أو جزئياً، لأن كل أحكامها أو بعضها قد اعتمدت وفقاً لأساس قانوني خاطئ. وقد أشير صراحة في تعديل البيان إلى المقرر الإطاري بشأن الهجمات ضد نظم المعلومات.

ولم تدرج في المقرر الإطاري جوانب القانون الجنائي الإجرائي – وخاصة تحقيق التواؤم بين الأدوات اللازمة للتحقيق في الجريمة السيبرانية والملاحقة القضائية لها. غير أن المفوضية قد أعدت في عام 2005 اقتراحاً بشأن توجيه للاتحاد الأوروبي يتعلق باحتجاز البيانات. واعتمد المجلس الاقتراح بعد ثلاثة أشهر فقط من تقديمه إلى البرلمان الأوروبي.[858] والعنصر الرئيسي في هذا التوجيه هو الواجب المنوط بمقدمي خدمة الإنترنت بأن يخزنوا بعض بيانات الحركة اللازمة للكشف عن هوية الجناة الجنائيين في الفضاء السيبراني:

---

[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:
"Legislative action at the level of the European Union also needs to take into account developments in other international fora. In the context of approximation of substantive criminal law on attacks against information systems, the Council of Europe (C.o.E.) is currently the most far-advanced. The Council of Europe started preparing an international Convention on cyber-crime in February 1997, and is expected to complete this task by the end of 2001. The draft Convention seeks to approximate a range of criminal offences including offences against the confidentiality, integrity and availability of computer systems and data. This Framework Decision is intended to be consistent with the approach adopted in the draft Council of Europe Convention for these offences."

[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

المادة 3 – الالتزام بالاحتفاظ بالبيانات

1 على سبيل الاستثناء من أحكام المواد 5 و6 و9 من التوجيه 2002/58/EC، تعتمد الدول الأعضاء تدابير تضمن الاحتفاظ بالبيانات المحددة في المادة 5 من هذا التوجيه وفقاً لأحكامه، وذلك بالقدر الذي تُولّد فيه هذه البيانات أو تعالج من قبل مقدمي خدمات الاتصالات الإلكترونية المتاحة بصفة عمومية أو من قبل مقدمي خدمات شبكة اتصالات عمومية خاضعة لولايتها القضائية في إطار عملية توفير خدمات الاتصالات المعنية.

2 يشمل الالتزام بالاحتفاظ بالبيانات المنصوص عليه في الفقرة 1 احتجاز البيانات المحددة في الفقرة 5 المتعلقة بمحاولات النداء غير الناجحة عندما تُولّد تلك البيانات أو تعالج أو تخزن (فيما يتعلق بالبيانات الهاتفية) أو تسجل (فيما يتعلق ببيانات الإنترنت)، من قبل مقدمي خدمات الاتصالات الإلكترونية المتاحة بصفة عمومية أو من قبل مقدمي خدمات شبكات الاتصال العمومية الخاضعة للولاية القضائية للدولة العضو المعنية في إطار عملية توفير خدمات الاتصالات المعنية. ولا يستوجب هذا التوجيه الاحتفاظ بالبيانات المتعلقة بالنداءات التي لم يتم توصيلها.

ولما كان التوجيه سيغطي المعلومات الرئيسية عن أي اتصال يتم على الإنترنت فقد أثار ذلك نقداً شديداً من جانب منظمات حقوق الإنسان، الأمر الذي قد يفضي إلى إعادة النظر في التوجيه وفي تنفيذه من جانب المحاكم الدستورية.[859]

وفي عام 2007، نشرت المفوضية بياناً معنوناً نحو وضع سياسة عامة بشأن مكافحة الجريمة السيبرانية.[860] ويلخص البيان الوضع الراهن ويؤكد على أهمية اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية بوصفها الصك الدولي الأساسي لمكافحة الجريمة السيبرانية. كما أشار البيان إلى القضايا التي ستركز عليها المفوضية في أنشطتها المقبلة. وتشمل هذه القضايا ما يلي:

- تعزيز التعاون الدولي على مكافحة الجريمة السيبرانية؛
- تحسين تنسيق الدعم المالي للأنشطة التدريبية؛
- تنظيم اجتماع لخبراء إنفاذ القانون؛
- تعزيز الحوار مع الصناعة؛
- رصد التهديدات المتطورة للجريمة السيبرانية من أجل تقييم الحاجة إلى مزيد من التشريعات.

وفي عام 2008، بدأ الاتحاد الأوروبي نقاشاً بشأن مشروع تعديل المقرر الإطاري المتعلق بمكافحة الإرهاب.[861] وفي مقدمة مشروع التعديل، سلط الاتحاد الأوروبي الضوء على أن الإطار القانوني القائم يجرم المساعدة أو التحريض ولكنه لا يجرم نشر الخبرات الإرهابية عن طريق الإنترنت.[862] ويستهدف الاتحاد الأوروبي، بهذا التعديل، اتخاذ تدابير لسد هذه الثغرة ولتقريب التشريعات المطبقة في جميع أنحاء الاتحاد الأوروبي من اتفاقية مجلس أوروبا بشأن منع الإرهاب.

المادة 3 – الجرائم المرتبطة بالأنشطة الإرهابية

1 لأغراض هذا المقرر الإطاري:

(أ) يعني "التحريض العام على ارتكاب جريمة إرهابية" توزيع رسالة على الجمهور، أو إتاحتها بأي شكل آخر، بنية التحريض على ارتكاب أحد الأفعال المبينة في المادة (1) (أ) إلى (ح)، حيث يسبب هذا السلوك، سواء كان يدعو بشكل مباشر أو لا إلى جرائم إرهابية، خطراً باحتمال ارتكاب واحدة أو أكثر من هذه الجرائم؛

(ب) يعني "التجنيد لأغراض الإرهاب" إغواء شخص آخر بارتكاب أحد الأفعال المبينة في المادة (1.1)، أو في المادة (2.2)؛

(ج) يعني "التدريب على الإرهاب" توفير إرشادات عن صنع أو استخدام المتفجرات، أو الأسلحة النارية، أو الأسلحة الأخرى، أو المواد الخطيرة أو الضارة، أو عن أي أساليب أو تقنيات محددة أخرى بغرض ارتكاب أحد الأفعال المبينة في المادة 1 (1)، مع معرفة أن المقصود من اكتساب هذه المهارات هو استخدامها لهذا الغرض.

---

[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 *تتخذ كل دولة عضو التدابير اللازمة لضمان أن تشمل الجرائم المرتبطة بالإرهاب الأفعال العمدية التالية:*

(أ) *التحريض العام على ارتكاب جريمة إرهابية؛*

(ب) *التجنيد لأغراض الإرهاب؛*

(ج) *التدريب على الإرهاب؛*

(د) *السرقة، في ظروف مُشدّدة للجرم، بغية ارتكاب أحد الأفعال المبينة في المادة 1 (1)؛*

(هـ) *الابتزاز بهدف ارتكاب أحد الأفعال المبينة في المادة 1 (1)؛*

(و) *تحرير وثائق إدارية رسمية بهدف ارتكاب أحد الأفعال المبينة في المادة 1 (1) (أ) إلى (ح) والمادة 2 (2) (ب).*

3 *لا يلزم أن ترتكب بالفعل جريمة إرهابية للمعاقبة على أي فعل منصوص عليه في الفقرة (2)."*

واستناداً إلى الفقرة 1 (ج) من المادة 3[863] من الإطار، تعد الدول الأعضاء ملزمة مثلاً بتجريم نشر إرشادات عن كيفية استخدام المتفجرات، مع معرفة أن الغرض من هذه المعلومات هو أن تستخدم في أغراض تتعلق بالإرهاب. ومن المرجح للغاية أن تحد الحاجة إلى دليل على أن الغرض من المعلومات هو أن تستخدم في أغراض تتعلق بالإرهاب من تطبيق الحكم فيما يخص أغلبية الإرشادات عن كيفية استخدام الأسلحة المتاحة على الخط، لأن نشرها لا يربطها مباشرة بالهجمات الإرهابية. ولما كان بالوسع استخدام معظم الأسلحة والمتفجرات لارتكاب جرائم "عادية" بالإضافة إلى جرائم تتعلق بالإرهاب (استخدام مزدوج)، فإن المعلومات ذاتها لا يمكن استخدامها عملياً لإثبات أن الشخص الذي ينشر تلك المعلومات كان يعرف الطريقة التي ستستخدم بها بعد ذلك. ولذا يتعين أن يؤخذ سياق النشر في الاعتبار (كأن تكون قد نشرت مثلا في موقع ويب تديره منظمة إرهابية).

2.2.5 منظمة التعاون والتنمية في الميدان الاقتصادي[864]

في عام 1983، استهلت منظمة التعاون والتنمية في الميدان الاقتصادي دراسة عن إمكانية تحقيق التواؤم بين القوانين الجنائية على الصعيد الدولي من أجل معالجة مشكلة الجريمة الحاسوبية.[865] وفي عام 1985، نشرت المنظمة تقريراً حلل التشريعات الراهنة وقدم اقتراحات بشأن مكافحة الجريمة السيبرانية.[866] وأوصى التقرير بقائمة دنيا من الجرائم ينبغي أن تنظر البلدان في تجريمها، مثل الاحتيال الحاسوبي، والتزييف الحاسوبي، وتحوير البرامج والبيانات الحاسوبية، واعتراض الاتصالات. وفي عام 1990، أنشأت لجنة سياسة المعلومات والحاسوب والاتصالات فريق خبراء ليضع مجموعة من المبادئ التوجيهية لأمن المعلومات، فعكف هذا الفريق على إعدادها حتى عام 1992 ثم اعتمدها مجلس منظمة التعاون والتنمية في الميدان الاقتصادي.[867] وتشمل المبادئ التوجيهية جوانب شتى من بينها القضايا المتعلقة بالعقوبات:

تعد العقوبات الموقعة على إساءة استخدام نظم المعلومات وسيلة هامة لحماية مصالح من يعتمدون على نظم المعلومات من الضرر الناجم عن الهجمات التي تستهدف تيسّر نظم المعلومات ومكوناتها وسريتها وتكامليتها.

وتشمل أمثلة هذه الهجمات إتلاف نظم المعلومات أو تعطيلها عن طريق إدراج فيروسات وديدان، وتحوير البيانات، والنفاذ غير القانوني إلى البيانات، والاحتيال أو التزييف الحاسوبي، والاستنساخ غير المأذون به للبرامج الحاسوبية. وقد اختارت البلدان، لدى مكافحة هذه الأخطار، أن تصف الأعمال الإجرامية وتستجيب لها بطرق متنوعة. وهناك اتفاق دولي متنام على المجموعة الأساسية من الجرائم المتعلقة بالحاسوب التي ينبغي أن تغطيها القوانين الجنائية الوطنية. ويتجلى هذا في قيام البلدان الأعضاء بمنظمة التعاون والتنمية في الميدان الاقتصادي خلال العقدين الماضيين بوضع تشريعات بشأن الجريمة الحاسوبية وحماية البيانات، كما يتجلى في أعمال المنظمة والهيئات الدولية الأخرى بشأن التشريعات الرامية إلى مكافحة الجريمة المتعلقة بالحاسوب[...]. وينبغي أن تستعرض التشريعات الوطنية بصفة دورية بما يكفل تصديها بصورة وافية للأخطار الناشئة عن إساءة استخدام نظم المعلومات.

وبعد استعراض المبادئ التوجيهية في عام 1997، أنشأت لجنة سياسة المعلومات والحاسوب والاتصالات في عام 2001 فريق خبراء ثانياً تولى تحيين المبادئ التوجيهية. وفي عام 2002 اعتمدت نسخة جديدة من المبادئ التوجيهية بعنوان "المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي بشأن أمن نظم وشبكات المعلومات: نحو ثقافة أمن"، بوصفها توصية مقدمة لمجلس المنظمة.[868] وتتضمن المبادئ التوجيهية تسعة مبادئ متكاملة هي:

---

[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.

[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

1) الوعي

ينبغي أن يكون المشاركون واعين بضرورة أمن نظم وشبكات المعلومات وبما يمكنهم أن يقوموا به من أجل تعزيز الأمن.

2) المسؤولية

جميع المشاركين مسؤولون عن أمن نظم وشبكات المعلومات.

3) الاستجابة

ينبغي أن يتصرف المشاركون بطريقة سريعة وتعاونية لمنع الحوادث الأمنية واكتشافها والتصدي لها.

4) الأخلاقيات

ينبغي أن يحترم المشاركون المصالح المشروعة للآخرين.

5) الديمقراطية

ينبغي أن يتوافق أمن نظم وشبكات المعلومات مع القيم الجوهرية للمجتمع الديمقراطي.

6) تقدير المخاطر

ينبغي أن يجري المشاركون تقديراً للمخاطر.

7) تصميم تدابير الأمن وتنفيذها

ينبغي أن يدرج المشاركون الأمن بوصفه عنصراً جوهرياً في نظم وشبكات المعلومات.

8) إدارة الأمن

ينبغي أن يعتمد المشاركون نهجاً شاملاً إزاء إدارة الأمن.

9) إعادة التقييم

ينبغي أن يستعرض المشاركون أمن نظم وشبكات المعلومات وأن يعيدوا تقييمه، وأن يدخلوا ما يلزم من تعديلات على السياسات والممارسات والتدابير والإجراءات الأمنية.

وفي عام 2005، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي تقريراً حلل تأثير الرسائل الاقتحامية على البلدان النامية.[869] وأظهر التقرير أن الرسائل الاقتحامية تشكل مشكلة أشد خطراً في البلدان النامية عنها في البلدان الغربية لأن الموارد في البلدان النامية أقل حجماً وأعلى تكلفة.[870]

وفي عام 2007، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي، بعد أن تلقت طلباً من وحدة التخطيط الاستراتيجي التابعة للمكتب التنفيذي للأمين العام للأمم المتحدة بشأن إعداد مخطط مقارن للحلول التشريعية المحلية المتعلقة باستخدام الإنترنت في أغراض إرهابية، تقريراً عن المعالجة التشريعية "للإرهاب السيبراني" في القانون المحلي لآحاد الدول.[871]

3.2.5 مجموعة التعاون الاقتصادي في آسيا والمحيط الهادئ[872]

في عام 2002، قام قادة مجموعة التعاون الاقتصادي في آسيا والمحيط الهادئ بإصدار "بيان بشأن مكافحة الإرهاب وتعزيز النمو" من أجل سن قوانين شاملة تتعلق بالجريمة السيبرانية وتنمية القدرات الوطنية على التحقيق في الجريمة السيبرانية.[873] وأعلنوا التزامهم بما يلي:

- السعي إلى سن مجموعة شاملة من القوانين المتعلقة بالأمن السيبراني والجريمة السيبرانية تتسق مع أحكام الصكوك القانونية الدولية، بما فيها قرار الجمعية العامة للأمم المتحدة 55/63 (2000) واتفاقية الجريمة السيبرانية (2001)، بحلول أكتوبر 2003.
- تعيين وحدات وطنية معنية بالجريمة السيبرانية وجهات اتصال دولية للمساعدة في مجال التكنولوجيا الراقية، وإنشاء هذه القدرات إن كانت لا تتوافر بالفعل، بحلول أكتوبر 2003.

[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.
[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.

- إنشاء مؤسسات تتبادل التقييمات المتعلقة بالتهديدات وبأوجه الضعف (مثل أفرقة الاستجابة للطوارئ الحاسوبية)، بحلول أكتوبر 2003.

ودعا قادة المجموعة إلى توثيق التعاون بين المسؤولين المعنيين بمكافحة الجريمة السيبرانية.[874] وفي عام 2005، نظمت المجموعة مؤتمراً بشأن تشريعات الجريمة السيبرانية.[875] وتوخت الأهداف الرئيسية للمؤتمر ما يلي:

- الترويج لإنشاء أطر قانونية شاملة لمكافحة الجريمة السيبرانية وتعزيز الأمن السيبراني؛
- مساعدة سلطات إنفاذ القانون على التصدي للقضايا المتعلقة بأحدث التطورات العلمية وللتحديات التي تطرحها أوجه التقدم في مجال التكنولوجيا؛
- تعزيز التعاون بين المحققين في الجرائم السيبرانية في جميع أنحاء المنطقة.

وشارك فريق العمل المعني بالاتصالات والمعلومات التابع للمجموعة[876] مشاركة نشيطة في نُهج المجموعة الرامية إلى زيادة الأمن السيبراني.[877] وفي عام 2002، اعتمد الفريق استراتيجية الأمن السيبراني لمجموعة التعاون الاقتصادي في آسيا والمحيط الهادئ.[878] وأبدى فريق العمل موقفه من تشريعات الجريمة السيبرانية بالإشارة إلى النهج الدولية المعمول بها في الأمم المتحدة ومجلس أوروبا.[879] وسلط الإعلان الصادر عن الاجتماع الذي عقده وزراء الاتصالات والمعلومات في بلدان المجموعة، في بانكوك بتايلاند في عام 2008، الضوء على أهمية مواصلة التعاون في مكافحة الجريمة السيبرانية.[880]

4.2.5 الكومنولث

قرر وزراء العدل في الكومنولث، آخذين تزايد أهمية الجريمة السيبرانية في حسبانهم، أن يكلفوا فريق خبراء بوضع إطار قانوني لمكافحة الجريمة السيبرانية، بالاستناد إلى اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[881] وكان الدافع وراء اتباع هذا النهج الرامي، ضمن جملة أمور، إلى تحقيق التواؤم بين التشريعات داخل الكومنولث وإفساح المجال أمام التعاون الدولي، إدراك مفاده أن الأمر سيقتضي لولا ذلك إبرام ما لا يقل عن 1272 معاهدة ثنائية في إطار الكومنولث لتغطية متطلبات التعاون الدولي في هذا الشأن.[882] وقدم فريق الخبراء تقريره وتوصياته في مارس 2002.[883] ثم قدم في وقت لاحق من عام 2002 مشروع القانون النموذجي الخاص بالحاسوب والجريمة المتعلقة بالحاسوب.[884] وجاء القانون النموذجي متماشياً مع المعايير التي حددتها اتفاقية الجريمة السيبرانية، عملاً بالتعليمات الواضحة التي تلقاها فريق الخبراء، وإدراكاً منه لكون اتفاقية الجريمة السيبرانية تشكل معياراً دولياً.

---

[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

[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.

5.2.5 الجامعة العربية ومجلس التعاون لدول الخليج[885]

اتخذ بالفعل عدد من البلدان في المنطقة العربية تدابير وطنية واعتمد نهجاً لمكافحة الجريمة السيبرانية، أو هو بصدد صوغ تشريعات في هذا الشأن.[886] ومن أمثلة هذه البلدان: باكستان،[887] ومصر،[888] والإمارات العربية المتحدة.[889] وأوصى مجلس التعاون لدول الخليج[890] في مؤتمر عُقد في عام 2007 بأن تسعى بلدان المجلس إلى اتباع نهج مشترك يأخذ المعايير الدولية في الاعتبار.[891]

6.2.5 منظمة الدول الأمريكية[892]

تعكف منظمة الدول الأمريكية بشكل نشط منذ عام 1999 على معالجة قضية الجريمة السيبرانية داخل المنطقة التي تعنى بها. وقامت المنظمة، ضمن ما اضطلعت به من أنشطة في هذا الصدد، بعقد عدد من الاجتماعات في إطار تفويض وولاية وزراء العدل في الأمريكتين.[893]

ففي عام 1999، أوصى وزراء العدل في الأمريكتين بإنشاء فريق خبراء حكومي دولي معني بالجريمة السيبرانية. وفوض فريق الخبراء في القيام بما يلي:

- وضع تشخيص كامل للنشاط الإجرامي الذي يستهدف الحواسيب والمعلومات، أو الذي يستخدم الحواسيب كوسيلة لارتكاب الجريمة؛
- وضع تشخيص كامل للتشريعات والسياسات والممارسات الوطنية المتعلقة بهذا النشاط؛
- تعيين الكيانات الوطنية والدولية التي تملك خبرة في هذا الصدد؛
- تحديد آليات التعاون في إطار منظومة الدول الأمريكية لمكافحة الجريمة السيبرانية.

وفي عام 2000، بحث وزراء العدل في الأمريكتين موضوع الجريمة السيبرانية واتفقوا على عدد من التوصيات.[894] وقد تكرر التأكيد على هذه التوصيات في اجتماع عام 2003[895] وهي تشمل ما يلي:

- أن يُدعم اعتبار التوصيات التي وضعها فريق الخبراء الحكومي في اجتماعه الأولي إسهاماً من وزراء العدل في الأمريكتين في وضع الاستراتيجية المشتركة بين الدول الأمريكية لمكافحة تهديدات الجريمة السيبرانية، المشار إليها في قرار الجمعية العامة لمنظمة الدول الأمريكية AG/RES. 1939 /XXXIII-O/03، وأن يطلب إلى الفريق، من خلال رئيسه، أن يواصل دعم إعداد الاستراتيجية.
- أن تستعرض الدول الأعضاء، في إطار فريق الخبراء، الآليات الكفيلة بتيسير التعاون الواسع والفعال فيما بينها على مكافحة الجريمة السيبرانية وأن تدرس، متى كان ذلك ممكناً، تنمية القدرات التقنية والقانونية بغية الانضمام إلى شبكة 7/24 التي أنشأتها مجموعة الثمانية للمساعدة في التحقيقات المتعلقة بالجريمة السيبرانية.

---

[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) 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

- أن تُقيّم الدول الأعضاء مدى استصواب تنفيذ المبادئ الواردة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (2001)، وأن تنظر في إمكانية الانضمام إلى تلك الاتفاقية.
- أن تستعرض الدول الأعضاء وأن تُحين، إذا كان ذلك ملائماً، هيكل وعمل الهيئات المحلية، أو الوكالات المعنية بإنفاذ القوانين كي تتكيف مع الطبيعة المتحولة للجريمة السيبرانية، وذلك بسبل منها استعراض العلاقة بين الوكالات التي تكافح الجريمة السيبرانية والوكالات التي توفر خدمات الشرطة التقليدية أو تتبادل المساعدة القانونية.

وأوصى الاجتماع الرابع لوزراء العدل في الأمريكتين بأن يجري، في إطار أنشطة فريق العمل التابع للمنظمة المتعلقة بمتابعة توصيات وزراء العدل، دعوة فريق الخبراء الحكوميين المعني بالجريمة السيبرانية[896] إلى الانعقاد مجدداً وتفويضه بما يلي:

- متابعة تنفيذ التوصيات التي أعدها ذلك الفريق والتي اعتمدها وزراء العدل في الأمريكتين في اجتماعهم الثالث؛
- النظر في إعداد صكوك قانونية وتشريعات نموذجية ملائمة للدول الأمريكية بغرض تعزيز التعاون في نصف الكرة الغربي على مكافحة الجريمة السيبرانية، مع مراعاة المعايير المتعلقة بالخصوصية، وحماية المعلومات، والجوانب الإجرائية، ومنع الجريمة.

وقد عقد وزراء العدل في الأمريكتين سبعة اجتماعات حتى الآن.[897] وعُقد آخر اجتماعين لهما في مدينة واشنطن بالولايات المتحدة في أبريل 2006 ثم في أبريل 2008. وكان من بين التوصيات المنبثقة عن اجتماع عام 2006 ما يلي:[898]

- مواصلة تعزيز التعاون مع مجلس أوروبا، بحيث تنظر الدول الأعضاء في منظمة الدول الأمريكية في تطبيق المبادئ الواردة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية[899] والانضمام إليها، واعتماد التدابير القانونية والتدابير الأخرى المطلوبة لتنفيذها. وبالمثل، أن تتواصل الجهود من أجل تقوية آليات تبادل المعلومات والتعاون مع المنظمات والوكالات الدولية الأخرى في مجال الجريمة السيبرانية، مثل الأمم المتحدة، والاتحاد الأوروبي، ومحفل التعاون الاقتصادي في آسيا والمحيط الهادئ، ومنظمة التعاون والتنمية في الميدان الاقتصادي، ومجموعة الثمانية، والكومنولث، والإنتربول، كي تنتفع الدول الأعضاء في منظمة الدول الأمريكية من التقدم المحرز في تلك المحافل؛
- أن تنشئ الدول الأعضاء وحدات متخصصة للتحقيق في الجريمة السيبرانية وأن تعين السلطات التي ستقوم بدور جهات الاتصال في هذا المجال، وأن تعجل بتبادل المعلومات والحصول على الأدلة. وأن تقوم، علاوة على ذلك، بتوطيد التعاون في الجهود الرامية إلى مكافحة الجريمة السيبرانية بين السلطات الحكومية ومقدمي خدمة الإنترنت وغيرها من شركات القطاع الخاص التي توفر خدمات نقل البيانات.

وقد تكرر التأكيد على هاتين التوصيتين في اجتماع عام 2008 الذي دعا فضلاً عن ذلك إلى ما يلي:[900]

- أن تنظر الدول، مع مراعاة التوصيات التي اعتمدتها أفرقة الخبراء الحكومية والاجتماعات السابقة لوزراء العدل في الأمريكتين، في تطبيق المبادئ الواردة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والانضمام إليها، واعتماد التدابير القانونية والتدابير الأخرى المطلوبة لتنفيذها. وأن تواصل، تحقيقاً لهذه الغاية، تنفيذ أنشطة التعاون التقني تحت رعاية الأمين العام لمنظمة الدول الأمريكية، من خلال أمانة الشؤون القانونية، ومجلس أوروبا. وأن يتواصل كذلك بذل الجهود من أجل تدعيم تبادل المعلومات والتعاون مع المنظمات والوكالات الدولية الأخرى في مجال الجريمة السيبرانية كي تنتفع الدول الأعضاء في منظمة الدول الأمريكية من التقدم المحرز في تلك المحافل.
- أن تواصل أمانة لجنة الدول الأمريكية لمكافحة الإرهاب وأمانة لجنة الدول الأمريكية للاتصالات وفريق العمل المعني بالجريمة السيبرانية إعداد تدابير التنسيق والتعاون الدائمين لضمان تنفيذ الاستراتيجية الشاملة للأمن السيبراني في الدول الأمريكية التي اعتمدت بموجب قرار الجمعية العامة لمنظمة الدول الأمريكية AG/RES. 2004 (XXXIV-O/04).

[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

3.5 النهج العلمية

من الأمثلة المعروفة للنهج العلمي في وضع إطار قانوني للتصدي للجريمة السيبرانية على المستوى العالمي مشروع اتفاقية ستانفورد الدولية.[901] وقد أعدت هذه الاتفاقية في إطار متابعة مؤتمر استضافته جامعة ستانفورد بالولايات المتحدة في عام 1999.[902] وتُظهر مقارنتها مع اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية،[903] التي صيغت في الفترة ذاتها تقريباً، عدداً من أوجه التماثل. فكلتا الاتفاقيتين تغطي جوانب القانون الجنائي الموضوعي، والقانون الإجرائي، والتعاون الدولي. ويتمثل أهم اختلاف بينهما في أن الجرائم والأدوات الإجرائية التي استحدثها مشروع ستانفورد لا تنطبق إلا فيما يتعلق بالهجمات على البنية التحتية للمعلومات والهجمات الإرهابية، في حين أن الأدوات المتعلقة بالقانون الإجرائي والتعاون الدولي المذكورة في اتفاقية الجريمة السيبرانية يمكن أن تنطبق على الجرائم التقليدية أيضاً.[904]

4.5 العلاقة بين النهج الدولية والتشريعية المختلفة

يدعو نجاح معايير شتى تأخذ بها البروتوكولات التقنية إلى التساؤل عن كيفية تجنب الصراعات بين النهج الدولية المختلفة.[905] وتشكل اتفاقية الجريمة السيبرانية في الوقت الحاضر الإطار الدولي الرئيسي الراهن الذي يغطي جميع الجوانب الهامة للجريمة السيبرانية، ولكن تناقش أيضاً مبادرات أخرى. ويتبع الاتحاد الدولي للاتصالات في الوقت الحاضر نهجاً دولياً ثانياً.[906] وقد اختارت القمة العالمية لمجتمع المعلومات الاتحاد الدولي للاتصالات ليكون الميسر لما يسمى خط العمل جيم5 للقمة العالمية لمجتمع المعلومات. ويتعلق خط العمل جيم5، كما عرفته مرحلة جنيف من القمة العالمية في عام 2003، ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.[907] وقد أكد الأمين العام للاتحاد الدولي للاتصالات، في اجتماع التيسير الثاني لمتابعة خط العمل جيم5، على أهمية التعاون الدولي في مكافحة الجريمة السيبرانية. وأعقب ذلك الإعلان عن إعداد البرنامج العالمي للأمن السيبراني التابع للاتحاد الدولي للاتصالات.[908] ويتوخى هذا البرنامج العالمي للأمن السيبراني سبعة أهداف رئيسية.[909] ويتمثل أحد هذه الأهداف في وضع استراتيجيات لإعداد تشريع نموذجي بشأن الجريمة السيبرانية. وقد أنشئ فريق خبراء ليعد الاستراتيجيات

---

[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.

[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.

المتعلقة بالبرنامج العالمي للأمن السيبراني.[910] وتتوقف الإجابة عن السؤال الخاص بكيفية تفاعل قانون نموذجي محتمل مع المعايير الراهنة على النهج المتبع في صوغ القانون النموذجي الجديد. وتوجد بوجه عام ثلاث علاقات ممكنة:

- قواعد تنظيمية مثيرة للخلاف

إذا حدد قانون نموذجي جديد معايير لا تتفق مع المعايير الراهنة فقد يكون لذلك، على الأقل في البداية، أثر سلبي على عملية تحقيق التواؤم الضرورية.

- حدوث ازدواجية جزئية مع معايير الاتفاقية

يمكن أن يستند القانون النموذجي الجديد إلى اتفاقية الجريمة السيبرانية ويمكن أن يزيل الأحكام التي أدت إلى صعوبات أو حتى منعت بعض البلدان من التوقيع على الاتفاقية. ومن الأمثلة على ذلك الحكم الذي كان موضع خلاف في المادة 32ب من اتفاقية الجريمة السيبرانية. فقد انتقد الوفد الروسي هذا الحكم إبان الاجتماع الذي عقدته لجنة الجريمة السيبرانية في عام 2007.[911]

- استكمال معايير الاتفاقية

يمكن أن يمضي قانون نموذجي جديد إلى مدى أبعد من المعايير التي حددتها اتفاقية الجريمة السيبرانية وأن يقوم، على سبيل المثال، بتجريم أعمال معينة تتعلق بالجريمة السيبرانية ويحدد أدوات إجرائية لم تكن الاتفاقية قد غطتها بعد. فمنذ عام 2001، استجد عدد من التطورات الهامة. فحين صيغت الاتفاقية، لم تكن جرائم "التصيد الاحتيالي"،[912] و"سرقة الهوية"[913] والجرائم المتعلقة بالألعاب المتاحة على الخط والشبكات الاجتماعية تتسم بنفس القدر من الأهمية الذي اكتسبته منذ ذلك الحين. وبمقدور قانون نموذجي جديد أن يواصل عملية تحقيق التواؤم بإدراج مزيد من الجرائم ذات البعد الدولي.[914]

وفي هذا الصدد، تستهدف مجموعة الأدوات المتعلقة بتشريعات الجريمة السيبرانية[915] التي وضعها الاتحاد الدولي للاتصالات تزويد البلدان بمواد مرجعية يمكن أن تساعدها في إنشاء إطار تشريعي لردع الجريمة السيبرانية. وتسلط هذه الأدوات الضوء على أهمية أن تحقق البلدان التواؤم بين أطرها القانونية من أجل مكافحة الجريمة السيبرانية بمزيد من الفعالية، وتيسير التعاون الدولي. وقد أُعدت مجموعة الأدوات المذكورة من قبل فريق خبراء دولي متعدد التخصصات، وطرح مشروع أول لها في مطلع عام 2009.

[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.

[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.

5.5 العلاقة بين النهج التشريعية الوطنية والدولية

تعد الجريمة السيبرانية بحق، كما سلفت الإشارة، جريمة عبر وطنية.[916] ولما كان الجناة يستطيعون، بوجه عام، أن يستهدفوا مستخدمين موجودين في أي بلد في العالم، فإن التعاون الدولي لوكالات إنفاذ القانون يعد شرطاً جوهرياً للتحقيقات الدولية في الجريمة السيبرانية.[917] فالتحقيقات تقتضي التعاون وتعتمد على تحقيق التواؤم بين القوانين. وإعمالاً للمبدأ المشترك المتعلق بالإجرام المزدوج،[918] يتطلب التعاون الفعال، بادئ ذي بدء، تحقيق التواؤم بين الأحكام الموضوعية للقانون الجنائي للحيلولة دون توافر ملاذات آمنة.[919] ومن الضروري، بالإضافة إلى ذلك، تحقيق التواؤم بين أدوات التحقيق لضمان امتلاك جميع البلدان المشاركة في تحقيق دولي لأدوات التحقيق اللازمة لإجراء التحقيقات. وأخيراً، يتطلب التعاون الفعال بين وكالات إنفاذ القانون إجراءات فعالة تتعلق بالجوانب العملية.[920] ولذا، فإن أهمية تحقيق التواؤم، وضرورة المشاركة في عملية تحقيق التواؤم هذه على الصعيد العالمي تشكلان على الأقل اتجاهاً، إن لم تشكلا ضرورة، لأي استراتيجية وطنية لمكافحة الجريمة السيبرانية.

1.5.5 أسباب شعبية النهج الوطنية

على الرغم من الاعتراف الواسع بأهمية تحقيق التواؤم، فإن عملية تنفيذ المعايير القانونية الدولية ما زالت لم تستكمل إلى حد بعيد.[921] ومن أسباب اضطلاع النهج الوطنية بدور هام في مكافحة الجريمة السيبرانية أن تأثير الجرائم ليس واحداً على النطاق العالمي. ومن الأمثلة على ذلك، النهج المتبع في مكافحة الرسائل الاقتحامية.[922] فهذه الرسائل تؤثر بوجه خاص على البلدان النامية، وقد حُللت هذه المسألة في تقرير صادر عن منظمة التعاون والتنمية في الميدان الاقتصادي.[923] فلما كانت الموارد في البلدان النامية أكثر ندرة وأعلى تكلفة، فإن الرسائل الاقتحامية تعد مشكلة أخطر في هذه البلدان عنها في البلدان الغربية.[924] ويعتبر اختلاف تأثيرات الجريمة السيبرانية، إلى جانب اختلاف الهياكل والتقاليد القانونية القائمة، السببين الرئيسيين لعدد كبير من المبادرات التشريعية المضطلع بها على المستوى الوطني والتي لا تتوخى، أو لا تتوخى إلا بشكل جزئي، تنفيذ المعايير الدولية.

2.5.5 الحلول الدولية في مقابل الحلول الوطنية

قد تثير هذه المناقشة الدهشة إلى حد ما لأن أي شخص يريد أن يتصل بالإنترنت يحتاج، في عصر العولمة التقنية هذا، إلى أن يستخدم البروتوكولات المعيارية (التقنية) الراهنة.[925] واتباع معايير واحدة شرط جوهري لتشغيل الشبكات. غير أن المعايير القانونية ما زالت تتباين، على عكس المعايير التقنية.[926] ويجب التساؤل عن مدى فعالية النهج الوطنية في ضوء البعد الدولي للجريمة السيبرانية.[927] وهذا سؤال له أهميته لجميع النهج الوطنية والإقليمية التي تطبق تشريعات لا تتفق مع المعايير الدولية الراهنة. والافتقار إلى تحقيق التواؤم يمكن أن يعوق بصورة خطيرة التحقيقات الدولية، في حين أن النهج الوطنية والإقليمية التي تمضي إلى مدى أبعد من المعايير الدولية تتجنب ما يصادف لدى إجراء التحقيقات الدولية من مشكلات وصعوبات.[928]

---

[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.*

[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.

وثمة سببان رئيسيان لتزايد عدد النهج الإقليمية والوطنية. والسبب الأول هو السرعة التشريعية. فمجلس أوروبا لا هو يستطيع إلزام الدول الأعضاء فيه بتوقيع اتفاقية الجريمة السيبرانية ولا هو يستطيع إلزام دولة وقعت الاتفاقية بأن تصدق عليها. ولذا تعتبر عملية تحقيق التواؤم في كثير من الأحيان عملية بطيئة بالقياس إلى النهج التشريعية الوطنية والإقليمية[929] أما الاتحاد الأوروبي فيملك، خلافاً لمجلس أوروبا، القوة المطلوبة لإلزام الدول الأعضاء بتنفيذ المقررات والتوجيهات الإطارية. وهذا هو السبب الذي يوضح لماذا عمد عدد من بلدان الاتحاد الأوروبي التي وقعت اتفاقية الجريمة السيبرانية في عام 2001، ولكنها لم تصدق عليها بعد، إلى القيام، مع ذلك، بتنفيذ المقرر الإطاري للاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات لعام 2005.

ويتعلق السبب الثاني بالاختلافات الوطنية والإقليمية. فبعض الأفعال لا تجرم إلا في بلدان معينة من إحدى المناطق. ومن الأمثلة على ذلك الجرائم الدينية.[930] وعلى الرغم من أن تحقيق التواؤم الدولي بين أحكام القانون الجنائي المتعلقة بالجرائم ضد الرموز الدينية لن يكون ممكناً على الأرجح، فإن اتباع نهج وطني يمكنه أن يضمن في هذا الصدد إمكانية الحفاظ على المعايير القانونية المطبقة في البلد المعني.

3.5.5 صعوبات النهج الوطنية

تواجه النهج الوطنية عدداً من المشكلات. ففيما يتعلق بالجرائم التقليدية يمكن أن يؤثر القرار الذي يتخذه بلد واحد، أو عدد قليل من البلدان، بتجريم سلوكيات معينة على قدرة الجناة على الإتيان بأفعالهم في تلك البلدان. ولكن عندما يتعلق الأمر بجرائم الإنترنت، فإن قدرة بلد واحد على التأثير في الجناة تكون أقل كثيراً لأن الجناة يستطيعون، بوجه عام، الإتيان بأفعالهم من أي مكان موصول بالشبكة.[931] فإذا ما أتى الجناة بأفعالهم في بلد لا يجرم سلوكاً معيناً، فإن التحقيقات الدولية، فضلاً عن طلبات تسليم الجناة، ستمنى بالفشل في كثير من الأحيان. ولذا، فإن من الأهداف الرئيسية للنهج القانونية الدولية الحيلولة دون إيجاد تلك الملاذات الآمنة عن طريق وضع وتطبيق معايير عالمية.[932] وبناء على ذلك، تتطلب النهج الوطنية بوجه عام تدابير جانبية إضافية كي تصبح مؤثرة.[933] ومن أكثر التدابير الجانبية انتشاراً ما يلي:

- تجريم استخدام المحتوى غير القانوني بالإضافة إلى تقديمه

يتمثل أحد النهج في تجريم استخدام الخدمات غير القانونية بالإضافة إلى تجريم تقديم هذه الخدمات. فتجريم أفعال المستخدمين الموجودين داخل الولاية القضائية نهج يستهدف التعويض عن غياب التأثير على مقدم الخدمات الذي يعمل من الخارج.

- تجريم الخدمات المستخدمة في ارتكاب الجريمة

ويتمثل نهج ثان في تنظيم، بل وتجريم، تقديم خدمات معينة داخل الولاية القضائية تستخدم في أغراض إجرامية. ويمضي هذا الحل إلى مدى أبعد من النهج الأول لأنه يتعلق بالشركات والمنظمات التي توفر خدمات محايدة تستخدم في أنشطة قانونية وأنشطة غير قانونية. ومن الأمثلة على هذا النهج قانون إنفاذ حظر المقامرة غير القانونية على الإنترنت لعام 2006 في الولايات المتحدة.[934]

[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.
[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.

ومما يتعلق عن كثب بهذا التدبير فرض التزامات بترشيح محتوى معين متاح على الإنترنت.[935] وقد نوقش هذا النهج في إطار القرار الشهير المتعلق بياهو Yahoo،[936] وهو يناقش في الوقت الحاضر في إسرائيل، حيث ينبغي لمقدمي خدمة النفاذ إن يلتزموا بتقييد النفاذ إلى مواقع الويب التي تتضمن محتوى خاصاً بالكبار. ولا تقتصر المحاولات الرامية إلى التحكم في محتوى الإنترنت على المحتوى الخاص بالكبار؛ فبعض البلدان تستخدم تكنولوجيا الترشيح لتقييد النفاذ إلى مواقع الويب التي تتناول موضوعات سياسية. وقد أفادت مبادرة الشبكة المفتوحة (OpenNet Initiative)[937] أن هذا النوع من الرقابة يمارس من جانب ما يزيد على عشرين بلداً.[938]

[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.*

[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.

6 الاستجابة القانونية

يقدِّم الفصل التالي عرضاً عاماً للاستجابة القانونية لظاهرة الجريمة السيبرانية من خلال توضيح النُهج القانونية لتجريم بعض الأفعال.[939] وستُعرض النُهج الدولية كلما أمكن. أما في تلك الحالات التي لا توجد فيها نُهج دولية فسوف تُعرض أمثلة للنُهج الوطنية أو الإقليمية.

1.6 *القانون الجنائي الموضوعي*

1.1.6 النفاذ غير القانوني (القرصنة)

منذ تطوير شبكات الحاسوب وقدرتها على توصيل الحواسيب وإتاحة النفاذ إلى الأنظمة الحاسوبية الأخرى أمام المستعملين ظل القراصنة يستعملون الحواسيب لأغراض إجرامية.[940] وتتباين حوافز القراصنة تبايناً كبيراً.[941] وليس من الضروري أن يتواجد القراصنة في مسرح الجريمة؛[942] إذ إنهم يحتاجون فقط إلى الالتفاف على الحماية التي تؤمِّن الشبكة.[943] وفي كثير من حالات النفاذ غير القانوني تكون أنظمة الأمن التي تحمي الموقع المادي لعتاد الشبكة أكثر تعقيداً عن نُظم الأمن التي تحمي المعلومات الحساسة في الشبكات حتى ولو كانت في نفس المبنى.[944]

والنفاذ غير القانوني إلى أنظمة الحواسيب يعوق مشغلي الحواسيب عن إدارة وتشغيل ومراقبة أنظمتهم بدون إزعاج أو موانع.[945] وهدف الحماية هو الحفاظ على سلامة الأنظمة الحاسوبية.[946] ومن الأهمية الحاسمة التمييز بين النفاذ غير القانوني وما يعقبه من جرائم (مثل التجسُّس على البيانات[947])، نظراً لأن نقطة تركيز الحماية تختلف في الأحكام القانونية. وفي معظم الحالات لا يكون النفاذ غير القانوني (عندما يهدف القانون إلى حماية سلامة النظام الحاسوبي ذاته) هو الهدف النهائي، ولكنه يمثِّل بالأحرى الخطوة الأولى صوب ارتكاب جرائم أخرى، مثل تعديل البيانات المخزَّنة أو الحصول عليها (عندما يسعى القانون إلى حماية سلامة وسرية البيانات).[948]

والسؤال هو ما إن كان ينبغي تجريم فعل النفاذ غير القانوني بالإضافة إلى الجرائم اللاحقة؟[949] ويتضح من تحليل مختلف نُهج تجريم النفاذ غير القانوني إلى الحواسيب على الصعيد الوطني أن الأحكام المطبَّقة تخلط في بعض الأحيان بين النفاذ غير القانوني والجرائم اللاحقة، أو تسعى إلى اقتصار تجريم النفاذ غير القانوني على الانتهاكات الخطيرة وحدها.[950] وتجرِّم بعض البلدان مجرَّد النفاذ في حين تقصر بلدان أخرى التجريم على الجرائم في الحالات التي يكون فيها النظام الحاسوبي المخترق خاضعاً لحماية تدابير أمنية، أو عندما يكون لدي الجاني نية إحداث ضرر، أو في حالات الحصول على بيانات أو تعديلها أو إفسادها.[951] ولا تجرِّم بلدان أخرى النفاذ بحد ذاته ولكنها تجرِّم الجرائم اللاحقة.[952] ويشير معارضو

---

[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.

[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.

تجريم النفاذ غير القانوني إلى الحالات التي لا يحدث فيها خطر بمجرَّد التدخل أو إذا كانت أفعال ''القرصنة'' قد أدَّت إلى اكتشاف ثغرات ونقاط ضعف في أمن الأنظمة الحاسوبية المستهدفة.[953]

الاتفاقية المتعلقة بالجريمة الإلكترونية

تشمل الاتفاقية المتعلقة بالجريمة الإلكترونية حكماً بشأن النفاذ غير القانوني يحمي سلامة الأنظمة الحاسوبية بتجريم النفاذ غير المأذون به إلى النظام. ومع ملاحظة النُهج غير المتسقة على الصعيد الوطني،[954] تعرض الاتفاقية إمكانية وضع حدود تؤدي – في معظم الحالات على الأقل – إلى تمكين البلدان التي ليس لديها تشريع من الاحتفاظ بقوانين أكثر حرية بشأن النفاذ غير القانوني.[955]

الحكم:

المادة 2 – الدخول الغير مشروع:

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما أُرتكب عمداً، وبغير حق: الدخول على كامل أو على جزء من منظومة كمبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات كمبيوتر أو بقصد آخر غير أمين، أو فيما يتعلق بمنظومة كمبيوتر متصلة بمنظومة كمبيوتر أخرى.

الأفعال المشمولة:

لا يحدِّد مصطلح ''الدخول'' وسيلة معيَّنة للاتصال، ولكنه مصطلح مفتوح الحدود ويمكن أن تدخل عليه تطورات تقنية أخرى.[956] ويشمل جميع وسائل النفاذ إلى منظومة حاسوبية أخرى، بما في ذلك هجمات الإنترنت[957]، وكذلك النفاذ غير القانوني إلى الشبكات اللاسلكية. بل إن هذا الحكم يشمل أيضاً النفاذ غير المأذون به إلى حواسيب غير متصلة بأي شبكة (مثل الالتفاف وحماية كلمة المرور).[958] وهذا النهج الواسع يعني أن النفاذ غير المشروع لا يشمل فقط التطورات التقنية المقبلة ولكنه يشمل أيضاً البيانات السرية التي ينفذ إليها المطَّلعون والعاملون.[959] والجملة الثانية من المادة 2 تتيح إمكانية اقتصار تجريم النفاذ غير القانوني على النفاذ عبر شبكة.[960]

وهكذا وضع تعريف للأفعال غير القانونية والأنظمة المحمية بحيث يبقى مفتوحاً لاحتمالات التطورات المقبلة. ويتضمن التقرير التفسيري قائمة بالعتاد والمكوِّنات والبيانات المخزونة والأدلة وبيانات الحركة والبيانات المتصلة بالمحتوى باعتبارها أمثلة لأجزاء أنظمة الحواسيب التي يمكن النفاذ إليها.[961]

---

[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.

[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.

