الأمن السيبراني

فَهْم الجريمة السيبرانية: الظواهر والتحديات والاستجابة القانونية

تقرير

قطاع تنمية الاتصالات

فَهْم الجريمة السيبرانية:
الظواهر والتحديات
والاستجابة القانونية

نوفمبر 2014

منشور الاتحاد الدولي للاتصالات، *فهم الجريمة السيبرانية: الظواهر والتحديات والاستجابة القانونية*، أعده الأستاذ الدكتور ماركو جيركي. ويود المؤلف أن يعرب عن شكره لدائرة البيئة التمكينية للبنى التحتية والتطبيقات الإلكترونية التابعة لمكتب تنمية الاتصالات بالاتحاد الدولي للاتصالات.
هذا المنشور متاح إلكترونياً على العنوان: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

يرجى مراعاة البيئة قبل طباعة هذا التقرير.

جدول المحتويات

الغرض

الغرض من منشور *"فهم الجريمة السيبرانية: الظواهر والتحديات والاستجابة القانونية"* ، الصادر عن الاتحاد الدولي للاتصالات، هو مساعدة البلدان على فهم الجوانب القانونية للجريمة السيبرانية والأمن السيبراني، ومعاونتها على تحقيق التواؤم بين أُطُرها القانونية. ومن هذا المنطلق، يرمي الدليل إلى مساعدة البلدان 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 المنشور لمحة عامة شاملة عن أهم المواضيع المتصلة بالجوانب القانونية للجريمة السيبرانية. ويركز الدليل، في النهج الذي يتوخّاه، 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 متوفرة علناً تشمل كثيراً من الإصدارات المجانية للمجلات القانونية المتاحة على الخط.

ويحتوي المنشور 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 وانتحال 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، والأدلة الرقمية، والتعاون الدولي، ومسؤولية مقدمي خدمة الإنترنت (*الفصل 6*)؛ وضُربت في هذا الصدد أمثلة للنهج الدولية، وأمثلة للممارسات الجيدة المستقاة من الحلول الوطنية.

ويتناول هذا المنشور الهدف الأول من الأهداف الاستراتيجية السبعة للبرنامج العالمي للأمن السيبراني للاتحاد الدولي للاتصالات (GCA) 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 نهج تنظيم الجهود الوطنية في مجال الأمن السيبراني في إطار المسألة 22/1 للجنة الدراسات 1، التابعة لقطاع تنمية الاتصالات في الاتحاد الدولي للاتصالات. ويعد إنشاء الإطار القانوني الملائم عنصراً جوهرياً في الاستراتيجية الوطنية للأمن السيبراني. ويتم تأكيد ولاية الاتحاد ذات الصلة فيما يتعلق ببناء القدرات بالقرار 130 (المراجَع في غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين المتعلق بتعزيز دور الاتحاد في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات. ويشكل اعتماد جميع البلدان لتشريعات ملائمة للحماية من 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 تُعد، 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 أُطرها القانونية الرامية إلى مكافحة الجريمة السيبرانية وتيسير التعاون الدولي.

إخلاء المسؤولية فيما يتعلق بالروابط المرجعية

تحتوي هذه الوثيقة على عدة مئات من الروابط المرجعية بالوثائق المتاحة للجمهور. وقد تم فحص جميع المراجع في الوقت الذي تمت فيه إضافة الروابط المرجعية إلى الحواشي. ومع ذلك، لا يمكن توفير أي ضمانة بأن يكون المحتوى المحدث للصفحات التي تحيل إليها الروابط المرجعية لا يزال كما هو. ولذلك فإن المرجع يشمل، كلما كان ذلك ممكناً، معلومات عن المؤلف ومؤسسة النشر والعنوان وسنة النشر إن أمكن لتمكين القارئ من البحث عن الوثيقة في حال لم تعد الوثيقة المحال إليها من خلال الرابط متوفرة.

1 مقدمة

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

1.1 البنية التحتية والخدمات

تُعد الإنترنت أحد المجالات الأسرع نمواً من زاوية تطور البنية التحتية التقنية.[1] واليوم، تنتشر تكنولوجيا المعلومات والاتصالات (ICT) 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 توفر تكنولوجيا الاتصالات اللاسلكية عبر مسافات طويلة مثل تكنولوجيا WiMAX[5] (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 اليُسر.[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]

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[12] والتجارة الإلكترونية[13] والتعليم الإلكتروني[14] والصحة الإلكترونية[15] 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، يشكل الآن انتحال 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.[16]

كما تُعدّ تكاليف الخدمات المتاحة على الإنترنت أقل إلى حد كبير في أحيان كثيرة من تكاليف الخدمات المناظرة المتاحة خارج الشبكة.[17] فخدمات البريد الإلكتروني تتوافر في أحيان كثيرة مجاناً أو بتكلفة ضئيلة للغاية بالقياس إلى الخدمات البريدية التقليدية.[18] وموسوعة ويكيبديا[19] المتاحة على الخط يمكن استخدامها مجاناً، شأنها شأن المئات من الخدمات التي توفر البيانات على الخط.[20] وانخفاض التكلفة هو من الأهمية بمكان لأنه ييسر الانتفاع بالخدمات لأعداد أكبر من المستخدمين، من بينهم محدودي 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.[21] ويتيح تطور مجتمع المعلومات فرصاً كبيرة.[22] فالنفاذ دون عائق إلى المعلومات بمقدوره أن يدعم الديمقراطية، لأنه ينتزع تدفق المعلومات من سيطرة سلطات الدولة (كما حدث مثلاً في أوروبا الشرقية وشمال إفريقيا).[23] وقد حَسَّنت التطورات التقنية الحياة اليومية – وما الصرافة والتسوق على الخط، واستخدام خدمات البيانات المتنقلة، والمهاتفة عن طريق نقل الصوت بواسطة بروتوكول الإنترنت (VoIP) إلا بعض الأمثلة على مدى تغلغل تكنولوجيا المعلومات والاتصالات في حياتنا اليومية.[24]

غير أن نمو مجتمع المعلومات تصاحبه تهديدات جديدة وخطيرة.[25] فالخدمات الأساسية مثل الإمداد بالماء والكهرباء باتت تعتمد الآن على تكنولوجيا المعلومات والاتصالات.[26] كما تعتمد السيارات، وتنظيم المرور، والمصاعد، وتكييف الهواء، والهواتف على سلاسة أداء تكنولوجيا المعلومات والاتصالات.[27] ولذا، فإن الهجمات التي قد تشن الآن ضد البنية التحتية للمعلومات وخدمات الإنترنت بمقدورها إلحاق الأذى بالمجتمع بطرق جديدة وحرجة.[28]

وقد تعرضت البنية التحتية للمعلومات وتعرضت خدمات الإنترنت للهجمات بالفعل.[29] وما الاحتيال الذي يمارس على الخط وهجمات القرصنة إلا بعض الأمثلة على الجرائم المتعلقة بالحاسوب التي ترتكب على نطاق واسع كل يوم.[30] وتشير المعلومات إلى أن الضرر المالي الذي تسببه الجريمة السيبرانية هائل.[31] ففي عام 2003 وحده، سببت البرمجيات الخبيثة أضراراً وصل مقدارها إلى 17 مليار دولار أمريكي.[32] 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.[33]

وبناءً على البحوث التي نشرت في عام 2014 قد تصل الخسارة السنوية الإجمالية الناجمة عن الجريمة السيبرانية حتى 400 مليار دولار أمريكي.[34] ويعتقد نحو 60 في المائة من المؤسسات التجارية في الولايات المتحدة أن الجرائم السيبرانية[35] تُكبِّدها تكلفة أبهظ مما تلحقه بها الجرائم المادية. وتبين هذه التقديرات بوضوح أهمية حماية البنى التحتية للمعلومات.[36]

ومعظم الهجمات المذكورة أعلاه ضد البنية التحتية للحاسوب لا تستهدف بالضرورة البنية التحتية الحرجة. غير أن البرمجيات الضارة "Stuxnet" التي اكتشفت في 2010 تزيد من التهديد الذي تمثله الهجمات التي تركز على البنية التحتية الحيوية.[37] وركزت البرمجية التي تتضمن أكثر من 4 000 وظيفة،[38] على أنظمة الحاسوب التي تعمل ببرمجية تستخدم عادة للتحكم في البنية التحتية الحيوية.[39]

3.1 الأمن السيبراني والجريمة السيبرانية

تُعدّ الجريمة السيبرانية والأمن السيبراني من القضايا التي يمكن بالكاد الفصل بينها في بيئة موصلة بينياً. ومما يؤكد ذلك قرار الجمعية العامة للأمم المتحدة لعام 2010 بشأن الأمن السيبراني[40] الذي يتناول الجريمة السيبرانية باعتبارها أحد التحديات الكبرى.

ويؤدي الأمن السيبراني[41] دوراً هاماً في التنمية الراهنة لتكنولوجيا المعلومات وخدمات الإنترنت.[42] ويُعد 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.[43] 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.[44] 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.[45] ويمثل وضع ودعم استراتيجيات الأمن السيبراني عنصراً حيوياً في مكافحة الجريمة السيبرانية.[46]

وتُعدّ 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.[47] وفي هذا الصدد، اعترفت القمة العالمية لمجتمع المعلومات (WSIS)[48] بالمخاطر الحقيقية والهامة الناجمة عن عدم كفاية الأمن السيبراني وعن تفشي الجريمة السيبرانية. وترسم أحكام الفقرات من 108 إلى 110 من *برنامج عمل تونس بشأن مجتمع المعلومات*، الصادر عن *القمة العالمية لمجتمع المعلومات*،[49] وكذلك ملحق برنامج العمل هذا، خطة عمل تتيح لأصحاب المصلحة المتعددين أن يُنفِّذوا على المستوى الدولي *خطة عمل جنيف للقمة العالمية لمجتمع المعلومات*،[50] وتصف عملية التنفيذ التي سيشارك فيها أصحاب المصلحة المتعددون وفقاً لأحد عشر خط عمل، وتوزع المسؤوليات عن تيسير تنفيذ خطوط العمل 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.[51]

وفي هذا الصدد، قام الأمين العام للاتحاد الدولي للاتصالات، في 17 مايو 2007، بإطلاق البرنامج العالمي للأمن السيبراني (GCA)[52] 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؛ 2) التدابير التقنية والإجرائية؛ 3) الهياكل التنظيمية؛ 4) بناء القدرات؛ و5) التعاون الدولي.[53]

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.[54] 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.

ويُشكّل سَنّ 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.[55] ولا يعني وجود أحكام في القانون الجنائي تطبق على أفعال مماثلة ترتكب خارج الشبكة أن بالمقدور تطبيقها أيضاً على الأفعال المرتكبة على الإنترنت.[56] ولذا يُعد إجراء تحليل وافٍ للقوانين الوطنية الحالية أمراً حيوياً للوقوف على أي ثغرات محتملة.[57] وإلى جانب الأحكام الموضوعية للقانون الجنائي،[58] تحتاج الوكالات المعنية بإنفاذ القانون إلى الأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية.[59] وهذه التحقيقات تطرح هي ذاتها عدداً من التحديات.[60] فمرتكبو الجرائم يمكن أن يقوموا بأفعالهم من أي مكان في العالم تقريباً، وأن يتخذوا من التدابير ما يسعون به إلى إخفاء هويتهم.[61] والأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية يمكن أن تكون مختلفة بقدر ملموس عن الأدوات والصكوك المستخدمة في التحقيق في الجرائم العادية.[62]

4.1 البُعد الدولي للجريمة السيبرانية

تنطوي الجريمة السيبرانية في كثير من الأحيان على بُعد دولي.[63] 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[64]. ولدى التحقيق في الجريمة السيبرانية، يُعد التعاون الوثيق بين البلدان المعنية أمراً بالغ الأهمية.[65] بيد أن الاتفاقات المتعلقة بتبادل المساعدة القانونية تستند إلى إجراءات رسمية ومعقدة تُعد مستنزفة للوقت في كثير من الأحيان، وإضافة إلى ذلك

كثيراً ما لا تغفل التحقيقات الخاصة بالحاسوب.[66] ولذا، فإن مما يتسم بأهمية حاسمة وضع إجراءات تكفل الاستجابة السريعة للحوادث ولطلبات التعاون الدولي.[67]