العنصر الذهني:

كما حدث في حالة جميع الجرائم الأخرى المعرَّفة في الاتفاقية المتعلقة بالجريمة الإلكترونية، تقتضي المادة 2 أن يرتكب الجاني جريمته عمداً.[962] ولا تتضمن الاتفاقية تعريفاً لمصطلح ''عمداً''. وفي التقرير التفسيري يشير واضعو الاتفاقية إلى أن تعريف ''عمداً'' ينبغي أن يجري على صعيد وطني.[963]

بغير حق:

لا يمكن ملاحقة النفاذ إلى الحاسوب بموجب المادة 2 من الاتفاقية إلاّ إذا حدث ''بغير حق''.[964] أما الدخول إلى نظام يسمح بنفاذ مجاني ومفتوح للجمهور أو نفاذ إلى نظام بإذن من مالك النظام أو غيره من أصحاب الحق فلا يعتبر ''بغير حق''.[965] وبالإضافة إلى موضوع النفاذ بحرية، نوقشت أيضاً شرعية إجراء اختبار الأمن.[966] وكان مديرو الشبكات وشركات الأمن التي تختبر حماية النُظم الحاسوبية من أجل تعيين الفجوات المحتملة في تدابير الأمن يشعرون بالتوجس من احتمال التجريم بموجب النفاذ غير القانوني.[967] ورغم أن هؤلاء المهنيين يعملون عموماً بإذن من المالك وبالتالي يعملون بصورة قانونية، فإن واضعي نص الاتفاقية أكدوا على أن ''اختبار أو حماية أمن النظام الحاسوبي بإذن من جانب المالك أو المشغِّل، [...] يجري بحق''.[968]

ولكن قيام ضحية الجريمة بتسليم كلمة مرور أو رمز نفاذ مشابه إلى الجاني لا يعني بالضرورة أن الجاني قد تصرَّف بحق عند نفاذه إلى النظام الحاسوبي الخاص بالضحية. وإذا أقنع الجاني الضحية بالكشف عن كلمة مرور أو شفرة النفاذ على أساس اقتراب احتيالي اجتماعي ناجح[969] فسيكون من الضروري التحقق مما إذا كان الإذن الذي أعطاه الضحية يشمل فعلاً التصرُّف الذي قام به الجاني.[970] ولكن الأمر لا يكون على هذا النحو عموماً ولذلك يكون الجاني قد تصرف بغير حق.

التقييدات والتحفظات:

تتيح الاتفاقية كبديل لهذا النهج العريض إمكانية تقييد التجريم بعناصر إضافية يرد ذكرها في الجملة الثانية.[971] وتنص المادة 42 من الاتفاقية على الإجراءات التي يمكن بها استخدام هذا التحفُّظ.[972] والتحفظات المحتملة تتصل بالتدابير الأمنية،[973] أو قصد الحصول على بيانات الحاسوب،[974]

---

[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.

[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.*

[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.

أو القصد الآخر غير الأمين الذي يبرِّر الجُرم الجنائي، أو اقتضاء ارتكاب الجريمة ضد نظام حاسوبي من خلال شبكة.[975] ويمكن الاطلاع على نهج مشابه في القرار الصادر عن الاتحاد الأوروبي[976] باسم القرار الإطاري بشأن الهجمات ضد أنظمة المعلومات.[977]

قانون الكومنولث النموذجي بشأن الجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في المادة 5 من قانون الكومنولث النموذجي لعام 2002.[978]

المادة 5

أي شخص يقوم عمداً وبدون عذر أو مبرِّر مشروع بالنفاذ إلى نظام حاسوبي بأكمله أو إلى جزء منه يرتكب جريمة يعاقب عليها في حالة الإدانة بالحبس لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.

والاختلاف الرئيسي عن الاتفاقية المتعلقة بالجريمة الإلكترونية هو أن المادة 5 من قانون الكومنولث النموذجي لا تتضمن خيارات لإبداء تحفظات، بعكس المادة 2 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

مشروع اتفاقية ستانفورد

يعترف مشروع اتفاقية ستانفورد غير الرسمي[979] لعام 1999 بالنفاذ غير المشروع باعتباره أحد الجرائم التي ينبغي أن تجرمها الولايات الموقِّعة على مشروع الاتفاقية.

الحكم:

المادة 3 – الجرائم

1 تكون الجرائم المنصوص عليها بموجب هذه الاتفاقية قد ارتكبت إذا قام أي شخص بصورة غير مشروعة وعمداً بالانخراط في أي سلوك مذكور أدناه بدون سلطة أو تصريح أو موافقة معترف بها قانوناً:

[...]

(ج) الدخول في نظام سيبراني يكون النفاذ إليه مقيَّداً بطريقة ظاهرة لا لبس فيها؛

[...]

---

[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.

الأفعال المشمولة:

يظهر في مشروع الحكم عدد من نقاط التشابه مع المادة 2 من الاتفاقية المتعلقة بالجريمة الإلكترونية. فالإثنان يتطلبان ارتكاب الفعل عمداً وبدون حق/بدون سلطة. وفي هذا السياق، فإن الاقتضاء الوارد في مشروع الحكم (*"بدون سلطة أو تصريح أو موافقة معترف بها قانوناً"*) أكثر دقة من مصطلح "بغير حق"[980] المستعمل في الاتفاقية المتعلقة بالجريمة الإلكترونية ويهدف صراحة إلى إدخال مفهوم الدفاع عن النفس.[981] والاختلاف الرئيسي عن الاتفاقية هو أن مشروع الحكم يستخدم مصطلح "نظام سيبراني". والنظام السيبراني معرَّف في الفقرة 3 من المادة 1 من مشروع الاتفاقية. وهو يغطي أي حاسوب أو شبكة حواسيب تستعمل لإرسال أو إحالة أو تنسيق أو مراقبة اتصالات بيانات أو برامج. ويظهر من هذا التعريف كثير من نقاط التشابه مع تعريف مصطلح "منظومة كمبيوتر" المنصوص عليه في الفقرة (أ) من المادة 1 من الاتفاقية المتعلقة بالجريمة الإلكترونية.[982] ورغم أن مشروع الاتفاقية يشير إلى أفعال تتصل بتبادل البيانات، وبالتالي لا يركّز أساساً على الأنظمة الحاسوبية القائمة على الشبكات، فإن كلا التعريفين يشملان الحواسيب المتصلة توصيلاً بينياً إلى جانب الأجهزة القائمة بذاتها.[983]

2.1.6 التجسس على البيانات

تتضمن الاتفاقية المتعلقة بالجريمة الإلكترونية وكذلك قانون الكومنولث النموذجي ومشروع اتفاقية ستانفورد حلولاً قانونية للاعتراض غير المشروع فقط.[984] ومن المشكوك فيه أن المادة 3 من الاتفاقية المتعلقة بالجريمة الإلكترونية تنطبق على حالات أخرى خلاف الحالات التي تنطوي على ارتكاب جرائم من خلال اعتراض عمليات نقل البيانات. وكما يلاحظ أدناه،[985] نوقشت باهتمام كبير مسألة ما إن كان النفاذ غير القانوني إلى المعلومات المخزونة على قرص صلب تدخل في عداد المسائل التي تشملها الاتفاقية.[986] ونظراً لأن عملية النقل عملية مطلوبة، فمن المرجَّح أن المادة 3 من الاتفاقية المتعلقة بالجريمة الإلكترونية لا تغطي أشكال التجسُّس على البيانات خلاف اعتراض عمليات النقل.[987]

ومن القضايا التي تناقش كثيراً في هذا السياق مسألة ما إن كان تجريم عمليات النفاذ غير القانوني يجعل من تجريم التجسُّس على البيانات غير ضروري. ففي الحالات التي يستطيع فيها الجاني النفاذ بصورة مشروعة إلى النظام الحاسوبي (بسبب إعطائه أمراً بإصلاح النظام مثلاً) ثم يقوم في هذه المناسبة (انتهاكاً للإذن الشرعي المحدود) بنقل ملفات من النظام، فإن الفعل لا يكون مشمولاً عموماً بأحكام تجريم النفاذ غير القانوني.[988]

ونظراً لتخزين الكثير من البيانات الحيوية اليوم في الأنظمة الحاسوبية، فمن الجوهري تقييم ما إن كانت الآليات القائمة لحماية البيانات هي آليات كافية أو ما إن كان من الضروري وجود أحكام أخرى في القانون الجنائي لحماية المستعمل من التجسُّس على البيانات.[989] واليوم يستطيع مستعملو الحاسوب استعمال مختلف أجهزة العتاد وأدوات البرمجيات لحماية المعلومات السرية. فهم يستطيعون إقامة حواجز نيران للحماية أو

---

[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.

[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.

أنظمة مراقبة النفاذ أو تشفير المعلومات المخزونة ويستطيعون بذلك تقليل خطر التجسُّس على البيانات.[990] ورغم أن الأجهزة سهلة الاستعمال متوفِّرة ولا تتطلَّب سوى معارف محدودة من جانب المستعملين، فإن الحماية الفعَّالة حقاً للبيانات في النظام الحاسوبي تتطلب في كثير من الأحيان معرفة لا يملكها سوى قلَّة من المستعملين.[991] وبصورة خاصة لا تتمتع البيانات المخزونة في أنظمة الحواسيب الخاصة في كثير من الأحيان بحماية كافية من التجسُّس على البيانات. ولذلك يمكن أن تتيح أحكام القانون الجنائي حماية إضافية.

أمثلة:

قرَّرت بعض البلدان توسيع الحماية المتوفِّرة من خلال تدابير تقنية وذلك بتجريم التجسُّس على البيانات. وهناك نهجان رئيسيان في التعامل مع هذه المسألة. فبعض البلدان تعتنق نهجاً ضيقاً وتجرِّم التجسُّس على البيانات عندما يقتصر ذلك على الحصول على بيانات سرية محدَّدة – ومن أمثلة ذلك البند 1831 من العنوان 18 من مدونة الولايات المتحدة (18 U.S.C § 1831) لتجريم التجسُّس الاقتصادي. وهذا الحكم لا يغطي فقط التجسُّس على البيانات ولكنه يغطي الطرق الأخرى للحصول على المعلومات السرية أيضاً.

البند 1831 – التجسُّس الاقتصادي

(أ) عموماً – أي شخص قاصداً أو عالماً أن الجريمة ستفيد أي حكومة أجنبية أو أداة أجنبية أو عميل أجنبي وعن علم –

(1) يقوم بسرقة أي سر تجاري أو يقوم بدون إذن بمصادرته أو أخذه أو نقله أو إخفائه أو يحصل عليه عن طريق الغش أو الخديعة أو التضليل؛

(2) أو يقوم، بدون إذن، بنسخ سر تجاري أو نقله أو رسمه أو تخطيطه أو تصويره فوتوغرافياً أو تنزيله أو تحميله أو تغييره أو تدميره أو تصويره ضوئياً أو استنساخه أو إرساله بوسائل الاتصالات أو توصيله أو إرساله بالبريد أو غيره أو تبليغه أو نقله؛

(3) أو يقوم باستلام أو شراء أو امتلاك سر تجاري مع معرفته بسرقة هذا السر أو مصادرته أو امتلاكه أو تحويله بدون إذن؛

(4) أو يحاول ارتكاب أي جريمة موصوفة في الفقرات من (1) إلى (3)؛

(5) أو يتآمر مع شخص أو أكثر لارتكاب أي جريمة موصوفة في أي فقرة من الفقرات (1) إلى (3) ومع شخص أو أكثر للقيام بأي فعل لتنفيذ غرض التآمر،

يتعرَّض، باستثناء ما جاء في المادة الفرعية (ب)، لغرامة لا تزيد عن 000 500 دولار أو السجن لمدة لا تزيد عن 15 سنة أو كلاهما.

(ب) المنظمات – أي منظمة ترتكب أي جريمة موصوفة في الفقرة الفرعية (أ) تتعرَّض لغرامة لا تزيد عن 000 000 10 دولار.

وقد اعتنقت بلدان أخرى نهجاً أوسع وجرَّمت فعل الحصول على البيانات المخزونة في الحواسيب حتى إذا لم تكن تتضمن أسراراً اقتصادية. ومن أمثلة ذلك الصيغة السابقة للمادة 202 أ من قانون العقوبات الألماني.[992]

المادة 202 أ – التجسُّس على البيانات:

(1) أي شخص يحصل، بدون إذن، لنفسه أو لغيره، على بيانات غير مخصَّصة له وتخضع لحماية خاصة من النفاذ غير المأذون به يعاقب بالحبس لمدة لا تزيد عن ثلاث سنوات أو بغرامة.

(2) البيانات المشمولة بالفقرة 1 هي فقط البيانات المخزونة أو المنقولة إلكترونياً أو مغناطيسياً أو بأي شكل لا يكون مرئياً بصورة مباشرة.

---

[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.

[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.

وهذا الحكم لا يغطي فقط الأسرار الاقتصادية ولكنه يغطي البيانات المخزونة في الحاسوب عموماً.[993] ومن ناحية أهداف الحماية يعتبر هذا النهج أكثر اتساعاً بالمقارنة بالبند 1831 من العنوان 18 من مدونة الولايات المتحدة ولكن تطبيق هذا الحكم محدود نظراً لأن تجريم الحصول على البيانات يقتصر على الحالة التي تكون فيها هذه البيانات خاضعة لحماية خاصة من النفاذ غير المأذون.[994] وهكذا، فإن حماية البيانات المخزونة في الحواسيب بموجب القانون الجنائي الألماني تقتصر على حالة الأشخاص أو الشركات التجارية التي تتخذ تدابير لتجنُّب وقوعها ضحية لهذه الجرائم.[995]

أهمية هذا الحكم:

تطبيق هذا الحكم هام بصفة خاصة في صدد الحالات التي يكون فيها مرتكب الجُرم حاصلاً على إذن بالدخول إلى النظام الحاسوبي (وذلك مثلاً بسبب تلقيه أمراً بإصلاح مشكلة في الحاسوب) ثم يسئ استغلال هذا الإذن للحصول بصورة غير مشروعة على معلومات مخزونة في النظام الحاسوبي.[996] وفيما يتعلق بمسألة تغطية هذا التصريح للنفاذ إلى النظام الحاسوبي، فإنه ليس من الممكن عموماً أن يندرج هذا الإذن تحت الأحكام التي تجرِّم النفاذ غير القانوني.

من غير حق:

يتطلب تطبيق الأحكام المتصلة بالتجسُّس على البيانات عموماً أن تكون البيانات التي يتم الحصول عليها بدون موافقة الضحية. ونجاح هجمات التصيُّد الاحتيالي[997] يثبت بوضوح نجاح الرسائل الاقتحامية استناداً إلى التلاعب بالمستعملين.[998] ولا يمكن، استناداً إلى الأحكام المذكورة أعلاه، ملاحقة الجناة الذين ينجحون في التلاعب بالمستعملين للإفصاح عن المعلومات السرية، وذلك نظراً لموافقة الضحية.

3.1.6 الاعتراض غير القانوني

يقترن استعمال تكنولوجيا المعلومات والاتصالات بعدة مخاطر تتصل بأمن نقل المعلومات.[999] وعلى العكس من عمليات طلبات البريد التقليدية في داخل أي بلد، تنطوي عمليات نقل البيانات عبر الإنترنت على مشاركة العديد من مقدمي الخدمات ومختلف النقاط التي يمكن عندها اعتراض نقل البيانات.[1000] وأضعف نقطة للاعتراض هي المستعمل، وخاصة مستعمل الحاسوب المنزلي الخاص، الذي لا يتمتع في كثير من الأحيان بحماية كافية من الهجمات الخارجية. ونظراً لأن الجناة يستهدفون عموماً النقطة الأضعف، فإن خطر الهجمات ضد المستعملين الخاصين خطر كبير وخاصة في ضوء ما يلي:

- تطوير تكنولوجيات يسهل اختراقها؛
- اكتساب المعلومات الشخصية أهمية أكبر للجناة.

---

[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; *Tadros*, 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.

[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.

وتتيح تكنولوجيات الشبكات الجديدة (مثل "شبكة المنطقة المحلية اللاسلكية") عدة مزايا للنفاذ إلى الإنترنت.[1001] وعلى سبيل المثال، يسمح إنشاء شبكة لا سلكية في المسكن الخاص للأُسرة بالتوصيل بالإنترنت من أي مكان في داخل دائرة معيَّنة، دون الحاجة إلى توصيلات سلكية. ولكن يقترن الإقبال على هذه التكنولوجيا والراحة الناشئة عنها بمخاطر جدية على أمن الشبكة. وإذا توافرت شبكة لا سلكية بدون حماية، فإن الجناة يستطيعون الدخول إلى هذه الشبكة واستعمالها لأغراض إجرامية بدون الحاجة إلى الدخول إلى المبنى. إذ إنهم يحتاجون فقط إلى الدخول داخل دائرة الشبكة اللاسلكية لإطلاق هجومهم. وتشير الاختبارات الميدانية إلى أن نسبة تصل إلى 50 في المائة من الشبكات اللاسلكية الخاصة لا تتمتع في بعض الأماكن بأي حماية ضد الاعتراض غير المأذون أو النفاذ غير المأذون.[1002] وفي معظم الحالات ينشأ الافتقار إلى الحماية عن الافتقار إلى المعرفة بطريقة تشكيل تدابير الحماية.[1003]

وفي الماضي، كان الجناة يركزون أساساً على الشبكات التجارية لاعتراضها بصورة غير قانونية.[1004] إذ إن اعتراض مراسلات الشركات يولِّد على الأرجح معلومات ذات فائدة أكبر من البيانات المنقولة داخل الشبكات الخاصة. ويشير ارتفاع عدد حالات انتحال هوية البيانات الشخصية الخاصة إلى أن نقطة تركيز الجناة ربما تكون قد تغيَّرت.[1005] فقد أصبحت البيانات الخاصة، مثل أرقام بطاقات الائتمان وأرقام الضمان الاجتماعي[1006]، وكلمات المرور ومعلومات الحسابات المصرفية ذات أهمية كبيرة للجناة.[1007]

الاتفاقية المتعلقة بالجريمة الإلكترونية

تشمل الاتفاقية المتعلقة بالجريمة الإلكترونية حكماً لحماية سلامة الإرسالات غير العامة بتجريم الاعتراض غير المأذون. ويهدف هذا الحكم إلى مساواة حماية عمليات النقل الإلكترونية بحماية المحادثات الصوتية من التنصُّت و/أو التسجيل غير القانوني، وهي الحماية الموجودة بالفعل في معظم الأنظمة القانونية.[1008]

الحكم:

المادة 3 – الاعتراض الغير مشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً، وبغير حق: الاعتراض باستخدام وسائل فنية، لعمليات إرسال غير عمومية لبيانات كمبيوتر إلى أو من أو خلال منظومة كمبيوتر، بما في ذلك ما ينبعث من منظومة كمبيوتر من موجات كهرمغنطيسية تحمل هذه البيانات. يجوز لطرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات كمبيوتر أو بقصد آخر غير أمين، أو فيما يتعلق بمنظومة كمبيوتر متصلة بمنظومة كمبيوتر أخرى.

[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.

[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.

الأفعال المشمولة:

يقتصر انطباق المادة 3 على اعتراض الإرسالات الذي يتحقق بتدابير تقنية.[1009] والاعتراضات التي تتصل بالبيانات الإلكترونية يمكن تعريفها بأنها فعل بقصد الحصول على بيانات أثناء عملية النقل.[1010] وكما جاء أعلاه، يثور الجدل عند مناقشة مسألة تغطية النفاذ غير القانوني إلى المعلومات المخزونة على قرص صلب بموجب هذا الحكم.[1011] وعموماً ينطبق الحكم فقط على اعتراض الإرسالات – وعدم اعتبار النفاذ إلى المعلومات المخزونة اعتراضاً لعملية الإرسال.[1012] ومناقشة تطبيق الحكم حتى في الحالات التي ينفذ فيها الجاني مادياً إلى نظام حاسوبي قائم بذاته هي مناقشة تنشأ في جانب منها لأن الاتفاقية المتعلقة بالجريمة الإلكترونية لا تتضمن حكماً يتصل بالتجسُّس على البيانات[1013] ولأن التقرير التفسيري للاتفاقية يتضمن تفسيرين غير دقيقين إلى حد ما بشأن تطبيق المادة 3:

- يشير التقرير التفسيري أولاً إلى أن الحكم يغطي عمليات الاتصال التي تجري داخل منظومة حاسوبية.[1014] ومع ذلك، فإن ذلك يترك دون حسم مسألة ما إن كان الحكم ينبغي أن ينطبق في الحالات التي يرسل فيها الضحايا بيانات يتم بعد ذلك اعتراضها من جانب الجناة أو ما إن كان ينبغي أن ينطبق أيضاً عندما يقوم الجاني بتشغيل الحاسوب بنفسه.

- ويشير الدليل إلى أن الاعتراض يمكن ارتكابه إما بصورة غير مباشرة من خلال استعمال أجهزة التنصُّت أو ''من خلال النفاذ إلى المنظومة الحاسوبية واستعمالها''.[1015] وإذا تمكَّن الجناة من النفاذ إلى منظومة حاسوبية واستعمالها لإصدار نُسخ غير مأذون بها من البيانات المخزونة على محرِّك قرص خارجي، وعندما يؤدي هذا الفعل إلى نقل بيانات (إرسال بيانات من القرص الصلب الداخلي إلى قرص صلب خارجي)، فإن الجاني لا يكون قد *اعترض* هذه العملية ولكنه *بدأها*. وعدم وجود عنصر الاعتراض التقني حُجة قوية ضد تطبيق الحكم في حالات النفاذ غير القانوني إلى المعلومات المخزونة.[1016]

ويغطي مصطلح ''الإرسال'' جميع عمليات إرسال البيانات، سواء كان ذلك بالهاتف أو الفاكس أو البريد الإلكتروني أو نقل الملفات.[1017] وتنطبق الجريمة المحدَّدة بموجب المادة 3 على الإرسالات غير العمومية فقط.[1018] ويكون الإرسال ''غير عمومي'' إذا كانت عملية الإرسال سرية.[1019] والعنصر الجوهري للتمييز بين الإرسالات العمومية وغير العمومية ليس طابع البيانات المرسلة ولكنه طابع عملية الإرسال ذاتها. وحتى نقل المعلومات المتوفِّرة بصورة علنية يمكن اعتباره إجرامياً إذا كان الأطراف المنخرطون في النقل يعتزمون إبقاء محتوى اتصالاتهم سرياً. واستعمال الشبكات العمومية لا يستبعد الاتصالات ''غير العمومية''.

[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.

[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.

العنصر الذهني:

كما حدث في حالة جميع الجرائم الأخرى المعرَّفة في الاتفاقية المتعلقة بالجريمة الإلكترونية، تقتضي المادة 3 أن يرتكب الجاني جريمته عمداً.[1020] ولا تتضمن الاتفاقية تعريفاً لمصطلح ''عمداً''. وفي التقرير التفسيري يشير واضعو الاتفاقية إلى أن تعريف ''عمداً'' ينبغي أن يجري على صعيد وطني.[1021]

بغير حق:

لا يمكن ملاحقة اعتراض الاتصال بموجب المادة 3 من الاتفاقية إلاّ إذا وقع هذا الاعتراض ''بغير حق''.[1022] ويقدِّم واضعو الاتفاقية مجموعة من الأمثلة لعمليات الاعتراض التي لا تجري بغير حق:

- التصرُّف بناءً على تعليمات أو إذن من جانب المشاركين في عملية الإرسال؛[1023]
- الاختبار المأذون أو أنشطة الحماية المأذونة التي يوافق عليها المشاركون؛[1024]
- الاعتراض القانوني استناداً إلى أحكام القانون الجنائي أو لصالح الأمن القومي.[1025]

وأثيرت قضية أخرى في إطار المفاوضات بشأن الاتفاقية وهي مسألة ما إذا كان استعمال ملفات الارتباط ''الكوكيز'' تؤدي إلى جزاءات جنائية بموجب المادة 3.[1026] وأشار واضعو الاتفاقية إلى أن الممارسات التجارية الشائعة (مثل ملفات الكوكيز) لا تعتبر عمليات اعتراض بغير حق.[1027]

التقييدات والتحفُّظات:

تتيح المادة 3 خيار تقييد التجريم باشتراط عناصر إضافية يرد ذكرها في الجملة الثانية، وتشمل ''قصد غير أمين'' أو الصلة بمنظومة حاسوبية متصلة بمنظومة حاسوبية أخرى.

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مماثل في المادة 8 من قانون الكومنولث النموذجي لعام 2002.[1028]

المادة 8

عندما يعترض أي شخص بوسائل تقنية عمداً وبدون عذر أو مبرِّر قانوني:

(أ) أي إرسال غير عمومي إلى منظومة حاسوبية أو منها أو في داخلها؛

(ب) أو إرسالات كهرمغنطيسية من منظومة حاسوبية تحمل بيانات حاسوبية؛ فإنه يرتكب جريمة يعاقب عليها في حالة الإدانة بالسجن لفترة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.

[1020] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[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.

مشروع اتفاقية ستانفورد

لا يجرِّم مشروع اتفاقية ستانفورد غير الرسمي[1029] لعام 1999 صراحة اعتراض البيانات الحاسوبية.

4.1.6 التدخل في البيانات

تُعتبر حماية الأشياء الملموسة أو المادية من الضرر المتعمَّد عنصراً تقليدياً في التشريعات العقابية الوطنية. ومع استمرار الرقمنة يتم تخزين مزيد من المعلومات التجارية الحرجة في شكل بيانات.[1030] ويمكن أن تؤدي الهجمات أو الحصول على هذه المعلومات إلى خسائر مالية.[1031] وإلى جانب حذف هذه المعلومات، فإن تغييرها يمكن أيضاً أن ينطوي على عواقب جسيمة.[1032] ولم تحقِّق التشريعات السابقة في بعض الحالات حماية كاملة للبيانات تماشياً مع حماية الأشياء الملموسة. وأدّى ذلك إلى تمكين الجناة من تصميم اقتحامات لا تؤدي إلى جزاءات جنائية.[1033]

الاتفاقية المتعلقة بالجريمة الإلكترونية

تتضمَّن الاتفاقية المتعلقة بالجريمة الإلكترونية في المادة 4 حكماً يحمي سلامة البيانات من التداخل غير المأذون.[1034] وهدف الحكم هو ملء الثغرات القائمة في بعض قوانين العقوبات الوطنية وتوفير حماية لبيانات الحواسيب وبرامج الحواسيب على نسق الحماية التي تتمتَّع بها الأشياء الملموسة من تعمُّد إلحاق الضرر.[1035]

الحكم:

المادة 4 – التدخُّل في البيانات

(1) تعتمد كل دولة طرق ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً، وبغير حق: إتلاف، أو محو، أو إفساد، أو تعديل، أو تدمير بيانات موجودة على كمبيوتر.

(2) يجوز لطرف أن يحتفظ بحقه في أن يستلزم أن تتسبَّب الأفعال الموضَّحة بالفقرة 1 في ضرر جسيم.

[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.

الأفعال المشمولة:

- يعني مصطلحا ''إتلاف'' و''إفساد'' أي فعل يتصل بالتعديل السلبي لسلامة المحتوى المعلوماتي في البيانات والبرامج؛[1036]
- ومصطلح ''محو'' يغطي أي أفعال يتم بموجبها إزالة المعلومات من وسيط التخزين ويعتبر مشابهاً لتدمير الأشياء الملموسة. ولدي وضع التعريف لم يفرِّق واضعو الاتفاقية بين الطرق المختلفة التي يمكن بها حذف البيانات.[1037] وإلقاء أي ملف في سلة المهملات الافتراضية لا يزيل الملف من القرص الصلب.[1038] وحتى ''تفريغ'' سلة المهملات لا يزيل الملف بالضرورة.[1039] ولذلك، فليس من المؤكد إذا كانت القدرة على استعادة ملف محذوف توقف تطبيق الحكم.[1040]
- ويشير ''تدمير'' البيانات الحاسوبية إلى عمل يؤثر على توفر البيانات للشخص الذي يملك النفاذ إلى الوسيط، حيث يتم تخزين المعلومات بطريقة سلبية.[1041] ونوقش تطبيق هذا الحكم بصورة خاصة في صدد منع الخدمة[1042] بسبب الهجمات.[1043] وأثناء الهجوم لا تعود المعلومات المتوفِّرة على المنظومة الحاسوبية المستهدفة متوفِّرة للمستعمل المحتمل وكذلك لصاحب المنظومة الحاسوبية.[1044]
- ومصطلح ''تعديل''يغطي تغيير البيانات القائمة بدون أن يؤدي ذلك بالضرورة إلى تقليل إمكانية الاستفادة من البيانات.[1045] وهذا الفعل يغطي بوجه خاص تركيب برمجيات ضارة مثل برمجيات التجسُّس أو الفيروسات أو برامج الإعلانات في حاسوب الضحية.[1046]

[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] 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.

[1043] With regard to the criminalisation of "Denial-of-Service" attacks see as well below: Chapter 6.1.5.

[1044] In addition criminalisation of "Denial of Service" attacks is provided by Art. 5 Convention on Cybercrime. See below: Chapter 6.1.5.

[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.

العنصر الذهني:

كما يحدث في حالة جميع الجرائم الأخرى المعرَّفة في الاتفاقية المتعلقة بالجريمة الإلكترونية، تقتضي المادة 4 أن يرتكب الجاني جريمته عمداً.[1047] ولا تتضمن الاتفاقية تعريفاً لمصطلح ''عمداً''. وفي التقرير التفسيري يشير واضعو الصياغة إلى أن تعريف ''عمداً'' ينبغي أن يجري على صعيد وطني.[1048]

بغير حق:

يجب أن يكون ارتكاب الأفعال ''بغير حق''[1049] على نحو مشابه للأحكام التي نوقشت أعلاه. وقد نوقش الحق في تغيير البيانات، وخاصة في سياق ''أنظمة إعادة إرسال الرسائل''.[1050] وتستعمل أنظمة إعادة إرسال الرسائل لتعديل بعض البيانات بغرض تسهيل الاتصالات مجهولة الهوية.[1051] ويذكر التقرير التفسيري أن هذه الأفعال تعتبر من ناحية المبدأ حماية مشروعة للخصوصية ولهذا يمكن اعتبار أنها تجري بأذن.[1052]

التقييدات والتحفظات

تتيح المادة 4 خيار تقييد التجريم من خلال الاقتصار على الحالات التي ينشأ عنها ضرر جسيم، وهو نهج يشبه النهج المتبع في القرار الإطاري للاتحاد الأوروبي بشأن الهجمات ضد أنظمة المعلومات[1053]، وهو ما يمكّن الدول الأعضاء من الاقتصار في تطبيق حكم القانون الجنائي الموضوعي على ''الحالات غير البسيطة''.[1054]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج يتسق مع المادة 4 من الاتفاقية المتعلقة بالجريمة الإلكترونية في المادة 8 من قانون الكومنولث النموذجي لعام 2002.[1055]

المادة 6

(1) عندما يقوم أي شخص، عمداً أو باستهتار، وبدون عذر أو مبرِّر قانوني، بارتكاب أحد الأفعال التالية:

(أ) تدمير أو تغيير بيانات؛

(ب) أو تحويل البيانات لتصبح بدون معنى أو بدون فائدة أو بدون فعالية؛

[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.
[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.

(ج) أو إعاقة أو تعطيل الاستعمال المشروع للبيانات أو التدخل فيه؛

(د) أو إعاقة أو تعطيل أي شخص يستعمل البيانات استعمالاً مشروعاً أو التدخل في عمله؛

(ه) أو حرمان أي شخص يحق له النفاذ إلى البيانات من النفاذ إليها؛

فإنه يرتكب جريمة يعاقب عليها بعد الإدانة بالحبس لفترة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.

(2) تنطبق المادة الفرعية (1) سواء كان أثر فعل الشخص أثراً مؤقتاً أو أثراً دائماً.

مشروع اتفاقية ستانفورد

يتضمن مشروع اتفاقية ستانفورد غير الرسمي[1056] لعام 1999 حكمين يجرمان الأفعال المتصلة بالتداخل في البيانات الحاسوبية.

الحكم:

المادة 3

1 بموجب هذه الاتفاقية، تُرتكب جرائم إذا قام أي شخص بصورة غير قانونية وعمداً بأي سلوك مذكور أدناه بدون سلطة أو إذن أو موافقة معترف بها قانونياً:

(أ) إنشاء بيانات أو برامج في نظام سيبراني أو تخزينها أو تغييرها أو حذفها أو إرسالها أو تحويلها أو تسييرها بطريقة خاطئة أو التلاعب بها أو التداخل فيها بغرض إحداث تعطيل النظام السيبراني المذكور أو نظام سيبراني آخر عن العمل بالطريقة المتوخاة من النظام، مع معرفته بأن هذه الأنشطة ستُسبِّب ذلك، أو بغرض القيام بوظائف أو أنشطة لا يقصدها مالك النظام وتعتبر غير قانونية بموجب هذه الاتفاقية؛

(ب) إنشاء بيانات في نظام سيبراني أو تخزينها أو تغييرها أو حذفها أو إرسالها أو تحويلها أو تسييرها بطريقة خاطئة أو التلاعب بها أو التداخل فيها بغرض وبأثر توفير معلومات زائفة من أجل إحداث ضرر كبير للأشخاص أو الممتلكات؛

الأفعال المشمولة:

الاختلاف الرئيسي بين الاتفاقية المتعلقة بالجريمة الإلكترونية وقانون الكومنولث النموذجي والنهج المتبع في مشروع اتفاقية ستانفورد هو أن مشروع الاتفاقية يجرِّم فقط التداخل في البيانات إذا كان هذا التداخل يعطِّل تشغيل النظام الحاسوبي (المادة 3، الفقرة 1 أ) أو إذا كان ارتكاب الفعل بغرض تقديم معلومات زائفة من أجل إحداث ضرر للشخص أو الممتلكات (المادة 3، الفقرة 1 ب). ولذلك، فإن مشروع القانون لا يجرِّم حذف وثيقة نصية عادية في جهاز تخزين بيانات حيث إن ذلك لا يؤثر على تشغيل الحاسوب ولا يقدِّم معلومات زائفة. وتطبِّق كلا الاتفاقية المتعلقة بالجريمة الإلكترونية وقانون الكومنولث النموذجي نهجاً أكثر اتساعاً بحمايتهما سلامة البيانات الحاسوبية دون الاشتراط الإلزامي بإحداث آثار أخرى.

5.1.6 التداخل في النظام

يعتمد الأشخاص أو مؤسسات الأعمال التي تعرض خدمات تستند إلى تكنولوجيا المعلومات والاتصالات على سير عمل أنظمتهم الحاسوبية.[1057] وعدم توفُّر صفحات شبكة الويب التي تقع ضحية لهجمات منع الخدمة[1058] تثبت مدى خطورة تهديد هذه الهجمات.[1059] وهجمات من هذا

[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.

[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.

القبيل يمكن أن تسبِّب خسائر مالية خطيرة وتؤثر حتى على الأنظمة القوية.[1060] والأعمال التجارية ليست الهدف الوحيد. إذ يناقش الخبراء في أنحاء العالم في الوقت الحاضر سيناريوهات محتملة بشأن ''الإرهاب السيبراني'' تأخذ في الاعتبار الهجمات على البنية التحتية الحرجة مثل خدمات الطاقة الكهربائية والاتصالات.[1061]

الاتفاقية المتعلقة بالجريمة الإلكترونية

لحماية نفاذ المشغلين والمستعملين إلى تكنولوجيا المعلومات والاتصالات تدخل الاتفاقية المتعلقة بالجريمة الإلكترونية حكماً في المادة 5 يجرِّم الإعاقة المتعمَّدة للاستعمال القانوني للأنظمة الحاسوبية.[1062]

الحكم:

المادة 5 – التدخل الغير مشروع في المنظومة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما أرتُكِب عمداً، وبغير حق: الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن طريق إدخال أو إرسال، أو إتلاف، أو محو، أو تغيير، أو تبديل، أو تدمير بيانات كمبيوتر.

الأفعال المشمولة:

يتطلب تطبيق الحكم إعاقة تشغيل النظام الحاسوبي.[1063]

- وتعني ''الإعاقة'' أي فعل يتداخل في التشغيل الصحيح للنظام الحاسوبي.[1064] ويقتصر تطبيق الحكم على الحالات التي تحدث فيها الإعاقة بأحد الأفعال المذكورة.

وقائمة الأفعال التي تؤثر على تشغيل النظام الحاسوبي بطريقة سلبية قائمة جامعة.[1065]

[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", *Computer Security Journal*, 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/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. *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

[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.

- ولا تعرِّف الاتفاقية ذاتها مصطلح ''إدخال'' كما لا يعرفه واضعو الاتفاقية. وفيما يتعلق بأن الإرسال مذكور باعتباره فعل إضافي في المادة 5، فإن مصطلح ''إدخال'' يمكن تعريفه باعتباره أي فعل يتصل باستعمال السطح البيني المادي للمدخلات لنقل المعلومات إلى نظام حاسوبي في حين أن مصطلح ''إرسال'' يغطي الأفعال التي تصاحب إدخال البيانات عن بُعد.[1066]
- ومصطلح ''إتلاف'' و''تغيير'' يتداخلان ويعرفهما واضعو الاتفاقية في التقرير التفسيري بشأن المادة 4 باعتبارهما تبديل سلبي في سلامة المحتوى المعلوماتي للبيانات والبرامج.[1067]
- وعرَّف واضعو الاتفاقية أيضاً مصطلح ''محو'' ويغطي التقرير التفسيري بشأن المادة 4 الأفعال التي يتم بها إزالة المعلومات من وسيط التخزين.[1068]
- ومصطلح ''تبديل''يغطي تعديل البيانات القائمة بدون أن يقلِّل ذلك بالضرورة من إمكانية استخدام البيانات.[1069]
- ويشير ''تدمير'' البيانات الحاسوبية إلى فعل يؤثر على توفُّر البيانات للشخص الذي يملك النفاذ إلى الوسيط الذي يتم فيه تخزين المعلومات بطريقة سلبية.[1070]

وبالإضافة إلى ذلك، يقتصر تطبيق الحكم على الحالات التي تكون الإعاقة فيها ''خطيرة''. وتقع على الأطراف مسؤولية تحديد المعايير التي يتعيَّن الوفاء بها من أجل اعتبار الإعاقة خطيرة.[1071] ويمكن أن تشمل التقييدات المحتملة بموجب القانون الوطني قدراً أدنى من الضرر، وكذلك اقتصار التجريم على الهجمات ضد الأنظمة الحاسوبية الهامة.[1072]

تطبيق الحكم في صدد الرسائل الاقتحامية:

نوقشت إمكانية معالجة مشكلة رسائل البريد الإلكتروني الاقتحامية[1073] تحت المادة 5، نظراً لأن الرسائل الاقتحامية يمكن أن تشكِّل حمولة زائدة على الأنظمة الحاسوبية.[1074] وأعلن واضعو الاتفاقية بوضوح أن الرسائل الاقتحامية قد لا تؤدي بالضرورة إلى إعاقة ''خطيرة'' و''أن تجريم السلوك ينبغي أن يقتصر على حالة تعرُّض الإرسال أو الاتصال لإعاقة متعمَّدة وخطيرة''.[1075] ولاحظ واضعو الاتفاقية أيضاً أن الأطراف قد تعتنق نهجاً مختلفاً في التعامل مع الإعاقة بموجب تشريعاتها الوطنية،[1076] مثل اعتبار أفعال التداخل جرائم إدارية أو خاضعة للجزاءات.[1077]

العنصر الذهني:

كما يحدث في حالة جميع الجرائم الأخرى المعرَّفة في الاتفاقية المتعلقة بالجريمة الإلكترونية، تقتضي المادة 5 أن يرتكب الجاني جريمته عمداً.[1078] ويشمل ذلك قصد القيام بأحد الأفعال المذكورة وكذلك قصد إحداث إعاقة خطيرة لعمل النظام الحاسوبي.

[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. .

[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.

ولا تتضمن الاتفاقية تعريفاً لمصطلح ''عمداً''. وفي التقرير التفسيري يشير واضعو الاتفاقية إلى أن تعريف ''عمداً'' ينبغي أن يجري على صعيد وطني.[1079]

بغير حق:

يتعيَّن اقتراف الفعل ''بغير حق''.[1080] وكما ذكرنا أعلاه شعر مديرو الشبكات وشركات الأمن التي تختبر حماية الأنظمة الحاسوبية بالخوف من إمكانية تجريم عملهم.[1081] ويعمل هؤلاء المهنيون بإذن من المالك وبالتالي فإنهم يتصرفون بطريقة قانونية. وبالإضافة إلى ذلك، ذكر واضعو الاتفاقية صراحة أن اختبار أمن النظام الحاسوبي يستند إلى إذن من المالك ولا يعتبر بغير حق.[1082]

التقييدات والتحفظات:

بعكس المواد من 2-4 لا تتضمن المادة 5 إمكانية صريحة لاقتصار تطبيق الحكم على التنفيذ في القانون الوطني. ومع ذلك، فإن مسؤولية الأطراف في تحديد خطورة الجريمة يعطي لهذه الأطراف إمكانية تقييد تطبيق المادة. ويمكن الاطلاع على نهج مماثل في القرار الإطاري[1083] للاتحاد الأوروبي بشأن الهجمات ضد الأنظمة الحاسوبية.[1084]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج يتسق مع المادة 5 من الاتفاقية المتعلقة بالجريمة الإلكترونية في المادة 7 من قانون الكومنولث النموذجي لعام 2002.[1085]

المادة 7

(1) أي شخص يقوم عمداً أو باستهتار، وبدون عُذر أو مبرِّر قانوني:

(أ) بإعاقة سير عمل نظام حاسوبي أو التداخل فيه؛

(ب) أو إعاقة شخص يستعمل أو يشغِّل نظاماً حاسوبياً بصورة قانونية أو يتداخل في عمله؛

يرتكب جريمة يعاقب عليها بعد الإدانة بالحبس لفترة لا تزيد عن [الفترة] أو بغرامة لا تزيد عن [المبلغ] أو كلاهما.

[1079] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[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.

وفي الفقرة الفرعية (1) فإن الإعاقة، فيما يتصل بالنظام الحاسوبي، تشمل ما يلي دون الاقتصار عليه:

(أ) قطع الكهرباء عن النظام الحاسوبي؛

(ب) إحداث تداخل كهرمغنطيسي في النظام الحاسوبي؛

(ج) إفساد النظام الحاسوبي بأي وسيلة؛

(د) إدخال أو حذف أو تغيير بيانات الحاسوب؛

والاختلاف الرئيسي عن الاتفاقية هو أن المادة 7 من قانون الكومنولث النموذجي تنص على تجريم الأفعال التي تجري باستهتار. ويتجاوز القانون النموذجي باعتناقه هذا النهج الاشتراطات الواردة في الاتفاقية المتعلقة بالجريمة الإلكترونية. وهناك اختلاف آخر وهو أن تعريف ''الإعاقة'' في المادة 7 من قانون الكومنولث النموذجي يتضمن قائمة بالأفعال مقارنة بالمادة 5 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

مشروع اتفاقية ستانفورد

يتضمن مشروع اتفاقية ستانفورد غير الرسمي[1086] لعام 1999 حكماً يجرِّم الأفعال المتصلة بالتداخل في الأنظمة الحاسوبية.

الحكم:

المادة 3

1 بموجب هذه الاتفاقية، تُرتكب جرائم إذا دخل أي شخص بصورة غير قانونية وعمداً في أي سلوك مذكور أدناه بدون سلطة أو إذن أو موافقة معترف بها قانونياً:

(أ) إنشاء بيانات أو برامج في نظام سيبراني أو تخزينها أو تغييرها أو حذفها أو إرسالها أو تحويلها أو تسييرها بطريقة خاطئة أو التلاعب بها أو التداخل فيها بغرض إحداث تعطيل النظام السيبراني المذكور أو أي نظام سيبراني آخر عن العمل بالطريقة المتوخاة منه، مع معرفته بأن هذه الأنشطة تسبِّب هذا التعطيل، أو بغرض القيام بوظائف أو أنشطة لا يقصدها مالك النظام وتعتبر غير قانونية بموجب هذه الاتفاقية؛

الأفعال المشمولة

الاختلاف الرئيسي بين الاتفاقية المتعلقة بالجريمة الإلكترونية وقانون الكومنولث النموذجي والنهج المتبع في مشروع الاتفاقية هو أن مشروع الاتفاقية يغطي أي تلاعب في الأنظمة الحاسوبية، في حين أن الاتفاقية المتعلقة بالجريمة الإلكترونية وقانون الكومنولث النموذجي يقصران التشغيل على إعاقة تشغيل النظام الحاسوبي.

6.1.6 المواد المثيرة جنسياً أو المواد الفاضحة

يتباين تجريم المحتوى غير القانوني والمحتوى الصريح جنسياً كما تتباين خطورة هذا التجريم من بلد لأخر.[1087] وكانت الأطراف التي تفاوضت على الاتفاقية المتعلقة بالجريمة الإلكترونية قد ركَّزت على تنسيق القوانين المتعلقة باستخدام الأطفال في المواد الفاضحة واستبعدت التجريم الواسع للمواد المثيرة جنسياً والمواد الفاضحة. وعالجت بعض البلدان هذه المشكلة بتطبيق أحكام تجرِّم تبادل المواد الفاضحة عبر الأنظمة الحاسوبية. ومع ذلك، فإن الافتقار إلى تعريفات موحَّدة يجعل من العسير على وكالات إنفاذ القوانين إجراء تحقيقات في هذه الجرائم إذا تصرَّف الجناة من بلدان لا تجرِّم تبادل المحتوى الجنسي.[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;

أمثلة:

يرد أحد أمثلة تجريم تبادل المواد الفاضحة في المادة 184 من قانون العقوبات الألماني:

المادة 184 – نشر الكتابات الفاضحة

(1) أي شخص، فيما يتعلق بالكتابات الفاضحة (المادة 11 الفقرة الفرعية (3)):

1 يعرض هذه الكتابات على شخص تقل سنه عن 18 سنة أو يقدمها له أو يسهِّل اطلاعه عليها؛

2 يعرض هذه الكتابات أو ينشرها أو يقدِّمها أو يسهِّل الاطلاع عليها بطريقة أخرى في مكانٍ مفتوح للأشخاص الذين تقل سنهم عن 18 سنة، أو في مكان يستطيعون مشاهدتها فيه؛

3 يقدِّم أو يعطي هذه الكتابات إلى شخص آخر في محلات تجارة التجزئة خارج مواقع النشاط التجاري، أو في أكشاك أو في مناطق بيع لا يدخلها العميل عادة، عن طريق الأعمال التجارية بطلبات البريد أو في مكتبات إعارة تجارية أو حلقات قراءة؛

3 أ) يقدِّم أو يعطي هذه الكتابات إلى شخص آخر عن طريق التأجير التجاري أو عن طريق تجهيز تجاري مشابه للاستعمال، باستثناء المحالات غير المفتوحة للأشخاص الذين تقل سنهم عن 18 سنة حيث يستطيعون مشاهدتها فيها؛

4 يضطلع باستيراد هذه الكتابات بطريق الأعمال التجارية بالبريد؛

5 يقوم علناً بتقديم هذه الكتابات أو الإعلان عنها أو التوصية بها في أماكن مفتوحة لأشخاص تقل سنهم عن 18 سنة وفي أماكن يستطيعون مشاهدتها فيها، أو عن طريق توزيع كتابات خارج الصفقات التجارية عن طريق المنافذ التجارية العادية؛

6 يسمح لشخص آخر بالحصول عليها بدون أن يكون قد طلب منه ذلك؛

7 يعرضها في مكان عام لعرض الأفلام مقابل أجر يُطلب كله أو معظمه مقابل هذا العرض؛

8 يُنتج أو يحصل أو يقدِّم أو يخزِّن أو يستورد هذه الكتابات بغرض استعمالها أو استعمال نُسخ منها في إطار الفقرات من 1 إلى 7 أو يمكِّن شخصاً آخر من القيام بهذا الاستعمال؛

9 يضطلع بتصديرها من أجل نشرها أو نشر نُسخ منها في الخارج انتهاكاً لأحكام العقوبات المنطبقة هناك وإتاحتها علناً أو التمكين من هذا الاستعمال، يعاقب بالحبس بمدة لا تزيد عن سنة أو بغرامة.

ويستند هذا الحكم إلى المفهوم القائل بأن التجارة وغيرها من ضروب تبادل الكتابات الفاضحة لا ينبغي تجريمها إذا لم يمس الموضوع أشخاصاً قاصرين.[1089] واستناداً إلى ذلك يهدف القانون إلى حماية تنمية القُصَّر دون إزعاج.[1090] وتجري مناقشة حامية لمسألة ما إن كان النفاذ إلى المواد الفاضحة يؤثر سلباً على تنمية القُصَّر.[1091] ولا تجرِّم المادة 184 تبادل الكتابات الفاضحة بين الكبار. ومصطلح ''الكتابات'' لا يغطي فقط الكتابات التقليدية ولكنه يغطي أيضاً التخزين الرقمي.[1092] وبالمثل، فإن ''تسهيل الاطلاع عليها'' لا ينطبق فقط على الأفعال خارج الإنترنت ولكنه يغطي أيضاً الحالات التي يوفِّر فيها الجناة المحتوى الفاضح في مواقع شبكة الويب.[1093]

والمادة 4 جيم 1 من مشروع القانون التشريعي رقم 3777 لعام 2007[1094] في الفلبين يقدِّم مثالاً لنهج يتجاوز هذه القاعدة ويجرِّم أي محتوى جنسي.

المادة 4 – جيم 1 – *الجرائم المتصلة بالجنس السيبراني – بدون المساس بالمقاضاة بموجب المرسوم الجمهوري رقم 9208 والمرسوم الجمهوري رقم 7610، فإن أي شخص يقوم بأي طريقة بالإعلان عن الجنس السيبراني أو نشره أو تسهيل ارتكابه من خلال استعمال تكنولوجيا المعلومات والاتصالات، مثل الحواسيب والشبكات الحاسوبية والتليفزيون والسواتل والهواتف المتنقلة دون أن تقتصر عليها، […]*

المادة 3 'ألف': *الجنس السيبراني أو الجنس الافتراضي – ويشير إلى أي شكل من أشكال النشاط الجنسي أو الإثارة الجنسية بمساعدة الحواسيب أو شبكات الاتصال*

[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.

ويعتنق هذا الحكم نهجاً عريضاً جداً، نظراً لأنه يجرِّم أي نوع من الإعلانات الجنسية أو تسهيل النشاط الجنسي عبر الإنترنت. وبسبب مبدأ ازدواج الجُرم[1095] تسير التحقيقات الدولية في صدد هذه النُهج الواسعة بصعوبة.[1096]

7.1.6 استعمال الأطفال في المواد الفاضحة

تتجه الإنترنت إلى أن تكون الأداة الرئيسية لتجارة وتبادل المواد التي تحتوي على صور فاضحة للأطفال.[1097] والأسباب الرئيسية لهذا التطوُّر هي سرعة وكفاءة الإنترنت في نقل الملفات وانخفاض تكاليف الإنتاج والتوزيع والاعتقاد باختفاء الهوية.[1098] ويستطيع ملايين المستعملين في كل أنحاء العالم[1099] النفاذ إلى الصور المنشورة في صفحات الويب وتفريغها. ومن أهم أسباب ''نجاح'' صفحات الويب التي تعرض المواد الفاضحة أو حتى المواد الفاضحة التي تستخدم الأطفال هو أن مستعملي الإنترنت يشعرون بأنهم يتعرضون لمراقبة أقل عندما يجلسون في بيوتهم ويقومون بتنزيل المواد من الإنترنت. والانطباع بعدم إمكانية تعقُّب المستعمل انطباع خاطئ[1100] ما لم يلجأ المستعمل إلى أساليب الاتصال مجهول الهوية. ومعظم مستعملي الإنترنت لا يدركون الأثر الإلكتروني الذي يتركونه أثناء التصفُّح.[1101]

اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية

لتحسين وتنسيق حماية الأطفال من الاستغلال الجنسي،[1102] تشمل الاتفاقية مادة تعالج الصور الفاضحة للأطفال.

الحكم:

المادة 9 – الجرائم المتعلقة بالصور الفاضحة للأطفال:

(1) تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال والسلوكيات التالية في قانونها الوطني، إذا ما ارتُكبت عمداً، وبغير حق:

أ) إنتاج صور الأطفال الفاضحة بغرض توزيعها عبر منظومة كمبيوتر؛

ب) عرض أو توفير صور الأطفال الفاضحة عبر منظومة كمبيوتر؛

ج) توزيع أو بث صور أطفال فاضحة عبر منظومة كمبيوتر؛

د) الحصول على صور الأطفال الفاضحة عبر منظومة كمبيوتر لصالح الشخص ذاته أو لصالح الغير؛

هـ) حيازة صور الأطفال الفاضحة داخل منظومة كمبيوتر أو بوسيط تخزين بيانات كمبيوتر؛

(2) لغرض الفقرة 1 بعالية، تشمل عبارة ''صور الأطفال الفاضحة'' على المواد الفاضحة التي توضِّح بالصورة:

(أ) قاصر منشغل بارتكاب سلوك جنسي صريح؛

(ب) شخص يبدو أنه قاصر منشغلاً بارتكاب سلوك جنسي صريح؛

(ج) صورة واقعية تظهر قاصراً منشغلاً بارتكاب سلوك جنسي صريح.

[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.

(3) لغرض الفقرة 2 بعالية، يشمل تعبير ''قاصر'' كل من هو دون سن الثامنة عشرة. على أنه يجوز لأي طرف أن يشترط حداً عمرياً أقل، بما لا يقل عن سن السادسة عشرة.

(4) يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق البندين (د) و(ه) من الفقرة 1 والبندين (ب) و(ج) من الفقرة 2 كلياً أو جزئياً.

وتجرِّم معظم البلدان بالفعل سوء استغلال الأطفال، وكذلك الأساليب التقليدية لتوزيع المواد الفاضحة للأطفال.[1103] ولهذا، فإن الاتفاقية لم تقف عند حد سد الثغرات في القوانين الجنائية الوطنية[1104] – بل تسعى أيضاً إلى تنسيق مختلف اللوائح.[1105] وهناك ثلاث عناصر موضع للجدل في المادة 9:

- سن الشخص المعني؛
- تجريم حيازة المواد الفاضحة للأطفال؛
- إنشاء أو إدماج صور غير حقيقية.[1106]

حدّ سن القاصر:

من أهم الاختلافات بين التشريعات الوطنية سن الشخص المعني. فبعض الدول تعرِّف في قانونها الوطني مصطلح ''القاصر'' فيما يتصل باستخدام الأطفال في المواد الإباحية وفقاً لتعريف ''الطفل'' في المادة 1 من اتفاقية الأمم المتحدة لحقوق الطفل[1107] بأنه أي شخص يقل عمره عن 18 سنة. وتعرِّف بلدان أخرى القاصر بأنه شخص يقل عمره عن 14 سنة.[1108] ويوجد نهج مشابه في القرار الإطاري لمجلس الاتحاد الأوروبي لعام 2003 بشأن مكافحة الاستغلال الجنسي للأطفال والمواد الإباحية للأطفال[1109] واتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي.[1110] وتشدِّد الاتفاقية على أهمية وجود معيار دولي واحد يتعلَّق بالسن وتعرِّف الاتفاقية المصطلح وفقاً لاتفاقية الأمم المتحدة.[1111] ومع ذلك، تسمح الاتفاقية باقتضاء حد عمري مختلف لا يقل عن 16 سنة، وذلك اعترافاً منها بالاختلافات الكبيرة في القوانين الوطنية القائمة.

تجريم حيازة المواد الفاضحة للأطفال:

يختلف تجريم حيازة المواد الفاضحة للأطفال أيضاً بين مختلف الأنظمة القانونية الوطنية.[1112] ويمكن أن يؤدي الطلب على هذه المواد إلى استمرار إنتاجها.[1113] وحيازة هذه المواد يمكن أن يشجِّع على الاعتداء على الأطفال، ولذلك يشير واضعو الاتفاقية بأن إحدى الطرق الفعَّالة لتقليص

[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.

[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.

إنتاج المواد الفاضحة للأطفال أن تعتبر حيازتها غير قانونية.[1114] ومع ذلك، تمكّن الاتفاقية الأطراف في الفقرة 4 من استبعاد تجريم مجرَّد الحيازة، من خلال قصر المسؤولية الجنائية على إنتاج المواد الفاضحة للأطفال وعرضها وتوزيعها فقط.[1115]

إنشاء أو إدماج صور غير حقيقية

رغم أن واضعي الاتفاقية حاولوا تحسين حماية الأطفال من الاستغلال الجنسي، فإن نطاق الاهتمامات القانونية التي تغطيها الفقرة 2 أكثر اتساعاً من ذلك. فالفقرة 2 (أ) تركّز مباشرة على الحماية من الاعتداء على الأطفال. وتعطي الفقرتان 2 (ب) و2 (ج) الصور التي يتم إنتاجها دون انتهاك حقوق الأطفال – مثل الصور التي أُنشئت عن طريق استعمال برمجيات نماذج ثلاثية الأبعاد.[1116] والسبب في تجريم المواد الفاضحة غير الحقيقية للأطفال هو أن هذه الصور يمكن – دون أن تنشئ بالضرورة ضرراً على ''طفل'' حقيقي – أن تُستخدم لإغراء الأطفال بالمشاركة في هذه الأفعال.[1117]

العنصر الذهني

كما حدث في حالة جميع الجرائم المعرَّفة في الاتفاقية المتعلقة بالجريمة الإلكترونية، تقتضي المادة 9 أن يرتكب الجاني جريمته عمداً.[1118] وفي التقرير التفسيري يشير واضعو الاتفاقية صراحة إلى أن التفاعل مع المواد الفاضحة للأطفال بدون أي قصد ليس مشمولاً في الاتفاقية. ويمكن أن يكون عدم وجود القصد أمراً هاماً بصورة خاصة إذا كان الجاني قد فتح صفحة في شبكة الويب بصورة عرضية وكانت الصفحة تتضمن صوراً فاضحة لأطفال ورغم أن هذا الشخص قد أغلق الصفحة فوراً فقد تم تخزين بعض الصور في الملفات المؤقتة أو الملفات المخفية.

بغير حق:

لا يمكن ملاحقة الأفعال المتصلة بالمواد الفاضحة للأطفال بموجب المادة 9 من الاتفاقية إلاّ إذا حدثت هذه الأفعال ''بغير حق''.[1119] ولم يُدرج واضعو الاتفاقية أي نص آخر يوضّح الحالات التي يتصرف فيها المستعمل بموجب إذن. وعموماً يجري الفعل ''بغير حق'' إلاّ إذا كان تصرفاً من جانب وكالات إنفاذ القوانين في إطار أحد التحقيقات.

اتفاقية مجلس أوروبا لحماية الأطفال:

يرد نهج آخر لتجريم الأفعال المتصلة بالمواد الفاضحة للأطفال في المادة 20 من اتفاقية مجلس أوروبا لحماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي.[1120]

الحكم:

المادة 20 – الجرائم المتعلقة بالصور الفاضحة للأطفال

(1) يتخذ كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لكفالة تجريم السلوك المتعمَّد التالي في حالة ارتكابه بغير حق:

(أ) إنتاج صور الأطفال الفاضحة؛

(ب) عرض أو توفير صور الأطفال الفاضحة؛

[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.

[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).

(ج) توزيع أو بث صور أطفال فاضحة؛

(د) الحصول على صور أطفال فاضحة لصالح الشخص ذاته أو لصالح الغير؛

(هـ) حيازة صور الأطفال الفاضحة؛

(و) الحصول عن علم على طريق للنفاذ إلى صور فاضحة للأطفال من خلال تكنولوجيا المعلومات والاتصالات.

(2) لأغراض هذه الفقرة يعني مصطلح "صور الأطفال الفاضحة" أي مواد تصوِّر بصورة مرئية طفلاً ينشغل في سلوك جنسي صريح حقيقي أو تمثيلي أو أي تصوير لأعضاء جنسية لطفل لأغراض جنسية في المقام الأول.

(3) يجوز لأي طرف أن يحتفظ بالحق في عدم التطبيق الكلي أو الجزئي للفقرة 1 (أ) و(هـ) وإنتاج وحيازة المواد الفاضحة:

- التي تتألف فقط من تصويرات تمثيلية أو صور واقعية لأطفال غير حقيقيين؛

- تشمل أطفالاً بلغوا السن المحدَّد في تطبيق الفقرة 2 من المادة 18، في حالة إنتاجهم وحيازتهم هذه الصور بموافقتهم ولأغراض الاستعمال الخاص فقط.

(4) يجوز لكل طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 (و) كلياً أو جزئياً.

الأفعال المشمولة:

يستند الحكم إلى المادة 9 من الاتفاقية المتعلقة بالجريمة الإلكترونية ولذلك يتشابه إلى درجة كبيرة مع ذلك الحكم.[1121] والاختلاف الرئيسي هو أن الاتفاقية المتعلقة بالجريمة الإلكترونية تركّز على تجريم الأفعال المتصلة بخدمات المعلومات والاتصالات ("إنتاج صور الأطفال الفاضحة بغرض توزيعها عبر منظومة كمبيوتر") في حين أن اتفاقية حماية الطفل تعتنق نهجاً أوسعاً أساساً ("إنتاج صور أطفال فاضحة") بل وتغطي أفعالاً لا تتصل بشبكات الحاسوب.

ورغم أوجه التشابه بشأن الأفعال المشمولة، فإن المادة 20 من اتفاقية حماية الطفل تتضمن فعلاً لا تغطيه الاتفاقية المتعلقة بالجريمة الإلكترونية. فهي تجرِّم فعل الحصول على النفاذ إلى صور الأطفال الفاضحة عبر الحاسوب استناداً إلى الفقرة 1 من المادة 20 في اتفاقية حماية الطفل. ويمكّن ذلك وكالات إنفاذ القانون من ملاحقة الجناة في حالة تمكنها من إثبات أن الجاني فتح مواقع في شبكة الويب تتضمَّن صوراً فاضحة للأطفال ولكنها لا تستطيع إثبات أن الجاني قام بتنزيل المادة. وهذه الصعوبات في جمع الأدلة تنشأ، على سبيل المثال، إذا كان الجاني يستعمل تكنولوجيا التشفير لحماية الملفات التي يتم تنزيلها على وسيط التخزين لديه.[1122] ويشير التقرير التفسيري لاتفاقية حكومة الطفل إلى أن ذلك الحكم ينبغي أن ينطبق أيضاً في الحالات التي يقوم فيها الجاني فقط بمشاهدة صور الأطفال الفاضحة على الخط دون تنزيلها.[1123] وعموماً، فإن فتح موقع في شبكة الويب يبدأ عملية التنزيل تلقائياً – ويكون ذلك في كثير من الأحيان بمعرفة المستعمل.[1124] ولذلك، فإن الحالة المذكورة في التقرير التفسيري لا تتصل إلاّ بالحالات التي لا يحدث فيها تنزيل في الخلفية.

قانون الكومنولث النموذجي

يمكن الاطلاع على نهج يتمشى مع المادة 9 من الاتفاقية المتعلقة بالجريمة الإلكترونية في المادة 10 من قانون الكومنولث النموذجي لعام 2002.[1125]

[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.

المادة 10

(1) أي شخص يقوم بأحد الأفعال التالية عمداً:

(أ) نشر صور أطفال فاضحة عبر منظومة حاسوبية؛

(ب) أو إنتاج صور أطفال فاضحة بغرض نشرها من خلال منظومة حاسوبية؛

(ج) أو امتلاك صور أطفال فاضحة في منظومة حاسوبية أو في وسيط تخزين بيانات حاسوبي؛ يرتكب جريمة يعاقب عليها بعد الإدانة بالحبس لمدة لا تزيد عن [الفترة]، أو بغرامة لا تزيد عن [المبلغ] أو كلاهما.[1126]

(2) يعتبر دفاعاً ضد الاتهام بارتكاب جريمة بموجب الفقرة 1 (أ) أو (1) (ج) أن يثبت الشخص أن صور الأطفال الفاضحة هي لغرض علمي أو بحثي أو طبي صادق أو لغرض إنفاذ القوانين.[1127]

(3) وفي هذه المادة:

''صور الأطفال الفاضحة'' تشمل المواد التي تصوِّر بصورة مرئية:

(أ) قاصراً مشتركاً في سلوك جنسي صريح؛

(ب) أو شخصاً يظهر أنه قاصر منخرطاً في سلوك جنسي صريح؛

(ج) أو صوراً واقعية تمثِّل قاصراً مشتركاً في سلوك جنسي صريح.

ويعني ''القاصر'' أي شخص تحت سن [س].

ويشمل ''النشر'' ما يلي:

(أ) التوزيع أو الإرسال أو النشر أو التعميم أو التسليم أو العرض أو الإقراض بغرض الربح أو التبادل أو المقايضة أو البيع أو عرض البيع أو العرض للإيجار أو العرض بالسماح بالإيجار أو العرض بأي شكل آخر أو الإتاحة بأي طريقة أخرى؛

(ب) أو الاحتفاظ في الحيازة أو الملكية أو تحت السيطرة لغرض القيام بأحد الأفعال المشار إليها في الفقرة (أ)؛

(ج) أو طباعة أو تصوير أو نسخ أو صُنع بأي شكل آخر (سواء لنفس المادة أو لمادة أخرى ذات طابع مشابه) لأغراض القيام بفعل مشار إليه في الفقرة (أ).

والاختلافات الرئيسية عن الاتفاقية المعنية بالجريمة الإلكترونية هي أن قانون الكومنولث النموذجي لا يقدِّم تعريفاً محدَّداً لمصطلح القاصر ويترك ذلك للدول الأعضاء لتحديد الحد العمري.

مشروع اتفاقية ستانفورد

لا يتضمن مشروع اتفاقية ستانفورد غير الرسمي[1128] لعام 1999 نصاً يجرِّم تبادل صور الأطفال الفاضحة عبر المنظومات الحاسوبية. وأشار واضعو الاتفاقية إلى أنه ليس من المطلوب عموماً معاملة أي نوع من الحديث أو النشر باعتباره إجرامياً بموجب مشروع ستانفورد.[1129] وأقرّ واضعو الاتفاقية بمختلف النُهج الوطنية فتركوا للدول حرية تقرير هذا الجانب من التجريم.[1130]

[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.
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.

8.1.6 خطاب الكراهية، العنصرية

لا تجرِّم جميع البلدان خطاب الكراهية.[1131]

الاتفاقية المتعلقة بالجريمة الإلكترونية

نظراً لأن الأطراف التي تفاوضت على الاتفاقية المتعلقة بالجريمة الإلكترونية لم تتفق[1132] على موقف مشترك بشأن تجريم هذه المواد، فإن الأحكام المتصلة بهذا الموضوع أُدمجت في البروتوكول الأول للاتفاقية المعنية بالجريمة الإلكترونية،[1133] وهو بروتوكول منفصل.

الحكم:

المادة 3 – نشر مواد العنصرية وكراهية الأجانب عبر الأنظمة الحاسوبية

1 يعتمد كل طرف ما قد يكون ضرورياً من التدابير التشريعية وغيرها من التدابير اللازمة لاعتبار السلوك التالي جرائم جنائية بموجب قانونها المحلي إذا أُرتُكب عمداً وبغير حق: توزيع مواد عنصرية ومواد تحث على كراهية الأجانب على الجمهور من خلال منظومة حاسوبية، أو إتاحتها بأي شكل آخر.

2 يجوز لأي طرف أن يحتفظ بالحق في عدم تعليق المسؤولية الجنائية على سلوك معرَّف في الفقرة 1 من هذه المادة إذا كانت المادة المنشورة على النحو المعرَّف في الفقرة 1 من المادة 2 تدعو أو تشجِّع أو تحرِّض على التمييز دون أن يكون ذلك مرتبطاً بالكراهية أو العنف، شريطة توفُّر وسائل إنصاف فعَّالة أخرى.

3 رغم أحكام الفقرة 2 من هذه المادة يجوز لأي طرف أن يحتفظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز التي لا تستطيع، بسبب مبادئ ثابتة في نظامها القانوني الوطني فيما يتعلق بحرية التعبير، أن تنص بشأنها على وسائل إنصاف فعَّالة على النحو المشار إليه في الفقرة 2 المذكورة.

المادة 4 – التهديد بدافع العنصرية وكراهية الأجانب

يعتمد كل طرف ما قد يكون ضروري تدابير تشريعية وتدابير أخرى لاعتبار السلوك التالي جرائم جنائية في قانونها المحلي إذا أُرتُكب عمداً وبغير حق:

التهديد عبر منظومة حاسوبية بارتكاب جريمة جنائية خطيرة على النحو المحدَّد في قانونها المحلي، '1' ضد أشخاص بسبب انتمائهم إلى مجموعة تتميَّز بعرق أو لون أو مولد أو أصل قومي أو عرقي، وكذلك بسبب الدين، إذا استُعمل ذلك ذريعة لأيٍ من هذه العوامل، أو '2' مجموعة من الأشخاص تتميَّز بأيٍ من هذه السمات.

المادة 5 – الإهانة بدافع العنصرية وكراهية الأجانب

1 يعتمد كل طرف ما قد يكون ضرورياً من التدابير التشريعية والتدابير الأخرى لاعتبار السلوك التالي جرائم جنائية بموجب قانونها المحلي في حالة ارتكابه عمداً وبغير حق:

توجيه إهانة علنية، من خلال منظومة حاسوبية '1' إلى أشخاص بسبب انتمائهم إلى مجموعة تتميَّز بعنصر أو لون أو مولد أو أصل قومي أو إثني، وكذلك بالدين، إذا استُعمل ذلك ذريعة لأيٍ من هذه العوامل؛ أو '2' مجموعة من الأشخاص تتميَّز بأيٍ من هذه السمات.

2 يجوز لأي طرف إما:

(أ) أن يقتضي أن تؤدي الجريمة المشار إليها في الفقرة 1 من هذه المادة إلى تعرُّض الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 للكراهية أو الازدراء أو السخرية؛ أو

(ب) الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة كلياً أو جزئياً.

[1131] For an overview of hate speech legislation, see the database provided at: http://www.legislationline.org.

[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.

المادة 6 – إنكار الإبادة الجماعية أو الجرائم ضد البشرية أو تقليلها بصورة فجة أو الموافقة عليها أو تبريرها

1 يعتمد كل طرف ما قد يكون ضرورياً من التدابير التشريعية والتدابير الأخرى لاعتبار السلوك التالي جرائم جنائية في قانونه المحلي إذا أُرتُكب عمداً وبغير حق:

توزيع، أو إتاحة بطريقة أخرى للجمهور، عبر نظام حاسوبي، مواد تنكر الأفعال التي تشكِّل إبادة جماعية أو جرائم ضد البشرية أو تقللها بصورة فجة أو توافق عليها أو تبرِّرها، على النحو المحدَّد في القانون الدولي والمعترف بها بهذا الاسم بموجب قرارات نهائية وملزمة من المحكمة العسكرية الدولية التي أنشئت بموجب اتفاق لندن المؤرخ 8 آب/أغسطس 1945، أو أي محكمة دولية أخرى أنشئت بموجب صكوك دولية ذات صلة ويعترف الطرف بولايتها.

2 يجوز لأي طرف إما

اقتضاء أن يكون الإنكار أو التقليل بصورة فجَّة المشار إليه في الفقرة 1 من هذه المادة قد ارُتكب بقصد التحريض على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس العنصر أو اللون أو المولد أو الأصل الوطني أو الإثني وكذلك الدين، إذا استُعمل ذريعة لأي من هذه العوامل، وإما

(ب) الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة كلياً أو جزئياً.

وتتمثَّل إحدى الصعوبات الأساسية المتصلة بالأحكام التي تجرِّم مواد كراهية الأجانب في إقامة توازن بين كفالة حُرية التعبير[1134]، من ناحية، ومنع انتهاك حقوق الأفراد أو المجموعات، من ناحية أخرى. وبدون الدخول في التفاصيل، فإن الصعوبات التي نشأت في المفاوضات بشأن الاتفاقية المتعلقة بالجريمة الإلكترونية[1135] وحالة التوقيعات/التصديقات على البروتوكول الإضافي[1136] تثبت أن اختلاف مدى حماية حُرية التعبير يعوق عملية التنسيق.[1137] وفيما يتعلق بالمبدأ المشترك للجُرم المزدوج بالتحديد،[1138] يؤدي غياب التنسيق إلى صعوبات في الإنفاذ في الحالات التي تأخذ بُعداً دولياً.[1139]

مشروع اتفاقية ستانفورد

لا يتضمن مشروع اتفاقية ستانفورد غير الرسمي[1140] لعام 1999 حكماً يجرِّم خطاب الكراهية. وأشار واضعو الاتفاقية إلى أنه ليس من الضروري معاملة أي نوع من الخطاب أو المنشورات باعتبارها إجرامية بموجب مشروع ستانفورد.[1141] ومع الاعتراف بمختلف النُهج الوطنية ترك واضعو الاتفاقية للدول اتخاذ قرار بشأن هذا الجانب من التجريم.[1142]

[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;

[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.

9.1.6 الجرائم الدينية

تختلف شدة حماية الأديان ورموزها من بلد لأخر.[1143]

الاتفاقية المتعلقة بالجريمة الإلكترونية

واجهت المفاوضات بشأن هذا الموضوع بين أطراف الاتفاقية المتعلقة بالجريمة الإلكترونية نفس الصعوبات التي ظهرت بشأن مواد كراهية الأجانب.[1144] ومع ذلك، فإن البلدان التي تفاوضت بشأن أحكام البروتوكول الإضافي الأول للاتفاقية المتعلقة بالجريمة الإلكترونية وافقت على إضافة الدين كموضوع للحماية في إثنين من الأحكام.

الحكمان:

المادة 4 – التهديد بدافع العنصرية وكراهية الأجانب

يعتمد كل طرف ما قد يكون ضروري تدابير تشريعية وتدابير أخرى لاعتبار السلوك التالي جرائم جنائية في قانونها المحلي إذا أرتُكب عمداً وبغير حق:

التهديد عبر منظومة حاسوبية بارتكاب جريمة جنائية خطيرة على النحو المحدَّد في قانونها المحلي، '1' ضد أشخاص بسبب انتمائهم إلى مجموعة تتميَّز بعرق أو لون أو مولد أو أصل قومي أو إثني، وكذلك بسبب الدين، إذا استُعمل ذلك ذريعة لأيٍ من هذه العوامل، أو '2' مجموعة من الأشخاص تتميَّز بأيٍ من هذه السمات.

المادة 5 – الإهانة بدافع العنصرية وكراهية الأجانب

1 يعتمد كل طرف ما قد يكون ضرورياً من التدابير التشريعية والتدابير الأخرى لاعتبار السلوك التالي جرائم جنائية في قانونها المحلي إذا ارتُكب عمداً وبغير حق:

توجيه إهانة علنية، من خلال منظومة حاسوبية '1' إلى أشخاص بسبب انتمائهم إلى مجموعة تتميَّز بعرق أو لون أو مولد أو أصل قومي أو إثني، وكذلك بسبب الدين، إذا استُعمل ذلك ذريعة لأيٍ من هذه العوامل؛ أو '2' مجموعة من الأشخاص تتميَّز بأيٍ من هذه السمات.

ورغم أن هذين الحكمين يعاملان الدين باعتباره سمة من السمات فإنهما لا يحميان الدين أو الرموز الدينية من خلال التجريم. فالحكمان يجرمان التهديدات والإهانات للأشخاص بسبب انتمائهم لإحدى المجموعات.

أمثلة من التشريعات الوطنية

تتجاوز بعض البلدان هذا النهج وتجرِّم أيضاً الأفعال المتصلة بالقضايا الدينية. ومن أمثلة ذلك المادة 295 باء إلى المادة 295 جيم في قانون العقوبات الباكستاني.

295–باء – *تدنيس، إلخ، القرآن الكريم: أي شخص يقوم متعمداً بتدنيس القرآن الكريم أو تشويهه أو انتهاك حرمته أو نُسخة منه أو نص منه أو يستعمله بازدراء أو في أي غرض غير قانوني يعاقب بالحبس مدى الحياة.*

295– جيم – *استعمال تعبيرات ازدرائية، إلخ، عن النبي الكريم: أي شخص، يقوم باستعمال كلمات شفوية أو مكتوبة أو يقوم عن طريق أي تنسيب أو تعريض أو إيحاء مباشر أو غير مباشر بتدنيس اسم النبي الكريم محمد (صلى الله عليه وسلم) يعاقب بالإعدام أو السجن مدى الحياة ويتعرَّض أيضاً للحكم بغرامة.*

وفيما يتعلق بحالات عدم التأكد المتصلة بتطبيق هذا الحكم، يتضمن قانون الجريمة الإلكترونية الباكستاني لعام 2006 نصين يركزان على الجرائم المتصلة بالإنترنت[1145]:

20 تدنيس، إلخ، نسخة من القرآن الكريم *– أي شخص يستعمل نظاماً إلكترونياً أو جهازاً إلكترونياً ليقوم متعمداً بتدنيس نسخة من القرآن الكريم أو نص مأخوذ منه أو تشويهه أو انتهاك حرمته أو استعماله بأي طريقة فيها ازدراء أو لأي غرض غير قانوني يعاقب بالسجن مدى الحياة.*

[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.

[1145] The draft law was not in power, at the time this publication was finalised.

21 ***استعمال تعبيرات ازدرائية، عن الرسول الكريم*** – *أي شخص يستعمل نظاماً إلكترونياً أو جهازاً إلكترونياً بكلمات منطوقة أو مكتوبة أو بأي تمثيل مرئي أو يقوم عن طريق أي تنسيب أو تعريض أو إيحاء مباشر أو غير مباشر بتدنيس اسم النبي الكريم محمد (صلى الله عليه وسلم) يعاقب بالإعدام أو السجن مدى الحياة ويحكم عليه بغرامة.*

وكما يحدث في حالة الأحكام التي تجرِّم توزيع الكتابات التي تحض على كراهية الأجانب عن طريق الإنترنت، فإن أحد التحديات الرئيسية في النُهج العالمية لتجريم الجرائم الدينية يتصل بمبدأ حرية التعبير.[1146] وكما أُشير من قبل يمثِّل اختلاف مدى حماية حرية التعبير عائقاً يعترض عملية التنسيق.[1147] وفيما يتصل بصورة خاصة بالمبدأ المشترك بازدواج الجُرم[1148] يؤدي غياب التنسيق إلى صعوبات في الإنفاذ في الحالات التي تأخذ بُعداً دولياً.[1149]

10.1.6 المقامرة غير القانونية

هناك قلق[1150] من تزايد عدد مواقع شبكة الويب التي تعرض المقامرة غير القانونية، نظراً لإمكانية استعمال ذلك للالتفاف على حظر المقامرة المطبَّق في بعض البلدان.[1151] وإذا تم تشغيل هذه الخدمات من أماكن لا تحظر المقامرة على الخط فيصعب على البلدان التي تجرِّم تشغيل المقامرة على الإنترنت أن تمنع مواطنيها من استعمال هذه الخدمات.[1152]

أمثلة من التشريعات الوطنية

لا تتضمن الاتفاقية المتعلقة بالجريمة الإلكترونية حظراً على المقامرة على الخط. ومن أمثلة النُهج الوطنية في هذا الصدد المادة 284 من قانون العقوبات الألماني:

مثال:

المادة 284 – تنظيم إحدى ألعاب الحظ بدون إذن

(1) أي شخص يعمد، بدون إذن من سلطة عامة، إلى أن ينظِّم علناً أو يدير لعبة من ألعاب الحظ أو يتيح المعدات لها يعاقب بالحبس لمدة لا تزيد عن سنتين أو غرامة.

(2) ألعاب الحظ في النوادي أو الحفلات الخاصة التي يتم فيها تنظيم ألعاب الحظ بصورة منتظمة تعتبر منظَّمة تنظيماً عاماً.

[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;

[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.

(3) أي شخص يتصرَّف، في الحالات الموصوفة تحت الفقرة الفرعية (1):

1 بصفته المهنية؛

2 أو بوصفه عضواً في عصابة تجمَّعت لمواصلة ارتكاب هذه الأفعال، يعاقب بالحبس لمدة تتراوح من ثلاثة أشهر إلى خمس سنوات.

(4) أي شخص يقوم بالتوظيف لإحدى ألعاب الحظ العامة (الفقرتان الفرعيتان (1) و(2)) يعاقب بالحبس لمدة لا تزيد عن سنة أو بغرامة.

ويهدف هذا الحكم إلى تقليل مخاطر الإدمان[1153] على المقامرة من خلال تحديد إجراءات لتنظيم هذه الألعاب.[1154] ولا يركِّز صراحة على ألعاب الحظ المتصلة بالإنترنت، ولكنه يشملها أيضاً.[1155] وفي هذا الصدد يجرِّم النص تشغيل المقامرة غير القانونية بدون إذن من السلطات العامة المختصة. وبالإضافة إلى ذلك، يجرِّم أي شخص يتح (عمداً) معدات تستعمل بعد ذلك في المقامرة غير القانونية.[1156] وهذا التجريم يتجاوز عواقب المساعدة والتحريض، نظراً لأن مرتكبي الجرائم قد يواجهون عقوبات أعلى.[1157]

ولتجنُّب التحقيقات الجنائية يستطيع مشغِّل مواقع المقامرة غير القانونية أن ينقل مادياً أنشطته[1158] إلى بلدان لا تجرِّم المقامرة غير القانونية.[1159] وهذا الانتقال إلى أماكن أخرى يمثِّل تحدياً لوكالات إنفاذ القانون لأن وجود المخدِّم خارج أراضي البلد[1160] لا يؤثر عموماً على إمكانيات نفاذ المستعمل داخل البلد إلى الموقع.[1161] ولتحسين إمكانيات وكالات إنفاذ القانون لمكافحة المقامرة غير القانونية وسَّعت الحكومة الألمانية التجريم ليشمل المستعملين.[1162] واستناداً إلى المادة 285 تستطيع وكالات إنفاذ القانون أن تلاحق المستعملين الذين يشتركون في المقامرة غير القانونية وتستطيع أن تبدأ التحقيقات، حتى لو كان من غير الممكن ملاحقة مشغلي ألعاب الحظ إذا كانوا موجودين خارج ألمانيا:

المادة 285 – المشاركة في ألعاب حظ بدون إذن

أي شخص يشارك في ألعاب حظ عامة (المادة 284) يعاقب بالحبس لمدة لا تزيد عن ستة أشهر أو بغرامة لا تزيد عن مائة وثمانين معدلاً يومياً.

[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 Internetglueckspielen 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.

[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.

وإذا استعمل الجناة مواقع المقامرة لأنشطة غسيل الأموال، فإن تحديد هوية الجناة يكون عسيراً في كثير من الأحيان.[1163] ومن أمثلة النُهج المتبعة[1164] لمنع المقامرة غير القانونية وأنشطة غسيل الأموال قانون إنفاذ المقامرة غير القانونية على الإنترنت في الولايات المتحدة لعام 2005.[1165]

5363 – حظر قبول أي صك مالي لأغراض المقامرة غير القانونية على الإنترنت

لا يجوز لأي شخص يعمل في قطاع الرهانات أو المراهنة أن يقبل عن علم، فيما يتصل بمشاركة شخص آخر في مقامرة غير قانونية على الإنترنت

(1) ائتمانات، أو عوائد ائتمانات، مقدَّمة إلى هذا الشخص الآخر أو نيابة عنه (بما في ذلك الائتمانات المقدَّمة عن طريق استعمال بطاقات ائتمان)؛

(2) نقل أموال إلكترونياً أو نقل أموال بواسطة شركة نقل أموال أو من خلالها، أو عوائد نقل أموال إلكتروني أو خدمة إرسال أموال من هذا الشخص أو نيابة عنه؛

(3) أي شيك أو حوالة أو صك مماثل مسحوب على يد هذا الشخص الآخر أو نيابة عنه ومسحوب أو قابل للدفع في أي مؤسسة مالية أو من خلالها؛

(4) عوائد أي شكل آخر من الصفقات المالية، حسب ما قد يقرره الوزير بموجب اللوائح، وتنطوي على مشاركة مؤسسة مالية باعتبارها جهة دفع أو وسيط مالي نيابة عن هذا الشخص الآخر أو لصالحه.

5364 – سياسات وإجراء تعيين ومنع الصفقات المقيَّدة

قبل نهاية فترة 270 يوماً تبدأ في تاريخ سن هذا الفصل الفرعي يقوم الوزير، بالتشاور مع مجلس محافظي نظام الاحتياطي الفيدرالي والمدعي العام، بإصدار لوائح تتطلب أن يقوم كل نظام دفع مسمى، ويقوم جميع المشاركين فيه، بتعيين ومنع الصفقات المقيَّدة من خلال إنشاء سياسات وتدابير مصمَّمة بصورة معقولة لتعيين ومنع الصفقات المقيَّدة بأي شكل من الأشكال التالية:

(1) وضع سياسات وإجراءات تهدف إلى

(ألف) السماح لنظام الدفع وأي شخص يشارك في نظام الدفع بتعيين الصفقات المقيَّدة بواسطة رموز في رسائل الإذن أو بأي وسيلة أخرى؛ و

(باء) وقف الصفقات المقيَّدة التي تم تعيينها نتيجة السياسات والإجراءات الموضوعة عملاً بالفقرة الفرعية (ألف).

(2) وضع سياسات وإجراءات لمنع قبول منتجات أو خدمات نظام الدفع فيما يتصل بصفقة مقيَّدة.

(ب) عند إصدار اللوائح بموجب الفقرة الفرعية (أ) من المادة يقوم الوزير

(1) بتعيين أنواع السياسات والتدابير، بما فيها أمثلة غير حصرية، تعتبر حسب الانطباق، مصمَّمة بطريقة معقولة لتعيين أو وقف أو منع قبول المنتجات أو الخدمات في صدد كل نوع من أنواع الصفقات المقيَّدة؛

(2) السماح، بالقدر الممكن عملياً، لأي مشارك في نظام دفع بالاختيار بين وسائل بديلة لتعيين ووقف الصفقات المقيَّدة أو القيام بأي شكل آخر بمنع قبول منتجات أو خدمات نظام الدفع أو خدمات المشارك فيما يتصل بالصفقات المقيَّدة؛ و

(3) النظر في إعفاء الصفقات المقيَّدة من أي اقتضاء مفروض بموجب هذه اللوائح، إذا تبيَّن للوزير أنه ليس من العملي بصورة معقولة تعيين ووقف هذه الصفقات، أو منعها بشكل آخر.

[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.

(ج) يعتبر مقدِّم الصفقة المالية ممتثلاً للوائح الموصوفة تحت الفقرة الفرعية (أ) من هذه المادة في حالة

(1) اعتماد هذا الشخص على السياسات والتدابير الخاصة بنظام دفع مسمى يكون عضواً أو مشاركًا فيه، وامتثاله لهذه السياسات والتدابير، من أجل

(ألف) تعيين ووقف الصفقات المقيَّدة؛ أو

(باء) القيام بشكل آخر بمنع قبول المنتجات أو الخدمات لنظام الدفع أو العضو أو المشارك فيما يتصل بالصفقات المقيَّدة؛ و

(2) امتثال هذه السياسات والتدابير لنظام الدفع المسمى لمقتضيات اللوائح المقرَّرة بموجب الفقرة الفرعية (أ) من هذه المادة.

(د) أي شخص يخضع للائحة مقرَّرة أو لأمر صادر بموجب هذا الفصل الفرعي ويمنع أو يرفض بشكل آخر تنفيذ صفقة

(1) تكون صفقة مقيَّدة؛

(2) أو يعتقد هذا الشخص بصورة معقولة أنها صفقة مقيَّدة؛ أو

(3) أو باعتباره عضواً في نظام دفع مسمى يعتمد على سياسات وإجراءات نظام الدفع، وفي محاولة منه للامتثال للوائح المقرَّرة بموجب الفقرة الفرعية (أ) من هذه المادة، لا يكون مسؤولاً أمام أي طرف عن الإجراء الذي يقوم به.

(هـ) يجري إنفاذ مقتضيات هذه المادة بصورة حصرية على يد هيئات التنظيم الوظائفي الاتحادية ولجنة التجارة الاتحادية بالطريقة المنصوص عليها في المادة 505 (أ) من قانون غرام – ليتش – بلايلي.

5366 – العقوبات الجنائية

(أ) أي شخص ينتهك المادة 5363 يعاقب بغرامة بموجب العنوان 18 أو بالحبس لمدة لا تزيد عن خمس سنوات أو كلاهما.

(ب) بعد إدانة أي شخص بموجب هذه المادة يجوز للمحكمة أن تصدر أمرًا دائماً بمنع هذا الشخص من وضع أو استلام رهان أو مراهنة أو إجرائها بأي شكل آخر أو إرسالها أو تلقيها، أو طلب معلومات لتساعد على وضع الرهانات.

ويهدف هذا القانون إلى مواجهة تحديات وأخطار المقامرة على الإنترنت[1166] (عبر الحدود). ويتضمن لائحتين هامتين: الأولى هي حظر قبول أي صك مالي لأغراض مقامرة غير قانونية على الإنترنت من جانب أي شخص يعمل في أنشطة الرهانات. وهذا الحكم لا ينظِّم الإجراء الذي يقوم به مستعمل مواقع المقامرة في الإنترنت أو المؤسسات المالية.[1167] ويمكن أن يؤدي انتهاك هذا الحظر إلى عقوبات جنائية.[1168] وبالإضافة إلى ذلك، يتطلب القانون من وزير الخزانة ومجلس محافظي نظام الاحتياطي الفيدرالي إصدار لوائح تقتضي قيام مقدمي الصفقات المالية بتعيين ومنع الصفقات المقيَّدة فيما يتصل بالمقامرة غير القانونية على الإنترنت من خلال سياسات وتدابير معقولة. وهذه اللائحة الثانية تؤثر فقط على الأشخاص الداخلين في أنشطة الرهانات ولكنها تؤثر عموماً على جميع المؤسسات المالية. وبعكس قبول الصكوك المالية لأغراض المقامرة غير القانونية على الإنترنت من جانب الشخص العامل في أنشطة الرهانات، فإن المؤسسات المالية لا تواجه عموماً مسؤولية جنائية. وفيما يتعلق بالأثر الدولي لهذا التنظيم، فإن التعارض المحتمل مع الاتفاق العام المتعلق بالتجارة في الخدمات[1169] يجري بحثه في الوقت الحاضر.[1170]

11.1.6 القذف والتشهير

القذف ونشر المعلومات الزائفة أفعال لا يقتصر ارتكابها في الشبكات. ولكن كما أشير من قبل، فإن إمكانية الإرسال مجهول الهوية[1171] والتحديات اللوجستية التي تتصل بالعدد الكبير من المعلومات المتوفِّرة في الإنترنت[1172] هي باراميترات مجرَّدة تدعم تلك الأفعال.

[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.

وقد ثارت مناقشات خلافية[1173] بشأن السؤال عما إن كان ذلك يتطلب تجريم التشهير. وتتصل نقاط القلق المتعلقة بتجريم التشهير بصورة خاصة بإمكانية تعارض ذلك مع مبدأ "حُرية التعبير". ولذلك طالب عدد من المنظمات بتغيير قوانين التشهير الجنائي.[1174] وقد أعرب المقرر الخاص للأمم المتحدة المعني بحُرية الرأي والتعبير وممثل منظمة الأمن والتعاون في أوروبا المعني بحُرية وسائط الإعلام عن الرأي التالي:

"لا يمثّل التشهير الجنائي تقييداً مبرَّراً لحُرية التعبير؛ وينبغي إلغاء جميع قوانين التشهير الجنائي واستبدالها عند الضرورة بقوانين ملائمة للتشهير المدني".[1175]

ورغم هذا القلق قامت بعض البلدان[1176] بتطبيق أحكام في القانون الجنائي تجرِّم القذف، وكذلك نشر المعلومات الزائفة. ومن المهم أن نُبرز أن أعداد القضايا يتباين تبايُناً هائلاً حتى في البلدان التي تجرِّم الشهير. ففي حين أن الاتهام بالتشهير لم يوجَّه إلى أي شخص في المملكة المتحدة في عام 2004 ووجِّه إلى شخص واحد فقط في عام 2005،[1177] فإن الإحصاءات الجنائية الألمانية تسجِّل 527 187 جريمة تشهير في عام 2006.[1178] ولا تتضمن الاتفاقية المعنية بالجريمة الإلكترونية ولا قانون الكومنولث النموذجي ولا مشروع اتفاقية ستانفورد أي أحكام تعالج هذه الأفعال بصورة مباشرة.

أمثلة من التشريعات الوطنية

يوجد أحد أمثلة أحكام القانون الجنائي التي تعالج القذف في المادة 365 من القانون الجنائي لمقاطعة كوينزلاند (أستراليا). وقد أعادت كوينزلاند تطبيق المسؤولية الجنائية عن التشهير بموجب قانون تعديل التشهير الجنائي لعام 2002.[1179]

[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 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. "Based on Article 19 of the Universal Declaration of Human Rights, Article 10 of the 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

الحكم:

365 – التشهير الجنائي[1180]

(1) أي شخص يقوم بدون عذر قانوني بنشر مواد تشهيرية عن شخص آخر على قيد الحياة (الشخص المعني) –

(أ) مع معرفته أن هذه المواد زائفة أو بدون مراعاة ما إن كان الموضوع صحيحاً أو زائفاً؛ و

(ب) يعتزم إحداث ضرر كبير بالشخص المعني أو أي شخص آخر أو بدون مراعاة ما إن كان ذلك سيتسبب في ضرر خطير بالشخص المعني أو بأي شخص آخر؛ يكون مرتكباً لجنحة. العقوبة القصوى – السجن لمدة ثلاث سنوات.

(2) أي دعوى تقام بسبب جريمة معرَّفة في هذه المادة يكون للشخص المتهم إمكانية التذرُّع بعذر قانوني عن نشر مواد تشهيرية عن الشخص المعني في حالة واحدة فقط لا غير، وهي انطباق الفقرة الفرعية (3) على الحالة. [...]

وهناك مثال آخر لتجريم القذف وهو المادة 185 من قانون العقوبات الألماني:

الحكم:

المادة 185 – الإهانة

تعاقب الإهانة بالحبس بمدة لا تزيد عن سنة واحدة أو بغرامة، وإذا ارتُكبت الإهانة عن طريق العنف تعاقب بالحبس لمدة لا تزيد عن سنتين أو بغرامة.

ولا يهدف هذان الحكمان إلى تغطية الأفعال المتصلة بالإنترنت فقط. ولا يقتصر التطبيق على بعض أساليب الاتصال، ولهذا يمكن أن يغطي التطبيق الأفعال المرتكبة داخل الشبكة إلى جانب الأفعال المرتكبة خارجها.

12.1.6 الرسائل الاقتحامية

نظراً لما يتردَّد من أن نسبة تصل إلى 75 في المائة[1181] من جميع رسائل البريد الإلكتروني هي رسائل اقتحامية،[1182] فقد نوقشت بكثافة[1183] ضرورة فرض جزاءات جنائية على رسائل البريد الإلكتروني الاقتحامية. وتختلف الحلول التشريعية الوطنية التي تعالج مشكلة الرسائل الاقتحامية.[1184] ومن الأسباب الرئيسية التي تجعل الرسائل الاقتحامية مشكلة قائمة حتى الآن هو أن تكنولوجيا التنقية (الفلترة) لا تزال غير قادرة على تعيين ومنع رسائل البريد الإلكتروني الاقتحامية.[1185] ولا تتيح تدابير الحماية سوى حماية محدودة من رسائل البريد الإلكتروني غير المرغوبة.