وتؤسس عدد من البلدان نظامها الخاص بتبادل المساعدة القانونية على مبدأ "الإجرام المزدوج".[68] فتقتصر عادةً التحقيقات المنفذة على المستوى العالمي على الأفعال التي تجرمها البلدان المشاركة جميعاً. وعلى الرغم من أن هناك عدداً من الجرائم مثل توزيع المواد الإباحية التي يُستغل فيها الأطفال والتي يمكن ملاحقتها قضائياً في معظم النظم القضائية، فإن الفوارق الإقليمية تؤدي دوراً هاماً.[69] ومن أمثلة ذلك أنواع أخرى من المحتويات غير القانونية مثل الخطاب الذي يدعو إلى الكراهية. إذ يتباين تجريم المحتوى غير القانوني في البلدان المختلفة.[70] فالمواد التي يمكن توزيعها بشكل قانوني في بلد ما قد يكون توزيعها غير قانوني ببساطة في بلد آخر.[71]

وتُعدّ التكنولوجيا الحاسوبية المستخدمة حالياً في جميع أنحاء العالم تكنولوجيا واحدة من الناحية الأساسية.[72] 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 بروتوكولات الشبكة المستخدمة في القارة الإفريقية مماثلة لتلك المستخدمة في الولايات المتحدة.[73] فالتقييس يتيح للمستخدمين في كل أنحاء العالم النفاذ إلى الخدمات نفسها عن طريق الإنترنت.[74]

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.

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 (الاتفاقية بشأن الجريمة السيبرانية)،[75] ومع ذلك فإن مبادئ القانون الوطني تتغير بمعدل أبطأ كثيراً من وتيرة التطورات التقنية.[76]

وعلى الرغم من أن الإنترنت قد لا تعترف بالرقابة الحدودية، فإن هناك من الوسائل ما يتيح تقييد النفاذ إلى معلومات معينة.[77] 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").[78] وكلا النوعين من التدابير يمكن التحايل عليه، ولكنه يعد مع ذلك أداة يمكن استخدامها للاحتفاظ بفروق إقليمية في شبكة عالمية.[79] وتفيد تقارير مبادرة الشبكة المفتوحة (OpenNet Initiative)[80] أن هذا النوع من الرقابة يمارس في أكثر من عشرين دولة.[81]

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.[82] وإعداد هذه الصكوك وتنفيذها يستلزم وقتاً. وتعد تدابير الحماية التقنية كثيفة التكاليف بوجه خاص.[83] 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.[84]

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.[85] 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.

ويُعدّ 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.[86]

---

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

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

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

4 Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: 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 www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

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

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

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

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

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

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

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

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

14 See for example: *Molla*, The Impact of eReadingness on eCommerce Success in Developing Countries, 2004. See for example: *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 et seq.

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

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

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

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

19 www.wikipedia.org

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

57 For an overview of cybercrime-related legislation and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf;

Mitchison/Wilikens/Breitenbach/Urry/Portesi – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

58 See below: § 6.2.

59 See below: § 6.5.

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

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

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

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

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

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

66 See below: § 6.5.

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

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

69 See below: § 5.5. See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

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

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

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

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

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

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

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

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

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

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

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

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

82 See below:§ 4.

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

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

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

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

2 ظاهرة الجريمة السيبرانية

1.2 تعاريف

Bibliography (selected): *Carter,* Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney,* Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et seq., *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1; *Goodman,* Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469; *Goodman/Brenner,* The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No.2, page 144; *Gordon/Ford,* On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Hale,* Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; *Hayden,* Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004; *Wilson,* Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

تبدأ معظم التقارير والأدلة والمنشورات المتعلقة بالجريمة السيبرانية بتعريف مصطلحي "الجريمة المتصلة بالحاسوب" و"الجريمة السيبرانية".[87] وفي هذا السياق، اعتمدت نهج مختلف في العقود الأخيرة لوضع تعريف دقيق لكلا المصطلحين.[88] وقبل تقديم لمحة عامة عن مناقشة وتقييم هذه النهج، من المفيد تحديد العلاقة بين "الجريمة السيبرانية" و"الجرائم المتصلة بالحاسوب".[89] وبدون التطرق إلى التفاصيل في هذه المرحلة، فإن مصطلح "الجريمة السيبرانية" له معنى أضيق من مصطلح "الجرائم المتصلة بالحاسوب"[90] التي تتعلق بشبكة حاسوبية. وربما تشمل الجرائم المتصلة بالحاسوب الجرائم التي ليست لها علاقة بشبكة، وإن كانت تؤثر فقط على أنظمة حاسوبية قائمة بذاتها.

وخلال مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، وُضع تعريفان في إطار ورشة عمل ذات صلة:[91] وتشمل الجريمة السيبرانية بمعناها الضيق (الجريمة الحاسوبية) أي سلوكيات غير مشروعة موجهة عن طريق عمليات إلكترونية تستهدف أمن الأنظمة الحاسوبية والبيانات المعالجة بواسطة هذه الأنظمة. وتشمل الجرائم السيبرانية بمعنى أوسع (الجرائم المتصلة بالحاسوب) أي سلوكيات غير مشروعة تُرتكب عن طريق نظام أو شبكة حاسوبية أو فيما يتعلق بهما، بما في ذلك جرائم من قبيل حيازة غير قانونية لمعلومات وعرضها أو توزيعها بواسطة نظام أو شبكة حاسوبية.[92]

ويصف أحد التعاريف الشائعة الجريمة السيبرانية بأنها أي نشاط تستخدم فيه الحواسيب أو الشبكات كأداة أو هدف أو مكان لممارسة النشاط الإجرامي.[93] وينطوي هذا التعريف الواسع على عدة صعوبات. فإنه على سبيل المثال، يغطي الجرائم التقليدية مثل القتل، إذا قام الجاني بالمصادفة باستخدام لوحة مفاتيح لضرب الضحية وقتلها. ويرد تعريف آخر أوسع في المادة 1-1 من مشروع اتفاقية ستانفورد الدولية لتعزيز الحماية من الجريمة السيبرانية والإرهاب السيبراني (مشروع ستانفورد)[94] حيث ينص على أن الجريمة السيبرانية تشير إلى أفعال تتعلق بالأنظمة السيبرانية.[95]