وفي عام 2005، نشرت منظمة التنمية والتعاون في الميدان الاقتصادي تقريراً يحلل أثر الرسائل الاقتحامية على البلدان النامية.[1186] ويشير التقرير إلى أن ممثلي البلدان النامية يعربون في كثير من الأحيان عن رأيهم بأن مستعملي الإنترنت في بلدانهم يعانون بقدر أكبر كثيراً من تأثير الرسائل الاقتحامية وسوء استغلال الإنترنت. وأثبت تحليل نتائج التقرير أن انطباع هؤلاء الممثلين كان صحيحاً. وبسبب ضيق الموارد وارتفاع تكلفتها تتحوَّل الرسائل الاقتحامية إلى قضية أخطر بكثير في البلدان النامية عنها في البلدان الغربية.[1187]

[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.

[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.

ومع ذلك، فليس تعيين رسائل البريد الإلكتروني الاقتحامية وحده هو الذي يثير صعوبات. إذ إن الفصل بين رسائل البريد الإلكتروني التي لا يرغبها المتلقي ولكن يتم إرسالها بطريقة قانونية، من ناحية، والرسائل التي يتم إرسالها بطريقة غير قانونية، يمثّل تحدياً. ويبرز الاتجاه الحالي صوب الإرسال على أساس الحاسوب (بما في ذلك البريد الإلكتروني والصوت على بروتوكول إنترنت) أهمية حماية الاتصالات من الهجوم. وإذا زادت الرسائل الاقتحامية عن مستوى معيَّن، فإن رسائل البريد الإلكتروني الاقتحامية يمكن أن تعرقل بصورة خطيرة استعمال تكنولوجيا المعلومات والاتصالات وتقلّل إنتاجية المستعمل.

الاتفاقية المتعلقة بالجريمة الإلكترونية

لا تتضمن الاتفاقية المتعلقة بالجريمة الإلكترونية تجريماً صريحاً للرسائل الاقتحامية.[1188] ويشير واضعو الاتفاقية بأن يقتصر تجريم هذه الأفعال على الإعاقة الخطيرة والمتعمَّدة للاتصالات.[1189] ولا يركّز هذا النهج على رسائل البريد الإلكتروني غير المطلوبة ولكن على آثار ذلك على المنظومة الحاسوبية أو الشبكة. واستناداً إلى النهج القانوني في الاتفاقية المتعلقة بالجريمة الإلكترونية، يمكن أن تستند مكافحة الرسائل الاقتحامية إلى التداخل غير القانوني في الشبكات والنُظم الحاسوبية فقط:

المادة 5 – التدخل في المنظومة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتُكب عمداً، وبغير حق: الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن طريق إدخال أو إرسال، أو إتلاف، أو محو، أو تغيير، أو تبديل، أو تدمير بيانات كمبيوتر.

مشروع اتفاقية ستانفورد

لا يشمل مشروع اتفاقية ستانفورد غير الرسمي[1190] لعام 1999 نصاً يجرِّم الرسائل الاقتحامية. ومشروع هذه الاتفاقية، مثله مثل الاتفاقية المتعلقة بالجريمة الإلكترونية، يجرِّم فقط الرسائل الاقتحامية إذا كانت رسائل البريد الإلكتروني غير المطلوبة تؤدي إلى تداخل متعمَّد في النظام.

مثال من التشريعات الوطنية

يعني ذلك أن تجريم الرسائل الاقتحامية يقتصر على الحالات التي يؤثر فيها حجم رسائل البريد الإلكتروني الاقتحامية تأثيراً خطيراً على قوة تشغيل الأنظمة الحاسوبية. وتؤثر رسائل البريد الإلكتروني الاقتحامية على فعالية التجارة، ولكنها لا تؤثر بالضرورة على المنظومة الحاسوبية، ولا يمكن ملاحقتها لذلك. ولذلك يتبع عدد من البلدان نهجاً مختلفاً. ومن أمثلة ذلك تشريع الولايات المتحدة – العنوان 18 من مدونة الولايات المتحدة، البند 1037.[1191]

البند 1037 – الغش والأنشطة المتصلة فيما يتعلق بالبريد الإلكتروني

(أ) عموماً – في موضوع التجارة بين الولايات أو التجارة الخارجية أو ما يؤثر عليها، أي شخص يقوم عن علم –

(1) بالنفاذ إلى حاسوب يتمتع بالحماية بدون تصريح، ويبدأ عن عمد إرسال رسائل بريد إلكتروني تجارية متعددة من هذا الحاسوب أو عبره،

[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.

[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.

(2) باستعمال حاسوب يتمتع بالحماية لإرسال أو إعادة إرسال رسائل بريد إلكتروني تجارية متعددة، بغرض خداع أو تضليل المتلقين، أو أي خدمة للنفاذ إلى الإنترنت، عن مصدر هذه الرسائل،

(3) بتزييف مادي لمعلومات الرأسية في رسائل بريد إلكتروني تجارية عديدة ويبدأ عن عمد في إرسال هذه الرسائل،

(4) مستعملاً المعلومات التي تزيف مادياً هوية الشخص المسجِّل الفعلي، بالتسجيل لخمسة أو أكثر من حسابات البريد الإلكتروني أو حسابات للمستعملين على الخط أو اسمي ميدانين أو أكثر، ويبدأ عن عمد إرسال رسائل بريد إلكتروني تجارية متعددة من أي مجموعة من هذه الحسابات أو أسماء الميادين، أو

(5) يقدِّم نفسه بصورة زائفة باعتباره المسجِّل أو بالخلف الشرعي لمصلحة المسجِّل في خمس عناوين بروتوكولات إنترنت أو أكثر، ويتعمّد البدء في إرسال رسائل بريد إلكتروني تجارية متعددة من هذه العناوين،

أو يتآمر للقيام بذلك، يعاقَب على النحو المنصوص عليه في الفقرة الفرعية (ب).

(ب) العقوبات – تكون عقوبة الجريمة المنصوص عليها في الفقرة الفرعية (أ) هي –

(1) غرامة بموجب هذا العنوان، أو الحبس لمدة لا تزيد عن خمس سنوات أو كلاهما، في حالة –

(ألف) ارتكاب الجريمة لمتابعة جنحة بموجب قوانين الولايات المتحدة أو قانون أي ولاية؛ أو

(باء) إذا كان المتهم قد سبقت إدانته بموجب هذه المادة أو المادة 1030، أو بموجب قانون أي ولاية بسبب سلوك ينطوي على إرسال رسائل بريد إلكتروني تجارية متعددة أو النفاذ غير المسموح إلى منظومة حاسوبية؛

وقد طُبِّق هذا الحكم في قانون مكافحة الرسائل غير المرغوبة (الاقتحامية) الكندي لعام 2003.[1192] والقصد من القانون هو إقامة معيار وطني وحيد بغرض السيطرة على البريد الإلكتروني التجاري.[1193] وينطبق على الرسائل الإلكترونية التجارية، ولكنه لا ينطبق على الرسائل المتصلة بالصفقات والأعمال والعلاقات التجارية القائمة. ويتطلب النهج التنظيمي أن تشمل الرسائل الإلكترونية التجارية دلالة على طلب، بما في ذلك تعليمات خيار الرفض والعنوان الفعلي للراسل.[1194] ويُجرِّم البند 1037 من العنوان 18 من مدوّنة الولايات المتحدة مُرسلي رسائل البريد الإلكتروني الاقتحامية خاصة إذا كانت تزيِّف معلومات رأسية البريد الإلكتروني للالتفاف على تكنولوجيا التنقية (الفلترة).[1195] وبالإضافة إلى ذلك، يُجرِّم الحكم النفاذ غير المسموح إلى حاسوب متمتع بحماية وبدء إرسال رسائل بريد إلكتروني تجارية عديدة.

13.1.6 إساءة استخدام الأجهزة

هناك قضية خطيرة أخرى وهي وجود أدوات برمجيات وعتاد مخصصة لارتكاب الجرائم.[1196] فإلى جانب تكاثر ''أجهزة القرصنة'' يعتبر تبادل كلمات المرور الذي يمكّن المستعمِلين غير المأذون لهم من النفاذ إلى الأنظمة الحاسوبية تحدياً خطيراً.[1197] وتوفُّر هذه الأجهزة وتمديدها المحتمل يجعل من العسير تركيز التجريم على استعمال هذه الأدوات لارتكاب الجرائم فقط. وتضم معظم أنظمة القوانين الجنائية الوطنية بعض الأحكام التي تجرِّم إعداد وإنتاج هذه الأدوات، بالإضافة إلى ''محاولة ارتكاب الجريمة''. ويتمثّل أحد نُهُج مكافحة توزيع هذه الأجهزة في تجريم إنتاج الأدوات. وعموماً يقتصر هذا التجريم – الذي يقترن في العادة بدرجة واسعة من نقل المسؤولية الجنائية إلى الأمام – على أكثر الجرائم خطورة. وبالتحديد توجد اتجاهات في تشريعات الاتحاد الأوروبي لتوسيع التجريم عن أعمال الإعداد لتشمل جرائم أقل خطورة.[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.

الاتفاقية المتعلقة بالجريمة الإلكترونية

مع مراعاة مبادرات مجلس أوروبا الأخرى قرّر واضعو الاتفاقية النصّ على جريمة جنائية مستقلة عن الأفعال غير القانونية بصدد بعض الأجهزة أو الوصول إلى البيانات التي يساء استخدامها لأغراض ارتكاب جرائم ضد السرّية والسلامة وتوفُّر الأنظمة أو البيانات الحاسوبية[1199]:

الحكم:

المادة 6 – إساءة استخدام الأجهزة

(1) تعتمد كل دولة طرف ما قد يلزَم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبَت عمداً، وبغير حق:

(أ) الإنتاج أو البيع، والحصول بغرض الاستخدام، أو الجلب أو التوزيع أو بالأحرى التوفير:

'1' لجهاز يشمل برنامج كمبيوتر، صُمِّم أو طُوِّع ابتداءً، بغرض ارتكاب أيٍ من الجرائم المنصوص عليها أعلاه في المواد من 2-5؛

'2' لكلمة سر خاصة بكمبيوتر، أو كود دخول، أو بيانات مماثلة يمكن بواسطتها الدخول على كامل أو جزء من منظومة كمبيوتر، بغرض ارتكاب أيٍ من الجرائم المنصوص عليها أعلاه في المواد من 2-5؛ و

(ب) الحيازة لإحدى الأشياء المشار إليها بالفقرة (أ) '1' أو '2' بعاليه، بغرض ارتكاب أي من الجرائم المنصوص عليها أعلاه في المواد من 2-5. يجوز لطرف أن يستلزم قانوناً أن تكون حيازة عدد من هذه الأشياء قد تمت لقيام المسؤولية الجنائية.

(2) لا يجوز تفسير هذه المادة على أنها ترتِّب مسؤولية جنائية طالما أن الإنتاج أو البيع، أو الحصول بغرض الاستخدام، أو الجلب، أو التوزيع، أو بالأحرى التوفير، أو الحيازة المشار إليها بالفقرة 1 من هذه المادة ليست بغرض ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 2-5 من هذه الاتفاقية، كما في حالة اختبار منظومة كمبيوتر أو حمايتها بناءً على تصريح يبيح ذلك.

(3) يجوز لكل طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، بشرط ألاّ يكون هذا التحفُّظ متعلقاً بعمليات بيع، أو توزيع، أو بالأحرى توفير هذه الأشياء المشار إليها بالفقرة (1) (أ) '2' من هذه المادة.

الأشياء المشمولة:

تعيِّن الفقرة 1 (أ) الأجهزة[1200] المخصصة لارتكاب وتشجيع الجريمة السيبرانية وكلمات المرور التي تمكِّن من النفاذ إلى منظومة حاسوبية.

- ويغطي مصطَلح ''الأجهزة'' العتاد وكذلك البرمجيات التي تستند إلى حلول لارتكاب إحدى الجرائم المذكورة. ويذكر التقرير التفسيري مثلاً برمجية مثل برامج الفيروسات، أو البرامج المخصصة أو المكيّفة للحصول على النفاذ إلى المنظومات الحاسوبية.[1201]
- ''كلمة السر الخاصة بالكمبيوتر، أو كود الدخول أو بيانات مماثلة'' لا تشبه الأجهزة حيث لا تؤدّي عمليات ولكنها عبارة عن شفرات نفاذ. وكان أحد الأسئلة موضع المناقشة في هذا السياق هو السؤال الخاص بما إن كان نشر أوجه ضعف النظام يدخل تحت هذا الحكم.[1202] وبعكس شفرات النفاذ التقليدية لا تمكّن أوجه ضعف النظام بالضرورة من النفاذ فوراً إلى النظام الحاسوبي ولكنها تمكِّن الجاني من الاستفادة من أوجه الضعف للنجاح في هجومه على النظام الحاسوبي.

[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.

[1202] See in this context *Biancuzzi*, The Law of Full Disclosure, 2008, available at: http://www.securityfocus.com/print/columnists/466.

الأفعال المشمولة:

تُجَرِّم الاتفاقية مجموعة واسعة من الأفعال. فبالإضافة إلى الإنتاج، تعاقِب الاتفاقية أيضاً على بيع الأجهزة وكلمات المرور والحصول عليها بغرض استعمالها واستيرادها وتوزيعها أو توفيرها بشكل آخر. ويمكن الاضطلاع على نهج مشابه (يقتصر على الأجهزة المخصّصة للالتفاف على التدابير التقنية) في تشريع الاتحاد الأوروبي بشأن تنسيق حقوق الطبع.[1203] وطبّق عدد من البلدان أحكاماً مشابهة في قوانينها الجنائية.[1204]

- ''التوزيع'' ويغطّي الأفعال النشطة في تحويل الأجهزة أو كلمات المرور إلى آخرين.[1205]
- ''البيع'' ويصف الأنشطة الداخلة في بيع الأجهزة وكلمات المرور مقابل المال أو مقابل تعويض آخر.

[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.

- ''الحصول بغرض الاستخدام'' ويغطي الأفعال المتصلة بالأفعال النشطة للحصول على كلمات المرور والأجهزة.[1206] ونظراً لأن فعل الحصول يرتبط باستعمال هذه الأدوات عموماً يتطلب وجود قصد لدي الجاني للحصول على الأدوات لاستعمالها بطريقة تتجاوز القصد ''العادي'' وذلك بغرض ارتكاب أيٍ من الجرائم المنصوص عليها في المواد من 2-5''.

ويغطي الجلب أفعال الحصول على الأجهزة وشفرات النفاذ من بلدان أجنبية.[1207] ونتيجة لذلك، فإن مرتكبي الجرائم الذين يجلبون هذه الأدوات لبيعها يمكن ملاحقتهم حتى قبل قيامهم بعرض هذه الأدوات. وفيما يتعلق بالحقيقة المتمثلة في أن جلب هذه الأدوات لا يخضع للتجريم إلاّ إذا ارتبط باستعمالها، فإنه من المشكوك فيه أن مجرّد جلب الأدوات دون قصد البيع أو الاستعمال يقع تحت طائلة المادة 6 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

ويشير ''التوفير'' إلى فعل يمكّن المستعمِلين الآخرين من الحصول على الأصناف.[1208] ويشير التقرير التفسيري بأن مصطَلح ''التوفير'' يقصد أيضاً إلى تغطية إنشاء أو تجميع الوصلات الإلكترونية من أجل تسهيل النفاذ إلى هذه الأجهزة.[1209]

أدوات الاستعمال المزدوج:

بعكس نهج الاتحاد الأوروبي في تنسيق حقوق الطبع،[1210] لا يقتصر انطباق هذا الحكم على الأجهزة المخصصة حصرياً لتسهيل ارتكاب الجريمة الإلكترونية – بل إن الاتفاقية تغطي أيضاً الأجهزة التي تستعمل عادة في أغراض قانونية إذا كان الهدف المحدّد لمرتكبي الجرائم هو ارتكاب جريمة إلكترونية. وفي التقرير التفسيري يشير واضعو الاتفاقية إلى أن الاقتصار على الأجهزة المخصصة فقط لارتكاب جرائم هو تقييد ضيّق جداً ويمكن أن يؤدّي إلى صعوبات لا يمكن التغلّب عليها في مجال الإثبات في الدعاوى الجنائية، بما يجعل هذا الحكم غير قابل للتطبيق عملياً أو ينطبق فقط في حالات نادرة.[1211]

ولكفالة الحماية الصحيحة للأنظمة الحاسوبية، فإن الخبراء يستعملون ويملكون أدوات برمجية مختلفة تجعل منهم مجال تركيز محتمل لإنفاذ القانون. وتفحص الاتفاقية هذه الانشغالات بثلاث طرق[1212]:

- فهي تمكّن الأطراف في الفقرة 1 (ب) من المادة 6 من وضع تحفّظات تتعلّق بحيازة العدد الأدنى من هذه البنود قبل أن يمكن إسناد المسؤولية الجنائية.
- وإلى جانب ذلك يقتصر تجريم حيازة هذه الأجهزة على اشتراط أن يكون القصد من استعمال الجهاز هو ارتكاب جريمة محدّدة في الفقرات من 2 إلى 5 في الاتفاقية.[1213] ويشير التقرير التفسيري إلى أن هذا القصد الخاص قد أُدرج ''لتجنّب خطر الإفراط

[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.*

[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.

في التجريم عند إنتاج هذه الأجهزة وبيعها في السوق لأغراض مشروعة، وذلك مثلاً لمكافحة الهجمات ضد الأنظمة الحاسوبية''.[1214]

- وأخيراً، يعلن واضعو الاتفاقية بوضوح في الفقرة 2 أن الأدوات التي يتم إنتاجها لأغراض الاختبار المسموح به أو لحماية نظام حاسوبي لا تندرج تحت هذا الحكم نظراً لأن الحكم يغطي الفعل غير المسموح به.

تجريم الحيازة:

تذهب الفقرة 1 (ب) من التنظيم الوارد في الفقرة 1 (أ) خطوة أبعد عندما تُجرّم حيازة الأجهزة أو كلمات المرور، في حالة اتصالها بقصد ارتكاب جريمة إلكترونية. وتجريم حيازة أدوات هو موضع جدل.[1215] فالمادة 6 لا تقتصر على الأدوات المخصصة حصرياً لارتكاب جرائم ويشعر معارضو التجريم بالقلق لأن تجريم حيازة هذه الأجهزة يمكن أن ينشئ مخاطر غير مقبولة لمديري الأنظمة وخبراء أمن الشبكات.[1216] وتمكّن الاتفاقية الأطراف من اقتضاء وجود عدد معيَّن من هذه البنود في الحيازة قبل تعليق أي مسؤولية جنائية.

العنصر الذهني:

كما يحدث في حالة جميع الجرائم الأخرى المعرّفة في الاتفاقية المتعلقة بالجريمة الإلكترونية، تقتضي المادة 6 أن يرتكب الجاني جريمته عمداً.[1217] وبالإضافة إلى القصد العادي بشأن الأفعال المشمولة بالمادة 6 تقتضي الاتفاقية المتعلقة بالجريمة الإلكترونية إضافة قصد خاص لاستعمال الجهاز بغرض ارتكاب أيٍ من الجرائم المقرّرة في المواد من 2 إلى 5 من الاتفاقية.[1218]

بغير حق:

يجب ارتكاب الأفعال ''بغير حق''،[1219] ويتشابه ذلك مع الأحكام التي نوقشت أعلاه. وفيما يتعلق بالمخاوف من إمكانية استعمال هذا الحكم لتجريم التشغيل المشروع لأدوات البرمجيات في إطار حدود الحماية الذاتية، يشير واضعو الاتفاقية إلى أن القيام بهذه الأفعال لا يعتَبر ''بغير حق''.[1220]

التقييدات والتحفّظات:

نظراً للمناقشة التي جرت بشأن ضرورة تجريم حيازة الأجهزة تعرض الاتفاقية خيار تحفّظ معقّد في الفقرة 3 من المادة 6 (بالإضافة إلى الجملة 2 من الفقرة 1 (ب)). وإذا استعمَل أحد الأطراف هذا التحفّظ، فإنه يستطيع استبعاد تجريم حيازة الأدوات واستبعاد تجريم عدد من الأعمال غير المشروعة بموجب الفقرة 1 (أ) – مثل حالة إنتاج هذه الأجهزة.[1221]

[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.

[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.

قانون الكومنولث النموذجي

يمكن الاطلاع على نهج يتسق مع المادة 6 من الاتفاقية المتعلقة بالجريمة الإلكترونية في المادة 9 من قانون الكومنولث النموذجي لعام 2002.[1222]

المادة 9

(1) يرتكب أي شخص جريمة عندما يقوم هذا الشخص:

(أ) متعمّداً أو مستهتراً وبدون عذر أو مبرر قانوني، بإنتاج أو بيع، أو شراء بغرض الاستعمال، أو استيراد، أو تصدير، أو توزيع، أو إتاحة بشكل آخر:

'1' جهاز، بما في ذلك برنامج حاسوبي، مخصّص أو مكيَّف لغرض ارتكاب جريمة ضد المادة 5 أو 6 أو 7 أو 8؛ أو

'2' كلمة مرور حاسوب بشفرة نفاذ أو بيانات مشابهة يمكن بموجبها النفاذ إلى النظام الحاسوبي أو جزء منه؛

بقصد الاستعمال من جانب أي شخص بغرض ارتكاب جريمة ضد المواد 5 أو 6 أو 7 أو 8؛ أو

(ب) حيازة بند مذكور في الفقرة الفرعية '1' أو '2' بقصد استعمال هذا البند من جانب أي شخص بغرض ارتكاب جريمة ضد المادة 5 أو 6 أو 7 أو 8.

(2) ويتعرّض الشخص المدان بجريمة بموجب هذه المادة لعقوبة الحبس لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ]، أو كلاهما.

والاختلاف الرئيسي مع الاتفاقية المتعلقة بالجريمة الإلكترونية هو أن قانون الكومنولث النموذجي يُجرِّم الأفعال التي تجري باستهتار. وأثناء التفاوض بشأن قانون الكومنولث النموذجي نوقِشَت تعديلات أخرى للحكم الذي يجرّم حيازة هذه الأجهزة. وأشار فريق الخبراء بأن يكون تجريم الجناة الذين يمتلكون بنداً أو أكثر.[1223] واقتَرحت كندا نهجاً مشابهاً بدون تحديد مُسبَق لعدد البنود التي تؤدّي إلى التجريم.[1224]

مشروع اتفاقية ستانفورد

يتضمّن مشروع اتفاقية ستانفورد غير الرسمي[1225] لعام 1999 حكماً يُجرّم الأفعال المتصلة ببعض الأجهزة غير القانونية.

[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.

[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: *Subsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

[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: *Subsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

[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.

المادة 3 – الجرائم

1 تُرتكَب جرائم تندرج تحت طائلة هذه الاتفاقية إذا باشر أي شخص بطريقة غير قانونية وعمداً أي من السلوك التالي بدون سلطة أو إذن أو موافقة معترف بها قانونياً:

[...]

(هـ) صناعة أي جهاز أو برنامج أو بيعه أو استعماله أو نشره أو توزيعه بشكل آخر إذا كان مخصصاً لغرض ارتكاب أي سلوك محظور بموجب المادتين 3 و4 من هذه الاتفاقية؛

ويشير واضعو الاتفاقية بأنه ليس من المطلوب عموماً معاملة أي نوع من الخطاب أو النشر باعتباره إجرامياً بموجب مشروع اتفاقية ستانفورد.[1226] وكان الاستثناء الوحيد يتصل بالأجهزة غير القانونية.[1227] وفي هذا السياق أبرز واضعو الاتفاقية أن التجريم ينبغي أن يقتصر على الأفعال المذكورة وألاّ يشمل مثلاً مناقشة أوجه ضعف النظام.[1228]

14.1.6 التزوير المتصل بالحاسوب

الدعاوى الجنائية التي تنطوي على التزوير المتصل بالحاسوب نادرة عموماً، وذلك لأن معظم الوثائق القانونية وثائق ملموسة. وهذه الحالة في سبيلها إلى التغيُّر مع الرقمنة.[1229] والاتجاه نحو الوثائق الرقمية يدعمه إنشاء خلفية قانونية لاستعمالها، مثل الاعتراف القانوني بالتوقيعات الرقمية. وبالإضافة إلى ذلك، فإن الأحكام التي تكافح التزوير المتصل بالحاسوب تؤدّي دوراً هاماً في مكافحة "التصيُّد الاحتيالي".[1230]

الاتفاقية المتعلقة بالجريمة الإلكترونية

تُجرِّم معظم أنظمة القانون الجنائي جريمة التزوير في وثائق ملموسة.[1231] وأشار واضعو الاتفاقية إلى تباين هيكل القواعد المتصلة في النُهج القانونية الوطنية.[1232] وفي حين يستند أحد المفاهيم إلى صحة شخصية كاتب الوثيقة يستند مفهوم آخر إلى صحة البيان الوارد فيها. وقرّر واضعو الاتفاقية

[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.

[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.

تنفيذ المعايير الدنيا وحماية أمن وموثوقية البيانات الإلكترونية من خلال إنشاء جريمة موازية لجريمة التزوير التقليدية في الوثائق الملموسة لسد الثغرات في القانون الجنائي الذي قد لا ينطبق على البيانات المخزونة إلكترونيا.[1233]

الحكم:

المادة 7 – جريمة التزوير المتعلقة بالكمبيوتر

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبَت عمداً، وبغير حق: إدخال، أو تبديل، أو محو، أو تدمير بيانات كمبيوتر، ينتج عنها بيانات غير أصلية بقصد استخدامها أو التعويل عليها في أغراض قانونية كما لو كانت أصلية، بغض النظر عمّا إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر من عدمه. يجوز لطرف أن يشترط وجود نيّة التدليس، أو قصد غير أمين مشابه، لقيام المسؤولية الجنائية.

الغرض المشمول:

هدف التزوير المتصل بالحاسوب هو البيانات – بغض النظر عمّا إن كانت مقروءة و/أو مفهومة بصورة مباشرة. وتُعرَّف البيانات الحاسوبية في الاتفاقية بأنها[1234] ''أية عمليات عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية معالجة داخل منظومة الكمبيوتر، بما في ذلك برنامج مناسب لجعل منظومة كمبيوتر تؤدي وظائفها''. ولا يشير الحكم فقط إلى البيانات الحاسوبية باعتبارها هدف أحد الأعمال المذكورة. إذ إنه من الضروري بالإضافة إلى ذلك، أن تؤدّي الأعمال إلى بيانات غير أصلية.

وتتطلّب المادة 7 – على الأقل فيما يتعلق بالعنصر الذهني – أن تكون البيانات معادلاً لوثيقة عامة أو خاصة. ويعني ذلك أن البيانات يجب أن تكون ذات أهمية قانونية[1235] – ولا يشمل الحكم تزييف البيانات التي لا يمكن استعمالها في أغراض قانونية.

1) الأفعال المشمولة

- يجب أن يناظر ''إدخال'' البيانات[1236] إنتاج وثيقة ملموسة زائفة.[1237]
- يشير مصطَلح ''تبديل'' إلى تعديل بيانات موجودة.[1238] ويشير التقرير التفسيري خاصة إلى التباينات والتغييرات الجزئية.[1239]
- ويشير مصطَلح ''تدمير'' البيانات الحاسوبية إلى عمل يؤثّر على توفّر البيانات.[1240] ويشير واضعو الاتفاقية خاصة في التقرير التفسيري إلى حجب أو إخفاء البيانات.[1241] ويمكن مثلاً القيام بهذا الفعل بمنع بعض المعلومات عن قاعدة بيانات أثناء الإنشاء الأوتوماتي لوثيقة إلكترونية.
- ومصطَلح ''محو'' يناظر تعريف هذا المصطَلح الوارد في المادة 4 ويغطي أفعالاً تتم بموجبها إزالة معلومات.[1242] ويشير التقرير التفسيري فقط إلى إزالة معلومات من وسيط بيانات.[1243] ولكن نطاق الحكم يدعم بقوة تعريفاً أوسع لمصطَلح ''محو''. ويمكن، استناداً إلى هذا التعريف الأوسع، اقتراف الفعل إما بإزالة ملف كامل أو مسح المعلومات من الملف جزئياً.[1244]

العنصر الذهني:

كما يحدث في حالة جميع الجرائم الأخرى المعرَّفة في الاتفاقية المتعلقة بالجريمة الإلكترونية، تقتضي المادة 3 أن يرتكب الجاني جريمته عمداً.[1245] ولا تتضمن الاتفاقية تعريفاً لمصطلح ''عمداً''. وفي التقرير التفسيري يشير واضعو الصياغة إلى أن تعريف ''عمداً'' ينبغي أن يجري على صعيد وطني.[1246]

[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."

[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.

بغير حق:

لا يمكن ملاحقة أفعال التزييف بموجب المادة 7 من الاتفاقية إلاّ إذا ارتُكبت "بغير حق".[1247]

التقييدات والتحفّظات:

تتيح المادة 7 إمكانية إبداء تحفّظ من أجل الحدّ من التجريم، وذلك باقتضاء عناصر إضافية مثل قصد التزييف قبل إنشاء المسؤولية الجنائية.[1248]

قانون الكومنولث النموذجي

لا يتضمَّن قانون الكومنولث النموذجي لعام 2002 أي حكم يُجرِّم التزييف المتصل بالحاسوب.[1249]

مشروع اتفاقية ستانفورد

يتضمَّن مشروع اتفاقية ستانفورد غير الرسمي[1250] لعام 1999 حكماً يُجَرِّم الأفعال المتصلة ببيانات الحاسوب المزيّفة.

المادة 3 – الجرائم

1 بموجب هذه الاتفاقية تُرتَكب جرائم إذا قام أي شخص بصورة غير قانونية ومتعمّداً بمباشرة أي سلوك مذكور أدناه بدون سلطة أو تصريح أو موافقة معترف بها قانونياً:

[...]

(ب) إنشاء بيانات في نظام سيبراني أو تخزينها أو تبديلها أو حذفها أو إرسالها أو تحويلها أو تسييرها بطريقة خاطئة أو التلاعب بها أو التداخل فيها بغرض وبنتيجة تقديم معلومات زائفة من أجل إحداث ضرر كبير لأشخاص أو ممتلكات؛

[...]

والاختلاف الرئيسي عن المادة 7 في الاتفاقية المتعلقة بالجريمة الإلكترونية هو أن الفقرة 1(ب) من المادة 3 لا تركِّز على مجرّد التلاعب بالبيانات ولكنها تتطلب تداخلاً في النظام الحاسوبي. ولا تتطلّب المادة 7 من الاتفاقية المتعلقة بالجريمة الإلكترونية هذا الفعل. ويكفي أن يقوم الجاني بفعله بقصد اعتبار الفعل أو التصرّف حياله في الأغراض القانونية كما لو كان قصرياً.

[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.

15.1.6 سرقة الهوية

إذا وضعنا في الاعتبار التغطية الإعلامية،[1251] ونتائج الدراسات الاستقصائية الأخيرة[1252] وكذلك المنشورات العديدة القانونية والتقنية[1253] في هذا الميدان، فسوف يبدو من الملائم الحديث عن سرقة الهوية باعتبارها ظاهرة واسعة الانتشار.[1254] ورغم الجوانب العالمية لهذه الظاهرة لم تُطبِّق جميع البلدان بعد أحكاماً في نظام قانونها الجنائي الوطني لتجريم جميع الأفعال المتصلة بسرقة الهوية. وقد أعلنت مفوضية الاتحاد الأوروبي مؤخراً أن سرقة الهوية لم تخضع بعد للتجريم في جميع الدول الأعضاء في الاتحاد الأوروبي.[1255] وأعربت المفوضية عن رأيها بأن "التعاون في إنفاذ القوانين في الاتحاد الأوروبي سيكون أكثر فعالية لو تم تجريم سرقة الهوية في جميع الدول الأعضاء" وأعلنت أنها ستبدأ قريباً في مشاورات لتقييم ما إن كان من الملائم تطبيق تشريع من هذا القبيل.[1256]

ومن المشاكل المتصلة بمقارنة الصكوك القانونية القائمة في مكافحة سرقة الهوية أن هذه الصكوك تختلف اختلافاً هائلاً.[1257] والعنصر الثابت الوحيد في النُهُج القائمة هو أن السلوك المدان يتصل بمرحلة أو أخرى من المراحل التالية[1258]:

- المرحلة 1: فعل الحصول على المعلومات المتصلة بالهوية؛
- المرحلة 2: فعل حيازة أو نقل المعلومات المتصلة بالهوية؛
- المرحلة 3: فعل استعمال المعلومات المتصلة بالهوية في أغراض جنائية.

واستناداً إلى هذه الملاحظة يوجد نهجان منتظمان في تجريم سرقة الهوية:

- وضع حكم واحد يجرّم فعل الحصول على المعلومات المتصلة بالهوية (لأغراض جنائية) وحيازتها واستعمالها.
- التجريم المنفرد للتصرفات النمطية المتصلة بالحصول على المعلومات المتصلة بالهوية (مثل النفاذ غير القانوني وإنتاج ونشر البرمجيات الخبيثة والتزييف المتصل بالحاسوب والتجسس على البيانات والتداخل في البيانات) وكذلك الأفعال المتصلة بحيازة واستعمال هذه المعلومات (مثل الغش المتصل بالحاسوب).

مثال لنهج الحكم الوحيد

يمثِّل البندان 1028(أ) (7) و1028 ألف (أ) (1) من العنوان 18 من مدوّنة الولايات المتحدة أشهر مثالين لنهج الحكم الوحيد. ويغطي الحكمان مجموعة واسعة من الجرائم المتصلة بسرقة الهوية. وفي إطار هذا النهج لا يقتصر التجريم على مرحلة بعينها ولكنه يغطي جميع المراحل الثلاث المذكورة أعلاه. ومع ذلك، فمن المهم التأكيد على أن الحكم لا يغطي جميع الأنشطة المتصلة بسرقة الهوية – ولا يغطي خاصة تلك الأنشطة التي يكون الضحية هو الذي يتصرف وليس الجاني.

1028 – الغش والأنشطة المتصلة فيما يتعلق بوثائق الهوية وخصائص التصديق والمعلومات

(أ) أي شخص، يقوم في الظروف الموصوفة في الفقرة الفرعية (ج) من هذه المادة –

(1) عن علم وبدون سلطة قانونية بإنتاج وثيقة هوية أو خاصية تصديق أو وثيقة هويّة مزيَّفة؛

(2) عن علم بنقل وثيقة هوية أو خاصية تصديق أو وثيقة هوية مزيفة وهو يعلم أن هذه الوثيقة أو الخاصية مسروقة أو صادرة بدون سلطة قانونية؛

[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.

(3) عن علم بامتلاك – بقصد الاستعمال غير القانوني أو النقل غير القانوني – خمس وثائق هوية أو أكثر (خلاف الوثائق الصادرة قانونيا لاستعمال صاحب الوثيقة) أو خصائص تصديق أو وثائق هوية مزيَّفة؛

(4) عن علم بامتلاك وثيقة هوية (خلاف الصادرة بصورة قانونية لاستعمال صاحب الوثيقة) أو خاصية تصديق أو وثيقة هوية مزيَّفة، بقصد استعمال هذه الوثيقة أو الخاصية للاحتيال على الولايات المتحدة؛

(5) عن علم بإنتاج أو نقل أو حيازة أداة لإصدار الوثائق أو إنتاج أو نقل أو حيازة خاصية تصديق بقصد استعمال هذه الأداة لإنتاج الوثائق أو خاصية التصديق في إنتاج وثيقة هوية مزيَّفة أو إنتاج أدوات أخرى لصنع وثائق أو إنتاج خاصية تصديق تُستعمل على النحو المذكور؛

(6) عن علم بامتلاك وثيقة هوية أو خاصية تصديق تكون أو يظهر منها أنها وثيقة هوية أو خاصية تصديق خاصة بالولايات المتحدة مسروقة أو منتَجة بدون سلطة قانونية مع العلم بأن هذه الوثيقة أو الخاصية سُرقت أو أنتُجت بدون هذه السلطة؛

(7) عن علم بنقل أو امتلاك أو استعمال، بدون سلطة قانونية، وسيلة تعرِّف على هوية شخص آخر بقصد ارتكاب نشاط غير قانوني أو المساعدة أو التحريض عليه أو فيما يتصل به، إذا كان يشكِّل انتهاكاً لقانون فيدرالي، أو يشكِّل جريمة بموجب أي قانون منطبق من قوانين الولايات أو القوانين المحلية؛ أو

(8) عن علم بالاتجار في خصائص التصديق المزيَّفة أو الفعلية لاستعمالها في وثائق هوية مزيَّفة أو أدوات صُنع الوثائق أو وسائل إثبات الهوية؛

يعاقب على النحو المنصوص عليه في الفقرة الفرعية (ب) من هذه المادة.

1028 ألف– سرقة الهوية في ظروف مشدَّدة

(أ) الجرائم –

(1) عموماً – أي شخص يقوم عن علم، أثناء وفيما يتصل بأي انتهاك جُرمي وارد في الفقرة الفرعية (ج) بنقل أو امتلاك أو استعمال، بدون سلطة قانونية، وسيلة إثبات هوية لشخص آخر يحكم عليه، بالإضافة إلى العقوبة المنصوص عليها عن هذه الجريمة، بالسجن لمدة سنتين.

المرحلة 1

يحتاج الجاني من أجل ارتكاب جرائم تتصل بسرقة الهوية إلى التوصل إلى حيازة البيانات المتصلة بالهوية.[1259] ومن خلال تجريم ''نقل'' وسيلة إثبات الهوية بقصد ارتكاب جريمة، فإن الأحكام تجرِّم الأفعال المتصلة بالمرحلة 1 بطريقة عريضة جداً.[1260] وبسبب تركيز الأحكام على فعل النقل فإنها لا تغطي الأفعال التي يقوم بها الجاني قبل بدء عملية النقل.[1261] فالأفعال من قبيل إرسال رسائل احتيالية وتصميم برمجية خبيثة يمكن استعمالها للحصول على البيانات المتصلة بالهوية الحاسوبية من الضحايا ليست مشمولة بالبندين 1028 (أ) (7) و1028 ألف (أ) (1) من العنوان 18 من مدونة الولايات المتحدة.

المرحلة 2

عندما تجرِّم الأحكام الحيازة بقصد ارتكاب الجريمة فإنها تعمد مرة أخرى إلى اعتناق نهج واسع فيما يتعلق بتجريم الأفعال المتصلة بالمرحلة الثانية. ويشمل ذلك بالخصوص المعلومات المتصلة بالهوية بقصد استعمالها فيما بعد في إحدى الجرائم التقليدية المتصلة بسرقة الهوية.[1262] وحيازة البيانات المتصلة بالهوية بدون قصد استعمالها ليس مشمولاً.[1263]

[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.

[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.

المرحلة 3

عندما تجرِّم الأحكام "الاستعمال" بقصد ارتكاب جريمة فإنها تغطي الأفعال المتصلة بالمرحلة 3. وكما جاء أعلاه، لا يتصل البند 1028 (أ) (7) من العنوان 18 من مدونة الولايات المتحدة بجريمة محدَّدة (مثل الغش).

مثال نهج متعدد الأحكام

الفرق الرئيسي بين الاتفاقية المتعلقة بالجريمة الإلكترونية ونُهج الحكم الوحيد (مثل نهج الولايات المتحدة على سبيل المثال) هو أن الاتفاقية لا تحدِّد جريمة سيبرانية منفصلة للاستعمال غير القانوني للمعلومات المتصلة بالهوية.[1264] وعلى نسق الحالة في صدد تجريم الحصول على المعلومات المتصلة بالهوية، لا تغطي الاتفاقية كل الأفعال الممكنة المتصلة بالاستعمال غير القانوني للمعلومات الشخصية.

المرحلة 1

تتضمن الاتفاقية المتعلقة بالجريمة الإلكترونية[1265] عدداً من الأحكام التي تجرِّم أفعال سرقة الهوية المتصلة بالإنترنت في المرحلة 1. وهذه الأحكام بالتحديد هي:

- الدخول الغير مشروع (المادة 2)[1266]
- الاعتراض الغير مشروع (المادة 3)[1267]
- التدخل في البيانات (المادة 4)[1268]

ومع مراعاة مختلف الطرق الممكنة التي يستطيع بها الجاني النفاذ إلى البيانات، فمن الضروري أن يشار إلى أن جميع الأفعال المحتملة في المرحلة 1 ليست مشمولة. فالتجسس على البيانات هو أحد أمثلة الجرائم التي تتصل في كثير من الأحيان بالمرحلة 1 من سرقة الهوية ولكنها غير مشمولة بالاتفاقية المتعلقة بالجريمة الإلكترونية.

المرحلة 2

لا يمكن بسهولة أن تغطي الاتفاقية المتعلقة بالجريمة الإلكترونية الأفعال التي تجري بين الحصول على المعلومات واستعمال المعلومات في أغراض إجرامية. وليس من الممكن بصورة خاصة منع وجود سوق سوداء متنامية للمعلومات المتصلة بالهوية من خلال تجريم بيع هذه المعلومات استناداً إلى أحكام تنص عليها الاتفاقية.

المرحلة 3

تعرِّف الاتفاقية المتعلقة بالجريمة الإلكترونية الصادرة عن مجلس أوروبا عدداً من الجرائم المتصلة بالجريمة السيبرانية. ويمكن أن يقترف الجناة هذه الجرائم باستعمال المعلومات المتصلة بالهوية. وأحد الأمثلة على ذلك هو الغش المتصل بالحاسوب الذي يُذكَر كثيراً في سياق سرقة الهوية.[1269] وتشير الدراسات الاستقصائية بشأن سرقة الهوية إلى أن معظم البيانات التي يتم الحصول عليها تُستعمل في الغش المتصل ببطاقات الائتمان.[1270]

[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.

[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 .

وفي حالة ارتكاب الغش المتصل ببطاقات الائتمان على الخط، فمن المرجح أن يمكن ملاحقة الجاني استناداً إلى المادة 8 من الاتفاقية المتعلقة بالجريمة الإلكترونية. أما الجرائم الأخرى التي يمكن القيام بها من خلال استعمال المعلومات المتصلة بالهوية والتي تم الحصول عليها من قبل ولكنها غير مذكورة في الاتفاقية فهي ليست مشمولة بالإطار القانوني. وليس من الممكن خصوصاً ملاحقة استعمال المعلومات المتصلة بالهوية بقصد إخفاء الهوية.

16.1.6 الغش المتصل بالحاسوب

الغش جريمة شائعة في الفضاء السيبراني.[1271] وهو أيضاً مشكلة شائعة خارج الإنترنت، ولهذا تتضمن معظم القوانين الوطنية أحكاماً تجرِّم هذه الجرائم.[1272] ومع ذلك، فإن تطبيق الأحكام الحالية على الحالات المتصلة بالإنترنت قد يكون عسيراً، حيث تستند أحكام القانون الجنائي الوطنية التقليدية إلى تزييف الشخص.[1273] وفي كثير من حالات الغش الجاني عبر الإنترنت يكون النظام الحاسوبي في الواقع هو الذي يستجيب لأفعال الجاني. وإذا كانت الأحكام الجنائية التقليدية التي تتناول الغش لا تغطي الأنظمة الحاسوبية فسيكون من الضروري تحديث القانون الوطني لهذا الغرض.[1274]

الاتفاقية المتعلقة بالجريمة الإلكترونية

تسعى الاتفاقية إلى تجريم أي تلاعب غير صحيح بمجرى تجهيز البيانات بقصد إحداث نقل غير قانوني للممتلكات من خلال النص على مادة تتعلق بالغش المتصل بالحاسوب.[1275]

[1271] See above: Chapter 2.7.1.

[1272] Regarding the criminalisation 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, 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.

الحكم:

المادة 8 – جريمة النصب المتعلقة بالكمبيوتر

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمداً، وبغير حق، وتسبَّبت في إلحاق خسارة بملكية شخص آخر عن طريق:

أ) أي إدخال، أو تبديل، أو محو، أو تدمير لبيانات كمبيوتر؛

ب) أي تدخل في وظيفة منظومة كمبيوتر، بقصد احتيالي أو غير أمين للحصول وبدون وجه حق، على منفعة اقتصادية لصالح الشخص ذاته أو لصالح الغير.

الأفعال المشمولة

تتضمن الفقرة (أ) من المادة 8 قائمة بأهم أفعال الغش المتصل بالحاسوب.[1276]

- يغطي ''إدخال'' بيانات حاسوبية جميع أنواع التلاعب بالمدخلات مثل تغذية بيانات غير صحيحة في حاسوب وكذلك عمليات التلاعب ببرمجيات الحاسوب وغير ذلك من عمليات التداخل في سياق تجهيز البيانات.[1277]
- ويشير مصطلح ''تبديل'' إلى تعديل البيانات الموجودة.[1278]
- ويشير مصطلح ''تدمير'' البيانات الحاسوبية إلى فعل يؤثر على توفر البيانات.[1279]
- ويناظر مصطلح ''محو'' تعريف المصطلح في المادة 4 التي تغطي أفعال إزالة معلومات.[1280]

وبالإضافة إلى قائمة الأفعال تتضمن الفقرة ب) من المادة 8 بنداً عاماً يجرِّم ''أي تدخل في وظيفة منظومة كمبيوتر'' فيما يتصل بالغش. وقد أُضيف البند العام إلى قائمة الأفعال المشمولة من أجل فتح هذا الحكم ليشمل أي تطورات أخرى.[1281]

ويشير التقرير التفسيري إلى أن أي ''تدخل في وظيفة منظومة كمبيوتر'' يغطي الأفعال من قبيل التلاعب بالعتاد وأفعال تدمير الصفحات المطبوعة والأفعال التي تؤثر على تسجيل أو تدفق البيانات أو تتابع تسيير البرامج.[1282]

الخسارة الاقتصادية:

تنص معظم القوانين الجنائية الوطنية على أن الفعل الجنائي يجب أن يؤدي إلى خسارة اقتصادية. وتتبع الاتفاقية مفهوماً مشابهاً وتقصر التجريم على تلك الأفعال التي ينجم فيها التلاعب عن خسارة اقتصادية أو حيازة مباشرة لممتلكات شخص آخر بما فيها الأموال والأصول المادية والأصول غير المادية ذات القيمة الاقتصادية.[1283]

العنصر الذهني:

كما حدث في حالة الجرائم المذكورة الأخرى تقتضي المادة 8 من الاتفاقية المتعلقة بالجريمة الإلكترونية أن يرتكب الجاني جريمته عمداً. ويشير هذا العمد إلى التلاعب وكذلك إلى الخسارة المالية.

[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.
[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.

وبالإضافة إلى ذلك، تقتضي الاتفاقية أن يتصرف الجاني بقصد احتيالي أو غير أمين للحصول على فوائد اقتصادية أو فوائد أخرى لنفسه أو للغير.[1284] ومن أمثلة الأفعال المستبعدة من المسؤولية الجنائية بسبب عدم توفر الدافع المحدَّد يذكر التقرير التفسيري الممارسات التجارية الناشئة عن التنافس في السوق والتي قد تسبب ضرراً اقتصادياً بأحد الأشخاص وفائدة لشخص آخر، ولكنها لا تجري بغرض احتيالي أو غير أمين.[1285]

بغير حق:

لا يمكن ملاحقة الغش المتصل بالحاسوب بموجب المادة 8 من الاتفاقية إلاّ إذا تم ارتكابه "بغير حق".[1286] ويشمل ذلك اقتضاء أن الفائدة الاقتصادية يجب الحصول عليها بغير حق. وأشار واضعو الاتفاقية إلى أن الأفعال لا تعتبر قد جرت بغير حق إذا كانت قد جرت عملاً بعقد صحيح بين الأشخاص المتأثرين.[1287]

قانون الكومنولث النموذجي

لا يتضمن قانون الكومنولث النموذجي لعام 2002 حكماً يجرِّم الغش المتصل بالحاسوب.[1288]

مشروع معاهدة ستانفورد

لا يتضمن مشروع معاهدة ستانفورد غير الرسمي[1289] لعام 1999 حكماً يجرِّم الغش المتصل بالحاسوب.