وتحاول بعض التعاريف أن تأخذ المقاصد أو النوايا في الحسبان وتطرح توصيفاً أكثر دقة للجريمة السيبرانية،[96] 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".[97] وهذه التوصيفات الأكثر دقة تستبعد الحالات التي تستخدم فيها الأجهزة المادية لارتكاب جرائم عادية، لكنها قد تستبعد بذلك أيضاً جرائم تدرجها اتفاقات دولية مثل القانون النموذجي للكومنولث بشأن الجرائم الحاسوبية والجرائم المتصلة بالحاسوب أو اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في باب الجريمة السيبرانية.[98] ومن ذلك مثلاً، أن الشخص الذي ينتج أجهزة USB[99] تحتوي على برمجيات خبيثة تدمر البيانات الموجودة على الحواسيب عند توصيل تلك الأجهزة بها يكون قد ارتكب جريمة بمفهوم المادة 4 الجريمة السيبرانية.[100] ولكن نظراً لأن الفعل المتمثل في حذف البيانات، باستخدام جهاز مادي لاستنساخ شفرة ضارة، فعل لم يرتكب عن طريق الشبكات الإلكترونية العالمية، فإنه لن 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.

وتبين هذه النُّهُج المتنوعة والمشاكل ذات الصلة أن هناك صعوبات كبيرة تكتنف تعريف مصطلحي "الجريمة الحاسوبية" و"الجريمة السيبرانية".[101] 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 النهج القانونية الإقليمية والدولية المختلفة لمعالجة هذه المسألة مع استبعاده في الوقت نفسه الجرائم التقليدية التي تُيسَّر باستعمال الأجهزة المادية (العتاد). وعدم توافر تعريف واحد "للجريمة السيبرانية" لا ينبغي اعتباره أمراً ذا بال، ما دام هذا المصطلح لا يستخدم كمصطلح قانوني.[102] وبدلاً من الإشارة إلى تعريف، ستستند الفصول التالية إلى نهج متصل بالتصنيف.

2.2 تصنيف الجريمة السيبرانية

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

يُستعمل مصطلح "الجريمة السيبرانية" لتغطية مجموعة واسعة من السلوكيات الإجرامية.[103] ونظراً لأن الجرائم التي تم الوقوف عليها تشمل طائفة واسعة من الأفعال الإجرامية المختلفة، من الصعب وضع نظام لتصنيف الجريمة السيبرانية.[104] ويمكن العثور على أحد النهج في اتفاقية بشأن الجريمة السيبرانية[105] التي تفرق بين أربعة أنواع مختلفة من الجرائم:[106]

1. الجرائم التي تستهدف سرية البيانات والنظم الحاسوبية وتكامليتها وتيسُرها؛[107]
2. الجرائم المتعلقة بالحاسوب؛[108]
3. الجرائم المتعلقة بالمحتوى؛[109]
4. الجرائم المتعلقة بحقوق المؤلف.[110]

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"[111]؛ و"الجرائم المتعلقة بالمحتوى"؛[112] و"الجرائم المتعلقة بحقوق المؤلف".[113] أما الفئة الرابعة، وهي "الجرائم المتعلقة

بالحاسوب"،[114] فلا تركز على موضوع الحماية القانونية بل على الأسلوب المستخدم لارتكاب الجريمة. ويؤدي عدم الاتساق هذا إلى بعض التداخل بين الفئات.

وبالإضافة إلى ذلك، تغطي بعض المصطلحات المستخدمة لوصف الأفعال الإجرامية (مثل "الإرهاب السيبراني"[115] أو التصيُّد الاحتيالي"[116]) أفعالاً تندرج ضمن عدة فئات. ومع ذلك، فإن الفئات الأربع يمكن أن تشكل أساساً مفيداً لمناقشة ظاهرة الجريمة السيبرانية.

3.2 تطور الجرائم الحاسوبية والجرائم السيبرانية

إن الاستغلال الإجرامي لتكنولوجيا المعلومات والتعامل القانوني اللازم مع هذا الاستغلال من الأمور التي خضعت للدراسة منذ تبني التكنولوجيا. وخلال السنوات الخمسين الماضية نُفذت حلول مختلفة على الصعيدين الوطني والإقليمي. ومن الأسباب التي تجعل من هذا الموضوع تحدياً مستمراً، التطور التقني المستمر، فضلاً عن تغيّر الأساليب والطرق التي تُرتكب بها الجرائم باستمرار.

1.3.2 *ستينات القرن الماضي*

أدى إدخال أنظمة الحاسوب القائمة على الترانزستور، التي كانت أصغر حجماً وأقل تكلفة من الآلات القائمة على الصمامات المفرغة في ستينات القرن الماضي إلى زيادة استخدام تكنولوجيا الحاسوب.[117] وفي هذه المرحلة المبكرة، ركزت الجرائم على الأضرار المادية المتعلقة بأنظمة الحاسوب والبيانات المخزنة.[118] وجرى التبليغ عن حوادث كهذه، ففي كندا على سبيل المثال، حيث تسببت أعمال شغب قام بها طلاب في 1969 في حريق أدى إلى دمار بيانات أجهزة الحاسوب التي تستضيفها الجامعة.[119] وفي منتصف الستينات، بدأت الولايات المتحدة مناقشة بشأن إنشاء سلطة مركزية لتخزين البيانات الخاصة بجميع الوزارات.[120] وفي هذا السياق، نوقشت مسألة الاستغلال الإجرامي المحتمل لقواعد البيانات[121] وما يتصل بها من مخاطر[122] بالنسبة للخصوصية.[123]

2.3.2 *سبعينات القرن الماضي*

وفي السبعينات، ازداد كثيراً استخدام أنظمة الحاسوب والبيانات الحاسوبية.[124] وفي نهاية العقد، بلغ العدد المقدّر لأجهزة الحاسوب الرئيسية الكبيرة المشغَّلة في الولايات المتحدة 100 000 جهاز.[125] ومع انخفاض الأسعار، أصبحت تكنولوجيا الحاسوب تُستخدم على نطاق أوسع في الإدارة والأعمال التجارية ومن جانب الجمهور. وتميزت السبعينات بتحول من الجرائم التقليدية المتعلقة بالممتلكات ضد أنظمة الحاسوب[126] التي هيمنت على فترة الستينات، إلى أشكال جديدة من الجرائم.[127] ففي حين استمر الضرر المادي في كونه شكلاً ذا صلة بالاستغلال الإجرامي لأنظمة الحاسوب، جرى تحديد أشكال جديدة من الجريمة الحاسوبية. حيث شملت الاستخدام غير المشروع لأنظمة الحاسوب[128] والتلاعب بالبيانات الإلكترونية.[129] وأدى الانتقال من المعاملات اليدوية إلى المعاملات القائمة على استخدام الحاسوب إلى شكل جديد آخر للجرائم ألا وهو الاحتيال المتصل بالحاسوب.[130] وفي هذا الوقت كانت الخسائر الناجمة عن الاحتيال المتصل بالحاسوب قد وصلت إلى عدة ملايين من الدولارات.[131] وكان الاحتيال المتصل بالحاسوب[132]، على وجه الخصوص، يشكل تحدياً حقيقياً، وكانت وكالات إنفاذ القانون تقوم بتحقيقات في قضايا من هذا النوع على نحو متزايد.[133] ونظراً لأن تطبيق التشريعات القائمة في قضايا الجرائم المتصلة بالحاسوب[134] أدى إلى صعوبات[135] بدأ النقاش حول الحلول القانونية في مختلف أجزاء العالم.[136] وناقشت الولايات المتحدة مشروع قانون أُعد خصيصاً لمعالجة الجرائم السيبرانية.[137] وناقشت منظمة إنتربول الظواهر والإمكانيات المتعلقة بالاستجابة القانونية.[138]

3.3.2 *ثمانينات القرن الماضي*

وفي الثمانينات، أصبحت الحواسيب الشخصية أكثر انتشاراً بصورة متزايدة. ومع هذا التطور، ازداد عدد أنظمة الحاسوب ومن ثم عدد الأهداف المحتملة للمجرمين. وشملت الأهداف للمرة الأولى، مجموعة واسعة من البُنى التحتية الحرجة.[139] وكان من الآثار الجانبية لانتشار أنظمة الحاسوب زيادة الاهتمام بالبرمجيات مما أسفر عن ظهور الأشكال الأولى من قرصنة البرامج

والجرائم المتصلة ببراءات الاختراع.[140] وجلب التوصيل البيني لأنظمة الحاسوب أنواعاً جديدة من الجرائم.[141] ومكّنت الشبكات مرتكبي الجرائم من الدخول إلى أنظمة الحاسوب دون أن يكونوا حاضرين في مسرح الجريمة.[142] وبالإضافة إلى ذلك، فإن إمكانية توزيع البرمجيات عن طريق الشبكات مكّنت مرتكبي الجرائم من نشر البرمجيات الضارة، وتم اكتشاف المزيد من الفيروسات الحاسوبية.[143] وبدأت البلدان في تحديث تشريعاتها من أجل الوفاء بمتطلبات البيئة الإجرامية المتغيرة.[144] وشاركت المنظمات الدولية في هذه العملية أيضاً[145]. وأنشأت منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) ومجلس أوروبا[146] لجان دراسات لتحليل الظواهر وتقييم إمكانيات الاستجابة القانونية.

4.3.2 تسعينات القرن الماضي

أدى اعتماد السطح البيني البياني ("WWW") في التسعينات الذي أعقبه نمو سريع في عدد مستعملي الإنترنت إلى ظهور تحديات جديدة. فقد أصبحت المعلومات المتاحة قانوناً في بلد ما متاحة على الصعيد العالمي وحتى في البلدان التي تجرم نشر مثل هذه المعلومات[147]. وبرز شاغل آخر ارتبط بالخدمات المتاحة على الخط والتي أصبحت تشكل تحدّياً خاصاً فيما يتعلق بالتحقيق في الجريمة متعددة الجنسيات، ألا وهو سرعة تبادل المعلومات.[148] وأخيراً، تحوّل توزيع المواد الإباحية التي يُستغل فيها الأطفال من التبادل المادي للكتب والأشرطة إلى التوزيع على الخط من خلال المواقع الإلكترونية وخدمات الإنترنت.[149] وعلى الرغم من أن جرائم الحاسوب كانت جرائم محلية عموماً، حولت الإنترنت الجرائم الإلكترونية إلى جريمة متعددة الجنسيات. ونتيجة لذلك، بادر المجتمع الدولي إلى معالجة المسألة باهتمام أكبر. وليس قرار الجمعية العامة للأمم المتحدة 45/121 المعتمد في 1990[150] والدليل بشأن منع ومكافحة الجرائم المتصلة بالحاسوب الصادر في 1994 سوى مثالين بهذا الصدد.[151]

5.3.2 القرن الحادي والعشرون

وكما هو الحال في كل عقد من العقود السابقة، استمر اكتشاف اتجاهات جديدة في مجال جرائم الحاسوب والجرائم السيبرانية في القرن الحادي والعشرين. وفي العقد الأول من الألفية الجديدة هيمنت أساليب جديدة وبالغة التعقيد فيما يخص ارتكاب الجرائم مثل "التصيد الاحتيالي"[152]، والهجمات الروبوتية[153]، وظهور استخدام تكنولوجيا يصعب على هيئات إنفاذ القانون التعامل معها والتحقيق فيها مثل الاتصالات الصوتية[154] عبر بروتوكول الإنترنت (VoIP) و"الحوسبة السحابية".[155] ولم تتغير الأساليب فقط وإنما التأثير أيضاً. فمع قدرة مرتكبي الجرائم على أتمتة الهجمات، ارتفع عدد الجرائم. وبادرت البلدان والمنظمات الإقليمية والدولية إلى الاستجابة للتحديات المتزايدة وأعطت أولوية عالية للتصدي للجرائم السيبرانية. والتطورات الجديدة من قبيل "البيانات الكبيرة[156]" و"الأجهزة المحكومة[157]" و"الأجهزة الملبوسة" هي مجالات من المرجح أنها سوف تنتقل أكثر من ذي قبل إلى محط تركيز الجناة في المستقبل.