[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.

[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.

17.1.6 جرائم حقوق الطبع

كان التحوُّل من التوزيع التماثلي إلى التوزيع الرقمي للمحتوى الخاضع لحماية حقوق الطبع نقطة تحول في انتهاكات حقوق الطبع.[1290] وقد كان استنساخ الأعمال الفنية الموسيقية وشرائط الفيديو عملية محدودة تاريخياً نظراً لأن استنساخ مصدر تماثلي كان يقترن في كثير من الأحيان بفقد جودة النسخة وهو ما كان يحد بالتالي من خيار استعمال النُسخة كمصدر لعمليات استنساخ أخرى. ومع التحوُّل إلى الموارد الرقمية يتم الاحتفاظ بالنوعية وأصبح من الممكن صُنع نُسخ ذات جودة واحدة.[1291]

وقد استجابت صناعة الترفيه لذلك بتنفيذ تدابير تقنية (إدارة الحقوق الرقمية لمنع الاستنساخ)،[1292] ولكن حتى الآن يتم الالتفاف على هذه التدابير نمطياً بعد فترة قصيرة من تطبيقها.[1293] وتتوفَّر عدة أدوات برمجيات على الإنترنت تمكِّن المستعملين من نسخ الأقراص المدمجة الموسيقية (سي دي) وأقراص الفيديو الرقمية (دي في دي) المحمية بنُظم إدارة الحقوق الرقمية. وبالإضافة إلى ذلك، تتيح الإنترنت فرص توزيع غير محدودة. ونتيجة لذلك، أصبح انتهاك حقوق الملكية الفكرية (وخاصة حقوق الطبع) من الجرائم التي تُرتكب على نطاق واسع عبر الإنترنت.[1294]

الاتفاقية المتعلقة بالجريمة الإلكترونية

تتضمن الاتفاقية لذلك حكماً يغطي جرائم حقوق الطبع ويسعى هذا الحكم إلى تنسيق مختلف اللوائح في القوانين الوطنية:

المادة 10 – الجرائم المتعلقة بالانتهاكات الخاصة بحقوق الملكية الفكرية والحقوق المتعلقة بها:

(1) تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق الملكية الفكرية، بحسب تعريفها وفقاً للقانون الخاص بهذا الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس الصادرة في 24 يوليو 1971 المنقّحة لاتفاقية برن الخاصة بحماية الأعمال الأدبية والفنية، والاتفاقية الخاصة بالنواحي التجارية لحقوق الملكية الفكرية، ومعاهدة المنظمة العالمية للملكية الفكرية الخاصة بحقوق الملكية الفكرية، باستثناء أية حقوق معنوية تم التشاور بشأنها من خلال هذه الاتفاقيات، عندما ترتكب هذه الأفعال عمداً، وعلى نطاق تجاري، وبواسطة منظومة كمبيوتر.

(2) تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق المجاورة بحسب تعريفها وفقاً للقانون الخاص بهذا الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية ممثلي ومنتجي الفونوغراف والهيئات الإذاعية (اتفاقية روما)، والاتفاقية الخاصة بالنواحي التجارية لحقوق الملكية الفكرية، ومعاهدة المنظمة العالمية للملكية الفكرية الخاصة بالأعمال الإبداعية، والتمثيل، وأجهزة الفونوغراف، باستثناء أية حقوق معنوية تم التشاور بشأنها من خلال هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً، وعلى نطاق تجاري، وبواسطة منظومة كمبيوتر.

[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.

(3) يجوز لطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و2 من هذه المادة في ظروف محدَّدة، بشرط أن تتوافر وسائل علاجية فعَّالة أخرى، وألّا يخل هذا التحفُّظ بالالتزامات الدولية للطرف بموجب الاتفاقيات الدولية المشار إليها بالفقرتين 1 و2 من هذه المادة.

ويخضع التعدي على حقوق الطبع للتجريم في معظم البلدان بالفعل[1295] وتعالجه عدة معاهدات دولية.[1296] وتهدف الاتفاقية إلى توفير مبادئ أساسية تتعلق بتجريم انتهاكات حقوق الطبع من أجل تنسيق التشريعات الوطنية القائمة. ولا يشمل الحكم الانتهاكات المتصلة ببراءات الاختراع أو العلامات التجارية.[1297]

[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.
(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.

الإحالة إلى اتفاقات دولية:

بعكس الأُطر القانونية الأخرى لا تسمي الاتفاقية صراحة الأفعال التي يتعيَّن تجريمها، ولكنها تحيل إلى عدد من الاتفاقات الدولية.[1298] وهذا الجانب هو أحد الجوانب التي تعرَّضت للنقد في صدد المادة 10. وإلى جانب أن هذه الإحالة تزيد من صعوبة اكتشاف مدى التجريم وأن هذه الاتفاقات قد تتغيَّر فيما بعد فقد أثير السؤال بشأن ما إن كانت الاتفاقية تفرض على الدول الموقِّعة التوقيع أيضاً على الاتفاقات الدولية المذكورة في المادة 10. ويشير واضعو الاتفاقية المتعلقة بالجريمة الإلكترونية إلى أن الاتفاقية لا تفرض التزاماً من هذا القبيل.[1299] ولذلك، فإن تلك الدول التي لم توقِّع على الاتفاقات الدولية المذكورة لا تكون ملزمة بالتوقيع على الاتفاقات ولا مرغمة على تجريم الأفعال المتصلة بالاتفاقات التي لم توقعها. ولذلك، فإن المادة 10 لا تعلِّق التزامات إلاّ على الأطراف التي وقَّعت أحد هذه الاتفاقات الدولية.

العنصر الذهني:

تقصر الاتفاقية التجريم على تلك الأفعال التي ارتُكبت بواسطة منظومة حاسوبية، نظراً لطابعها العام.[1300] وبالإضافة إلى الأفعال المرتكبة عبر نظام حاسوبي تقتصر المسؤولية الجنائية على الأفعال المرتكبة عمداً على نطاق تجاري. ويناظر مصطلح ''عمداً'' مصطلح التعمُّد المستعمل في الأحكام القانونية الموضوعية الأخرى للاتفاقية ويراعي المصطلح المستعمل في المادة 61 من الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة،[1301] التي تحكم الالتزام بتجريم انتهاكات حقوق الطبع.[1302]

النطاق التجاري:

الاقتصار على الأفعال المرتكبة على نطاق تجاري يراعي أيضاً الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، الذي يتطلب فرض جزاءات جنائية فقط على ''القرصنة على نطاق تجاري''. ونظراً لأن معظم انتهاكات حقوق الطبع في أنظمة تقاسم الملفات لا تُرتكب على نطاق تجاري فإنها ليست مشمولة بالمادة 10. وتسعى الاتفاقية إلى وضع حد أدنى من المعايير للجرائم المتصلة بالإنترنت. وهكذا تستطيع الأطراف أن تذهب إلى ما هو أبعد من عتبة ''النطاق التجاري'' في تجريم انتهاكات حقوق الطبع.[1303]

[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.

[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.

بغير حق:

عموماً تتطلب أحكام القانون الجنائي الموضوعي المحدَّدة في الاتفاقية المتعلقة بالجريمة الإلكترونية أن يكون ارتكاب الأفعال "بدون حق".[1304] وأشار واضعو الاتفاقية إلى أن مصطلح "انتهاك" ينطوي بالفعل على أن الفعل قد أرتُكب بدون إذن.[1305]

التقييدات والتحفظات:

تمكِّن الفقرة 3 الموقعين من إبداء تحفظ طالما توفَّرت وسائل انتصاف فعَّالة أخرى وطالما أن التحفظ لا ينتقص من الالتزامات الدولية للأطراف.

مشروع اتفاقية ستانفورد

لا يتضمن مشروع اتفاقية ستانفورد غير الرسمي[1306] لعام 1999 حكماً يجرِّم انتهاكات حقوق الطبع. وأشار واضعو هذه الاتفاقية إلى أن جرائم حقوق الطبع لم تُدرج نظراً لأن ذلك قد يكون عسيراً.[1307] وبدلاً من ذلك أشاروا بصورة مباشرة إلى الاتفاقات الدولية القائمة.[1308]

2.6 القانون الإجرائي

1.2.6 مقدمة

كما يتضح من الأقسام الواردة أعلاه تتطلَّب مكافحة الجريمة السيبرانية وجود أحكام كافية في القانون الجنائي الموضوعي.[1309] فلن تتمكَّن وكالات إنفاذ القانون في بلدان القانون المدني على الأقل من التحقيق في الجرائم بدون وجود قوانين. ولكن احتياجات وكالات إنفاذ القانون في مكافحة الجرائم السيبرانية لا تقتصر على أحكام القانون الجنائي الموضوعي.[1310] فالقيام بتحقيقات يتطلب منها– بالإضافة إلى التدريب والمعدات – الاضطلاع بأدوات إجرائية تمكِّنها من اتخاذ التدابير اللازمة لتعيين الجاني وجمع الأدلة المطلوبة لإقامة الدعاوى الجنائية.[1311] ويمكن أن تكون هذه التدابير هي نفسها التدابير التي يتم اتخاذها في حالة التحقيقات الأخرى غير المتصلة بالجريمة السيبرانية – ولكن فيما يتعلق بواقع أن الجاني

[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.

[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-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

لا يحتاج بالضرورة إلى أن يكون موجوداً في مسرح الجريمة أو حتى قريباً منه، فإنه من المرجح جداً أن الحاجة ستقوم إلى إجراء التحقيقات في الجرائم السيبرانية بطريقة مختلفة مقارنة بالتحقيقات التقليدية.[1312]

والسبب في ضرورة تطبيق تقنيات تحقيق مختلفة لا يرجع فقط إلى الاستقلال عن مكان الفعل ومسرح الجريمة. ففي معظم الحالات يتجمَّع عدد من التحديات المذكورة أعلاه أمام وكالات إنفاذ القانون ليجعل التحقيقات في الجرائم السيبرانية تحقيقات فريدة.[1313] فإذا كان مقر الجاني في بلد مختلف،[1314] ويستخدم خدمات تجعل من الممكن الاتصال دون الكشف عن الهوية، ثم بالإضافة إلى ذلك، يرتكب جرائمه باستعمال أجهزة إنترنت طرفية عمومية مختلفة، فسيكون من الصعب التحقيق في الجريمة بواسطة الأدوات التقليدية مثل البحث والقبض وحدهما. ومن المهم، لتجنُّب سوء الفهم، أن يشار إلى أن تحقيقات الجرائم السيبرانية تتطلَّب إجراءات تحقيقات الشرطة التقليدية وتطبيق أدوات التحقيقات التقليدية – ولكن تحقيقات الجرائم السيبرانية تنطوي على تحديات لا يمكن حلها فقط باستعمال أدوات التحقيقات التقليدية.[1315]

وقد وضعت بعض البلدان بالفعل أدوات جديدة تمكِّن وكالات إنفاذ القوانين من التحقيق في الجرائم السيبرانية، وكذلك الجرائم التقليدية التي تتطلب تحليل البيانات الحاسوبية.[1316] وكما حدث في حالة القانون الجنائي الموضوعي تتضمَّن الاتفاقية المتعلقة بالجريمة الإلكترونية التي وضعها مجلس أوروبا مجموعة من الأحكام التي تعبِّر عن المعايير الدنيا المقبولة قبولاً واسعاً في شأن الأدوات الإجرائية المطلوبة للتحقيقات في الجرائم السيبرانية.[1317] ولذلك، فإن العرض العام التالي يشير إلى الأدوات التي تتيحها هذه الاتفاقية الدولية ويبرز، بالإضافة إلى ذلك، النُهج الوطنية التي تتجاوز التنظيمات الواردة في الاتفاقية.

2.2.6 التحقيقات المتصلة بالحاسوب والإنترنت (التحليلات القضائية الحاسوبية (الطب الشرعي الحاسوبي)

هناك تعاريف مختلفة لمصطَلح "التحليلات القضائية الحاسوبية" ("الطب الشرعي الحاسوبي").[1318] إذ يمكن تعريف هذا المصطلح بأنه يعني "فحص معدات وأنظمة تكنولوجيا المعلومات من أجل الحصول على معلومات لأغراض التحقيقات الجنائية والمدنية".[1319] فالجناة يتركون آثاراً تدل عليهم أثناء ارتكابهم جرائمهم.[1320] وينطبق ذلك في التحقيقات التقليدية كما ينطبق في التحقيقات الحاسوبية. والفرق الرئيسي بين التحقيق التقليدي والتحقيق في الجريمة السيبرانية هو أن التحقيق في الجريمة السيبرانية يتطلب عموماً تقنيات بحثية تتصل بالبيانات بوجه خاص ويمكن تسهيلها بأدوات برمجيات متخصصة.[1321] ويتطلب هذا التحليل، بالإضافة إلى أدوات إجرائية كافية، قدرة السلطات على إدارة وتحليل البيانات

[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/.

[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.

ذات الصلة. وتختلف المتطلبات المتعلقة بأداة التحقيق الإجرائي وتصاحب تقنيات التحليل القضائي (الطب الشرعي) الحاسوبي[1322] تحديات فريدة[1323] حسب الجرائم المرتكبة والتكنولوجيا الحاسوبية المستخدَمة.

وعموماً يتصل هذان الجانبان من تحقيقات الجرائم السيبرانية اتصالاً وثيقاً ويوصف الجانبان بمصطَلح نوعي عام هو ''التحليلات القضائية الحاسوبية''، (''الطب الشرعي الحاسوبي'') أو جمع وتحليل الأدلّة.[1324] وكما وصفنا أعلاه يصف مصطَلح التحليلات القضائية الحاسوبية (الطب الشرعي الحاسوبي) تطبيق تقنيات التحقيق والتحليل الحاسوبية لتحديد الأدلة المحتملة. ويغطي ذلك مجموعة واسعة من التحليلات تتراوح من التحليل العام مثل البحث عن المواد الفاضحة التي تصوِّر الأطفال على الأقراص الصلبة الحاسوبية،[1325] إلى التحقيقات المحدّدة مثل التحليلات القضائية الخاصة بأجهزة الاستماع المحمولة iPod[1326] والنفاذ إلى الملفات المشفَّرة.[1327] ويدعم خبراء التحليلات القضائية الحاسوبية (الطب الشرعي الحاسوبي) التحقيقات التي يقوم بها ضباط شرطة ووكلاء نيابة متخصصون. وفي سياق تحقيقات الإنترنت يستطيع خبراء التحليل القضائي (الطب الشرعي) الحاسوبي مثلاً المساعدة فيما يلي[1328]:

- تعيين آثار الفعل الرقمية المحتملة (وخاصة الموقع المحتمل لبيانات الحركة)؛[1329]
- دعم مقدّمي خدمة الإنترنت في تعيين المعلومات التي يستطيعون تقديمها لدعم التحقيقات؛
- حماية البيانات الهامة المجموعة وكفالة تسلسل المسؤوليات.[1330]

وبمجرد تعيين الأدلّة المحتملة يستطيع الخبراء مثلاً تقديم المساعدة فيما يلي:

- حماية النظام الحاسوبي المعني أثناء التحليل من إمكانية تعديل أو إفساد البيانات؛[1331]
- اكتشاف الملفات ذات الصلة في النظام الحاسوبي المعني ووسائط التخزين؛[1332]

[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.*

[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.

- فك تشفير الملفات المشفَّرة؛[1333]
- استعادة الملفات المحذوفة؛
- تعيين مستعمل النظام الحاسوبي في الحالات التي يملك أكثر من شخص النفاذ إلى الجهاز أو التقسيم؛[1334]
- إظهار محتويات الملفات المؤقتة التي استُعمِلت في التطبيق ونظام التشغيل؛
- تحليل الأدلة المجموعة؛[1335]
- توفير وثائق التحليل؛[1336]
- توفير الأدلة لمواصلة التحقيقات؛
- توفير مشاورات وشهادات الخبراء.

وبوجه خاص تُبرز مشاركة خبراء التحليل القضائي (الطب الشرعي) في حماية سلامة الأدلة أن أعمال خبراء التحليل القضائي (الطب الشرعي) تجمع بين الجانبين التقني والقانوني. ومن التحديات الرئيسية في هذا السياق أن سلسلة المسؤوليات التي تتطلب مراجعة دقيقة للبيانات الأصلية تسير إلى جانب متطلبات متعمّقة تتصل بالعمل الفعلي لخبراء التحليل القضائي (الطب الشرعي).[1337]

ويُثبت مدى المشاركة المحتملة من جانب خبراء التحليل القضائي (الطب الشرعي) الحاسوبي أهمية هذا التحليل في عملية التحقيق. وبالإضافة إلى ذلك، فإن توقُّف نجاح تحقيقات الإنترنت على توفُّر موارد التحليل القضائي (الطب الشرعي) يُبرز ضرورة التدريب في هذا المجال. ولا يمكن إجراء تحقيق فعّال وملاحقة فعّالة في الجريمة السيبرانية إلاّ إذا كان المحققون حاصلين على تدريب في مجال التحليلات القضائية الحاسوبية (الطب الشرعي الحاسوبي) أو يستطيعون الاستفادة من الخبراء في هذا المجال.

3.2.6 الضمانات

أبرزت وكالات إنفاذ القانون في أنحاء العالم خلال السنوات القليلة الماضية الحاجة الماسة لوجود أدوات كافية لإجراء التحقيقات.[1338] ومع وضع ذلك في الاعتبار فقد يكون من المدهِش أن الاتفاقية المتعلقة بالجريمة الإلكترونية تعرضت للنقد في صدد الأدوات الإجرائية.[1339] ويركز النقد أساساً على جانب أن الاتفاقية تتضمن عدداً من الأحكام لإثبات أدوات التحقيق (المواد من 16 إلى 21) ولكنها تتضمّن حكماً واحداً فقط (المادة 15) يتناول الضمانات.[1340] وبالإضافة إلى ذلك، يمكن أن يلاحَظ أنه بعكس أحكام القانون الجنائي الموضوعي في الاتفاقية لا توجد سوى احتمالات قليلة جداً لإدخال تعديلات وطنية في تطبيق الاتفاقية.[1341] ويركِّز النقد لذلك على الجوانب الكمّية أساساً. ومن الصحيح أن الاتفاقية تعتنق مفهوم التنظيم المركزي للضمانات بدلاً من ربطها بصورة منفردة بكل أداة من أدوات التحقيق. ولكن ذلك لا يعني بالضرورة ضعف حماية حقوق المشتبه فيهم.

[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.
[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 Financial 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.

وكانت الاتفاقية المتعلقة بالجريمة الإلكترونية قد صُمِّمت منذ بدايتها لتكون إطاراً وصكّاً دوليين لمكافحة الجريمة السيبرانية دون أن يقتصر ذلك فقط على البلدان الأعضاء في مجلس أوروبا.[1342] وأثناء التفاوض على الأدوات الإجرائية اللازمة أدرك واضعو الاتفاقية، الذين كانوا يضمون ممثلين من بلدان غير أوروبية مثل الولايات المتحدة واليابان، أن النُهُج الوطنية القائمة المتصلة بالضمانات، وخاصة طريقة حمايتها للمشتبه فيهم في مختلف الأنظمة القانونية الجنائية، تختلف اختلافاً كبيراً بحيث لا يمكن توفير حلّ واحد تفصيلي لكل الدول الأعضاء.[1343] ولذلك قرّر واضعو الاتفاقية عدم إدراج قواعد تنظيمية محدّدة في نصّ الاتفاقية والاكتفاء بدلاً من ذلك بمطالبة الدول الأعضاء بكفالة تطبيق المعايير الوطنية والدولية الأساسية للضمانات.[1344]

المادة 15 – الشروط والضمانات

1 على كل طرف أن يتأكد من أن إقامة، وتنفيذ، وتطبيق الصلاحيات والإجراءات الواردة بهذا القسم تخضع للضمانات والشروط المنصوص عليها في قانونه الوطني، الذي يتعيَّن أن يوفِّر الحماية الكافية لحقوق الإنسان والحريات، بما في ذلك الحقوق الناشئة عن التزاماته بموجب اتفاقية مجلس أوروبا لعام 1950 الخاصة بحماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966 الخاص بالحقوق المدنية والسياسية، وغيرها من الآليات الدولية الأخرى المنطبقة والخاصة بحقوق الإنسان، والتي تتضمّن مبدأ الملاءمة.

2 تشمل هذه الشروط والضمانات، كلما كان الأمر ملائماً بالنسبة لطبيعة الإجراءات أو الصلاحيات ذات الصلة، الإشراف من قِبَل القضاء أو بواسطة إشراف محايد، ووضع مبررات للتطبيق، وحدود ومجال ومدة هذا الإجراء أو الصلاحية.

3 في حدود الصالح العام وبخاصة الإدارة السليمة للعدالة، يقوم كل طرف بدراسة تأثير الصلاحيات والإجراءات في هذا القسم على الحقوق والمسؤوليات، والمصالح المشروعة للغير.

وتستند المادة 15 إلى مبدأ أن الدول الموقّعة تطبِّق الشروط والضمانات الموجودة فعلاً في قانونها المحلي. وإذا كان القانون ينصّ على معايير مركزية تنطبق على جميع أدوات التحقيق، فإن هذه المبادئ تنطبق أيضاً على الأدوات المتصلة بالإنترنت.[1345] وفي حالة عدم استناد القانون المحلي إلى تنظيم مركزي للضمانات والشروط، فمن الضروري تحليل الضمانات والشروط المنفَّذة في صدد الأدوات التقليدية المشابهة للأدوات المتصلة بالإنترنت.

ولكن الاتفاقية لا تشير فقط إلى الضمانات الموجودة في التشريعات الوطنية. ويقترن ذلك بعيب يتمثَّل في أن مقتضيات التطبيق تختلف بحيث لا تعود الجوانب الإيجابية للتنسيق منطبقة. ولكفالة قيام الدول الموقّعة التي توجد لديها تقاليد وضمانات قانونية مختلفة بتطبيق معايير معيَّنة،[1346] فإن الاتفاقية المتعلقة بالجريمة الإلكترونية تعرِّف المعايير الدنيا بإشارتها إلى الأُطر الأساسية مثل الأُطر التالية:

- اتفاقية مجلس أوروبا لعام 1950 لحماية حقوق الإنسان والحريات الأساسية؛
- العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966 الصادر عن الأمم المتحدة؛
- الصكوك الدولية الأخرى المنطبقة والخاصة بحقوق الإنسان.

[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 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.

ونظراً لأن الاتفاقية يمكن أن تكون مفتوحة للتوقيع والتصديق من جانب بلدان ليست أعضاء في مجلس أوروبا،[1347] فمن المهم التأكيد على أن تقييم أنظمة الضمانات في الدول الموقّعة غير الأعضاء في الاتفاقية المتعلقة بالجريمة الإلكترونية لن يراعي فقط العهد الدولي الخاص بالحقوق المدنية والسياسية الصادر عن الأمم المتحدة بل سيأخذ في الاعتبار أيضاً اتفاقية مجلس أوروبا لحماية حقوق الإنسان والحريات الأساسية.

وفيما يتعلق بتحقيقات الجريمة السيبرانية، فإن أحد أكثر النصوص صلة في المادة 15 من الاتفاقية المتعلقة بالجريمة الإلكترونية يتمثّل في الإشارة إلى الفقرة 2 من المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

المادة 8

1 لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته.

2 لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلّا وفقًا للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحريتهم.

وقد بذلت المحكمة الأوروبية لحقوق الإنسان جهوداً لوضع تعريف أكثر دقة للمعايير التي تحكم التحقيقات الإلكترونية وخاصة المراقبة. وقد أصبح قانون السوابق القضائية اليوم واحداً من أهم مصادر المعايير الدولية المتصلة بالتحقيقات المتعلقة بالاتصالات.[1348] ويراعي قانون السوابق القضائية بالتحديد خطورة التدخل في التحقيق[1349]، وغرضه[1350] وتناسبه.[1351] والمبادئ الأساسية التي يمكن استخراجها من قانون السوابق القضائية هي:

- ضرورة وجود أساس قانوني كافٍ لأدوات التحقيق؛[1352]
- يجب أن يكون الأساس القانوني واضحاً بشأن الموضوع؛[1353]
- يتعيَّن أن تكون اختصاصات وكالات إنفاذ القانون معروفة سلفاً؛[1354]
- لا يمكن تبرير مراقبة الاتصالات إلّا في سياق الجرائم الخطيرة.[1355]

[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.

[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.

وبالإضافة إلى ما سبق، فإن المادة 15 من الاتفاقية المتعلقة بالجريمة الإلكترونية تأخذ في الاعتبار مبدأ التناسب.[1356] ويتسم هذا الحكم بأهمية خاصة للدول الموقّعة غير الأعضاء في مجلس أوروبا. ففي الحالات التي لا يحمي فيها النظام الوطني القائم للضمانات المشتبه فيهم حماية كافية، يكون من الإلزامي أن تضع الدول الأعضاء الضمانات اللازمة في سياق عملية التصديق والتطبيق.

وأخيراً، تشير الفقرة 2 من المادة 15 من الاتفاقية المتعلقة بالجريمة الإلكترونية صراحة إلى بعض أهم الضمانات[1357]، بما فيها:

- الإشراف؛
- مبررات التطبيق؛
- حدود ومجال ومدة الإجراء.

وبعكس المبادئ الأساسية الموصوفة أعلاه لا يتعيَّن بالضرورة تطبيق الضمانات المذكورة هنا في صدد أي أداة بل يتعيَّن تطبيقها فقط إذا كانت ملائمة في ضوء طبيعة الإجراء المعني. وتُركت للهيئات التشريعية الوطنية حُرية تقرير الحالات التي يكون فيها ذلك ضروريا.[1358]

وهناك جانب هام يتصل بنظام الضمانات المنصوص عليه في الاتفاقية المتعلقة بالجريمة الإلكترونية، ويتمثّل هذا الجانب في أن قدرة وكالات إنفاذ القانون على استعمال الصكوك بطريقة مرنة، من ناحية، وضمان وجود ضمانات فعّالة، من ناحية أخرى، يتوقفان على تنفيذ نظام متدرّج من الضمانات. ولا تمنع الاتفاقية الأطراف صراحة من تنفيذ نفس الضمانات (مثل اقتضاء وجود أمر قضائي) في حالة جميع الأدوات ولكن هذا النهج سيؤثّر على مرونة وكالات إنفاذ القانون. والقدرة على كفالة حماية كافية لحقوق المشتبه فيهم في إطار نظام متدرّج من الضمانات تتوقّف إلى حدٍ كبير على التوازن بين الأثر المحتمَل لأداة التحقيق مع الضمانات المتصلة. ولتحقيق ذلك يلزَم التمييز بين الأدوات الأقل شدة والأكثر شدة. وهناك عدد من أمثلة هذا التمييز في الاتفاقية المتعلقة بالجريمة الإلكترونية تمكّن الأطراف من مواصلة صياغة نظام للضمانات المتدرجة. وتشمل هذه الأمثلة ما يلي:

- التمييز بين اعتراض بيانات المحتوى (المادة 21)[1359] وجمع بيانات الحركة (المادة 20)[1360]. وعلى العكس من جمع بيانات الحركة، يقتصر اعتراض بيانات المحتوى على الجرائم الخطيرة.[1361]
- التمييز بين الأمر العاجل بحفظ بيانات الحاسوب المخزونة (المادة 16)[1362] وتقديم بيانات الحاسوب التي تم الاحتفاظ بها استناداً إلى أمر الإبراز (المادة 18)[1363] فالمادة 16 تمكّن وكالات إنفاذ القانون فقط من إصدار أوامر حفظ البيانات دون الكشف عنها.[1364]
- التمييز بين الالتزام بتقديم "معلومات المشتَرِك"[1365] و"بيانات الحاسوب"[1366] في المادة 18.[1367]

وإذا تم تقييم شدة أداة التحقيق والأثر المحتمل على المشتبه فيه تقييماً صحيحاً وصُمِّمت الضمانات بحيث تناظِر نتائج التحليل، فإن نظام الضمانات المتدرجة لن يؤدّي إلى اختلال نظام الأدوات الإجرائية.

[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.

[1365] A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 Convention on Cybercrime.

[1366] A definition of the term "computer data" is provided in Art. 1 Convention on Cybercrime.

[1367] 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.

4.2.6 الحفظ العاجل لبيانات الحاسوب المخزونة والإفصاح عنها (إجراء التجميد السريع)

في كثير من الأحيان يتطلب تعيين الجاني الذي ارتكب جريمة إلكترونية تحليلاً لبيانات الحركة.[1368] وبصورة خاصة يمكن أن يساعد عنوان بروتوكول إنترنت الذي استعمله الجاني وكالات إنفاذ القانون على تعقبه. بل ومن الممكن في بعض الحالات تعيين أحد الجناة، رغم أنه كان يستعمل أجهزة إنترنت طرفية عمومية لا تتطلب الإفصاح عن الهوية طالما كانت وكالات إنفاذ القانون تملك النفاذ إلى بيانات الحركة ذات الصلة.[1369]

ومن الصعوبات الرئيسية التي يواجهها المحققون أن بيانات الحركة ذات الأهمية الكبيرة للمعلومات المحمية تُحذف في كثير من الأحيان بصورة تلقائية بعد فترة قصيرة من الوقت إلى حد ما. وسبب هذا الحذف الأوتوماتي هو أن انتهاء أي عملية (مثل إرسال بريد إلكتروني أو النفاذ إلى الإنترنت أو تنزيل أحد الأفلام) يعني انتهاء الحاجة إلى بيانات الحركة التي تولّدت أثناء العملية والتي تكفل إمكانية إجراء العملية. وفيما يتعلق بالجوانب الاقتصادية لهذا النشاط، يهتم معظم مقدمي الإنترنت بحذف المعلومات بأسرع ما يمكن نظراً لأن تخزينها لفترات طويلة يتطلب سعة تخزينية كبيرة جداً ومكلّفة.[1370]

ومع ذلك، فإن الجوانب الاقتصادية لا تشكّل السبب الوحيد لقيام وكالات إنفاذ القانون بتحقيقاتها بسرعة. فبعض البلدان تُطبِّق قوانين صارمة تحظر تخزين بيانات بعض الحركة بعد انتهاء العملية. ومن أمثلة هذا التقييد المادة 6 من توجيه الاتحاد الأوروبي بشأن الخصوصية والاتصال الإلكتروني.[1371]

المادة 6 – بيانات الحركة

1 يجب مسح بيانات الحركة المتصلة بالمشتركين والمستعملين التي يعالجها ويخزنها مقدِّم شبكة اتصالات عمومية أو خدمة اتصالات إلكترونية متوفرة للجمهور، أو إخفاء هويتها، بعد توقف الحاجة إليها لأغراض إرسال رسالة بدون المساس بالفقرات 2 و3 و5 من هذه المادة والفقرة 1 من المادة 15.

2 يجوز تجهيز بيانات الحركة اللازمة لأغراض فوترة المشترك ومدفوعات التوصيل البيني. ويسمح بهذا التجهيز فقط حتى نهاية الفترة التي يمكن خلالها قانوناً الطعن أو متابعة الدفع.

ولذلك يمثّل الوقت جانباً حرجاً في تحقيقات الإنترنت. ومن المرجح عموماً أن تمر فترة من الوقت بين إعداد الجريمة واكتشافها وتبليغ وكالات إنفاذ القانون بها، ولذلك فمن المهم تنفيذ آليات تمنع حذف البيانات ذات الصلة أثناء عملية التحقيق التي قد تستمر أحياناً لمدة طويلة. وفيما يتعلق بهذا الجانب، يجري في الوقت الحاضر مناقشة نهجين مختلفين[1372]:

- استبقاء البيانات؛ و
- حفظ البيانات ("إجراء التجميد السريع").

[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.

[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.

ويفرض التزام استبقاء البيانات على مقدِّم خدمات الإنترنت حفظ بيانات الحركة لفترة معيَّنة من الوقت[1373] ويتعيَّن في أحدث النُهج التشريعية إبقاء السجلات لمدة ستة أشهر وحتى 24 شهراً.[1374] ويمكِّن ذلك وكالات إنفاذ القانون من النفاذ إلى البيانات اللازمة لتعيين الجاني حتى بعد ارتكابها بأشهر كثيرة.[1375] وقد اعتمد برلمان الاتحاد الأوروبي مؤخراً التزام استبقاء البيانات[1376] ويجري مناقشة هذا الالتزام أيضاً في الولايات المتحدة في الوقت الحاضر.[1377] وفيما يتعلق بمبادئ استبقاء البيانات، يمكن الاطلاع أدناه على مزيد من المعلومات.

الاتفاقية المتعلقة بالجريمة الإلكترونية

حفظ البيانات نهج مختلف لكفالة عدم فشل التحقيق في الجريمة السيبرانية لا لسبب سوى حذف بيانات الحركة أثناء إجراءات التحقيق الطويلة.[1378] واستناداً إلى تشريع حفظ البيانات تستطيع وكالات إنفاذ القانون أن تأمر مقدِّم الخدمة بمنع حذف بعض البيانات. ويمثِّل الحفظ العاجل لبيانات الحاسوب أداة لا بد وأن تمكِّن وكالات إنفاذ القانون من التصرُّف فوراً وتجنُّب خطر الحذف بسبب طول الإجراءات.[1379] وقرَّر واضعو الاتفاقية المتعلقة بالجريمة الإلكترونية التركيز على "التحفظ على البيانات" بدلاً من "استبقاء البيانات".[1380] ويمكن الاطلاع على القاعدة التنظيمية في المادة 16 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

المادة 16 – سرعة التحفُّظ على بيانات الكمبيوتر المخزونة

1 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك حتى يمكن لسلطاتها المختصة الأمر أو طلب التحفُّظ بصورة عاجلة على بيانات بعينها على كمبيوتر، بما في ذلك خط سير البيانات المخزَّنة بواسطة منظومة كمبيوتر، وخاصة في حالة وجود أُسس للاعتقاد بإمكانية تعرُّض بيانات الكمبيوتر بصفة خاصة للفقد أو التعديل.

2 في حالة قيام طرف بتفعيل الفقرة 1 بعاليه بواسطة إصدار أمر إلى شخص ما للتحفظ على بيانات كمبيوتر مخزَّنة بعينها، بحوزة الشخص أو تحت سيطرته، فإنه يتعيَّن على هذا الطرف أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام ذلك الشخص بأن يحفظ ويتحفَّظ على سلامة بيانات الكمبيوتر المذكورة بالقدر اللازم، لفترة زمنية لا تزيد عن 90 يوماً على الأكثر، حتى تتمكَّن السلطات المختصة من السعي لكشفها. ويجوز لطرف إصدار مثل هذا الأمر لتجديده بالتالي.

3 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإلزام المسؤول أو أي شخص آخر يتحفظ على بيانات كمبيوتر، بالمحافظة على سرية القيام بمثل هذه الإجراءات للفترة الزمنية المنصوص بها بموجب قانونه الوطني المحلي.

4 تخضع الصلاحيات والإجراءات المشار إليها بهذه المادة للمادتين 14 و15.

[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.

[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.

ومن منظور مقدِّم خدمة الإنترنت، يعتبر حفظ البيانات أداة أقل شدة مقارنة باستبقاء البيانات.[1381] ولا يحتاج مقدمو خدمة الإنترنت إلى تخزين جميع البيانات الخاصة بجميع المستعملين ولكن عليهم بدلاً من ذلك كفالة عدم حذف بيانات محدَّدة بمجرد استلام أمر من سلطة مختصة. ويتيح حفظ البيانات مزايا نظراً لأنه يشمل البيانات لا من وجه نظر مقدِّم الخدمة وحسب ولكن أيضاً من منظور حماية البيانات. وليس من الضروري حفظ البيانات المتجمِّعة من ملايين مستعملي الإنترنت ولكن يكفي حفظ البيانات المتصلة بالأشخاص المحتملين للاشتباه في التحقيقات الجنائية. ومع ذلك، فمن المهم أن يشار إلى أن استبقاء البيانات يتيح مزايا في الحالات التي يتم فيها حذف البيانات بعد انتهاء ارتكاب الجريمة مباشرة. ففي هذه الحالات لا يمكن لأمر حفظ البيانات، – بعكس الالتزام باستبقاء البيانات – أن يمنع حفظ البيانات ذات الصلة.

والأمر الصادر بموجب المادة 16 يلزم مقدِّم الخدمة بأن يقوم فقط بحفظ البيانات التي تم تجهيزها من جانب المقدِّم وعدم حذفها عند استلامه الأمر.[1382] ولا يقتصر هذا الأمر على بيانات الحركة نظراً لأن بيانات الحركة قد ذُكرت باعتبارها مثالاً واحداً. ولا ترغم المادة 16 الجاني على أن يبدأ جمع معلومات لا يخزنها عادة.[1383] وبالإضافة إلى ذلك، لا تلزم المادة 16 مقدِّم الخدمة على تحويل البيانات ذات الصلة إلى السلطات. إذ إن النص يقتصر على إعطاء وكالات إنفاذ القانون سلطة منع حذف البيانات ذات الصلة ولكنه لا يفرض على مقدمي الخدمة نقل البيانات. والتزام النقل تنظمه المادة 17 والمادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية. ومزايا فصل التزام حفظ البيانات والتزام الإفصاح عنها هو أنه من المحتمل اقتضاء شروط مختلفة لتطبيقهما.[1384] وفيما يتعلق بأهمية التصرف الفوري، سيكون من المفيد مثلاً التنازل عن اقتضاء صدور أمر من القاضي وتمكين الادعاء أو الشرطة من إصدار أمر الحفظ.[1385] وسيمكِّن ذلك السلطات المختصة من التصرف بسرعة أكبر. ويمكن أن تتحقَّق حماية حقوق المشتبه فيهم باقتضاء صدور أمر للإفصاح عن البيانات.[1386]

والإفصاح عن البيانات المحتفظ بها هو جانب من الجوانب التي تنظمها المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية:

المادة 18 – إصدار الأوامر

1 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطات ذلك الطرف صلاحية توجيه الأمر إلى:

أ) أي شخص في إقليمه لتقديم بيانات محدَّدة موجودة على الكمبيوتر بحوزة ذلك الشخص أو تحت سيطرته، ومخزَّنة داخل نظام الكمبيوتر أو على أي وسيط تخزين بيانات آخر.

ب) أي مقدِّم خدمة يعرض خدماته في إقليم الطرف لتقديم معلومات للمشترك فيما يتعلق بتلك الخدمات الموجودة بحوزة أو تحت سيطرة مقدِّم الخدمة.

2 تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و15

3 لغرض هذه المادة – فإن مصطلح ''معلومات المشترك'' يعني أية معلومات في صورة بيانات كمبيوتر أو أية صورة أخرى يتم حفظها من جانب مقدِّم الخدمة، والتي تتعلق بالمشتركين في الخدمات الخاصة به بخلاف خط سير البيانات أو مضمونها والتي بموجبها يمكن التوصل إلى:

أ) نوعية خدمة الاتصال المستخدمة، والشروط الفنية التي يتم اتخاذها في ذلك والفترة الزمنية للخدمة؛

ب) هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم تليفونه وغير ذلك من أرقام الدخول الأخرى الخاصة به، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك؛

[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.

[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."

ج) أية معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الاتصالات، والتي تتوافر بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

واستناداً إلى الفقرة الفرعية 1 (أ) من المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية، يمكن إلزام مقدمي الخدمة الذين قاموا بحفظ البيانات بالإفصاح عنها.

والمادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية لا تنطبق فقط بعد إصدار أمر حفظ عملاً بالمادة 16 من الاتفاقية المتعلقة بالجريمة الإلكترونية.[1387] وهذا الحكم هو أداة عامة تستطيع وكالات إنفاذ القانون أن تستعملها. وإذا قامت وكالات إنفاذ القانون طوعاً بنقل البيانات المطلوبة فإنها لا تقتصر على ضبط العتاد ولكنها تستطيع تطبيق أمر إبراز أقل شدة. ومقارنة بضبط العتاد فعلاً، فإن أمر تقديم المعلومات ذات الصلة هو أقل شدة بصورة عامة. لذلك كان تطبيقه هاماً بصفة خاصة في الحالات التي لا تتطلَّب فيها تحقيقات التحليلات القضائية (الطب الشرعي) الحصول على العتاد.

وبالإضافة إلى الالتزام بتقديم بيانات الحاسوب تمكِّن المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية وكالات إنفاذ القانون من أن تأمر بتقديم معلومات المشترك. وهذه الأداة التحقيقية تتسم بأهمية كبرى في التحقيقات على أساس بروتوكول إنترنت. وإذا تمكَّنت وكالات إنفاذ القانون من تعيين عنوان بروتوكول إنترنت الذي استعمله الجاني أثناء قيامه بجريمته، فإنها تحتاج إلى تعيين الشخص[1388] الذي استعمل عنوان بروتوكول إنترنت في وقت ارتكاب الجريمة. واستناداً إلى الفقرة 1 (ب) من المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية، يكون مقدِّم الخدمة ملزماً بتقديم معلومات المشترك المذكورة في الفقرة الفرعية 3 من المادة 18.[1389]

وفي تلك الحالات التي تتعقَّب فيها وكالات إنفاذ القانون المسار إلى الجاني وتحتاج إلى نفاذ فوري لتعيين المسار الذي تم خلاله إرسال الاتصال، فإن المادة 17 تمكِّن الوكالات من أن تأمر بسرعة بالإفصاح الجزئي عن بيانات الحركة.

المادة 17 – سرعة التحفظ على خط سير البيانات والكشف الجزئي لها

1 يعتمد كل طرف، بالنسبة لخط سير البيانات المطلوب حفظها بموجب المادة 16، ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك:

أ) لضمان إمكانية سرعة التحفظ على خط سير البيانات المذكورة بصرف النظر عن مشاركة مقدِّم خدمة واحد أو أكثر في عملية نقل هذه الاتصالات.

ب) لضمان سرعة الكشف للسلطات المختصة بالطرف، أو للشخص الذي تعيِّنه تلك السلطات، عن القدر الكافي من خط سير البيانات حتى يمكن للطرف تحديد مقدِّم الخدمة والمسار الذي تم نقل الاتصال من خلاله.

2 تخضع الصلاحيات والإجراءات المشار إليها بهذه المادة للمادتين 14 و15.

وكما ذكرنا أعلاه تفصل الاتفاقية فصلاً صارماً بين التزام حفظ البيانات بناءً على الطلب والتزام الإفصاح عنها للسلطات المختصة.[1390] وتقدِّم المادة 17 تصنيفاً واضحاً حيث تجمع التزام كفالة حفظ بيانات الحركة في الحالات التي تشمل عدداً من مقدمي الخدمة، مع الالتزام بالإفصاح عن المعلومات اللازمة لتعيين المسار الذي مرَّت به الخدمة. وبدون هذا الإفصاح الجزئي لن تتمكَّن وكالات إنفاذ القانون في بعض الحالات من تعقُّب الجاني في حالة وجود أكثر من مقدِّم خدمة.[1391] ونظراً لتجمع الالتزامين اللذين يؤثران على حق المشتبه فيهم بطرق أخرى، فمن الضروري مناقشة نقطة تركيز الضمانات المتصلة بهذه الأداة.

[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.

[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.

قانون الكومنولث النموذجي المتعلق بالحاسوب والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نُهج مشابهة في قانون الكومنولث النموذجي لعام 2002.[1392]

الحكم:

المادة 15

إذا اقتنع قاضي تحقيق استناداً إلى طلب مقدَّم من ضابط شرطة بأن بيانات حاسوبية محدَّدة، أو مطبوعة منها أو أي معلومات أخرى، هي مطلوبة بصورة معقولة لأغراض تحقيق جنائي أو دعوى جنائية يجوز للقاضي أن يأمر:

(أ) شخصاً في إقليم [البلد الذي سن القانون] يسيطر على منظومة حاسوبية أن يقدِّم من المنظومة بيانات حاسوبية محدَّدة أو مطبوعة أو غير ذلك من النواتج المفهومة الأخرى من تلك البيانات؛ و

(ب) مقدِّم خدمة إنترنت في [البلد الذي سن القانون] أن يقدِّم معلومات عن الأشخاص الذين يشتركون في الخدمة أو يستعملونها بشكل آخر؛ و

(ج)[1393] أي شخص في إقليم [البلد الذي سن القانون] يملك النفاذ إلى نظام حاسوبي محدَّد أن يجهِّز ويجمع بيانات حاسوبية محدَّدة من النظام وأن يعطيها لشخص محدَّد.

المادة 16[1394]

إذا اقتنع ضابط شرطة بأن البيانات المخزونة في نظام حاسوبي مطلوبة بصورة معقولة لأغراض تحقيق جنائي يجوز لضابط الشرطة، بموجب إشعار مكتوب يقدَّم إلى الشخص الذي يسيطر على النظام الحاسوبي، أن يطالب الشخص بالإفصاح عن بيانات حركة كافية عن اتصال محدَّد من أجل تعيين:

(أ) مقدمي الخدمة؛

(ب) والمسار الذي تم من خلاله إرسال الاتصال.

المادة 17

(1) إذا اقتنع ضابط شرطة بأن:

(أ) البيانات المخزونة في نظام حاسوبي هي مطلوبة بصورة معقولة لأغراض تحقيق جنائي؛

(ب) وأن هناك خطراً من إمكانية تدمير البيانات وجعل النفاذ إليها غير ممكن؛

يجوز لضابط الشرطة، بموجب أشعار مكتوب مقدَّم إلى الشخص الذي يسيطر على النظام الحاسوبي، أن يطالب الشخص بكفالة حفظ البيانات المحدَّدة في الإشعار لفترة تصل إلى 7 أيام على النحو المحدَّد في الإشعار.

(2) يجوز تمديد الفترة بعد 7 أيام إذا قام [قاضٍ] [قاضي تحقيق] بناءً على طلب من طرف واحد أن يصرِّح بالتمديد لفترة أخرى محدَّدة.

[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.

[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.

5.2.6 استبقاء البيانات

يفرض التزام استبقاء البيانات على مقدِّم خدمات الإنترنت الاحتفاظ ببيانات الحركة لفترة معيَّنة من الوقت.[1395] وتنفيذ التزام استبقاء البيانات هو نهج يُتَّبع لتجنُّب الصعوبات المذكورة أعلاه في النفاذ إلى بيانات الحركة قبل حذفها. ومن أمثلة هذا النهج التوجيه الخاص باستبقاء البيانات الصادر عن الاتحاد الأوروبي.[1396]

المادة 3 – التزام استبقاء البيانات

1 على سبيل الاستثناء من المواد 5 و6 و9 من التوجيه 2002/58/EC، تعتمد الدول الأعضاء تدابير لكفالة استبقاء البيانات المنصوص عليها في المادة 5 من هذا التوجيه وفقاً لأحكام التوجيه، بقدر نشوء أو تجهيز هذه البيانات من جانب مقدّمي خدمات الاتصالات الإلكترونية المتاحة للجمهور أو حركة اتصالات عامة في حدود اختصاصاتهم في عملية توفير خدمات الاتصالات المعنية.

2 يشمل التزام استبقاء البيانات المنصوص عليه في الفقرة 1 استبقاء البيانات المحدّدة في المادة 5 فيما يتعلق بمحاولات النداء غير الناجحة في حالات نشوء هذه البيانات أو تجهيزها وتخزينها (فيما يتعلق ببيانات المهاتفة) أو تسجيلها (فيما يتعلق بالبيانات الإنترنت) من جانب مقدّمي خدمات الاتصالات الإلكترونية المتاحة للجمهور أو من جانب شبكة اتصالات عمومية في حدود الولاية القضائية للدول الأعضاء المعنية في سياق عملية توفير خدمات الاتصالات المعنية. ولا يقتضي هذا التوجيه استبقاء البيانات المتعلقة بالنداءات بدون توصيل.