4.2 مدى انتشار أذى الجريمة السيبرانية وتأثيرها

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

يمكن للأوساط الأكاديمية وواضعي السياسات استخدام الإحصاءات المتعلقة بالجريمة كأساس للمناقشة وعملية صنع القرار.[158] وعلاوةً على ذلك، سيمكّن حصول وكالات إنفاذ القانون على معلومات دقيقة بشأن الحجم الحقيقي للجريمة السيبرانية من تحسين استراتيجيات مكافحة الجريمة السيبرانية ومنع الهجمات المحتملة وسن تشريعات أنسب وأكثر فعالية. ومع ذلك، من الصعب تقدير الأثر الكمي للجريمة السيبرانية على المجتمع استناداً إلى عدد الجرائم التي نفذت في فترة زمنية معينة.[159] ويمكن استقاء هذه البيانات بصورة عامة من الإحصاءات والدراسات الاستقصائية المتعلقة بالجريمة[160]، بيد أن هذين المصدرين ينجم عنهما تحديات عندما يتعلق الأمر باستخدامهما من أجل صياغة توصيات السياسة العامة.

1.4.2 الإحصاءات المتعلقة بالجرائم

أُخذت الأرقام التالية من الإحصاءات الوطنية المتعلقة بالجريمة. وعلى نحو ما سيجري بحثه باستفاضة أدناه، فإن هذه الإحصاءات لا يُقصد بها أن تمثل تطور الجريمة السيبرانية على الصعيد العالمي، أو المدى الحقيقي لانتشار الجريمة السيبرانية على الصعيد الوطني، وبذلك فهي تُعرض فقط لتوفير إطلالة عن المعلومات القطرية.

- بالنسبة لعام 2013، أعلن مركز الولايات المتحدة المعني بالشكاوى المتعلقة بالإنترنت عن زيادة بنسبة 48,8 في المائة في الخسائر المبلغ عنها مقارنة بأرقام عام 2012.[161]
- تشير الإحصاءات الألمانية المتعلقة بالجرائم إلى أن العدد الإجمالي للجرائم المتصلة بالإنترنت زاد في عام 2013 بنسبة 12,2 في المائة مقارنة بعام 2012.[162]

ومن غير الواضح معرفة مدى تعبير الإحصاءات عن انتشار الجريمة وما إذا كانت توفر معلومات موثوق بها بهذا الخصوص. وهناك العديد من الصعوبات المرتبطة بتحديد التهديد الذي تشكله الجريمة السيبرانية[163] على الصعيد العالمي بالاستناد إلى الإحصاءات المتعلقة بالجرائم.[164]

فقبل كل شيء، فإن الإحصاءات المتعلقة بالجريمة تُحسب على الصعيد الوطني ولا تعكس النطاق الدولي لهذه القضية. وحتى لو كان من الممكن نظرياً الجمع بين البيانات المتاحة، فإن هذا النهج لن يسفر عن معلومات موثوق بها نظراً لأوجه الاختلاف في التشريعات وممارسات التسجيل.[165] كما أن تجميع الإحصاءات الوطنية المتعلقة بالجريمة ومقارنتها يتطلب درجة معينة من التوافق[166] تكون غير متوفرة عندما يتعلق الأمر بالجريمة السيبرانية. وحتى لو تم تسجيل البيانات المتعلقة بالجريمة السيبرانية، فإنها لا تُدرج بالضرورة كرقم منفصل.[167] وعلاوةً على ذلك، تقتصر الإحصاءات على إدراج الجرائم التي يتم كشفها والتبليغ عنها. وفيما يتعلق بالجرائم السيبرانية بوجه خاص،[168] هناك مخاوف تتعلق بكون عدد الحالات غير المبلغ عنها كبيراً. وقد تخشى دوائر الأعمال التجارية[169] من أن الدعاية السلبية يمكن أن تضر بسمعتها.[170] فإذا أعلنت شركة عن أن قراصنة نفذوا إلى مخدمها، قد يفقد العملاء ثقتهم فيها. ويمكن أن تكون التكاليف والتبعات الإجمالية أكبر من الخسائر التي يتسبب فيها هجوم القرصنة. ومن ناحية أخرى، إذا لم يتم التبليغ عن المجرمين ومحاكمتهم، فقد يبادرون إلى تكرار جرائمهم. كما أن الضحايا قد لا يكونوا على ثقة من أن وكالات إنفاذ القانون ستكون قادرة على تحديد هوية المجرمين.[171] ومن خلال مقارنة العدد الكبير للجرائم السيبرانية مع التحقيقات القليلة الناجحة، فإنهم قد لا يرون جدوى من التبليغ عن الجرائم.[172] ونظراً لأن أتمتة الهجمات تمكّن مرتكبي الجرائم السيبرانية من اتباع استراتيجية لجني أرباح كبيرة من العديد من الهجمات التي تستهدف مبالغ ضئيلة (كما هو الحال بالنسبة إلى النصب عن طريق تحصيل رسوم مقدماً[173])، فإن الأثر المحتمل للجرائم غير المبلَّغ عنها يمكن أن يكون كبيراً. وبالنسبة إلى المبالغ الصغيرة، قد تفضل الضحايا عدم اللجوء إلى إجراءات التبليغ التي تستغرق وقتاً طويلاً. وغالباً ما تنطوي الحالات المبلغ عنها على مبالغ كبيرة جداً.[174]

وخلاصة القول، تُعد المعلومات الإحصائية مفيدة لاسترعاء الانتباه إلى استمرار أهمية هذه المسألة وتزايدها، ومن الضروري الإشارة إلى أن أحد التحديات الرئيسية المتصلة بالجريمة السيبرانية هو عدم توفر معلومات موثوق بها بشأن حجم المشكلة فضلاً عن الاعتقالات والمحاكمات والإدانات. وكما سبق ذكره، فإن الإحصاءات المتعلقة بالجرائم لا تشير عموماً إلى الجرائم بشكل منفصل، والبيانات الإحصائية المتاحة بشأن تأثير الجريمة السيبرانية غير قادرة بصفة عامة على توفير معلومات موثوق

بها بشأن حجم أو مدى انتشار الجرائم على نحو كافٍ بالنسبة لواضعي السياسات.[175] وبدون هذه البيانات، من الصعب قياس أثر الجريمة السيبرانية على المجتمع كمياً ووضع استراتيجيات للتصدي لهذه المسألة.[176] ومع ذلك، يمكن أن تعمل الإحصاءات كأساس لتحديد الاتجاهات وهو ما يمكن تحقيقه من خلال مقارنة النتائج لعدة سنوات، كما يمكن لهذه الإحصاءات أن تعمل كأداة إرشادية فيما يتعلق بعملية الإبلاغ عن الجريمة السيبرانية.[177]

2.4.2 الدراسات الاستقصائية

الأرقام التالية مأخوذة من دراسات استقصائية مختلفة. وعلى نحو ما سيجري بحثه أدناه باستفاضة، فإن هذه الأرقام ليست تمثيلية بالضرورة وبالتالي فهي تُقدم فقط لإعطاء نظرة شاملة عن نتائج هذه الدراسات الاستقصائية.