المادة 4 – النفاذ إلى البيانات

تعتمد الدول الأعضاء تدابير لكفالة إتاحة استبقاء البيانات وفقاً لهذا التوجيه للسلطات الوطنية المختصة وحدها في حالات بعينها ووفقاً للقانون الوطني. وتحدِّد كل دولة عضو في قانونها الوطني الإجراءات التي تتبع والشروط التي تراعى من أجل الحصول على النفاذ إلى البيانات المستبقاة وفقاً لمتطلبات الضرورة والتناسب، ورهناً بالأحكام ذات الصلة في قانون الاتحاد الأوروبي أو القانون الدولي العام، وخاصة الاتفاقية الأوروبية لحقوق الإنسان حسب تفسيرها في إطار المحكمة الأوروبية لحقوق الإنسان.

المادة 5 – فئات البيانات التي يتعيَّن استبقاؤها

1 تكفل الدول الأعضاء استبقاء فئات البيانات التالية بموجب هذا التوجيه:

(أ) البيانات اللازمة لتعقُّب وتعيين مصدر الاتصال:

(1) فيما يتعلق بالمهاتفة على الشبكات الثابتة والمهاتفة المتنقلة:

'1' رقم الهاتف الطالب؛

'2' اسم وعنوان المشتَرِك أو المستعمِل المسجَّل؛

(2) فيما يتعلق بالنفاذ إلى الإنترنت والبريد الإلكتروني عبر الإنترنت والمهاتفة عبر الإنترنت:

'1' الرقم (الأرقام) المخصصة لهوية المستعمِل؛

'2' هوية المستعمِل ورقم الهاتف المخصص لأي اتصال يدخل في الشبكة الهاتفية العمومية؛

'3' اسم وعنوان المشتَرِك أو المستعمِل المسجَّل الذي خُصِّص له عنوان بروتوكول إنترنت أو هوية مستعمِل أو رقم هاتف عند القيام بالاتصال؛

[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.

(ب) البيانات اللازمة لتعيين مقصد الاتصال:

(1) فيما يتعلق بالمهاتفة على الشبكة الثابتة والمهاتفة المتنقلة:

'1' الرقم المطلوب (الأرقام المطلوبة) (رقم الهاتف المطلوب/أرقام الهاتف المطلوبة) وكذلك الرقم أو الأرقام التي يتم تسيير النداء إليه أو إليها، في الحالات التي تنطوي على خدمات تكميلية مثل تحويل النداء أو نقل النداء؛

'2' اسم (أسماء) وعنوان (عناوين) المشترك (المشتركين) أو المستعمِل المسجَّل (المستعملين المسجَّلين)؛

(2) فيما يتعلق بالبريد الإلكتروني على الإنترنت والمهاتفة على الإنترنت:

'1' هوية المستعمِل أو رقم الهاتف للمتلقي المقصود (المتلقّين المقصودين) لنداء هاتفي على الإنترنت؛

'2' اسم (أسماء) وعنوان (عناوين) المشترك (المشتركين) أو المستعمل المسجَّل (المستعملين المسجَّلين) وهوية المستعمِل الخاصة بمتلقي الاتصال المقصود؛

(ج) البيانات اللازمة لتعيين تاريخ الاتصال ووقته ومدته:

(1) فيما يتعلق بالمهاتفة على الشبكة الثابتة والمهاتفة المتنقلة، تاريخ ووقت بداية ونهاية الاتصال؛

(2) فيما يتعلق بالنفاذ إلى الإنترنت والبريد الإلكتروني على الإنترنت والمهاتفة على الإنترنت:

'1' تاريخ ووقت الدخول إلى خدمة النفاذ إلى الإنترنت والخروج منها، على أساس منطقة زمنية معيَّنة، إلى جانب عنوان بروتوكول إنترنت، سواء كان دينامياً أو ثابتاً، الذي خصَّصه مقدِّم خدمة النفاذ إلى الإنترنت للاتصال، هوية المستعمِل الخاصة بالمشتَرِك أو بالمستعمِل المسجَّل؛

(2) تاريخ وموعد الدخول على خدمة البريد الإلكتروني للإنترنت أو خدمة المهاتفة على الإنترنت على أساس منطقة زمنية معيَّنة؛

(د) البيانات اللازمة لتعيين نوع الاتصال:

(1) فيما يتعلق بالمهاتفة على الشبكة الثابتة والمهاتفة المتنقلة: الخدمة الهاتفية المستعملة؛

(2) فيما يتعلق بالبريد الإلكتروني والمهاتفة على الإنترنت: خدمة الإنترنت المستعملة؛

(هـ) البيانات اللازمة لتعيين معدات اتصال المستعملين أو ما يُفهم أنها معدات المستعمِلين؛

(1) فيما يتعلق بالمهاتفة على الشبكة الثابتة، ورقم الهاتف الطالب ورقم الهاتف المطلوب؛

(2) فيما يتعلق بالمهاتفة المتنقلة:

'1' رقم الهاتف الطالب والهاتف المطلوب؛

'2' الهوية الدولية للمشتَرِك المتنقّل الخاصة بالطرف الطالب؛

'3' الهوية الدولية للجهاز المتنقل للطرف الطالب؛

'4' الهوية الدولية للمشترك المتنقل الخاصة بالطرف المطلوب؛

'5' الهوية الدولية للجهاز المتنقل الخاصة بالطرف المطلوب؛

'6' في حالة الخدمات مجهولة الهوية المدفوعة سلفاً، تاريخ وموعد بداية تشغيل الخدمة وسمة الموقع (الهوية الخلوية) الذي بدأ منه تشغيل الخدمة؛

(3) فيما يتعلق بالنفاذ إلى الإنترنت والبريد الإلكتروني والمهاتفة على الإنترنت:

'1' رقم الهاتف الطالب في حالة النفاذ عن طريق الاتصال الهاتفي؛

'2' رقم المشترك الرقمي أو النقطة الطرفية الأخرى مصدر الاتصال؛

(و) البيانات اللازمة لتعيين موقع جهاز الاتصال المتنقل:

(1) سمة الموقع (الهوية الخلوية) لبداية الاتصال؛

(2) بيانات تعريف الموقع الجغرافي للخلايا بالإشارة إلى سمات مواقعها (الهوية الخلوية) أثناء الفترة المحدّدة لاستبقاء بيانات الاتصال.

2 لا يجوز استبقاء بيانات تكشف عن محتوى الاتصال عملاً بهذا التوجيه.

المادة 6 – فترات الاستبقاء

تكفل الدول الأعضاء استبقاء فئات البيانات المحدّدة في المادة 5 لفترات لا تقل عن ستة أشهر ولا تزيد عن سنتين من تاريخ الاتصال.

المادة 7 – حماية البيانات وأمن البيانات

بدون الإخلال بالأحكام المعتمدة عملاً بالتوجيه 95/46/EC والتوجيه 2002/58/EC، تكفل كل دولة عضو احترام مقدّمي خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة، كحدٍ أدنى، المبادئ التالية لأمن البيانات فيما يتعلق بالبيانات التي يتم استبقاؤها وفقاً لهذا التوجيه:

(أ) أن تكون البيانات المستبقاة بنفس النوعية وخاضعة لنفس الأمن والحماية مثل البيانات في الشبكة؛

(ب) أن تخضع البيانات لتدابير ملائمة تقنية وتنظيمية لحماية البيانات من التدمير العرضي أو غير القانوني أو الفقد أو التبديل العرضي أو التخزين أو التجهيز أو النفاذ أو الكشف غير المأذون به أو غير القانوني؛

(ج) أن تخضع البيانات لتدابير ملائمة تقنية وتنظيمية لكفالة النفاذ إليها من جانب الأشخاص المصرح لهم بصفة خاصة فقط؛

(د) تدمير البيانات، باستثناء تلك التي تم النفاذ إليها وحفظها، في نهاية فترة الاستبقاء.

المادة 8 – متطلبات تخزين البيانات المستبقاة

تكفل الدول الأعضاء استبقاء البيانات المنصوص عليها في المادة 5 وفقاً لهذا التوجيه بطريقة تجعل من الممكن إرسال البيانات المستبقاة وأي معلومات ضرورية أخرى تتعلق بهذه البيانات بناءً على طلب السلطات المختصة بدون أي تأخير لا داعي له.

وقد أدّت تغطية هذا التوجيه للمعلومات الرئيسية عن أي اتصال عن طريق الإنترنت إلى نقد حاد من منظمات حقوق الإنسان.[1397] ويمكن أن يؤدّي ذلك بدوره إلى قيام المحاكم الدستورية بإعادة النظر في هذا التوجيه وتطبيقه.[1398] وبالإضافة إلى ذلك، أشارت مستشارة المحامي العام لمحكمة العدل الأوروبية جوليان كوكوت في ختام مرافعتها في قضية منتجي الموسيقى في إسبانيا (Promusicae) ضد شركة الهاتف الإسبانية،[1399] إلى أنه من المشكوك فيه أن يمكن تطبيق التزام استبقاء البيانات بدون انتهاك الحقوق الأساسية.[1400] وقد سبقت الإشارة إلى الصعوبات في صدد تطبيق هذه القواعد التنظيمية في مجموعة الثمانية في 2001.[1401]

[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.

ولكن النقد لا ينصبّ على هذا الجانب وحده. فهناك سبب آخر يجعل استبقاء البيانات أقل فاعلية في مكافحة الجريمة الإلكترونية وهو إمكانية الالتفاف حول الالتزامات. وتشمل أسهل الطرق للالتفاف حول التزام استبقاء البيانات ما يلي:

- استعمال معدات طرفية عامة مختلفة للإنترنت أو خدمات البيانات الهاتفية المتنقلة المدفوعة سلفاً التي لا تتطلب أي تسجيل،[1402]
- واستعمال خدمات اتصال مجهولة الهوية يتم تشغيلها (جزئياً على الأقل) في بلدان لا تطبِّق نظام استبقاء البيانات.[1403]

وإذا استعمَل الجناة أجهزة طرفية عامة مختلفة أو خدمات بيانات هاتفية متنقلة مدفوعة سلفاً بحيث لا يكون من الضروري تسجيل البيانات المخزونة من جانب مقدّمي الخدمة، فإن التزام استبقاء البيانات سيقود وكالات إنفاذ القانون إلى مقدِّم الخدمة فقط وليس إلى الجاني الفعلي.[1404]

وبالإضافة إلى ذلك، يستطيع الجناة الالتفاف حول التزام استبقاء البيانات باستعمال مقدمات اتصالات مجهولة الهوية.[1405] وفي هذه الحالة قد تستطيع وكالات إنفاذ القانون أن تثبت أن الجاني قد استعمَل مُخَدِّم اتصالات مجهول الهوية، ولكن هذه الوكالات لن تتمكن، بسبب الافتقار إلى النفاذ إلى بيانات الحركة في البلد الذي يقع فيه مُخَدِّم الاتصالات مجهول الهوية، من إثبات مشاركة الجاني في ارتكاب جريمة جنائية.[1406]

وفيما يتعلق بالسهولة الشديدة للالتفاف على الحكم، فإن تطبيق تشريعات استبقاء البيانات في الاتحاد الأوروبي يقترن بالخوف من أن هذه العملية ستتطلب تدابير جانبية ضرورية لكفالة فعالية هذه الأداة. ويمكن أن تشمل التدابير الجانبية المحتملة الالتزام بالتسجيل قبل استعمال الخدمات الإلكترونية[1407] أو حظر استعمال تكنولوجيا الاتصالات مجهولة الهوية.[1408]

6.2.6 التفتيش والضبط

رغم أن أدوات التحقيق الجديدة مثل جمع بيانات المحتوى في الوقت الحقيقي واستعمال برمجيات التحليل القضائي (الطب الشرعي) عن بُعد لتعيين الجاني لا تزال موضع المناقشة ورغم تطبيقها بالفعل في بعض البلدان، يظل التفتيش والضبط يمثلان دائماً أداة من أهم أدوات التحقيق.[1409] وبمجرد تعيين الجاني وقيام وكالة إنفاذ القانون بضبط معداته الخاصة بتكنولوجيا المعلومات يستطيع خبراء التحليل القضائي (الطب الشرعي) الحاسوبي تحليل الجهاز لجمع الأدلة اللازمة للادعاء.[1410]

[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. 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.

وتجري في الوقت الحاضر مناقشة إمكانية استبدال أو تعديل إجراء التفتيش والضبط في بعض البلدان الأوروبية وفي الولايات المتحدة.[1411] وهناك إمكانية لتجنُّب ضرورة دخول مسكن المتهم تفتيشه وضبط جهازه الحاسوبي، وهذه الإمكانية هي إجراء التفتيش على الخط إلكترونياً. وتصف الأداة التي سيرد وصفها بمزيد من التفصيل في الأقسام التالية إجراءً تقوم بمقتضاه وكالات إنفاذ القانون بالنفاذ إلى حاسوب المشتبه فيه عن طريق الإنترنت للقيام بإجراءات التفتيش السرية.[1412] ورغم أن وكالات إنفاذ القانون تستطيع بوضوح أن تستفيد من عدم إدراك المتهم لوجود تحقيقات، فإن النفاذ المادي إلى العتاد يمكّن من تطبيق تقنيات تحقيقيه أكثر كفاءة.[1413] ويبرز ذلك الدور الهام لإجراءات التفتيش والضبط في إطار تحقيقات الإنترنت.

الاتفاقية المتعلقة بالجريمة الإلكترونية

تتضمن معظم قوانين الإجراءات الجنائية الوطنية أحكاماً تمكّن وكالات إنفاذ القانون من التفتيش وضبط الأشياء.[1414] والسبب في أن واضعي الاتفاقية قاموا رغم ذلك بإدراج أحكام تتناول التفتيش والضبط هو أن القوانين الوطنية لا تغطي في كثير من الأحيان إجراءات التفتيش والضبط المتصلة بالبيانات.[1415] إذ إن بعض البلدان، على سبيل المثال، تقصر تطبيق إجراءات الضبط على ضبط الأشياء المادية.[1416] واستناداً إلى مثل هذه الأحكام يستطيع المحققون القانونيون ضبط مخدِّم كامل ولكنهم لا يستطيعون ضبط البيانات ذات الصلة وحدها بنسخها من المخدِّم. ويمكن أن يسبب ذلك صعوبات في الحالات التي تكون فيها المعلومات ذات الصلة مخزونة على المخدِّم إلى جانب بيانات تخص مئات المستعملين الآخرين، ثم لا تكون متاحة لهم بعد قيام وكالات إنفاذ القانون بضبط المخدِّم. وهناك مثال آخر لعدم كفاية إجراءات التفتيش والضبط التقليدية المطبَّقة على البنود الملموسة، وذلك عندما لا تعرف وكالات إنفاذ القانون الموقع المادي للمخدِّم ولكنها تستطيع الوصول إليه عن طريق الإنترنت.[1417]

وتهدف الفقرة الفرعية 1 من المادة 19 من الاتفاقية المتعلقة بالجريمة الإلكترونية إلى إقامة أداة تمكّن من تفتيش الأنظمة الحاسوبية وتعادل في كفاءتها إجراءات التفتيش التقليدية.[1418]

المادة 19 – تفتيش ومصادرة بيانات الكمبيوتر المخزونة

1 يعتمد كل طرف ما قد يلزم من تدبير تشريعية وتدابير أخرى وذلك لمنح سلطات ذلك الطرف صلاحية تفتيش أو الدخول على:

أ) أي نظام كمبيوتر أو أي جزء منه والبيانات المخزَّنة فيه.

ب) أي وسيط تخزين تجوز أن تكون البيانات مخزَّنة فيه في إقليم ذلك الطرف.

ورغم أن إجراء التفتيش والضبط هو أداة يستعملها المحققون بصورة متكررة، فهناك عدد من التحديات التي تقترن بتطبيقها في التحقيقات في الجرائم السيبرانية.[1419] وتتمثَّل إحدى الصعوبات الأساسية في أن أوامر التفتيش تقتصر في كثير من الأحيان على أماكن بعينها (مثل مسكن

[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.

[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.

المشتبه فيه).[1420] وفي صدد التفتيش عن بيانات حاسوبية يمكن أن يتبيَّن أثناء التحقيق أن المشتبه فيه لم يخزِّن البيانات على المحركات الصلبة الداخلية بل على مخدِّم خارجي يستطيع النفاذ إليه عن طريق الإنترنت.[1421] ويتزايد إقبال مستعملي الإنترنت على مخدمات الإنترنت من أجل تخزين البيانات وتجهيزها (''الحوسبة بين السُحب''). ومن مزايا تخزين المعلومات على مخدِّم إنترنت أن المعلومات يمكن الوصول إليها من أي مكان توجد فيه توصيلة بالإنترنت. ومن المهم لكفالة إمكانية إجراءات التحقيقات بكفاءة الاحتفاظ بدرجة من المرونة في التحقيقات. فإذا اكتشف المحققون أن المعلومات ذات الصلة مخزَّنة على نظام حاسوبي آخر فلا بد أن يكون بإمكانهم توسيع التفتيش ليشمل هذا النظام.[1422] وتعالج الاتفاقية المتعلقة بالجريمة الإلكترونية هذه القضية في الفقرة الفرعية 2 من المادة 19.

المادة 19 – تفتيش ومصادرة بيانات الكمبيوتر المخزَّنة

[...]

2 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لضمان أنه في حالة قيام سلطاته بعمليات البحث أو الدخول على نظام كمبيوتر بعينه أو على جزء منه، وفقاً للفقرة 1 (أ)، وقيام أسباب لديها للاعتقاد بأن البيانات المطلوبة مخزَّنة داخل نظام كمبيوتر آخر أو جزء منه في إقليم ذلك الطرف، وأن هذه البيانات يمكن الدخول عليها قانوناً أو متاحة على النظام الأصلي، يكون للسلطات توسيع عملية البحث أو الدخول المماثل بسرعة على النظام الآخر.

ويتصل أحد التحديات الأخرى بضبط بيانات الحاسوب. فإذا استنتج المحققون أن ضبط العتاد المستعمل لتخزين المعلومات غير ضروري أو لن يكون كافياً فقد يحتاجون بعد ذلك إلى أدوات أخرى تمكِّنهم من مواصلة إجراء التفتيش والضبط في صدد البيانات الحاسوبية المخزونة.[1423] ولا تقتصر الأدوات اللازمة على نسخ البيانات ذات الصلة.[1424] إذ يوجد، بالإضافة إلى ذلك، عدد من التدابير الجانبية اللازمة للحفاظ على الكفاءة المطلوبة مثل ضبط النظام الحاسوبي ذاته. والجانب الأهم هو الحفاظ على سلامة البيانات المنسوخة.[1425] وإذا لم يكن المحققون يملكون تصريحاً باتخاذ التدابير اللازمة لكفالة سلامة البيانات المنسوخة، فإن البيانات المنسوخة قد لا تكون مقبولة كدليل في الإجراءات الجنائية.[1426] وبعد أن ينسخ المحققون البيانات ويتخذون التدابير اللازمة للحفاظ على سلامتها فسيتعيَّن عليهم اتخاذ قرار بشأن طريقة معاملة البيانات الأصلية. ونظراً لأن المحققين لا يأخذون العتاد معهم أثناء عملية الضبط، فإن المعلومات تظل في العتاد عموماً ولن يتمكَّن المحققون في التحقيقات المتصلة بالمحتوى غير القانوني خاصة[1427] (مثل المواد الفاضحة التي تستخدم الأطفال) من ترك البيانات على المخدِّم. ولذلك سيحتاجون إلى أداة تسمح لهم بإزالة البيانات أو التأكد على الأقل من أن هذه البيانات لن يمكن النفاذ إليها بعد ذلك.[1428] وتعالج الاتفاقية المتعلقة بالجريمة الإلكترونية هذه القضايا المذكورة أعلاه في الفقرة الفرعية 3 من المادة 19.

[1420] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

[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.

[1428] One possibility to prevent access to the information without deleting them is the use encryption technology.

المادة 19 – تفتيش ومصادر بيانات الكمبيوتر المخزَّنة

[...]

3 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطاته المختصة صلاحية ضبط أو تأمين بيانات الكمبيوتر التي يتم الدخول عليها طبقاً للفقرتين 1 أو 2، وتشمل هذه الإجراءات صلاحية:

أ) ضبط أو تأمين نظام الكمبيوتر أو جزء منه أو وسيط تخزين البيانات؛

ب) عمل نسخة من هذه البيانات الكمبيوترية والاحتفاظ بها؛

ج) المحافظة على تجانس بيانات الكمبيوتر المخزَّنة ذات الصلة؛

د) جعل هذه البيانات الكمبيوترية غير قابلة للدخول عليها أو إزالتها على نظام الكمبيوتر الذي يتم الدخول عليه.

ويتمثَّل أحد التحديات الأخرى في صدد أوامر التفتيش المتعلقة بالبيانات الحاسوبية في أنه من الصعب في بعض الأحيان أن تكتشف وكالات إنفاذ القانون مكان وجود البيانات. إذ إن هذه البيانات تخزَّن في كثير من الأحيان في أنظمة حاسوبية خارج أراضي البلد المحدَّد. وحتى في حالة معرفة الموقع الدقيق للبيانات، فإن مقدار البيانات المخزونة قد يعرقل في كثيرٍ من الأحيان التعجيل بالتحقيقات السريعة.[1429] وفي هذه الحالات، تواجه التحقيقات صعوبات فريدة في حالة وجود بُعد دولي يتطلب تعاوناً دولياً في التحقيقات.[1430] وحتى عندما تتصل التحقيقات بأنظمة حاسوبية تقع داخل الحدود الوطنية ويستطيع المحققون تعيين مقدِّم الخدمة المضيف الذي يقوم بتشغيل المخدِّم الذي خزَّن عليه الجاني البيانات ذات الصلة فقد يواجه المحققون صعوبات في تعيين المكان الدقيق لهذه البيانات. فمن المرجح جداً أن يملك حتى صغار أو متوسطي مقدمي خدمة الاستضافة مئات أجهزة المخدِّمات وآلاف الأقراص الصلبة. وفي حالات كثيرة جداً لا يتمكَّن المحققون من تعيين الموقع الدقيق بمساعدة مدير النظام المسؤول عن البنية التحتية للمخدِّم.[1431] ولكن حتى إذا تمكنوا من تعيين المحرك الصلب المحدَّد، فإن تدابير الحماية قد تمنعهم من البحث عن البيانات ذات الصلة. وقرَّر واضعو الاتفاقية معالجة هذه المسألة بتطبيق تدبير قسري لتسهيل تفتيش وضبط البيانات الحاسوبية. ولهذا تمكِّن الفقرة الفرعية 4 من المادة 19 المحققين من إرغام مدير أي نظام على مساعدة وكالات إنفاذ القانون. ورغم أن الالتزام بطاعة أمر المحقق يقتصر على المعلومات اللازمة وعلى تقديم الدعم للقضية، فإن هذه الأداة تغيِّر طابع إجراءات التفتيش والضبط. ففي كثيرٍ من البلدان لا ترغم أوامر التفتيش والضبط الأشخاص المتأثرين بالتحقيق إلاّ على تحمُّل الإجراءات – ولا يتعيَّن عليهم دعم التحقيق دعماً نشطاً. وفيما يتعلق بأي شخص يملك معرفة خاصة مطلوبة للتحقيق، فإن تطبيق الاتفاقية المتعلقة بالجريمة الإلكترونية يغيِّر الحالة بطريقتين. إذ عليهم أولاً توفير المعلومات اللازمة للمحققين. والتغيير الثاني يتصل بهذا الالتزام. فالالتزام بتقديم دعم – معقول – للمحققين يعفي الشخص الذي يملك المعرفة الخاصة من التزاماته التعاقدية أو الأوامر الصادرة إليهم من المشرفين.[1432] ولا تحدِّد الاتفاقية مصطلح "معقول" ولكن التقرير التفسيري يشير إلى أن المعقول *"قد يشمل الإفصاح عن كلمة مرور أو أي تدبير أمني آخر لسلطات التحقيق"* ولكنه لا يشمل عموماً *"الإفصاح عن كلمة مرور أو تدبير أمني آخر"* إذا صاحب ذلك *"تهديد غير معقول لخصوصية المستعملين الآخرين أو البيانات الأخرى التي لا يصرَّح بتفتيشها"*.[1433]

[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.

[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.

المادة 19 – تفتيش ومصادرة بيانات الكمبيوتر المخزَّنة

[...]

4 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطاته المختصة صلاحية إصدار الأمر لأي شخص لديه معلومات عن تشغيل نظام الكمبيوتر أو الإجراءات المطبَّقة لحماية البيانات الموجودة عليه من أجل أن يقدِّم – بالقدر المعقول – المعلومات اللازمة للتمكين من مباشرة الإجراءات المشار إليها في الفقرتين 1 و2.

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في قانون الكومنولث النموذجي لعام 2002.[1434]

المادة 11

في هذا الجزء:

[...]

يشمل "الضبط":

(أ) إنشاء واستبقاء نُسخة من البيانات الحاسوبية، بما في ذلك استعمال المعدات الموجودة في الموقع؛

(ب) وجعل البيانات الحاسوبية في النظام الحاسوبي الذي تم الدخول إليه غير قابلة للنفاذ إليها أو إزالتها من النظام؛

(ج) وأخذ مطبوعة من ناتج بيانات الحاسوب.

المادة 12[1435]

(1) إذا اقتنع قاضي تحقيق استناداً إلى [معلومات مقدَّمة بعد حلف يمين] [موثَّق] بوجود أسباب معقولة [للاشتباه] [تدعو إلى الاعتقاد] بأن شيئاً أو بيانات حاسوبية قد تكون موجودة في مكان ما وأنها:

(أ) قد تكون مادية كأدلة لإثبات ارتكاب جريمة؛

(ب) أو حصل عليها شخص نتيجة ارتكاب جريمة؛

فإن القاضي [له] [عليه] أن يصدر أمراً يصرِّح لضابط [إنفاذ قوانين] [شرطة]، بالدخول، بأي مساعدة قد تكون ضرورية، إلى المكان المعني وتفتيشه وضبط الشيء أو البيانات الحاسوبية.

المادة 13[1436]

(1) أي شخص يمتلك وسيط تخزين بيانات حاسوبية أو نظام حاسوبي أو يسيطر عليه ويكون هذا الوسيط أو النظام خاضعاً للتفتيش بموجب المادة 12 يجب أن يسمح، وأن يساعد عند الاقتضاء، الشخص الذي يقوم بالتفتيش:

(أ) النفاذ إلى النظام الحاسوبي أو وسيط تخزين البيانات الحاسوبية واستعمالها للبحث عن أي بيانات حاسوبية متوفِّرة للنظام أو في النظام؛

(ب) والحصول على البيانات الحاسوبية ونسخها؛

[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.*

[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.*

(ج) واستعمال معدات للحصول على نُسخ؛

(د) والحصول على ناتج مفهوم من النظام الحاسوبي في نسق نصي واضح يمكن أن يقرأه الشخص.

(2) أي شخص يمتنع بدون عذر أو مبرِّر قانوني عن السماح لهذا الشخص أو مساعدته يرتكب جريمة يعاقب عليها بعد الإدانة بالحبس لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ]، أو كلاهما.

7.2.6 أمر الإبراز

حتى إذا كان القانون الوطني لا يطبِّق التزاماً مثل الالتزام الوارد في الفقرة الفرعية 4 من المادة 19 من الاتفاقية المتعلقة بالجريمة الإلكترونية، فإن مقدمي الخدمة يتعاونون في كثير من الأحيان مع وكالات إنفاذ القانون لتجنُّب الأثر السلبي على أعمالهم التجارية. وإذا لم يتمكَّن المحققون – بسبب الافتقار إلى تعاون مقدِّم الخدمة – من العثور على البيانات أو أجهزة التخزين التي يحتاجونها للتفتيش والضبط، فمن المرجح أنهم سيحتاجون في هذه الحالة إلى ضبط عتاد أكثر من اللازم عموماً. ولذلك سيعمد مقدمو الخدمة عموماً إلى دعم التحقيقات وتقديم البيانات اللازمة عندما تطلبها وكالات إنفاذ القانون. وتتضمن الاتفاقية المتعلقة بالجريمة الإلكترونية أدوات تسمح للمحققين بالامتناع عن إصدار أوامر التفتيش إذا قدَّم الشخص الذي يملك البيانات ذات الصلة هذه البيانات إلى المحققين.[1437]

ورغم أن الجهود المشتركة لكلا وكالات إنفاذ القانون ومقدمي الخدمة حتى في الحالات التي لا يتوفر فيها أساس قانوني تبدو وكأنها مثالاً إيجابياً للشراكة بين الجهات العامة والخاصة فهناك عدد من الصعوبات التي تتصل بعدم تنظيم هذا التعاون. بالإضافة إلى قضايا حماية البيانات، فإن الاهتمام الرئيسي يتصل باحتمال انتهاك مقدمي الخدمة التزاماتهم التعاقدية مع عملائهم إذا اتبعوا طلب تقديم بعض البيانات دون أن يكون الطلب مستنداً إلى أساس قانوني كافٍ.[1438]

المادة 18 – إصدار الأوامر:

1 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطات ذلك الطرف صلاحية توجيه الأمر إلى:

أ) أي شخص في إقليمه لتقديم بيانات محدَّدة موجودة على الكمبيوتر بحوزة ذلك الشخص أو تحت سيطرته، ومخزَّنة داخل نظام الكمبيوتر أو على أي وسيط تخزين بيانات آخر.

ب) أي مقدِّم خدمة يعرض خدماته في إقليم الطرف لتقديم معلومات للمشترك فيما يتعلق بتلك الخدمات الموجودة بحوزة أو تحت سيطرة مقدِّم الخدمة.

وتتضمَّن المادة 18 التزامين إثنين. فالفقرة الفرعية 1 (أ) من المادة 18 تلزم أي شخص (بما في ذلك مقدِّم الخدمة) بتقديم بيانات حاسوبية محدَّدة تكون في حوزة ذلك الشخص أو تحت سيطرته. وبعكس الفقرة الفرعية 1 (ب) لا يقتصر تطبيق الحكم على بيانات محدَّدة. ويتطلب مصطلح ''حيازة'' أن يملك الشخص النفاذ المادي إلى أجهزة تخزين البيانات التي خُزنت فيها المعلومات المحدَّدة.[1439] وتم توسيع تطبيق هذا الحكم بمصطلح ''سيطرة''. وتكون البيانات تحت سيطرة الشخص إذا لم يكن يملك النفاذ المادي إليها ولكنه يدير المعلومات. ويحدث هذا مثلاً إذا كان الشخص المشتبه فيه قد خزَّن البيانات ذات الصلة على نظام تخزين إلكتروني على الخط عن بُعد. ورغم ذلك يشير واضعو الاتفاقية في التقرير التفسيري إلى أن مجرَّد وجود القدرة التقنية على الوصول عن بُعد إلى البيانات المخزَّنة لا يشكِّل سيطرة بالضرورة.[1440] ولذلك يقتصر تطبيق المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية على الحالات التي تتجاوز فيها درجة سيطرة الشخص المشتبه فيه الإمكانية المحتملة للنفاذ إليها.

[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.

[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.

وتتضمن الفقرة الفرعية 1 (ب) أمر إبراز يقتصر على بعض البيانات. واستناداً إلى الفقرة الفرعية 1 (ب) من المادة 18 يستطيع المحققون إصدار أمر لمقدِّم الخدمة بأن يقدِّم معلومات المشترك. ويمكن أن تكون معلومات المشترك ضرورية لتعيين الجاني. وإذا تمكَّن المحققون من اكتشاف عنوان بروتوكول إنترنت الذي استعمله الجاني، فإنهم يحتاجون إلى ربط هذا الرقم بالشخص.[1441] وفي معظم الحالات لا يقود عنوان بروتوكول إنترنت إلاّ إلى مقدِّم خدمة الإنترنت الذي قدَّم عنوان بروتوكول إنترنت إلى المستعمل. وقبل أن يمكن استعمال أي خدمة يتطلب مقدِّم خدمة الإنترنت عادة من المستعمل أن يسجِّل معلومات المشترك الخاصة به.[1442] وفي هذا السياق يكون من المهم أن نبرز أن المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية لا تطبِّق التزام استبقاء البيانات[1443] ولا التزام مقدِّمي الخدمة بتسجيل معلومات المشترك.[1444] وتسمح الفقرة الفرعية 1 (ب) من المادة 18 للمحققين بإصدار أمر إلى مقدِّم الخدمة بتقديم معلومات المشترك.

ولا يبدو التمييز بين ''البيانات الحاسوبية'' في الفقرة الفرعية 1 (أ) و''معلومات المشترك'' في الفقرة الفرعية 1 (ب) للوهلة الأولى ضرورياً حيث تكون معلومات المشترك المخزونة في شكل رقمي مشمولة أيضاً في الفقرة الفرعية 1 (أ). والسبب الأول للتمييز يتصل باختلاف تعاريف ''البيانات الحاسوبية'' و''معلومات المشترك''. فعلى العكس من ''البيانات الحاسوبية'' لا يتطلب مصطلح ''معلومات المشترك'' أن تكون المعلومات مخزونة باعتبارها بيانات حاسوبية. وتمكِّن الفقرة الفرعية 1 (ب) من المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية السلطات القانونية المختصة من تقديم معلومات محفوظة في شكل غير رقمي.[1445]

المادة 1 – تعريفات

لأغراض هذه الاتفاقية:

ب) يقصد ''ببيانات الكمبيوتر'' أية عمليات عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية معالجة داخل منظومة الكمبيوتر، بما في ذلك برنامج مناسب لجعل منظومة كمبيوتر تؤدي وظائفها؛

المادة 18 – إصدار الأوامر

3 لغرض هذه المادة – فإن مصطلح ''معلومات المشترك'' يعني أية معلومات في صورة بيانات كمبيوتر أو أي صورة أخرى يتم حفظها من جانب مقدِّم الخدمة، والتي تتعلَّق بالمشتركين في الخدمات الخاصة به بخلاف خط سير البيانات أو مضمونها والتي بموجبها يمكن التوصل إلى:

أ) نوعية خدمة الاتصال المستخدمة والشروط الفنية التي يتم اتخاذها في ذلك والفترة الزمنية للخدمة.

ب) هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم تليفونه وغير ذلك من أرقام الدخول الأخرى الخاصة به، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

ج) أية معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الاتصالات، والتي تتوافر بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

والسبب الثاني للتمييز بين ''البيانات الحاسوبية'' و''معلومات المشترك'' هو أن ذلك يمكِّن مشرِّعي القوانين من تنفيذ متطلبات مختلفة في صدد تطبيق الأدوات.[1446] إذ يمكن مثلاً تنفيذ متطلبات أكثر صرامة[1447] فيما يتعلق بأمر إبراز يتصل بالفقرة الفرعية 1 (ب)، نظراً لأن هذه الأدوات

[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.
[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.

تسمح لوكالات إنفاذ القانون بالنفاذ إلى أي نوع من البيانات الحاسوبية بما فيها بيانات المحتوى.[1448] والتفريق بين جمع بيانات الحركة في الوقت الحقيقي (المادة 20)[1449] وجمع بيانات المحتوى في الوقت الحقيقي (المادة 21)[1450] يوضِّح أن واضعي الاتفاقية أدركوا أن وكالات إنفاذ القانون تستطيع النفاذ إلى مختلف الضمانات التي يتعيَّن تنفيذها حسب نوع البيانات المعنية.[1451] وبهذا التفريق بين ''البيانات الحاسوبية'' و''معلومات المشترك'' تمكِّن المادة 18 من الاتفاقية المتعلقة بالجريمة الإلكترونية الدول الموقَّعة من إقامة نظام مشابه للضمانات المتدرجة بشأن أمر الإبراز.[1452]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في قانون الكومنولث النموذجي لعام 2002.[1453]

المادة 15

إذا اقتنع قاضي التحقيق استناداً إلى طلب مقدَّم من ضابط شرطة بأن بيانات حاسوبية معيَّنة، أو مطبوعة أو غير ذلك من المعلومات، مطلوبة بصورة معقولة لأغراض تحقيق جنائي أو دعوى جنائية يجوز لقاضي التحقيق أن يأمر:

(أ) أي شخص في إقليم [البلد الذي سن القانون] يسيطر على نظام حاسوبي أن يبرز من النظام البيانات الحاسوبية المحدَّدة أو مطبوعة منها أو أي ناتج من هذه البيانات في شكل مفهوم؛

(ب) أي مقدِّم خدمة إنترنت في [البلد الذي سن القانون] أن يبرز معلومات عن الأشخاص المشتركين في الخدمة أو المستعملين لها بشكل آخر؛

(ج)[1454] *أي شخص في إقليم [البلد الذي سن القانون] يملك النفاذ إلى نظام حاسوبي معيَّن بأن يجهِّز ويجمع بيانات حاسوبية محدَّدة من النظام وأن يعطيها إلى شخص محدَّد.*

8.2.6 جمع البيانات في الوقت الحقيقي

المراقبة الهاتفية أداة تستعمل في التحقيقات في الجرائم الكبرى في كثير من البلدان.[1455] وينطوي كثير من الجرائم على استعمال الهاتف – وخاصة الهواتف المتنقلة – سواء عند إعداد أو تنفيذ الجريمة. وفي الحالات التي تنطوي على الاتجار بالمخدرات خصوصاً يمكن أن تكون مراقبة المحادثات بين الجناة أمراً حيوياً لنجاح التحقيق. وتسمح هذه الأداة للمحققين بجمع معلومات قيِّمة رغم أن ذلك يقتصر على المعلومات المتبادلة عبر الخطوط/الهواتف المراقبة. وإذا استعمل الجاني وسيلة تبادل أخرى (مثل الخطابات) أو خطوط غير مشمولة بالمراقبة، فلن يتمكَّن المحققون من تسجيل المحادثة. ولا يختلف الوضع عموماً عندما يتعلق الأمر بمحادثة مباشرة بدون استعمال الهاتف.[1456]

[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.

[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.*

واليوم حلَّ تبادل البيانات محل المحادثات الهاتفية التقليدية. ولا يقتصر تبادل البيانات على البريد الإلكتروني ونقل الملفات، إذ إن قدراً كبيراً من المحادثات الصوتية يجري باستعمال تكنولوجيا تستند إلى بروتوكولات إنترنت (الصوت على بروتوكول إنترنت).[1457] وإذا نظرنا إلى المكالمة الهاتفية بالصوت على بروتوكول إنترنت من وجهة نظر تقنية فسوف نجد أنها أقرب شبهاً بتبادل البريد الإلكتروني عنها بالنداء الهاتفي التقليدي باستعمال أسلاك الهاتف، ويقترن اعتراض هذا النوع من المكالمات بصعوبات فريدة.[1458]

ونظراً لأن كثيراً من الجرائم الحاسوبية ينطوي على تبادل بيانات، فإن القدرة على اعتراض هذه العمليات بنفس الدرجة أو القدرة خلاف ذلك على استعمال بيانات تتصل بعمليات التبادل قد تكون مطلباً جوهرياً لنجاح التحقيقات. وقد تبيَّن أن تطبيق أحكام مراقبة الهاتف القائمة وكذلك تطبيق الأحكام المتصلة باستعمال بيانات حركة الاتصالات في تحقيقات الجرائم السيبرانية أمر عسير في بعض البلدان. وتتصل الصعوبات التي ظهرت بقضايا تقنية[1459] وكذلك بقضايا قانونية. ومن وجهة النظر القانونية لا يشمل التصريح بتسجيل المكالمات الهاتفية بالضرورة تصريحاً باعتراض عمليات نقل البيانات.

وتهدف الاتفاقية المتعلقة بالجريمة الإلكترونية إلى سد الثغرات القائمة في قدرة وكالات إنفاذ القانون على رصد عمليات نقل البيانات.[1460] وفي إطار هذا النهج تميِّز الاتفاقية المتعلقة بالجريمة الإلكترونية بين مجموعتين من مراقبة نقل البيانات. فالمادة 20 تصرِّح للمحققين بجمع بيانات الحركة. وتعرِّف الفقرة (د) من المادة 1 من الاتفاقية المتعلقة بالجريمة الإلكترونية ''بيانات الحركة''

المادة 1 – تعريفات

د) *يقصد بـ''بيانات المرور'' أي بيانات كمبيوتر متعلقة باتصال عن طريق منظومة كمبيوتر والتي تنشأ عن منظمة كمبيوتر تشكِّل جزءاً في سلسلة الاتصالات، توضِّح مصدر الاتصال، والجهة المرسلة إليها، والطريق الذي تسلكه، ووقت وتاريخ، وحجم، ومدة، ونوع الخدمة المذكورة.*

والتمييز بين ''بيانات المحتوى'' و''بيانات الحركة'' هو نفسه التمييز المستعمل في معظم القوانين الوطنية المتصلة.[1461]

9.2.6 جمع بيانات الحركة

الاتفاقية المتعلقة بالجريمة الإلكترونية

في صدد تباين تعريف بيانات الحركة من بلد لآخر،[1462] قرَّر واضعو الاتفاقية المتعلقة بالجريمة الإلكترونية تعريف هذا المصطلح لتحسين تطبيق الحكم المتصل في التحقيقات الدولية. ويستعمل مصطلح ''بيانات الحركة'' لوصف البيانات التي تولدها الحواسيب أثناء عملية الاتصال من أجل تسيير اتصال من المنشأ إلى المقصد. وكلما اتصل أي مستعمل بالإنترنت أو قام بتنزيل بريد إلكتروني أو فتح موقعاً في شبكة الويب، فإن ذلك يولِّد بيانات حركة. وفيما يتعلق بتحقيقات الجريمة السيبرانية، فإن أهم بيانات الحركة المتصلة بالمنشأ والمقصد هي عناوين بروتوكول إنترنت التي تحدِّد هوية شريك الاتصال في أي اتصال عن طريق الإنترنت.[1463]

[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.

[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.

وعلى العكس من 'بيانات المحتوى'، يغطي مصطلح ''بيانات الحركة'' فقط البيانات الناشئة داخل عمليات نقل البيانات ولكنه لا يغطي البيانات المنقولة نفسها. ورغم أن النفاذ إلى بيانات المحتوى قد يكون ضرورياً في بعض الحالات نظراً لأنه يمكّن وكالات إنفاذ القانون من تحليل الاتصال بطريقة أكثر فعالية، فإن بيانات الحركة تؤدي دوراً هاماً في تحقيقات الجرائم السيبرانية.[1464] وفي حين أن النفاذ إلى بيانات المحتوى يمكّن وكالات إنفاذ القانون من تحليل طبيعة رسائل الملفات المتبادلة، فإن بيانات الحركة يمكن أن تكون ضرورية لتعيين الجاني. وفي قضايا استخدام الأطفال في المواد الفاضحة، فإن بيانات الحركة يمكن، على سبيل المثال، أن تمكّن المحققين من تعيين صفحة الويب التي يقوم الجاني فيها بتحميل صور أطفال فاضحة. ومن خلال رصد بيانات الحركة المتولّدة أثناء استعمال خدمات الإنترنت تستطيع وكالات إنفاذ القانون من تعيين عنوان بروتوكول إنترنت للمخدِّم وتحاول بعد ذلك أن تحدِّد الموقع المادي.

المادة 20 – التجميع الفوري لبيانات الكمبيوتر:

1 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطاته المختصة صلاحية:

أ) جمع أو تسجيل، من خلال تطبيق الوسائل الفنية، في إقليم ذلك الطرف؛ و

ب) إجبار مقدِّم الخدمة، في نطاق قدرته الفنية على:

'1' جمع أو تسجيل، من خلال تطبيق الوسائل الفنية في إقليم ذلك الطرف؛ أو

'2' التعاون مع السلطات المختصة ومساعدتها في جمع أو تسجيل، بشكل فوري، خط سير البيانات المرتبطة باتصالات معيَّنة في إقليم ذلك الطرف التي تم نقلها بواسطة نظام الكمبيوتر.

2 في حالة تعذُّر تبني الطرف للإجراءات المشار إليها في الفقرة 1 (أ)، بسبب المبادئ القائمة في نظامه القانوني الوطني، يجوز له بدلاً من ذلك أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان الجمع أو التسجيل الفوريين لخط سير البيانات المرتبطة باتصالات معيَّنة تم نقلها في إقليمه، من خلال تطبيق الوسائل الفنية في ذلك الإقليم.

3 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإلزام مقدِّم الخدمة بالمحافظة على سرية وقائع تنفيذ أية صلاحيات تنص عليها هذه المادة وأية معلومات تتعلق بها.

4 تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و15.

وتتضمن المادة 20 نهجين مختلفين لجمع بيانات الحركة، ومن المفترض تنفيذ كلا النهجين.[1465]

- النهج الأول هو تطبيق التزام مقدِّمي خدمة الإنترنت بتمكين وكالات إنفاذ القانون من القيام مباشرة بجمع البيانات ذات الصلة. ويتطلب ذلك عموماً إنشاء سطح بيني تستطيع وكالات إنفاذ القانون أن تستعمله للنفاذ إلى البنية التحتية لمقدمي خدمة الإنترنت.[1466]
- النهج الثاني هو تمكين وكالات إنفاذ القانون من إرغام مقدِّم خدمة الإنترنت على تجميع البيانات بناءً على طلب وكالات إنفاذ القانون. ويمكّن هذا النهج المحققين من الاستفادة من القدرات التقنية الموجودة والمعارف المتوفرة لدي مقدمي الخدمة عموماً. وأحد أغراض الجمع بين هذين النهجين هو كفالة تمكين وكالات إنفاذ القانون من إجراء الوكالات بتحقيقاتها (على أساس الفقرة الفرعية 1 (ب) من المادة 20) بدون مساعدة من مقدِّم الخدمة في حالة عدم توفُّر التكنولوجيا لدى مقدمي الخدمة لتسجيل البيانات.[1467]

[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.*

[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.

وقد وضعت الاتفاقية المتعلقة بالجريمة الإلكترونية بدون تفضيل لأي تكنولوجيا محدَّدة وبدون أن تهدف إلى وضع معايير تستدعي ضرورة الدخول في استثمارات مالية عالية من جانب قطاع الصناعة المعني.[1468] ومن هذا المنظور يبدو أن الفقرة الفرعية 1 (أ) من المادة 20 من الاتفاقية المتعلقة بالجريمة الإلكترونية تمثِّل الحل الأفضل. ولكن القاعدة التنظيمية في الفقرة الفرعية 2 من المادة 20 توضح أن واضعي الاتفاقية كانوا يدركون أن بعض البلدان قد تواجه صعوبات في تطبيق تشريع يمكِّن وكالات إنفاذ القانون من القيام بالتحقيقات بصورة مباشرة.

وتتمثَّل إحدى الصعوبات الكبرى في التحقيقات استناداً إلى المادة 20 في استعمال وسائل الاتصال مجهول الهوية. وكما أوضحنا أعلاه[1469] يستطيع الجناة استعمال خدمات في الإنترنت تمكِّن من القيام بالإرسال مجهول الهوية. وإذا كان الجاني يستعمل خدمة إرسال مجهول الهوية مثل برمجية TOR[1470] لحماية الحركة، فإن المحققين في معظم الحالات لا يستطيعون القيام بتحليل ناجح لبيانات الحركة أو تعيين شريك الاتصال. ويستطيع الجاني أن يحقِّق نتيجة مشابهة من خلال استعمال المعدات الطرفية العامة للإنترنت.[1471]

ومقارنة بإجراءات التفتيش والضبط التقليدية يتمثَّل أحد مزايا جمع بيانات الحركة في أن الشخص الذي يشتبه في ارتكابه جريمة لا يدرك بالضرورة وجود تحقيق بشأنه.[1472] ويؤدي ذلك إلى تضييق إمكانياته في التلاعب بالأدلة أو حذفها. ولكفالة عدم قيام مقدمي الخدمة بإعلام الجناة بالتحقيق الجاري تعالج الفقرة الفرعية 3 من المادة 20 هذه المسألة وتُلزم الدول الموقِّعة بتطبيق تشريع يضمن أن مقدمي الخدمة سيكفلون بقاء المعرفة بالتحقيقات الجارية سرية. وبالنسبة لمقدم الخدمة يقترن ذلك بميزة إعفاء مقدِّم الخدمة من الالتزام[1473] بإبلاغ المستعملين.[1474]

وقد صُمِّمت الاتفاقية المتعلقة بالجريمة الإلكترونية لتحسين وتنسيق التشريعات بشأن القضايا المتصلة بالجريمة السيبرانية.[1475] ومن المهم في هذا السياق إبراز أن الحكم المستند إلى نص المادة 21 من الاتفاقية لا ينطبق فقط في صدد الجرائم المتصلة بالجريمة السيبرانية ولكنه ينطبق على أي جرائم أخرى. وفي صدد عدم اقتصار أهمية استعمال الاتصال الإلكتروني على قضايا الجرائم السيبرانية وحدها، فإن تطبيق هذا الحكم خارج الجرائم السيبرانية يمكن أن يكون مفيداً في إطار التحقيقات. فقد يمكِّن، على سبيل المثال، وكالات إنفاذ القانون من استعمال بيانات الحركة المتولِّدة أثناء تبادل البريد الإلكتروني بين الجناة عند التحضير لجريمة تقليدية. وتمكِّن الفقرة الفرعية 3 من المادة 14 الأطراف من إبداء تحفظات بشأن الحكم وقصر تطبيقه على بعض الجرائم.[1476]

[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/.

[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.

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في قانون الكومنولث النموذجي لعام 2002.[1477]

(1) إذا اقتنع ضابط شرطة أن بيانات الحركة المصاحبة لاتصال محدَّد هي بيانات مطلوبة بصورة معقولة لأغراض تحقيق جنائي يجوز لضابط الشرطة، بموجب إشعار مكتوب موجَّه إلى شخص يسيطر على هذه البيانات، أن يطلب من هذا الشخص:

(أ) جمع أو تسجيل بيانات الحركة المصاحبة لاتصال محدَّد أثناء فترة محدَّدة؛

(ب) تقديم السماح والمساعدة لضابط شرطة محدَّد لجمع أو تسجيل تلك البيانات.

(2) إذا اقتنع قاضي تحقيق استناداً إلى [معلومات مقدَّمة بعد حلف يمين] [إقرار موثَّق] بوجود أُسس معقولة [للاشتباه] بأن بيانات الحركة مطلوبة بصورة معقولة لأغراض تحقيق جنائي، فإن قاضي التحقيق [له] [عليه] أن يصرِّح لضابط شرطة بجمع أو تسجيل بيانات الحركة المصاحبة لاتصال محدَّد أثناء فترة محدَّدة من خلال تطبيق وسائل تقنية.

10.2.6 اعتراض بيانات المحتوى

الاتفاقية المتعلقة بالجريمة الإلكترونية

إلى جانب أن المادة 21 تتناول بيانات المحتوى، فإن هيكلها يشبه هيكل المادة 20. وإمكانية اعتراض عمليات تبادل البيانات قد تكون مهمة في تلك القضايا التي تعرف فيها فعلاً وكالات إنفاذ القانون من هم شركاء الاتصال ولكن ليس لديها معرفة بنوع المعلومات التي يجري تبادلها. وتعطي المادة 21 هذه الوكالات إمكانية تسجيل اتصالات البيانات وتحليل المحتوى.[1478] ويشمل ذلك الملفات التي يتم تنزيلها من مواقع شبكة الويب أو أنظمة تقاسم الملفات والبريد الإلكتروني الذي يرسله أو يستقبله الجاني ومحادثات الدردشة.

المادة 21 – اعتراض محتوى البيانات

1 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، وذلك فيما يتعلق بأنواع الجرائم الجسيمة التي يقررها القانون الوطني لمنح سلطاته المختصة صلاحية:

أ) جمع أو تسجيل، من خلال تطبيق الوسائل الفنية، في إقليم ذلك الطرف؛ و

ب) إجبار مقدِّم الخدمة، في نطاق قدرته الفنية على:

'1' جمع أو تسجيل، من خلال تطبيق الوسائل الفنية، في إقليم ذلك الطرف؛ أو

'2' التعاون مع السلطات المختصة ومساعدتها في جمع أو تسجيل، بشكل فوري،

لمحتوى البيانات المرتبطة باتصالات معيَّنة في إقليم ذلك الطرف التي تم نقلها بواسطة نظام الكمبيوتر

2 في حالة تعذُّر تبني الطرف للإجراءات المشار إليها في الفقرة 1 (أ)، بسبب المبادئ القائمة في نظامه القانوني الوطني، يجوز له بدلاً من ذلك أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان الجمع أو التسجيل الفوريين لمحتوى البيانات المرتبطة باتصالات معيَّنة تم نقلها في إقليمه، من خلال تطبيق الوسائل الفنية في ذلك الإقليم.

3 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإلزام مقدِّم الخدمة بالمحافظة على سرية وقائع تنفيذ أي صلاحيات تنص عليها هذه المادة وأية معلومات تتعلق بها.

4 تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين 14 و15.

[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.

[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.

وبعكس ما يحدث في حالة بيانات الحركة، لا تقدِّم الاتفاقية المتعلقة بالجريمة الإلكترونية تعريفاً لبيانات المحتوى. وكما يتضح من المصطلح المستعمل، تشير ''بيانات المحتوى'' إلى محتوى الاتصال.

وتشمل أمثلة بيانات المحتوى في تحقيقات الجرائم السيبرانية ما يلي:

- موضوع البريد الإلكتروني؛
- المحتوى في شبكة الويب الذي فتحه الشخص المشتبه فيه؛
- محتوى المحادثة على بروتوكول إنترنت.

ويعتبر استعمال تكنولوجيا التشفير من أهم الصعوبات في التحقيقات استناداً إلى المادة 21.[1479] وكما اقترحنا بالتفصيل من قبل، يمكن أن تمكِّن تكنولوجيا التشفير الجناة من حماية المحتوى المتبادل بطريقة تجعل من المستحيل على وكالات إنفاذ القانون النفاذ إلى ذلك المحتوى. وإذا قام الضحية بتشفير المحتوى الذي ينقله، فإن الجناة لا يستطيعون سوى اعتراض اتصال مشفَّر دون إمكانية تحليل المحتوى. وبدون النفاذ إلى المفتاح المستعمل في تشفير الملفات، فإن إمكانية إزالة التشفير قد تستغرق وقتاً طويلاً جداً.[1480]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في قانون الكومنولث النموذجي لعام 2002.[1481]

اعتراض الاتصالات الإلكترونية

18(1) إذا اقتنع [قاضي تحقيق] [قاضي] استناداً إلى [معلومات مقدَّمة بعد حلف يمين] [إقرار موثَّق] بوجود أسباب معقولة [للاشتباه] [للاعتقاد] بأن محتوى اتصالات إلكترونية مطلوب بصورة معقولة لأغراض تحقيق جنائي، فإن قاضي التحقيق [له] [عليه]:

أ) أن يأمر مقدِّم خدمة الإنترنت الذي تتوفر خدمته في [البلد الذي سن القانون] من خلال تطبيق أساليب تقنية وتجميع أو تسجيل، أو تقديم الإذن أو المساعدة للسلطات المختصة في تجميع أو تسجيل، بيانات المحتوى المصاحبة لاتصالات محدَّدة أُرسلت بواسطة نظام حاسوبي؛ أو

ب) الإذن لضابط شرطة بجمع أو تسجيل تلك البيانات بتطبيق وسائل تقنية.

11.2.6 القواعد التنظيمية المتصلة بتكنولوجيا التشفير

كما جاء أعلاه يستطيع الجناة عرقلة تحليل بيانات المحتوى باستعمال تكنولوجيا التشفير. وتتوافر منتجات برمجيات مختلفة تمكِّن المستعملين من توفير حماية فعَّالة للملفات ولعمليات نقل البيانات من تعرضها للنفاذ غير المأذون به.[1482] وإذا استعمل المشتبه فيهم هذه المنتجات و لم تتمكَّن سلطات التحقيق من النفاذ إلى المفتاح المستعمل لتشفير الملفات، فإن التشفير المطلوب قد يتطلب وقتاً طويلاً.[1483]

[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.

ويمثّل استعمال الجناة لتكنولوجيا التشفير تحدياً لوكالات إنفاذ القانون.[1484] وهناك نُهج وطنية ودولية مختلفة[1485] لمعالجة المشكلة.[1486] وبسبب اختلاف التقديرات بشأن التهديد الناجم عن تكنولوجيا التشفير لا يوجد حتى الآن أي نهج دولي مقبول بصورة واسعة في معالجة هذا الموضوع. وأكثر الحلول شيوعاً هي:

- حاجة وكالات إنفاذ القانون في إطار التحقيقات الجنائية إلى الحصول على إذن لفك التشفير إذا استلزم الأمر.[1487] وبدون هذا الإذن، أو بدون امتلاك إمكانية إصدار أمر إبراز يمكن أن تعجز سلطات التحقيق عن جمع الأدلة اللازمة. وبالإضافة إلى ذلك، أو كخيار آخر، يستطيع المحققون الحصول على إذن لاستعمال برمجية مسجِل المفتاح لاعتراض عبارة مرور إلى ملف مشفَّر من أجل حل التشفير.[1488]

- قاعدة تنظيمية تحدِّد أداء برمجية التشفير من خلال تقييد طول المفتاح.[1489] ويمكّن ذلك، حسب درجة التقييد، المحققين من كسر المفتاح في غضون فترة معقولة من الوقت. ويخشى معارضو هذا الحل أن التقييد لن يمكّن المحققين فقط من كسر التشفير ولكنه يمكّن أيضاً الجواسيس الاقتصاديين الذين يحاولون النفاذ إلى المعلومات التجارية المشفَّرة.[1490] وبالإضافة إلى ذلك، فإن هذا التقييد سيؤدي فقط إلى إعاقة الجناة عن استعمال تشفير أقوى في حالة عدم توفُّر أدوات البرمجيات المذكورة. ويتطلب ذلك في البداية وضع معايير دولية لمنع منتجي أداة التشفير القوية من عرض برمجياتهم في البلدان التي لا يوجد فيها تقييدات ملائمة بشأن طول المفتاح. وعلى أي حال يستطيع الجناة بسهولة نسبية صياغة برمجيات تشفير خاصة بهم لا تقيِّد طول المفتاح.

- الإلزام بإنشاء نظام لاستيداع المفاتيح أو وضع إجراء لاستعادة المفتاح في حالة منتجات التشفير القوية.[1491] وتنفيذ هذه القواعد التنفيذية يمكّن المستعملين من الاستمرار في استعمال تكنولوجيا التشفير القوي مع تمكين المحققين من النفاذ إلى البيانات ذات الصلة بإرغام المستعمل على تقديم المفتاح إلى سلطة خاصة تحتفظ بالمفتاح وتقدمه للمحققين في حالة الضرورة.[1492] ويخشى معارضو هذا الحل أن يتمكّن الجناة من النفاذ إلى المفاتيح المقدَّمة ويستطيعون بها فك تشفير معلومات سرية. وبالإضافة إلى ذلك، يستطيع الجناة بسهولة نسبية الالتفاف على هذا التنظيم من خلال صياغة برمجية تشفير خاصة بهم لا تتطلَّب تقديم المفتاح إلى السلطة.

[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.

[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

- وهناك نهج آخر وهو أمر الإبراز.[1493] ويصف هذا المصطلح التزام الإفصاح عن المفتاح المستعمل لتشفير البيانات. وقد نوقش تطبيق هذه الأداة في إطار اجتماع الثمانية في عام 1997 في دنفر.[1494] وطبَّق عدد من البلدان هذا الالتزام.[1495] ومن أمثلة التطبيق الوطني المادة 69 من قانون تكنولوجيا المعلومات لعام 2000 في الهند.[1496] ومن أمثلة هذا الالتزام المادة 49 من لائحة سلطات التحقيق لعام 2000 في المملكة المتحدة[1497]:

المادة 49

(1) تنطبق هذه المادة في حالة أي معلومات محمية

(أ) تقع أو يرجح أن تقع في حيازة أي شخص عن طريق ممارسة سلطة قانونية لضبط وثائق أو ممتلكات أخرى أو الاحتفاظ بها أو تفتيشها أو البحث عنها أو التدخل فيها بشكل آخر؛

(ب) تقع أو يرجَّح أن تقع في حيازة أي شخص بواسطة ممارسة سلطة قانونية لاعتراض مراسلات؛

(ج) تقع أو يرجَّح أن تقع في حيازة أي شخص بواسطة ممارسة سلطة ناشئة عن تصريح صادر بموجب الفقرة (3) من المادة 22 أو بموجب الجزء الثاني، نتيجة توجيه إشعار بموجب المادة 22 (4)؛

(د) تقع أو يرجَّح أن تقع في حيازة أي شخص نتيجة تقديمها أو الإفصاح عنها عملاً بأي واجب قانوني (سواء نشأ أو لم ينشأ نتيجة طلب بالحصول على معلومات)؛

(هـ) تقع أو يرجَّح أن تقع، بأي وسيلة قانونية أخرى لا تنطوي على ممارسة سلطات قانونية، في حيازة أي هيئة للمخابرات أو الشرطة أو الجمارك والمكوس؛

[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.

[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.

(2) إذا اعتقد أي شخص لديه تصريح ملائم بموجب الجدول 2، بناءً على أُسس معقولة –

(أ) أن مفتاح معلومات محمية موجود في حيازة أي شخص،

(ب) أن فرض مطلب الإفصاح في صدد المعلومات المحمية هو '1' ضروري لأسباب تندرج تحت الفقرة الفرعية (3) أو '2' ضروري لأغراض الحصول على ممارسة فعَّالة أو أداء صحيح من جانب السلطة العامة لسلطاتها القانونية أو واجبها القانوني،

(ج) أن فرض هذا المطلب متناسب مع ما يسعى هذا الفرض إلى تحقيقه،

(د) أنه ليس من العملي بدرجة معقولة أن يحصل الشخص الذي لديه تصريح ملائم على حيازة المعلومات المحمية بشكل مفهوم دون إصدار إشعار بموجب هذه المادة، يجوز للشخص الذي لديه هذا التصريح أن يفرض، بموجب إشعار إلى الشخص الذي يعتقد أن المفتاح يقع في حيازته، مطلب الإفصاح فيما يتعلق بالمعلومات المحمية.

(3) يكون مطلب الإفصاح في صدد المعلومات المحمية ضرورياً للأسباب المندرجة في هذه الفقرة الفرعية وكان من الضروري

(أ) لصالح الأمن القومي؛

(ب) لأغراض منع أو اكتشاف جريمة؛

(ج) لصالح الرفاه الاقتصادي للملكة المتحدة.

(4) الإشعار الموجَّه بموجب هذه المادة لفرض مطلب الإفصاح بشأن أي معلومات محمية

(أ) يجب أن يصدر كتابة أو (إذا لم يكن كتابة) يجب أن يصدر بطريقة تنشئ سجلاً عن إصداره؛

(ب) يجب أن يصف المعلومات المحمية التي يتعلق بها الإشعار؛

(ج) يجب أن ينص على الموضوعات المندرجة في الفقرة الفرعية 2 (ب) ('1') أو ('2') التي صدر الإشعار استناداً إليها؛

(د) يجب أن ينص على وظيفة أو رتبة أو موقع الشخص الذي أصدر الإشعار؛

(هـ) يجب أن ينص على وظيفة أو رتبة أو موقع الشخص الذي قام، لأغراض الجدول 2، بمنح التصريح لإصدار الإشعار أو (إذا كان الشخص الذي أصدر الإشعار مؤهلاً لإصداره بدون تصريح من شخص آخر) يجب أن يحدِّد الظروف التي نشأ فيها هذا الاستحقاق؛

(و) يجب أن ينص على الوقت الذي يتعيَّن في غضونه الامتثال للإشعار؛

(ز) يجب أن يحدِّد الإفصاح المطلوب بموجب الإشعار وشكل وطريقة هذا الإفصاح؛ ويجب أن يسمح الوقت المنصوص عليه لأغراض الفترة (و) بفترة للامتثال تكون معقولة في جميع الظروف.

وللتأكد من إرغام الشخص على الإفصاح عن المفتاح واتباع الأمر وتقديم المفتاح فعلاً يتضمن قانون سلطات التحقيق لعام 2000 في المملكة المتحدة حكماً يجرِّم عدم الامتثال لهذا الأمر.

المادة 53

(1) أي شخص وجِّه إليه إشعار بموجب المادة 49 يكون مذنباً بجريمة إذا أخفق عن علم في القيام، وفقاً للإشعار، بالإفصاح المطلوب بمقتضى إصدار الإشعار.

(2) في الدعوى المقامة ضد أي شخص عن جريمة ارتُكبت بموجب هذه المادة، إذا ثبت أن هذا الشخص يملك مفتاحاً لأي معلومات محمية في أي وقت قبل إصدار الإشعار بموجب المادة 49، يعتبر هذا الشخص لأغراض هذه الدعوى مستمراً في حيازة ذلك المفتاح في كل وقت لاحق، ما لم يثبت أن المفتاح لم يكون في حيازته بعد إصدار الإشعار وقبل مطالبته بالإفصاح عنه.

(3) لأغراض هذه المادة يعتبر الشخص قد أثبت عدم حيازته للمفتاح إلى معلومات محمية في وقت بعينه إذا:

(أ) تبيَّن وجود أدلة كافية لإثارة شكوك في هذا الصدد؛

(ب) لم يتم إثبات العكس فيما لا يدع مجالاً لشك معقول.

(4) في الدعوى ضد أي شخص بسبب جريمة بموجب هذه المادة يدافع الشخص عن نفسه بإظهار

(أ) أنه لم يكن من الممكن عملياً له بصورة معقولة أن يقوم بالإفصاح المطلوب موجب الإشعار الصادر بمقتضى الفقرة 49 قبل الوقت الذي كان مطلوباً فيه الإفصاح وفقاً للإشعار؛ ولكنه

(ب) قام بهذا الإفصاح بأسرع ما يمكن بمجرَّد أن أصبح من الممكن عملياً وبصورة معقولة أن يقوم بذلك.

(5) يعاقب الشخص المذنب بجريمة بموجب هذه المادة –

(أ) بعد الإدانة بموجب الاتهام، بالسجن لمدة لا تزيد عن سنتين أو بغرامة، أو كلاهما؛

(ب) بعد إدانة عاجلة، بالسجن لمدة لا تزيد عن ستة أشهر أو غرامة لا تزيد عن الحد الأقصى القانوني، أو كلاهما.

وترغم اللائحة التنفيذية لقانون سلطات التحقيق لعام 2006 الشخص المشتبه في ارتكابه جريمة بأن يدعم أعمال وكالات إنفاذ القانون. وتوجد ثلاثة انشغالات كبرى تتصل بهذه اللائحة:

- انشغال عام يتصل بأن الالتزام يؤدي إلى احتمال التنازع مع الحقوق الأساسية للمتهم ضد تجريم الذات.[1498] إذ يتعيَّن على المشتبه فيه أن يدعم بنشاط عملية التحقيق بدل أن يترك التحقيق للسلطات المختصة. والحماية القوية من تجريم الذات في كثير من البلدان تثير في صدد ذلك سؤالاً عن مدى إمكانية تحوُّل هذه القاعدة التنظيمية إلى حل نموذجي لمعالجة التحدي المتصل بتكنولوجيا التشفير.

- ويتصل انشغال آخر بأن التخلي عن المفتاح يمكن أن يؤدي إلى تحقيق جنائي. فرغم أن التجريم يتطلب أن يرفض الجاني عن علم الإفصاح عن المفتاح، فإن ضياع المفتاح يمكن أن يورط أشخاصاً يستعملون مفتاح التشفير في إجراءات جنائية غير مرغوبة. ولكن الفقرة الفرعية 2 من المادة 53 على وجه الخصوص تنطوي على احتمال التداخل في عبء الإثبات.[1499]

- وهناك حلول تقنية تمكِّن الجناة من الالتفاف على الالتزام بالإفصاح عن المفتاح المستعمل في تشفير البيانات. ومن أمثلة التفاف الجاني حول الالتزام استعمال برمجية التشفير على أساس مبدأ ''قدرة الإنكار المقبولة''.[1500]

[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.

12.2.6 برمجية التحليل القضائي (الطب الشرعي) عن بُعد

كما جاء أعلاه يتطلب البحث عن الأدلة على حاسوب المشتبه فيه نفاذاً مادياً إلى العتاد المعني (النظام الحاسوبي ووسيط التخزين الخارجي). وهذا الإجراء عموماً تصحبه ضرورة النفاذ إلى شقة المشتبه فيه أو بيته أو مكتبه. وفي هذه الحالة يعرف المشتبه فيه بوجود تحقيق في نفس اللحظة التي يبدأ فيها المحققون أعمال البحث.[1501] ويمكن أن تؤدي هذه المعلومات إلى تغيُّر في السلوك.[1502] فإذا هاجم الجاني مثلاً بعض الأنظمة الحاسوبية لاختبار قدراته من أجل المشاركة في إعداد سلسلة أكبر كثيراً من الهجمات مشتركاً مع جناة آخرين في تاريخ مقبل، فإن إجراء البحث يمكن أن يعرقِّل تعرُّف المحققين على الأشخاص الآخرين المشتبه فيهم نظراً لأنه من المرجح جداً أن الجاني سيتوقف عن الاتصال بهم.

ولتجنُّب اكتشاف التحقيقات الجارية تطالب وكالات إنفاذ القانون بوجود أداة تسمح لهم بالنفاذ إلى البيانات الحاسوبية المخزَّنة على حاسوب الشخص المشتبه فيه، ويمكن استعمالها بشكل سري، مثل مراقبة الهواتف لرصد المكالمات الهاتفية.[1503] وتمكِّن مثل هذه الأداة وكالات إنفاذ القانون من النفاذ عن بُعد إلى حاسوب المشتبه فيه وتفتيشه للحصول على المعلومات. وفي الوقت الحاضر تجري مناقشة حادة لما إن كانت هذه الأدوات ضرورية أو غير ضرورية.[1504] وبالفعل أشارت تقارير في عام 2001 إلى أن مكتب التحقيقات الفيدرالية في الولايات المتحدة يقوم بوضع أداة لتسجيل بيانات المفتاح وتحقيقات متصلة بالإنترنت تسمى "المصباح السحري".[1505] وفي عام 2007، نُشرت تقارير تقول بأن وكالات إنفاذ القانون في الولايات المتحدة تستعمل برمجية لتعقُّب المشتبه فيهم الذين يستعملون أدوات الاتصال مجهول الهوية.[1506] وكانت التقارير تشير إلى أمر تفتيش حيث كان استعمال أداة تسمى CIPAV (جهاز التحقق من الحاسوب وعنوان بروتوكول إنترنت)[1507] مطلوباً فيه.[1508] وبعد أن قرَّرت المحكمة الاتحادية في ألمانيا أن أحكام قانون الإجراءات الجنائية الموجودة لا تسمح للمحققين باستعمال برمجية التحليل القضائي (الطب

[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.*

[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] Computer and Internet Protocol Address Verifier.

[1508] 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.

الشرعي) عن بُعد للقيام سراً بتفتيش حاسوب المشتبه فيه بدأت مناقشة بشأن ضرورة تعديل القوانين القائمة في هذا المجال.[1509] وفي سياق المناقشة نُشرت معلومات تقول بأن سلطات التحقيق قد استعملت بصورة غير قانونية برمجية التحليل القضائي (الطب الشرعي) عن بُعد في إثنين من التحقيقات.[1510]

ونوقشت مختلف مفاهيم ''برمجية التحليل القضائي (الطب الشرعي) عن بُعد'' وخاصة وظائفها المحتملة.[1511] ويمكن أن تؤدي هذه البرمجية الوظائف التالية من منظور نظري:

- وظيفة التفتيش – تمكّن هذه الوظيفة وكالات إنفاذ القانون من البحث عن المحتوى غير القانوني وجمع المعلومات عن الملفات المخزونة في الحاسوب.[1512]
- التسجيل – يستطيع المحققون تسجيل بيانات يتم تجهيزها على النظام الحاسوبي للشخص المشتبه فيه بدون تخزينها بصورة دائمة. وإذا قام الشخص المشتبه فيه مثلاً باستعمال خدمات الصوت على بروتوكول إنترنت للاتصال بالأشخاص الآخرين المشتبه فيهم فسوف يتم عموماً تخزين محتوى المحادثة.[1513] ويمكن أن تسجل برمجية التحليل القضائي (الطب الشرعي) عن بُعد البيانات المجهَّزة للاحتفاظ بها كي يستعملها المحققون.
- مسجِّل المفتاح – إذا كانت برمجية التحليل القضائي (الطب الشرعي) عن بُعد تتضمَّن وحدة لتسجيل ضربات المفاتيح، فإن هذه الوحدة يمكن استعمالها لتسجيل كلمات المرور التي يستعملها الشخص المشتبه في تشفير الملفات.[1514]
- تحديد الهوية – يمكن أن تمكّن هذه الوظيفة المحققين من إثبات مشاركة المشتبه فيه جريمة جنائية حتى لو استعمل خدمات اتصال مجهولة الهوية تعرقِّل المحققين من أجل تعيين هوية الجاني بتعقُّب عنوان بروتوكول إنترنت المستعمل.[1515]
- تشغيل الوحدات المحيطة – يمكن استعمال البرمجية البعيدة لتشغيل آلة تصوير للإنترنت (ويبكام) أو ميكروفون لأغراض مراقبة الغرفة.[1516]

ورغم أن البرامج المحتملة لهذه البرمجية تبدو مفيدة جداً للمحققين، فمن المهم أن يشار إلى وجود عدد من الصعوبات القانونية والتقنية المتصلة باستعمال هذه البرمجية. ومن وجهة النظر التقنية يتعيَّن وضع الجوانب التالية في الاعتبار:

- الصعوبات في صدد عملية التركيب – يتعيَّن تركيب البرمجية على النظام الحاسوبي للشخص المشتبه فيه. وانتشار البرمجيات الخبيثة يثبت إمكانية تركيب برمجية على حاسوب مستعمل للإنترنت بدون إذن منه. ولكن الفرق الرئيسي بين الفيروس وبرمجية التحليل القضائي (الطب الشرعي) عن بُعد هو أن هذه البرمجية يتعيَّن تركيبها على نظام حاسوبي بعينه (حاسوب الشخص المشتبه فيه) في حين أن الفيروس الحاسوبي يهدف إلى تلويث أكبر عدد ممكن من الحواسيب بدون الحاجة إلى التركيز على نظام حاسوبي محدَّد. وهناك عدد من التقنيات الخاصة بطريقة إرسال برمجية إلى حاسوب الشخص المشتبه فيه. وعلى سبيل المثال: التركيب بعد النفاذ المادي إلى النظام الحاسوبي، ووضع البرمجية على موقع في شبكة الويب لتنزيله؛ والنفاذ على الخط إلى النظام الحاسوبي بالالتفاف على تدابير الأمن؛ وإخفاء البرمجية في تيار البيانات الذي يتولَّد أثناء نشاط الإنترنت، وهذه مجرَّد بضعة

[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.*

طرق.[1517] وبصدد تدابير الحماية مثل التفتيش عن الفيروسات وحوائط النيران التي تجهَّز بها معظم الحواسيب، فإن جميع أساليب التركيب عن بُعد تقترن بصعوبات تواجه المحققين.[1518]

- مزايا النفاذ المادي – يتطلب عدد من عمليات التحليل التي يجري القيام بها (مثل التفتيش المادي في وسيط تجهيز البيانات) نفاذاً إلى العتاد. وبالإضافة إلى ذلك، فإن برمجية التحليل القضائي (الطب الشرعي) عن بُعد ستمكِّن المحققين فقط من تحليل أنظمة حاسوبية موصولة بالإنترنت.[1519] ومن العسير، بالإضافة إلى ذلك، الحفاظ على سلامة النظام الحاسوبي للشخص المشتبه فيه.[1520] وفي صدد هذه الجوانب لن تكون برمجية التحليل القضائي (الطب الشرعي) عن بُعد قادرة عموماً على أن تحل محل الفحص المادي للنظام الحاسوبي للشخص المشتبه فيه.

وبالإضافة إلى ذلك، يتعيَّن وضع عدد من الجوانب القانونية في الاعتبار قبل تنفيذ حكم يمكِّن المحققين من تركيب برمجية للتحليل القضائي (الطب الشرعي) عن بُعد. والضمانات الموضوعة في قوانين الإجراءات الجنائية وكذلك في الدساتير في كثير من البلدان تقيِّد الوظائف المحتملة لهذه البرمجية. وبالإضافة إلى الجوانب الوطنية، فإن تركيب هذه البرمجية يمكن أن يمثِّل انتهاكاً لمبدأ السيادة الوطنية.[1521] وفي حالة تركيب البرمجية على حاسوب صغير أُخذ خارج البلد بعد عملية التركيب، فإن هذه البرمجية قد تمكِّن المحققين من أداء تحقيقات جنائية في أراضي بلد أجنبي بدون الحصول على التصريح اللازم من السلطات المسؤولة.

13.2.6 اشتراط الإذن

يستطيع أن يتخذ الجناة تدابير لتعقيد التحقيقات. فبالإضافة إلى استعمال برمجيات تمكِّن من الاتصال مجهول الهوية[1522] يمكن أن تتعقَّد عملية تحديد الهوية إذا استعمل المشتبه فيه أجهزة عمومية طرفية للإنترنت أو شبكات لا سلكية مفتوحة. وهناك تقييدات تحد من إنتاج برمجيات تمكِّن المستعمل من إخفاء شخصيته وتحد من توفير محطات طرفية عمومية للنفاذ إلى الإنترنت بدون تحديد الهوية، وهذه التقييدات يمكن أن تتيح لوكالات إنفاذ القانون إجراء التحقيقات بكفاءة أكبر. ومن أمثلة نُهج تقييد استعمال المحطات الطرفية العمومية في ارتكاب مخالفات جنائية المادة 7[1523] من المرسوم الإيطالي رقم 144،[1524] الذي تم تحويله في عام 2005 ليصبح قانوناً (القانون رقم 155/2005).[1525] ويفرض هذا الحكم على أي شخص يعتزم تقديم نفاذ عمومي إلى الإنترنت (مثل مقاهي الإنترنت أو الجامعات[1526] أن يطلب إذناً بذلك. وبالإضافة إلى ذلك، فإن الشخص المعني مُرغم على أن يطالب عملائه بتقديم ما يثبت الهوية قبل إعطائهم إمكانية النفاذ لاستعمال الخدمة. وفي صدد عدم تغطية هذا الالتزام عموماً لشخص خاص يقوم بإنشاء نقطة نفاذ لا سلكية، فإن الالتفاف على رصد ذلك قد يكون سهلاً إلى حد كبير إذا استعمل الجناة شبكات خاصة غير محمية لإخفاء هويتهم.[1527]

ومن المشكوك فيه أن يكون مدى تحسُّن التحقيقات مبرراً لتقييد النفاذ إلى الإنترنت وإلى خدمات الاتصال مجهول الهوية. فمن المعترف به اليوم أن حُرية النفاذ إلى الإنترنت تشكِّل جانباً هاماً من الحق في حُرية النفاذ إلى المعلومات، وهو حق يحميه الدستور في عدد من البلدان. ومن المرجح أن اقتضاء تحديد الهوية سيؤثر على استعمال الإنترنت نظراً لأن مستعملي الإنترنت سيخشون في هذه الحالة أن يجري رصد استعمالهم للإنترنت.

[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.*

[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.*

وحتى إذا كان المستعملون يعرفون أن أنشطتهم قانونية فسوف يظل ذلك عاملاً مؤثراً على تفاعلهم واستعمالهم.[1528] وفي الوقت نفسه، فإن الجناة الذين يربدون منع معرفة هويتهم يستطيعون بسهولة الالتفاف على إجراء تحديد الهوية. فهم يستطيعون مثلاً استعمال بطاقات هاتفية مدفوعة سلفاً يتم شراؤها في الخارج حيث لا يكون تحديد الهوية مطلوباً للنفاذ إلى الإنترنت.

3.6 التعاون الدولي

1.3.6 مقدمة

ينطوي عدد متزايد من الجرائم السيبرانية على بُعد دولي.[1529] وكما أُشير أعلاه يتمثَّل أحد أسباب هذه الظاهرة في عدم وجود حاجة كبيرة إلى تواجد الجناة بأنفسهم في مكان تقديم الخدمة.[1530] ونتيجة لذلك، لا يحتاج المجرمون عموماً إلى التواجد في المكان الذي توجد فيه الضحية. وعموماً تقترن تحقيقات الجريمة السيبرانية بضرورة التعاون الدولي.[1531] ومن المطالب الرئيسية للمحققين في التحقيقات عبر الوطنية وجود تفاعل فوري من جانب نظرائهم في البلد الذي يقع فيه مكان الجاني.[1532] وفي هذه المسألة على وجه الخصوص، فإن الصكوك التقليدية للمساعدة المتبادلة لا تفي، في معظم الحالات، بالمقتضيات المتعلقة بسرعة إجراء التحقيقات في الإنترنت.[1533] وتعالج الاتفاقية المتعلقة بالجريمة الإلكترونية الأهمية المتزايدة للتعاون الدولي في المواد 23 –35. ويمكن الاطلاع على نهج آخر في مشروع اتفاقية ستانفورد.[1534]

2.3.6 المبادئ العامة للتعاون الدولي

تعرِّف المادة 23 من الاتفاقية المتعلقة بالجريمة الإلكترونية المبادئ العامة في صدد التعاون الدولي بين الأعضاء في تحقيقات الجرائم السيبرانية.

المادة 23 – مبادئ عامة تتعلَّق بالتعاون الدولي

يتعاون الأطراف مع بعضهم البعض، وفقًا لنصوص هذا الباب، ومن خلال تطبيق الاتفاقية الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية، والترتيبات المتفق عليها بمقتضى التشريعات الموحَّدة والمتبادلة بالمثل، والقوانين الوطنية، لأقصى درجة ممكنة لأغراض إجراء التحقيقات التي تتعلَّق بجرائم نُظم وبيانات الكمبيوتر، أو من أجل تجميع أدلة الجريمة الجنائية في شكل إلكتروني.

ومن المفترض في المقام الأول أن يوفِّر الأعضاء التعاون في التحقيقات الدولية إلى أقصى مدى ممكن. ويعبِّر هذا الالتزام عن أهمية التعاون الدولي في تحقيقات الجرائم السيبرانية. وبالإضافة إلى ذلك، تلاحظ المادة 23 أن المبادئ العامة لا تنطبق فقط في حالة تحقيقات الجرائم السيبرانية بل تنطبق في أي تحقيق يتعيَّن في إطاره جمع أدلة في شكل إلكتروني. ويغطي ذلك تحقيقات الجرائم السيبرانية وكذلك التحقيقات في القضايا التقليدية. فإذا استعمل المتهم خدمة بريد إلكتروني في الخارج في قضية قتل، فإن المادة 23 ستكون منطبقة بشأن التحقيقات اللازمة في صدد البيانات المخزَّنة لدي مقدِّم الخدمة المضيف.[1535] ويلاحظ المبدأ الثالث أن الأحكام التي تتناول التعاون الدولي ليست بديلاً عن أحكام الاتفاقات الدولية بشأن المساعدة القانونية المتبادلة والتسليم أو الأحكام ذات الصلة في القوانين المحلية المتعلقة بالتعاون الدولي. وأكد واضعو الاتفاقية على أن المساعدة

[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.
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;

[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.

[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).

المتبادلة ينبغي أن تجري عموماً من خلال تطبيق المعاهدات ذات الصلة والترتيبات المماثلة المتعلقة بالمساعدة المتبادلة. ونتيجة لذلك، فإن الاتفاقية لا تقصد إنشاء نظام عام منفصل يتعلّق بالمساعدة المتبادلة. ولذلك لا يطالَب كل طرف بوضع أساس قانوني لتمكين إجراء التعاون الدولي على النحو المعرَّف في الاتفاقية إلاّ في الحالات التي لا تكون فيها المعاهدات والقوانين والترتيبات القائمة تتضمن فعلاً مثل هذه الأحكام.[1536]

3.3.6 تسليم المجرمين

يظل تسليم المواطنين جانباً من أصعب جوانب التعاون الدولي.[1537] وطلبات التسليم تؤدي في كثير من الأحيان إلى التنازع بين ضرورة حماية المواطن والحاجة إلى دعم تحقيق يجري في بلد في الخارج. وتحدِّد المادة 24 مبادئ التسليم. وبعكس المادة 23، فإن الحكم يقتصر على الجرائم المذكورة في الاتفاقية ولا ينطبق في الحالات البسيطة (الحرمان من الحرية لفترة لا تزيد عن سنة واحدة على الأقل.[1538] ولتجنُّب النزاعات التي يمكن أن تحدث بشأن قدرة الأطراف على إبداء تحفظات، تستند المادة 24 إلى مبدأ ازدواج الجُرم.[1539]

المادة 24 – تسليم المجرمين

1 أ) تُطبَّق هذه المادة على تسليم المجرمين فيما بين الأطراف بالنسبة للجرائم المنصوص عليها في المواد من 2 إلى 11 من هذه الاتفاقية بشرط أن تكون هذه الجرائم يعاقب عليها بموجب قوانين كلا الطرفين المعنيين، بعقوبة مقيِّدة للحُرية لمدة سنة على الأقل أو بعقوبة أشد.

ب) في حالة إذا ما كانت هناك عقوبة بحد أدنى مختلف واجبة التطبيق بموجب إجراء متفق عليه بمقتضى التشريعات الموحَّدة والمتبادلة بالمثل أو بموجب اتفاقية تسليم، بما في ذلك الاتفاقية الأوروبية بشأن تسليم المجرمين (ETS 24)، واجبة التطبيق بين طرفين أو أكثر، تُطبَّق العقوبة الدنيا المنصوص عليها بموجب مثل هذا الإجراء أو الاتفاقية.

2 تُعتبر الجرائم الجنائية الواردة في الفقرة 1 من هذه المادة مدرجة كجرائم يجب فيها التسليم في أي اتفاقية بشأن تسليم المجرمين قائمة بين الأطراف، ويتعهَّد الأطراف بإدراج هذه الجرائم على أنها جرائم يتم فيها تسليم المجرمين في أي اتفاقية بشأن تسليم المجرمين يتم إبرامها فيما بينهم.

3 في حالة تلقي أحد الأطراف، والذي يجعل تسليم المجرمين مشروطاً بوجود اتفاقية، طلباً للتسليم من طرف آخر لا تربطه به اتفاقية لتسليم المجرمين، يجوز لذلك الطرف اعتبار هذه الاتفاقية الأساس القانوني لعملية التسليم فيما يتعلق بأية جريمة مشار إليها في الفقرة 1 من هذه المادة.

4 يعتمد الأطراف الذين لا يجعلون تسليم المجرمين مشروطاً بوجود اتفاقية، الجرائم الجنائية المشار إليها في الفقرة 1 من هذه المادة على أنها جرائم يمكن فيها تسليم المجرمين فيما بينهم.

5 يخضع تسليم المجرمين للشروط التي ينص عليها قانون الدولة المطلوب منها التسليم، أو اتفاقيات تسليم المجرمين واجبة التطبيق، بما في ذلك الأسباب التي يجوز فيها للطرف المطلوب منه التسليم رفض التسليم.

6 في حالة رفض عملية تسليم المجرمين في إحدى الجرائم المشار إليها في الفقرة 1 من هذه المادة، على سند وحيد من جنسية الشخص المطلوب فقط، أو لو أن الطرف المطلوب منه التسليم يرى أنه له اختصاص قضائي يشمل هذه الجريمة، يقوم الطرف المطلوب منه التسليم بإحالة القضية، بناء على طلب الطرف الطالب إلى سلطاته المختصة بغرض المحاكمة ثم يقوم بإبلاغ النتيجة النهائية للطرف الطالب، في الوقت المناسب. تتخذ هذه السلطات قرارها وتُجري التحقيق والإجراءات الخاصة بها، بنفس الطريقة كما هو الحال بالنسبة لأية جريمة أخرى ذات طابع مشابه لها بموجب قانون ذلك الطرف.

7 أ) يقوم كل طرف، وقت التوقيع أو عند إيداع وثيقة التصديق، أو القبول، أو الموافقة، أو الانضمام، بإخطار السكرتير العام لمجلس أوروبا باسم وعنوان كل سلطة مسؤولة عن إصدار أو تلقي طلبات التسليم، أو أوامر الضبط التحفظي في حالة عدم وجود اتفاقية.

ب) يقوم السكرتير العام لمجلس أوروبا بإنشاء وتحديث سجل خاص بالسلطات المسؤولة التي يعيِّنها الأطراف، ويلتزم كل طرف بالتأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت.

[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.

4.3.6 المبادئ العامة للمساعدة المتبادلة

فيما يتعلق بالمساعدة المتبادلة تستكمل المادة 25 المبادئ المعروضة في المادة 23. والفقرة 3 هي واحدة من أهم القواعد التنظيمية في المادة 25 وهي تبرز أهمية الاتصال السريع في تحقيقات الجرائم السيبرانية.[1540] وكما أشير من قبل، يفشل عدد من تحقيقات الجرائم السيبرانية على الصعيد الوطني لأنها تستغرق وقتاً طويلاً أكثر من اللازم وهكذا يتم حذف البيانات الهامة قبل اتخاذ التدابير الإجرائية للحفاظ عليها.[1541] وعموماً تستغرق التحقيقات التي تتطلَّب مساعدة قانونية متبادلة وقتاً أطول من ذلك بسبب الاشتراطات الرسمية التي تستغرق كثيراً من الوقت في الاتصال بين وكالات إنفاذ القانون. وتعالج الاتفاقية هذه المشكلة بإبراز أهمية التمكين من استعمال وسائل سريعة للاتصال.[1542]

المادة 25 – مبادئ عامة تتعلَّق بالمساعدة المتبادلة

1 يقوم الأطراف بتقديم المساعدات المتبادلة لبعضهم البعض إلى أقصى حد ممكن وذلك لأغراض التحقيق أو الإجراءات المتعلقة بالجرائم ذات العلاقة بُنظم وبيانات الكمبيوتر، أو جمع أدلة الجريمة في شكل إلكتروني.

2 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لتنفيذ الالتزامات الواردة في المواد من 27 إلى 35

3 يجوز لكل طرف في الظروف العاجلة تقديم الطالبات الخاصة بتبادل المساعدات أو الاتصالات المتعلقة بذلك عن طريق وسائل الاتصال العاجلة، بما في ذلك أجهزة الفاكس أو البريد الإلكتروني، بالحد الذي توفر به مثل هذه الوسائل مستويات ملائمة للأمن والتوثيق (بما في ذلك استخدام التشفير عند الضرورة) مع اتباعها بتأكيد رسمي عندما يُطلب ذلك من الطرف المطلوب منه تقديم المساعدة. يقبل الطرف المطلوب منه تقديم المساعدة ويستجيب للطلب بأية وسيلة من وسائل الاتصال العاجلة.

4 فيما ما عدا ما هو منصوص عليه في مواد هذا القسم، يخضع تبادل المساعدة للشروط التي ينص عليها قانون الطرف المطلوب منه المساعدة، أو اتفاقيات تبادل المساعدة واجبة التطبيق بما في ذلك الأسس التي يجوز بسببها للطرف المطلوب منه المساعدة أن يرفض التعاون. ولا يجوز للطرف المطلوب منه المساعدة ممارسة الحق في رفض المساعدة المتبادلة فيما يتعلق بالجرائم المشار إليها في المواد من 2 إلى 11 على أساس أن الطلب يتعلق بجريمة يعتبرها جريمة مالية.

5 متى كان مسموحاً للطرف المطلوب منه المساعدة، طبقاً لنصوص هذا القسم، بتقديم المساعدة المتبادلة في حالة وجود جريمة مزدوجة، فإن هذا الشرط يعتبر مستوفياً، بغض النظر عما إذا كانت قوانينه تدرج الجريمة داخل التصنيف ذاته للجريمة أو تصبغ على الجريمة نفس المسمى القانوني للطرف الطالب، طالما أن السلوك الذي يحدِّد الجريمة المطلوب تقديم المساعدة بشأنها يشكِّل جريمة بموجب قوانينه.

وفي إطار تحقيقات الجرائم السيبرانية التي تجري على صعيد وطني قد يتم اكتشاف روابط بجرائم تتصل ببلد آخر. فإذا كانت سلطات إنفاذ القانون تحقِّق مثلاً في قضية من قضايا استخدام الأطفال في المواد الفاضحة، فإنها قد تجد معلومات عن أشخاص يشتهون الأطفال من بلدان أخرى شاركوا في تبادل المواد الفاضحة للأطفال.[1543] وتعرض المادة 26 قواعد تنظيمية تتسم بأنها ضرورية لوكالات إنفاذ القانون من أجل تبليغ وكالات إنفاذ القانون الأجنبية بدون المساس بالتحقيقات التي تقوم هي بها.[1544]

المادة 26 – المعلومات التلقائية

1 يجوز لأي طرف، في حدود قانونه الوطني، ودون طلب مسبق أن يرسل إلى طرف آخر معلومات يتم الحصول عليها في إطار تحقيقات ذلك الطرف في حالة إذا ما رأي أن الإفصاح عن هذه المعلومات قد يساعد الطرف المتلقي لهذه المعلومات في البدء فيه أو القيام بالتحقيق أو الإجراءات التي تتعلق بجرائم تنص عليها هذه الاتفاقية، أو أن ذلك قد يؤدي إلى تقديم طلب للتعاون من جانب ذلك الطرف بموجب هذا القسم.

[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.

[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.

2 يجوز للطرف الذي يقدِّم هذه المعلومات قبل تقديمها أن يطلب المحافظة على سرية هذه المعلومات أو استخدامها وفقاً لشروط معيَّنة فقط. وفي حالة عدم استطاعة الطرف المتلقي لهذه المعلومات الاستجابة لمثل هذا الطلب، عليه أن يخطر الطرف مقدِّم المعلومات، والذي يقرِّر عندئذ إذا ما كان ينبغي مع ذلك تقديم هذه المعلومات من عدمه. وفي حالة قبول هذه المعلومات من جانب الطرف المتلقي وفقاً لشروط، فإنه يكون ملزماً بها.

وتتصل واحدة من أهم القواعد في المادة 26 بسرية المعلومات. وفيما يتعلق بما هو معروف من أن عدداً من التحقيقات لا يمكن أن تجري بنجاح إلاّ إذا كان الجاني لا يعرف بسير التحقيقات، فإن المادة 26 تمكِّن الطرف مقدِّم المعلومات أن يطلب الاحتفاظ بسرية المعلومات المنقولة. وإذا لم يكن ممكناً ضمان السرية، فإن الطرف مقدِّم المعلومات يستطيع أن يرفض تقديم المعلومات.

5.3.6 الإجراءات المتصلة بطلبات المساعدة المتبادلة في حالة عدم وجود اتفاقات دولية منطبقة

تستند المادة 27، مثلها مثل المادة 25، إلى فكرة القيام بالمساعدة القانونية المتبادلة من خلال تطبيق المعاهدات ذات الصلة والترتيبات المشابهة بدلاً من الإشارة إلى الاتفاقية وحدها. وقرَّر واضعو الاتفاقية عدم إقامة نظام منفصل للمساعدة القانونية المتبادلة الإلزامية في إطار الاتفاقية.[1545] وفي حالة وجود صكوك أخرى بالفعل، فإن المادتين 27 و28 تصبحان بدون أهمية في إطار أي طلب ملموس. ولكن في الحالات التي لا تنطبق فيها أية قواعد أخرى، فإن المادتين 27 و28 تتيحان آليات يمكن استعمالها لتنفيذ طلبات المساعدة القانونية المتبادلة.