- المعلومات بشأن بطاقات الائتمان والحسابات المصرفية هي من بين أكثر المعلومات شيوعاً التي يعلن عنها في خدمات الاقتصاد غير الرسمي. وتتراوح الأسعار بين 0,85 و30 دولاراً أمريكياً (معلومات بشأن بطاقة ائتمان واحدة) وبين 15 و850 دولاراً أمريكياً (معلومات بشأن حساب مصرفي واحد).[178]
- في 2007، كانت عمليات الاحتيال المتعلقة بالمزاد من بين الأعمال الاحتيالية على الإنترنت التي احتلت الصدارة في الولايات المتحدة إذ بلغ متوسط الخسارة أكثر من 1 000 دولار أمريكي لكل عملية.[179]
- في 2005، بلغ مجموع الخسائر الناتجة عن الجرائم المتصلة بالهوية في الولايات المتحدة 56,6 مليار دولار أمريكي.[180]
- تختلف التكلفة المالية والشخصية للجريمة السيبرانية اختلافاً كبيراً بين فرادى الحوادث في أيرلندا، مما يولد تكاليف إجمالية تزيد عن 250 000 يورو.[181]
- استحدثت شركة واحدة لأمن الحاسوب أكثر من 450 000 توقيع شفري خبيث في ربع واحد من العام.[182]
- أبلغت ربع الشركات التي ردت على استبيان أُطلق في 2010 عن خسائر تشغيلية نتيجة لجرائم سيبرانية.[183]
- أبلغ المهنيون في مجال الأمن عن تناقص عدد هجمات رفض الخدمة وفيروسات الحاسوب بين عامي 2004 و2008.[184]
- في 2009، كانت الولايات المتحدة والصين والبرازيل وألمانيا والهند من بين أكثر البلدان التي أبلغت عن أنشطة خبيثة.[185]
- في 2014، بلغت تقديرات الخسارة السنوية العالمية بسبب الجريمة السيبرانية ما بين 375 و575 مليار دولار أمريكي.[186]
- ألمانيا، التي سجلت خسارة تقدر بما يعادل 1,6 في المائة من مجموع الناتج المحلي الإجمالي، هي الدولة الأكثر تضرراً من الجرائم السيبرانية.[187] وفي الولايات المتحدة تقدر الخسائر بنسبة 0,64 في المائة من الناتج المحلي الإجمالي، وفي البرازيل 0,32 في المائة من الناتج المحلي الإجمالي، وفي كينيا 0,01 في المائة.[188]
- متوسط تكلفة خرق البيانات هي 136 دولار أمريكي للفرد الواحد.[189] ونتيجة لهجوم قرصنة واحد، تناول قاعدة بيانات العملاء، تكبّدت شركة سوني تكاليف مباشرة بلغت حوالي 000 000 170 دولار أمريكي.[190]

وهناك العديد من الشواغل المتعلقة باستخدام مثل هذه الدراسات الاستقصائية في إطار تحديد مدى انتشار الجريمة السيبرانية وتأثيرها.

ومن الصعب إلى حد كبير تقديم تقديرات موثوق بها للخسائر المالية. وتقدر بعض المصادر الخسائر التي تلحق بالشركات والمؤسسات في الولايات المتحدة[191] من جراء الجريمة السيبرانية بمبلغ ضخم يصل إلى 67 مليار دولار أمريكي في عام واحد؛ ولكن ليس من المؤكد ما إذا كان استقراء نتائج عينة مستقاة من دراسة استقصائية أمراً مسوغاً.[192] ويصدق هذا النقد المنهجي لا على حجم الخسائر فحسب، بل يصدق أيضاً على عدد الجرائم التي تم الوقوف عليها.

وهناك صعوبة أخرى تتصل بالمعلومات الإحصائية تتمثل في أن المعلومات المنقولة تكون في كثير من الأحيان إما غير موثوق بها أو غير قابلة للتحقق منها. ويتعلق أحد هذه الأمثلة بالمعلومات الإحصائية بشأن الجوانب التجارية لاستغلال الأطفال في المواد الإباحية على الإنترنت. والعديد من التحليلات تفيد بأن الموقع الإلكتروني "TopTenReviews" مثلاً، قدّر أن استغلال الأطفال في المواد الإباحية على الإنترنت يولد 2,5 مليار دولار سنوياً في العالم.[193] بيد أن الموقع الإلكتروني"TopTenReviews" لا يقدم أي معلومات أساسية عن الطريقة التي تم بها البحث. وأخذاً بعين الاعتبار أن الموقع الإلكتروني "TopTenReviews" يدعي أن الشركة "*توفر لك المعلومات التي تحتاجها للقيام بعملية شراء مربحة. كما نقدم توصية بأفضل المنتجات في كل فئة. ومن خلال جداول المقارنة والأخبار والمقالات وأشرطة الفيديو المتاحة لدينا، فإننا نقوم بتبسيط عملية الشراء لدى المستهلك*"، وقد تكون هناك شواغل جادة فيما يتعلق باستخدام مثل هذه البيانات. وكشفت صحيفة "وول ستريت جورنال" في 2006[194] عن مثال آخر للأرقام التي تطلق دون مرجع قابل للتحقق. ولدى التحقيق في بيان يفيد بأن استغلال الأطفال في المواد الإباحية يمثل نشاطاً تجارياً تقدر أرباحه بمليارات الدولارات (20 مليار دولار سنوياً)، أفاد الصحفي أن وثيقتين رئيسيتين تحتويان على معلومات حول إيرادات تتراوح بين 3 و20 مليار دولار أمريكي، إحداهما عبارة عن منشور من المركز الوطني للأطفال المفقودين والمستغلين (NCMEC) والأخرى من مجلس أوروبا — تشيران إلى مؤسسات لم تؤكد هذه الأرقام.