وتشمل أهم الجوانب التي تنظمها المادة 27 ما يلي:

- الالتزام بإقامة نقطة اتصال مسماة لطلبات المساعدة القانونية المتبادلة؛[1546]
- اقتضاء الاتصال المباشر بين نقاط الاتصال لتجنُّب الدخول في إجراءات تستغرق وقتاً طويلاً؛[1547]
- قيام الأمين العام لمجلس أوروبا بإنشاء قاعدة بيانات لجميع نقاط الاتصال.

وبالإضافة إلى ذلك، تحدِّد المادة 27 قيوداً تتعلَّق بطلبات المساعدة. فأطراف الاتفاقية يستطيعون بصورة خاصة رفض التعاون:

- بشأن القضايا السياسية؛ و/أو
- إذا كانت تعتبر أن التعاون سيمس بسيادتها أو أمنها أو نظامها العام أو مصالحها الجوهرية الأخرى.

ورأى واضعو الاتفاقية أن الحاجة تقوم إلى تمكين الأطراف من رفض التعاون في بعض الحالات، من ناحية، ولكنهم أشاروا، من ناحية أخرى، إلى أن الأطراف ينبغي أن تمارس رفض التعاون بضبط نفس لتجنُّب أي نزاع مع المبادئ المستقرة من قبل.[1548] ولذلك، فمن المهم بصفة خاصة تعريف مصطلح "المصالح الجوهرية الأخرى" تعريفاً ضيقاً. ويشير التقرير التفسيري للاتفاقية المتعلقة بالجريمة الإلكترونية إلى أن ذلك قد يكون هو واقع الحال إذا كان من الممكن أن يؤدي التعاون إلى صعوبات أساسية لدي الطرف المطلوب منه التعاون.[1549] ومن منظور واضعي الاتفاقية، فإن الانشغالات المتعلقة بعدم كفاية قوانين حماية البيانات لا تعتبر مصالح جوهرية.[1550]

6.3.6 المساعدة المتبادلة فيما يتعلق بالتدابير المؤقتة

تتضح في المواد 28-33 الأدوات الإجرائية الواردة في الاتفاقية المتعلقة بالجريمة الإلكترونية.[1551] وتتضمَّن هذه الاتفاقية عدداً من الأدوات الإجرائية المصمَّمة لتحسين التحقيقات في الدول الأعضاء.[1552] وفيما يتعلق بمبدأ السيادة الوطنية،[1553] يمكن استعمال هذه الأدوات في التحقيقات على

[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.

الصعيد الوطني فقط.[1554] وإذا أدرك المحققون أن هناك حاجة إلى جمع الأدلة من خارج أراضي بلدهم، فإنه يتعيَّن عليهم طلب مساعدة قانونية متبادلة. وبالإضافة إلى المادة 18 يوجد لكل أداة بموجب المواد من 16 إلى 21 حكم مناظر في المواد من 28 إلى 33 يمكِّن وكالات إنفاذ القانون من تطبيق الأدوات الإجرائية بناءً على طلب وكالة أجنبية لإنفاذ القانون.

الأداة الإجرائية	الحكم المناظر في أحكام المساعدة القانونية المتبادلة
المادة 16 – سرعة التحفُّظ على بيانات الكمبيوتر المخزونة[1555]	المادة 29
المادة 17 – سرعة التحفُّظ على خط سير البيانات والكشف الجزئي لها[1556]	المادة 30
المادة 18 – إصدار الأوامر[1557]	
المادة 19 – تفتيش ومصادرة بيانات الكمبيوتر المخزَّنة[1558]	المادة 31
المادة 20 – التجميع الفوري لبيانات الكمبيوتر[1559]	المادة 33
المادة 21 – اعتراض محتوى البيانات[1560]	المادة 34

7.3.6 النفاذ عبر الحدود إلى البيانات الحاسوبية المخزونة

بالإضافة إلى التعبير البحت عن الأحكام الإجرائية، ناقش واضعو الاتفاقية الظروف التي يُسمح فيها لوكالات إنفاذ القانون بالنفاذ إلى البيانات الحاسوبية التي لا تكون مخزونة في أراضيهم ولا تقع تحت سيطرة شخص في أراضيهم. وتمكَّن واضعو الاتفاقية من الاتفاق فقط على إثنين من التصورات التي ينبغي فيها إجراء التحقيق على يد وكالة إنفاذ قانون واحدة بدون الحاجة إلى طلب مساعدة قانونية متبادلة.[1561] ولم يمكن التوصل إلى اتفاقات أخرى[1562] بل ولا يزال الحل الذي تم التوصل إليه موضعاً للنقد من جانب الدول الأعضاء في مجلس أوروبا.[1563]

والحالتان التي يُسمح فيهما لوكالات إنفاذ القانون بالنفاذ إلى البيانات المخزونة خارج أراضيهم تتصلان بما يلي:

- معلومات متوفِّرة للجمهور؛ و/أو
- النفاذ بموافقة الشخص صاحب السيطرة.

المادة 32 – الدخول عبر الحدود على بيانات مخزَّنة على كمبيوتر عن طريق الموافقة أو حيثما تكون متاحة علناً

يجوز لأي طرف، وبدون تفويض من أي طرف آخر:

أ) الدخول على بيانات كمبيوتر مخزَّنة ومتاحة علناً (مصدر مفتوح)، بغض النظر عن مكان تواجد البيانات جغرافياً؛ أو

ب) الدخول على، أو تلقي، عن طريق نظام كمبيوتر في إقليمه، بيانات كمبيوتر مخزَّنة موجودة في طرف آخر، وذلك في حالة حصول ذلك الطرف على الموافقة القانونية والطوعية من الشخص الذي له السلطة القانونية في الكشف عن البيانات لذلك الطرف من خلال نظام الكمبيوتر المذكور.

ولا تشمل المادة 32 حالات أخرى، ولكن هذه الحالات الأخرى ليست مستبعدة أيضاً.[1564]

[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 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.
[1564] See Explanatory Report to the Convention on Cybercrime, No. 293.

وتلاحظ المادة 32 أنه إذا كانت البيانات ذات الصلة متاحة علناً، فإن وكالات إنفاذ القانون الأجنبية يُسمح لها بالنفاذ إلى هذه المعلومات. ومن أمثلة المعلومات المتاحة علناً المعلومات المتوفرة في مواقع شبكة الويب بدون التحكُّم في النفاذ (مثل كلمات المرور). وإذا لم يُسمح للمحققين – مثل أي مستعمل آخر – النفاذ إلى هذه المواقع، فإن ذلك يمكن أن يعرقل عملهم بصورة خطيرة. ولذلك كانت هذه الحالة الأولى التي عالجتها المادة 32 مقبولة على نطاق واسع.

والحالة الثانية التي يُسمح فيها لوكالات إنفاذ القانون بالنفاذ إلى البيانات الحاسوبية المخزونة خارج إقليمهم هي حالة حصول المحققين على موافقة قانونية وطوعية من الشخص الذي يملك قانونياً سلطة الكشف عن البيانات. ويتعرَّض هذا الإذن لنقد كثيف.[1565] فهناك حجج قوية تعارض هذه القاعدة التنظيمية. وأهم هذه الحجج هي أن واضعي الاتفاقية ينتهكون، بإقامة هذا الإعفاء الثاني، الهيكل المتشدِّد لنظام المساعدة القانونية المتبادلة. فقد مكَّن واضعو الاتفاقية من خلال المادة 18 المحققين إصدار أمر لتقديم بيانات. ولا يمكن تطبيق هذه الأداة في التحقيقات الدولية لأن الحكم المناظر في الفصل 3 من الاتفاقية غير موجود. وبدلاً من التخلي عن الهيكل المتشدِّد بالسماح للمحققين الأجانب بالاتصال مباشرة بالشخص الذي يسيطر على البيانات ومطالبتهم بتقديم هذه البيانات فقد اكتفى واضعو الاتفاقية بتطبيق الحكم المناظر في الفصل 3 من الاتفاقية.[1566]

8.3.6 شبكة نقاط الاتصال على مدار الساعة كل يوم (7/24)

تتطلَّب تحقيقات الجرائم السيبرانية في كثير من الأحيان تصرفاً فورياً.[1567] وكما شرحنا أعلاه ينطبق ذلك بصورة خاصة في حالة بيانات الحركة اللازمة لتعيين الشخص المشتبه فيه، نظراً لأن هذه البيانات يجري حذفها في كثير من الأحيان بعد فترة قصيرة إلى حد ما.[1568] ولزيادة سرعة التحقيقات الدولية تُبرز الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية أهمية التمكين من استعمال وسائل الاتصال العاجلة في المادة 25. ولزيادة تحسين كفاءة طلبات المساعدة المتبادلة يُلزم واضعو الاتفاقية الأطراف بتسمية نقطة اتصال لطلبات المساعدة المتبادلة تكون حاضرة بدون أي حدود من ناحية الوقت.[1569] وأكد واضعو الاتفاقية على أن إقامة نقاط الاتصال هو أداة من أهم الأدوات التي تنص عليها الاتفاقية المتعلقة بالجريمة الإلكترونية.[1570]

المادة 35 – شبكة 7/24

يعيِّن كل طرف نقطة اتصال تكون متاحة طوال 24 ساعة يومياً ولمدة سبعة أيام أسبوعياً وذلك لضمان توافر المساعدة الفورية لأغراض التحقيقات أو الإجراءات الخاصة بالجرائم الجنائية التي تتعلَّق بُنظم وبيانات الكمبيوتر، أو من أجل جمع الأدلة الخاصة بجريمة جنائية في شكل إلكتروني، وتشمل هذه المساعدة تسهيل، أو إذا كان القانون الوطني والإجراءات المتبعة لذلك الطرف تجيز بشكل مباشر، تنفيذ التدابير التالية:

أ) توفير المشورة الفنية؛

ب) التحفظ على البيانات طبقاً للمادتين 29 و30؛

ج) جمع الأدلة وتوفير المعلومات القانونية والاستدلال على المشتبه فيهم.

2 أ) تكون لنقطة اتصال أي طرف القدرة على إجراء الاتصالات بمثيلتها بأي طرف آخر على وجه السرعة.

ب) إذا كانت نقطة الاتصال التي يعيِّنها أي طرف ليست جزءاً من السلطة أو السلطات المسؤولة عن المساعدة الدولية المتبادلة أو تسليم المجرمين، فإنه على نقطة الاتصال أن تضمن أنها قادرة على التنسيق مع تلك السلطة أو السلطات على وجه السرعة.

3 يضمن كل طرف توافر العاملين المدرَّبين والمزودين بالأجهزة والمعدات وذلك من أجل تسهيل عمل الشبكة.

[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.

وتستند فكرة شبكة 7/24 إلى شبكة جهات الاتصال الموجودة حالياً طوال 24 ساعة لخدمة مكافحة الجرائم الدولية ذات التكنولوجيا العالية التابعة لمجموعة الثمانية.[1571] وبإنشاء شبكة لنقاط الاتصال تعمل على مدى اليوم طوال الأسبوع يهدف واضعو الاتفاقية إلى معالجة تحديات مكافحة الجريمة السيبرانية – وخاصة التحديات التي تتصل بسرعة عمليات تبادل البيانات[1572] والتي تنطوي على بُعد دولي.[1573] ويلتزم أطراف الاتفاقية بإنشاء نقاط الاتصال المذكورة وكفالة تمكنها من القيام بإجراءات فورية وكذلك الحفاظ على الخدمة. وكما جاء في الفقرة الفرعية 3 من المادة 35 من الاتفاقية المتعلقة بالجريمة الإلكترونية، يشمل ذلك توفُّر العاملين المدرَّبين والمزوَّدين بالأجهزة.

وفيما يتعلق بعملية إقامة نقطة الاتصال وخاصة المبادئ الأساسية لهذا الهيكل، تسمح الاتفاقية للدول الأعضاء بأقصى قدر من المرونة. فالاتفاقية لا تتطلَّب إنشاء سلطة جديدة ولا تحدِّد السلطات القائمة التي يمكن أو ينبغي أن تلحق بها نقطة الاتصال. وأشار واضعو الاتفاقية كذلك إلى أن نقطة شبكة 7/24 تهدف إلى توفير مساعدة تقنية وقانونية، وسوف يؤدي ذلك إلى عدة حلول محتملة في صدد تنفيذ هذه المساعدة.

وفيما يتعلق بتحقيقات الجريمة السيبرانية، ينطوي إنشاء نقاط الاتصال على وظيفتين. ويشمل ذلك ما يلي:

- التعجيل بالاتصالات من خلال توفير نقطة اتصال وحيدة؛
- التعجيل بالتحقيقات من خلال السماح لنقاط الاتصال بإجراء بعض التحقيقات فوراً.

وينطوي الجمع بين الوظيفتين على إمكانية اقتراب سرعة التحقيقات الدولية من مستوى السرعة في التحقيقات الوطنية.

وتحدِّد المادة 32 من الاتفاقية المتعلقة بالجريمة السيبرانية الحد الأدنى من القدرات المطلوبة لنقاط الشبكة. فإلى جانب توفير المساعدة التقنية وتقديم المعلومات القانونية تشمل المهام الرئيسية لنقطة الاتصال ما يلي:

- حفظ البيانات؛
- جمع الأدلة؛
- الاستدلال على مكان المشتبه فيهم.

ومن المهم أيضاً في هذا السياق أن نبرز أن الاتفاقية لا تحدِّد السلطة التي ينبغي أن تكون مسؤولة عن تشغيل نقطة الاتصال على مدار الأربع والعشرين ساعة كل يوم. فإذا كانت نقطة الاتصال تخضع لإدارة سلطة مختصة بإصدار أوامر حفظ البيانات،[1574] وطلبت نقطة اتصال أجنبية حفظ هذه البيانات، فإن هذا التدبير يمكن تنفيذه فوراً بأمر من نقطة الاتصال المحلية. وإذا كانت نقطة الاتصال خاضعة لإدارة سلطة غير مختصة بأن تصدر بنفسها أوامر حفظ البيانات، فمن المهم أن تتوفَّر لنقطة الاتصال قدرة الاتصال فوراً بالسلطات المختصة لكفالة تنفيذ هذا التدبير فوراً.[1575]

وقد أُشير صراحة في الاجتماع الثاني للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية إلى أن مشاركة شبكة اتصالات 7/24 لا يتطلب التوقيع أو التصديق على الاتفاقية.[1576]

9.3.6 التعاون الدولي في سياق مشروع اتفاقية ستانفورد

اعترف واضعو مشروع اتفاقية ستانفورد[1577] بأهمية البُعد الدولي في الجريمة السيبرانية والتحديات المتصلة بذلك. ولمعالجة هذه التحديات قاموا بإدراج أحكام محدَّدة تعالج موضع التعاون الدولي. وتغطي الأحكام الموضوعات التالية:

- المادة 6 – المساعدة القانونية المتبادلة
- المادة 7 – تسليم المجرمين

[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: *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.
[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.

- المادة 8 – الادعاء
- المادة 9 – الانتصاف المؤقت
- المادة 10 – استحقاقات الشخص المتهم
- المادة 11 – التعاون في إنفاذ القانون

ويتضح من هذا النهج عدد من أوجه التشابه مع النهج الذي اعتنقته الاتفاقية المتعلقة بالجريمة الإلكترونية. والاختلاف الرئيسي هو أن القواعد التنظيمية المنصوص عليها في الاتفاقية المتعلقة بالجريمة الإلكترونية أشد صرامة وأكثر تعقيداً وأكثر دقة في التحديد مقارنة بمشروع اتفاقية ستانفورد. وكما أشار واضعو مشروع اتفاقية ستانفورد، فإن نهج الاتفاقية المتعلقة بالجريمة الإلكترونية عملي بقدر أكبر ولذلك ينطوي على بعض المزايا الواضحة من ناحية التطبيق الفعلي.[1578] وقرّر واضعو مشروع اتفاقية ستانفورد اتباع نهج مختلف نظراً لأنهم توقعوا أن تطبيق تكنولوجيا جديدة قد يؤدي إلى بعض الصعوبات. ونتيجة لذلك، لم يقدموا سوى بعض التعليمات العامة دون إضفاء مزيد من التحديد عليها.[1579]

4.6 مسؤولية مقدمي خدمات الإنترنت

1.4.6 مقدمة

يشمل ارتكاب جريمة سيبرانية تلقائياً عدداً من الأشخاص والأعمال التجارية حتى إذا كان الجاني يتصرف وحده. وبسبب هيكل الإنترنت، فإن إرسال بريد إلكتروني بسيط يتطلب خدمة عدد من مقدمي الخدمات.[1580] وبالإضافة إلى مقدِّم خدمة البريد الإلكتروني ينطوي الإرسال على مقدمي خدمة النفاذ وكذلك جهات التسيير وإرسال البريد الإلكتروني إلى المتلقي. ولا يوجد اختلاف في حالة تنزيل الأفلام التي تحتوي على المناظر الفاضحة للأطفال. إذ إن عملية التنزيل تشمل مقدِّم المحتوى الذي قام بتحميل الصور (مثلاً في الموقع في شبكة الويب)، ومقدِّم خدمة الاستضافة الذي يوفِّر وسيط التخزين لموقع الويب، وجهات التسيير التي ترسل الملفات إلى المستعمل وأخيراً مقدِّم خدمة النفاذ الذي مكَّن المستعمل من النفاذ إلى الإنترنت.

وبسبب تورط أطراف عديدة ظل مقدمو خدمة الإنترنت دائماً محوراً للتحقيقات الجنائية التي تنطوي على جناة يستعملون خدمات مقدمي الإنترنت لارتكاب الجريمة.[1581] ومن الأسباب الرئيسية لهذا التطور أنه حتى في حالة قيام الجاني بعمله من الخارج، فإن مقدمي الخدمة الموجودين داخل الحدود الوطنية للبلد هم موضوع مناسب للتحقيقات الجنائية دون انتهاك مبدأ السيادة الوطنية.[1582]

ونظراً لأن الجريمة السيبرانية لا يمكن ارتكابها بدون مشاركة مقدمي الخدمة، من ناحية، ولأن مقدمي الخدمة يستطيعون في كثير من الأحيان منع هذه الجرائم، من ناحية أخرى، فإن ذلك يثير سؤالاً عما إن كان من الضروري تحديد مسؤولية مقدمي الخدمة.[1583] والإجابة على هذا السؤال تتسم بأهمية حاسمة في سياق التطوير الاقتصادي للبنية التحتية لتكنولوجيا المعلومات والاتصالات، إذ إن مقدمي الخدمة لن يشغِّلوا خدماتهم إلاّ إذا كانوا يستطيعون تجنُّب التجريم في إطار الأسلوب العادي للتشغيل. وبالإضافة إلى ذلك، تهتم وكالات إنفاذ القانون أيضاً اهتماماً كبيراً بهذه المسألة. إذ إن عمل وكالات إنفاذ القانون يعتمد في كثير من الأحيان على التعاون المقدَّم من مقدمي خدمة الإنترنت والتعاون معهم. ويثير ذلك بعض القلق لأن تحديد مسؤولية مقدمي خدمة الإنترنت عن الأعمال التي يرتكبها عملائهم من المستعملين يمكن أن تؤثر على تعاون مقدمي خدمة الإنترنت ودعمهم لتحقيقات الجرائم السيبرانية، وكذلك في منع وقوع الجرائم بالفعل.

[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.
[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

2.4.6 نهج الولايات المتحدة

هناك نُهج مختلفة لإقامة التوازن بين ضرورة إشراك مقدمي الخدمة إشراكاً نشطاً في التحقيقات، من ناحية، وتقييد مخاطر المسؤولية الجنائية عن أفعال أطراف ثالثة، من ناحية أخرى.[1584] ويمكن الاطلاع على مثال لنهج تشريعي في البند 517 (أ) و(ب) من العنوان 16 من مدونة الولايات المتحدة.

البند 512 – تحديدات المسؤولية المتعلقة بالمادة المنشورة على الخط

(أ) الاتصالات العابرة من شبكة رقمية

لا يكون مقدِّم الخدمة مسؤولاً عن التعويض النقدي، أو التعويض الزجري أو غير ذلك من التعويض المنصف، باستثناء الحالات المنصوص عليها في الفقرة الفرعية (ي)، عن انتهاكات حقوق الطبع بسبب قيامه بإرسال أو تسيير مواد، أو توفير توصيلات لها، من خلال نظام أو شبكة تحت السيطرة أو التشغيل على يد مقدِّم الخدمة أو لصالحه، أو بسبب تخزين عابر ووسيط لتلك المادة في سياق العملية المذكورة من الإرسال أو التسيير أو توفير التوصيلات، إذا –

(1) بدأ إرسال المادة على يد أو بتوجيه من شخص خلاف مقدِّم الخدمة؛

(2) جرى الإرسال أو التسيير أو توفير التوصيلات أو التخزين من خلال عملية تقنية أوتوماتية بدون اختيار المادة من جانب مقدِّم الخدمة؛

(3) لم يقم مقدِّم الخدمة باختيار الأشخاص الذين يتلقون هذه المادة إلّا بصفة استجابة أوتوماتية لطلب شخص آخر؛

(4) لم يتم الاحتفاظ بنسخة من المادة يكون مقدِّم خدمة قد استنسخها في سياق هذه العملية الوسيطة والعابرة من التخزين في النظام أو الشبكة بطريقة تجعل من الممكن لأي شخص النفاذ إليها عادة خلاف المتلقّين المنتظرين و لم يتم الاحتفاظ بمثل هذه النُسخة في النظام أو الشبكة بطريقة تجعل المتلقّين المنتظرين قادرين على النفاذ إليها لفترة أطول من الفترة اللازمة بصورة معقولة للإرسال أو التسيير أو توفير التوصيلات؛

(5) أُرسلت المادة من النظام أو الشبكة بدون تعديل لمحتواها.

(ب) الإخفاء في النظام

(1) الحد على المسؤولية. – لا يكون مقدِّم الخدمة مسؤولاً عن التعويض النقدي أو عن التعويض الزجري أو غير ذلك من التعويض المنصف، باستثناء الحالات المنصوص عليها في الفقرة الفرعية (ي) عن انتهاك حقوق الطبع بسبب التخزين الوسيط أو المؤقت لمادة في نظام أو شبكة تحت السيطرة أو التشغيل على يد مقدِّم الخدمة أو لصالحه في الحالة التي –

(ألف) تكون فيها المادة قد أُتيحت على الخط من جانب شخص خلاف مقدِّم الخدمة

(باء) تكون فيها المادة قد أُرسلت من شخص موصوف في الفقرة (ألف) من خلال النظام أو الشبكة إلى شخص خلاف الشخص الموصوف في الفقرة (ألف) بناءً على توجيه من ذلك الشخص الآخر؛

(جيم) يتم فيها التخزين من خلال عملية تقنية أوتوماتية بغرض إتاحة المادة لمستعملي النظام أو الشبكة الذين يطلبون، بعد إرسال المادة على النحو الموصوف في الفقرة الفرعية (باء)، النفاذ إلى المادة، من الشخص الموصوف في الفقرة الفرعية (أ) إذا تم الوفاء بالشروط المعروضة في الفقرة (2).

[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."

ويستند الحكم إلى قانون حقوق الطبع الرقمية للألفية (DMCA) الذي تم توقيعه ليصبح قانوناً في عام 1998.[1585] وبإقامة نظام للملاذ الآمن استبعد القانون مسؤولية مقدمي بعض الخدمات من انتهاكات حقوق الطبع التي يرتكبها طرف ثالث.[1586] ومن المهم أولاً لهذا السياق إبراز أن جميع مقدمي الخدمة غير مشمولين بهذا التقييد.[1587] إذ إن تقييد المسؤولية ينطبق فقط على مقدمي الخدمة[1588] ومقدمي خدمة الإخفاء.[1589] ومن المهم، بالإضافة إلى ذلك، أن يشار إلى أن المسؤولية تتصل ببعض الاشتراطات. وهذه الاشتراطات هي ما يلي في صدد مقدمي الخدمة:

- أن يكون إرسال المادة قد بدأ من جانب أو بتوجيه شخص خلاف مقدِّم الخدمة؛
- أن يجري الإرسال من خلال عملية تقنية أوتوماتية بدون اختيار المادة من جانب مقدِّم الخدمة؛
- ألاّ يختار مقدِّم الخدمة الأشخاص الذين يتلقَّون المادة؛
- ألاّ يتم الاحتفاظ بالنسخة التي يستنسخها مقدِّم الخدمة من المادة في سياق عملية التخزين الوسيطة أو العابرة في النظام أو الشبكة بطريقة تجعل النفاذ إليها مفتوحاً عادة أمام أي شخص خلاف المتلقين المنتظرين.

وهناك مثال آخر لتقييد مسؤولية مقدِّم الخدمة ويرد في البند 230 (ج) من العنوان 47 من مدونة الولايات المتحدة ويستند إلى قانون الآداب في الاتصالات[1590]:

البند 230 – حماية قيام شخص خاص بمنع وفرز المواد المسيئة

(ج) حماية المنع والفرز "التطوعي" للمواد المسيئة

(1) معاملة الناشر أو المتحدث

لا يعامل مقدِّم أو مستعمل خدمة حاسوبية تفاعلية باعتباره ناشراً أو متحدثاً لأي معلومات مقدَّمة من ناشر آخر لمحتوى معلوماتي.

(2) المسؤولية المدنية

لا يعتبر أي مقدِّم أو مستعمل لخدمة حاسوبية تفاعلية مسؤولاً بسبب –

(ألف) أي فعل يقوم به تطوعاً وبنِّية حسنة لتقييد النفاذ أو الحصول على مواد يعتبرها المقدِّم أو المستعمل فاضحة أو داعرة أو فاسقة أو قذرة أو مفرطة العنف أو تسبب المضايقة أو غير مقبولة بأي شكل آخر، سواء كانت أو لم تكن هذه المادة تتمتع بحماية دستورية؛ أو

(باء) أي فعل يتخذه لتمكين أو تزويد مقدمي المحتوى المعلوماتي أو غيرهم بوسائل تقنية لتقييد النفاذ إلى المادة الموصوفة في الفقرة (1).

وبهذين النهجين يشترك البندان 517 (أ) من العنوان 17 من مدونة الولايات المتحدة والبند 230 (ج) من العنوان 47 من مدونة الولايات المتحدة في أنهما يركزان على المسؤولية في صدد مجموعات خاصة من المقدمين ومجالات خاصة من القانون. ولذلك يتضمن الجزء الباقي من هذا الفصل نظرة عامة عن النهج التشريعي الذي اضطلع به الاتحاد الأوروبي ويتبع نهجاً أكثر اتساعاً.

[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)

[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;

3.4.6 توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية

يعتبَر توجيه الاتحاد الأوروبي الخاص بالتجارة الإلكترونية[1591] مثالاً من أمثلة النهج التشريعي لتنظيم مسؤولية مقدمي خدمة الإنترنت. وفي مواجهة التحديات المتصلة بالبعد الدولي للإنترنت قرَّر واضعو التوجيه صياغة معايير قانونية توفر إطاراً قانونياً للتطوير الشامل لمجتمع المعلومات، وبذلك يتم دعم التنمية الاقتصادية الشاملة وأعمال وكالات إنفاذ القانون.[1592] وتستند القاعدة التنظيمية المتعلقة بالمسؤولية إلى مبدأ المسؤولية المتدرجة.

ويتضمّن التوجيه عدداً من الأحكام التي تحد من مسؤولية بعض مقدّمي الخدمة.[1593] وهذه الحدود تتصل بمختلف فئات الخدمات التي يشغِّلها مقدِّم الخدمة.[1594] والمسؤولية غير مستبعدة بالضرورة في جميع الحالات الأخرى، وإذا لم تكن هناك قواعد أخرى. تحد من المسؤولية، فإن الطرف الفاعل يصبح مسؤولاً مسؤولية كاملة. والدافع إلى إصدار هذا التوجيه هو الحد من المسؤولية في الحالات التي لا تتوافر فيها لمقدِّم الخدمة سوى إمكانيات محدودة لمنع الجريمة. وقد تكون أسباب ضيق الاحتمالات تقنية بطبيعتها، إذ قد لا تتمكّن المسيِّرات مثلاً من تنقية البيانات التي تمر من خلالها ولا تكاد تستطيع منع عمليات تبادل البيانات – بدون ضياع كبير للسرعة. ويستطيع مقدمو الاستضافة إزالة البيانات إذا أدركوا وجود أنشطة إجرامية. ومع ذلك، فإن كبار مقدّمي خدمة الاستضافة، مثلهم مثل مقدمي خدمة التسيير، لا يستطيعون السيطرة على جميع البيانات المخزونة في المخدِّمات الخاصة بهم.

وفيما يتعلق بتباين القدرة على السيطرة الفعلية على الأنشطة الإجرامية، تختلف مسؤولية مقدّمي الاستضافة والنفاذ. وفيما يتعلق بهذا الجانب، فإن الأمر الذي يتعيّن وضعه في الاعتبار هو أن التوازن في هذا التوجيه يستند إلى المعايير التقنية الجارية. وهناك في الوقت الحاضر أدوات يمكن أن تكتشف أوتوماتياً الصور الفاضحة غير المعروفة. وإذا استمرت التطورات التقنية في هذا المجال فقد يكون من الضروري تقييم القدرة التقنية لمقدمي الخدمة في المستقبل بل وتعديل النظام إذا استلزم الأمر.

4.4.6 مسؤولية مقدّم خدمة النفاذ (توجيه الاتحاد الأوروبي)

تُعَرِّف المواد 12-15 درجة الحدّ من مسؤولية مختَلف مقدّمي الخدمة. واستناداً إلى المادة 12 تُستبعَد تماماً مسؤولية مقدّمي خدمة النفاذ ومشغّلي معدات التسيير طالما امتثلوا للشروط الثلاثة المحدّدة في المادة 12. ونتيجة لذلك، فإن مقدِّم الخدمة لا يكون عموماً مسؤولاً عن الجرائم الجنائية التي يرتكبها مستعملو خدماته. وهذا الاستبعاد الكامل للمسؤولية لا يعفي مقدِّم الخدمة من الالتزام بمنع الجرائم الأخرى إذا صدر إليه أمر من المحكمة أو من سلطة إدارية للقيام بذلك.[1595]

المادة 12 – "مجرّد مجرى"

1 في حالة تقديم خدمة مجتمع معلومات تتألف من إرسال معلومات يقدمها متلقي الخدمة عبر شبكة اتصالات، أو توفير النفاذ إلى شبكة اتصالات، تكفل الدول الأعضاء ألّا يكون مقدّم الخدمة مسؤولاً عن المعلومات المرسَلة، شريطة أن مقدّم الخدمة:

(أ) لا يبدأ الإرسال؛

(ب) لا يختار متلقي الإرسال؛

(ج) لا يختار أو يعدِّل المعلومات المتضمّنة في الإرسال.

2 وتشمل أفعال الإرسال وتقديم خدمة النفاذ المشار إليها في الفقرة 1 عملية التخزين الأوتوماتي والوسيط والعابر للمعلومات المُرسَلة بمقدار حدوثها لغرض وحيد وهو تنفيذ عملية الإرسال في شبكة الاتصال، وبشرط عدم تخزين المعلومات لأي فترة تزيد عن المدة اللازمة بصورة معقولة للإرسال.

3 لا تؤثر هذه المادة على إمكانية قيام محكمة أو سلطة إدارية، وفقاً للأنظمة القانونية للدول الأعضاء، بمطالبة مقدّم الخدمة بإنهاء أو منع أي انتهاك.

[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:

[1595] See Art. 12 paragraph 3 E-Commerce Directive.

ويشبه هذا النهج البند 517 (أ) من العنوان 17 من مدوّنة الولايات المتحدة.[1596] إذ يهدف التنظيمان إلى تقرير مسؤولية مقدّمي الخدمة، ويربط هذان التنظيمان تقييد المسؤولية بمقتضيات متشابهة. والفرق الرئيسي هو أن تطبيق المادة 12 من توجيه الاتحاد الأوروبي الخاص بالتجارة الإلكترونية لا ينحصر في انتهاكات حقوق الطبع ولكنه يستبعد المسؤولية في صدد جريمة من أي نوع.

5.4.6 المسؤولية عن الإخفاء (توجيه الاتحاد الأوروبي)

يُستعمَل مصطَلح "الإخفاء" في هذا السياق ليصف تخزين مواقع شائعة في شبكة الويب على وسيط تخزين محلي من أجل تقليل عرض النطاق وجعل النفاذ إلى البيانات أكثر كفاءة.[1597] ويتمثل أحد التقنيات المستعملة لتقليل عرض النطاق في إنشاء مخدِّمات وكيلة.[1598] وفي هذا النطاق يمكن استخدام المخدِّم الوكيل لخدمة الطلبات بدون الاتصال بالمخدِّم المحدَّد (اسم الميدان الذي يُدخله المستعمل) وذلك باستعادة المحتوى الذي تم تخزينه على وسيط التخزين المحلي من طلب سابق. واعترف واضعو التوجيه بالأهمية الاقتصادية للإخفاء وقرروا استبعاد المسؤولية عن التخزين المؤقت الأوتوماتي إذا امتثل مقدّم الخدمة للشروط المحدّدة في المادة 13. ومن هذه الشروط أن يمتثل مقدِّم الخدمة للمعايير المعتَرف بها على نطاق واسع بشأن تحديث المعلومات.

المادة 13 – "الإخفاء"

1 في حالة تقديم خدمة من خدمات مجتمع المعلومات تتألف من إرسال معلومات يقدمها متلقي الخدمة في شبكة اتصال، تكفل الدول الأعضاء عدم توقيع المسؤولية على مقدّم الخدمة بسبب التخزين الأوتوماتي والوسيط والمؤقت لهذه المعلومات، إذا كان ذلك لغرض وحيد وهو زيادة كفاءة الإرسال الأمامي للمعلومات إلى متلقين آخرين للخدمة بناءً على طلبهم، شريطة:

(أ) أن مقدّم الخدمة لا يُعدِّل المعلومات؛

(ب) أن مقدّم الخدمة يمتثل للشروط المفروضة على النفاذ إلى المعلومات؛

(ج) أن مقدّم الخدمة يمتثل للقواعد المتصلة بتحديث المعلومات، المحدَّدة بطريقة تلقى الاعتراف والاستعمال على نطاق واسع في الصناعة؛

(د) أن مقدِّم الخدمة لا يتدخَّل في الاستعمال المشروع للتكنولوجيا، المعتَرف به والمنطبق على نطاق واسع في الصناعة، للحصول على بيانات عن استعمال المعلومات؛

(هـ) أن مقدِّم الخدمة يتصرّف بسرعة لإزالة أو وقف النفاذ إلى المعلومات التي خزّنها بعد الحصول على معرفة فعلية بأن المعلومات قد أزيلت في المصدر الأوّلي للإرسال من الشبكة، أو أن النفاذ إليها قد تم وقفه، وأن محكمة أو سلطة إدارية قد أمرت بإزالته أو وقفه.

2 لا تؤثّر هذه المادة على إمكانية قيام محكمة أو سلطة إدارية، وفقاً للأنظمة القانونية للدول الأعضاء، بمطالبة مقدِّم الخدمة بإنهاء أو منع أي انتهاك.

والمادة 13 من توجيه الاتحاد الأوروبي الخاص بالتجارة الإلكترونية هي مثال آخر لأوجه التشابه بين الهيكل المتشدد للولايات المتحدة والنهج الأوروبي. ويشبه النهج الأوروبي البند 517 (ب) من العنوان 17 من مدونة الولايات المتحدة.[1599] ويهدف التنظيمان إلى النص على مسؤولية

[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.

[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

مقدّمي خدمة الإخفاء ويربط هذان التنظيمان تحديد المسؤولية بمقتضيات متشابهة. وفي صدد مسؤولية مقدّمي الخدمة،[1600] يتمثل الاختلاف الرئيسي بين النهجين في أن تطبيق المادة 13 من توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية لا يقتصر على انتهاكات حقوق الطبع ولكنه يستبعد المسؤولية في صدد جريمة من أي نوع.

6.4.6 مسؤولية مقدِّم خدمة الاستضافة (توجيه الاتحاد الأوروبي)

فيما يتعلق بالمحتوى القانوني على وجه الخصوص يؤدي مقدّم خدمة الاستضافة وظيفة هامة في إطار ارتكاب الجريمة. إذ إن الجناة الذين يتيحون المحتوى غير القانوني على الخط لا يقومون عموماً بتخزين هذا المحتوى في مخدِّماتهم. ويتم تخزين معظم مواقع شبكة الويب على مخدّمات يتيحها مقدمو خدمة الاستضافة. وأي شخص يرغب في عرض صفحة من صفحات الويب يستطيع أن يستأجر سعة تخزينية من مقدّم خدمة استضافة لتخزين الموقع. بل ويعرض بعض مقدّمي الخدمة حيِّزاً في شبكة الويب بدون مقابل نظير رعاية الإعلانات.[1601]

وتعيين المحتوى غير القانوني يمثل تحدياً لمقدمي خدمة الاستضافة. ويستحيل على مقدّمي الخدمة الذائعين بصورة خاصة الذين لديهم الكثير من مواقع الويب القيام ببحث يدوي عن المحتوى غير القانوني بين عدد كبير جداً من المواقع. ونتيجة لذلك، قرّر واضعو التوجيه الحد من مسؤولية مقدّمي خدمات الاستضافة. ومع ذلك، وبعكس الحالة المنطبقة على مقدّم خدمة النفاذ، لا يتم استبعاد مسؤولية مقدم خدمة الضيافة. ولا يكون مقدّم الخدمة المضيف مسؤولاً طالما لم تكن لديه معرفة فعلية بالأنشطة غير القانونية أو المحتوى غير القانوني المخزون على مخدماته. وافتراض إمكانية تخزين محتوى غير قانوني على المخدّمات لا يعتبر هنا معادلاً للحصول على معرفة فعلية بهذه المسألة. وإذا حصل مقدّم الخدمة على معرفة ملموسة بالأنشطة غير القانونية أو المحتوى غير القانوني، فإنه يستطيع تجنُّب المسؤولية بمجرد قيامه فوراً بإزالة المعلومات غير القانونية.[1602] والإخفاق في التصرّف الفوري يؤدي إلى تحقق مسؤولية مقدّم خدمة الاستضافة.[1603]

المادة 14 – الاستضافة

1 عندما يتم تقديم خدمة من خدمات مجتمع المعلومات تتألف من تخزين معلومات مقدّمة من متلقي الخدمة، تكفل الدول الأعضاء ألاّ يكون مقدِّم الخدمة مسؤولاً عن المعلومات المخزّنة بناءً على طلب متلقي الخدمة بشرط:

(أ) أن مقدِّم الخدمة لا تكون لديه معرفة فعلية بنشاط غير قانوني أو بمعلومات غير قانونية وأنه لا يدرك، في صدد مطالبات التعويض، الوقائع أو الظروف التي يظهر منها النشاط غير القانوني أو المعلومات غير القانونية؛ أو

(ب) أن يتصرف مقدّم الخدمة بسرعة، بعد حصوله على هذه المعرفة أو هذا الإجراء بإزالة أو وقف النفاذ إلى المعلومات.

2 لا تنطبق الفقرة 1 إذا كان متلقي الخدمة يتصرف تحت سلطة أو مراقبة مقدِّم الخدمة.

3 لا تؤثّر هذه المادة على إمكانية قيام محكمة أو سلطة إدارية، وفقاً للأنظمة القانونية للدول الأعضاء، بمطالبة مقدِّم الخدمة بإنهاء أو منع أي انتهاك، كما لا تؤثر على إمكانية وضع الدول الأعضاء تدابير تحكم إزالة أو وقف النفاذ إلى المعلومات.

ولا تنطبق المادة 14 فقط على مقدِّم الخدمة الذي يقتصر في خدماته على تأجير البنية التحتية لتخزين البيانات التقنية. إذ إن خدمات الإنترنت التي يكثر الإقبال عليها مثل منصّات المزادات تعرض أيضاً خدمات الاستضافة.[1604]

7.4.6 الاستبعاد من الالتزام بالرصد (توجيه الاتحاد الأوروبي)

لم يكن من الواضح في بعض الدول الأعضاء قبل تنفيذ التوجيه إذا كان من الممكن ملاحقة مقدّمي الخدمة استناداً إلى انتهاك الالتزام برصد أنشطة المستعملين. وإلى جانب إمكانيات التنازع مع لوائح حماية البيانات وسرّية الاتصالات، فإن هذا الالتزام يمكن أن يسبّب صعوبات بصورة خاصة لمقدّمي خدمات الاستضافة الذين يقومون بتخزين آلاف مواقع شبكة الويب. ولتجنّب هذا النزاع يستبعد التوجيه وضع التزام عام برصد المعلومات المرسَلة أو المخزونة.

المادة 15 – لا يوجد التزام عام بالرصد

1 لا تفرض الدول الأعضاء التزاماً عاماً على مقدّمي الخدمة إذا كان تقديم الخدمات مشمولاً بالمواد 12 و13 و14، برصد المعلومات التي يقومون بإرسالها أو تخزينها، ولا التزاماً عاماً بالسعي بنشاط للحصول على وقائع أو ظروف تشير إلى نشاط غير قانوني.

[1600] See above: Chapter 6.4.4.

[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.

2 يجوز للدول الأعضاء أن تضع التزامات لمقدّمي خدمات مجتمع المعلومات بتبليغ السلطات العامة المختصة فوراً بأي أنشطة غير قانونية مزعومة يجري القيام بها أو معلومات مقدّمة من متلقي خدماتهم أو التزامات بتبليغ السلطات المختصة، بناء على طلبها، بمعلومات تمكّنها من تعيين متلقّي خدماتهم الذين يبرمون معهم اتفاقات تخزين.

8.4.6 المسؤولية عن وصلات الإحالة الإلكترونية (قانون التجارة الإلكترونية – النمسا)

تؤدّي وصلات الإحالة الإلكترونية دوراً هاماً في الإنترنت. فهي تمكّن مقدّم وصلة الإحالة الإلكترونية من توجيه المستعمِل إلى معلومات محدّدة متوفرة على الخط. وبدلاً من مجرد عرض التفاصيل التقنية عن الطريقة التي يمكن بها النفاذ إلى المعلومات (وذلك مثلاً بتقديم اسم ميدان الموقع الذي توجد فيه المعلومات)، فإن المستعمِل يستطيع أن ينفذ مباشرة إلى المعلومات بالنقل على وصلة إحالة نشطة. وتوفّر وصلة الإحالة أمر لمتصفح شبكة الويب بفتح عنوان الإنترنت الموضوع في الوصلة.

وفي سياق صياغة توجيه الاتحاد الأوروبي نوقشت ضرورة وضع قاعدة تنظيمية بشأن وصلات الإحالة مناقشة مكثّفة.[1605] وقرّر واضعو التوجيه عدم إلزام الدول الأعضاء بتنسيق قوانينها فيما يتعلق بالمسؤولية عن وصلات الإحالة. وبدلاً من ذلك نفّذوا إجراءً لإعادة الفحص لكفالة مراعاة الحاجة إلى اقتراحات تتعلق بمسؤولية مقدّمي وصلات الإحالة وخدمات أدوات المواقع.[1606] وإلى أن يتم تعديل قاعدة تنظيمية بشأن المسؤولية عن وصلات الإحالة في المستقبل، فإن للدول الأعضاء حرية صياغة حلول وطنية.[1607] وقد قرّرت بعض بلدان الاتحاد الأوروبي معالجة مسؤولية مقدّمي وصلات الإحالة في حكم خاص.[1608] واستندت هذه البلدان في تقرير مسؤولية مقدّمي وصلات الإحالة إلى نفس المبادئ التي يتضمنها التوجيه الأوروبي بشأن مسؤولية مقدّمي خدمة الاستضافة.[1609] وهذا النهج هو نتيجة منطقية لتشابه حالة مقدّمي خدمة الاستضافة ومقدّمي وصلات الإحالة. ففي الحالتين يسيطر مقدّم الخدمة على المحتوى غير القانوني، أو على الأقل يسيطر على الوصلة التي تحيل إلى هذا المستوى.

ومن أمثلة ذلك المادة 17 من قانون التجارة الإلكترونية النمساوي[1610]:

المادة 17 – من قانون التجارة الإلكترونية (النمسا) – المسؤولية عن وصلات الإحالة

(1) لا يكون مقدّم الخدمة الذي يتيح، من خلال وصلة إلكترونية، النفاذ إلى المعلومات المقدّمة من طرف ثالث مسؤولاً عن هذه المعلومات إذا

1 لم تكن لديه معرفة فعلية بالأنشطة أو المعلومات غير القانونية ولم يكن يدرك، في حالة المطالبة بتعويض، الوقائع أو الظروف التي يبدو واضحاً منها لمقدّم الخدمة أن هذه الأنشطة أو المعلومات غير قانونية؛

2 تصرّف بسرعة، بعد الحصول على هذه المعرفة أو هذا الإدراك، بإزالة الوصلة الإلكترونية.

9.4.6 المسؤولية عن محرّكات البحث

يعرض مقدّمو محرّكات البحث خدمات البحث لتعيين وثائق ذات أهمية على أساس تحديد معايير معيَّنة. وتبحث محرّكات البحث عن الوثائق ذات الصلة التي تضاهي المعايير التي يدخلها المستعمِل. وهذه المحرّكات تؤدّي دوراً هاماً في نجاح تطوير الإنترنت. ولا يمكن النفاذ إلى محتوى يتوافر في أحد مواقع شبكة الويب ولكنه غير مذكور في فهرس محرّك البحث إلاّ إذا كان الشخص الذي يرغب في النفاذ إليه يعرف عنوان الموارد الموحّد الكامل. ويشير إنترونا/نسينباوم إلى إنه "يمكن القول بدون مبالغة كبيرة إن الوجود في الحياة يتوقف على الوجود في فهرس أحد محرّكات البحث".[1611]

[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.

[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

وكما يحدث في حالة وصلات الإحالة الإلكترونية لا يتضمّن توجيه الاتحاد الأوروبي معايير تحدّد مسؤولية مشغّلي محركات البحث. ولذلك قرّرت بعض بلدان الاتحاد الأوروبي معالجة مسؤولية مقدّمي محرّكات البحث في نصّ خاص.[1612] وبعكس حالة وصلات الإحالة الإلكترونية، لم تستند جميع البلدان في تنظيمها إلى نفس المبادئ.[1613] فإسبانيا[1614] والبرتغال استندتا في تنظيمهما المتعلق بمسؤولية مشغّلي محرّكات البحث إلى المادة 14 من التوجيه في حين استندت النمسا[1615] في تحديد المسؤولية إلى المادة 12.

المادة 14 من قانون التجارة الإلكترونية (النمسا) – مسؤولية مشغلي محرّكات البحث

(1) لا يكون مقدّم الخدمة الذي يتيح محرّك بحث وأدوات إلكترونية أخرى للبحث عن معلومات يقدمها طرف ثالث مسؤولاً بشرط أن مقدّم الخدمة:

1 لا يبدأ عملية الإرسال؛

2 لا يختار تلقّي الإرسال؛

3 لا يختار أو يعدّل المعلومات المتضمّنة في الإرسال.

7 المراجع القانونية

الاتفاقية المتعلقة بالجريمة الإلكترونية الصادرة عن مجلس أوروبا[1616]

قانون الكومنولث النموذجي لجرائم الحاسوب والجرائم المتصلة بالحاسوب[1617]

مشروع اتفاقية ستانفورد[1618]

[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.
[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