ونظراً لأن الدراسات الاستقصائية تقتصر على تعداد الحوادث دون تقديم مزيد من المعلومات أو التفاصيل، من الصعب استخلاص استنتاجات فيما يتعلق بالاتجاهات. ومن الأمثلة المتاحة في هذا الصدد الدراسة الاستقصائية للجرائم الحاسوبية والأمن الحاسوبي لعام 2007، الصادرة عن معهد الأمن الحاسوبي في الولايات المتحدة، [195] التي تحلل اتجاهات شتى من بينها عدد ما تم ارتكابه من جرائم متعلقة بالحاسوب.[196] وتستند الدراسة إلى ردود 494 من المشتغلين بأمن الحواسيب في شركات ووكالات حكومية ومؤسسات مالية بالولايات المتحدة.[197] وتوثّق 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 اختراق النظام) قد انخفضت منذ عام 2001. ولا تشرح الدراسة سبب حدوث هذا الانخفاض.

وليس بمقدور الدراسات الاستقصائية المتعلقة بالجريمة السيبرانية أن توفر معلومات موثوق بها عن نطاق أو مدى انتشار الجرائم.[198] وعدم التيقن من مدى قيام المستهدفين بالجرائم بالإبلاغ عنها،[199] فضلاً عن عدم توافر تفسير لانخفاض عدد الجرائم السيبرانية، يجعلان هذه الإحصاءات عرضة للتأويلات. ولا تتيسّر في الوقت الحاضر أدلة كافية تتيح التنبؤ بالاتجاهات والتطورات التي يحملها المستقبل في طياته.

5.2 الجرائم التي تستهدف سرية البيانات والأنظمة الحاسوبية وتكامليتها وتيسرها

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

www.aic.gov.au/publications/tandi2/tandi329t.html; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.250; Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 et seq.

تستهدف جميع الجرائم المندرجة في هذه الفئة واحدة (على الأقل) من المبادئ القانونية الثلاثة المتمثلة في السرية، والتكاملية، والتيسُّر. وخلافاً للجرائم التي غطاها القانون الجنائي منذ قرون (مثل السرقة أو القتل)، فإن تَحَوسُب الجرائم أمر حديث نسبياً، لأن الأنظمة والبيانات الحاسوبية لم تستحدث إلا منذ ما يقرب من ستين عاماً.[200] 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.[201] ويقدم هذا الفرع لمحة عامة عن أكثر الجرائم التي تندرج في هذه الفئة شيوعاً.

1.5.2 النفاذ غير القانوني (القرصنة، التسلل)[202]

تشير الجريمة التي توصف بـ "القرصنة" إلى نفاذ غير قانوني إلى نظام حاسوبي،[203] وهي واحدة من أقدم الجرائم المتعلقة بالحاسوب.[204] وفي أعقاب تطور الشبكات الحاسوبية (ولا سيما الإنترنت)، أصبحت هذه الجريمة ظاهرة واسعة النطاق.[205] وتشمل الجهات الشهيرة التي استهدفتها هجمات القرصنة الإدارة الوطنية للملاحة الجوية والفضاء بالولايات المتحدة (NASA) (ناسا)، والقوات الجوية للولايات المتحدة، والبنتاغون، وياهو، وغوغل، وإباي (eBay)، والحكومة الألمانية.[206]

وتشمل أمثلة جرائم القرصنة اختراق كلمة السر الخاصة بمواقع الويب المحمية بكلمة سر،[207] والالتفاف على الحماية المكفولة لكلمة السر على أي نظام حاسوبي. غير أن الأعمال المتصلة بتعبير "القرصنة" تشمل أيضاً الأفعال التحضيرية مثل استخدام الأجهزة أو البرمجيات بطريقة معيبة من أجل الحصول بطريقة غير قانونية على كلمة السر للدخول إلى نظام حاسوبي،[208] وإنشاء مواقع "إيهامية" على شبكة الويب لجعل المستخدمين يفصحون عن كلمات السر الخاصة بهم،[209] وتركيب أجهزة وبرمجيات تعتمد على أساليب تسجل كل نقرة تضرب على لوحة المفاتيح – وبالتالي أي كلمة سر تستخدم على الحاسوب و/أو الجهاز.[210]

وتتباين دوافع مرتكبي هذه الجرائم. فبعضهم يُقصر أنشطته على الالتفاف على التدابير الأمنية لمجرد إثبات ما يتمتعون به من قدرات.[211] ويتصرف آخرون بوحي من دافع سياسي (يُعرف باسم "القرصنة الحركية"[212]) – ومن الأمثلة عليه حادث تعرض له مؤخراً الموقع الرئيسي للأمم المتحدة على شبكة الويب.[213] ومع ذلك، في 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 (DoS).[214] وفي معظم الحالات، لا يمثل النفاذ غير المشروع إلى النظام الحاسوبي إلا خطوة أولى حيوية.[215]

ويسلم كثير من المحللين بارتفاع عدد محاولات النفاذ غير المشروع إلى الأنظمة الحاسوبية، إذ سُجل في شهر أغسطس وحده من عام 2007 ما يربو على 250 مليون حادث من هذا النوع في العالم.[216] ويعزى تزايد عدد هجمات القرصنة إلى ثلاثة عوامل رئيسية هي: قصور ونقص الحماية الموفرة للنظم الحاسوبية واستحداث أدوات برمجياتية تُؤتمت الهجمات وتنامي دور حواسيب الأفراد باعتبارها هدفاً لهجمات القرصنة.

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.[217] ويبين التحليل الذي أجرته جامعة مريلاند أن النظام الحاسوبي غير المحمي الموصول بالإنترنت سيتعرض على الأرجح لإحدى الهجمات خلال أقل من دقيقة واحدة.[218] 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.[219]

استحداث أدوات برمجياتية تُؤتمت الهجمات

ما برحت تستخدم في الآونة الأخيرة أدوات برمجياتية تستهدف أتمتة الهجمات.[220] ويستطيع أحد الجناة منفرداً، مستعيناً ببرمجيات وبهجمات سابقة التبييت، أن يشن خلال يوم واحد هجمات على آلاف النظم الحاسوبية غير مستخدم في ذلك سوى حاسوب واحد.[221] أما إذا أتيح للجاني النفاذ إلى مزيد من الحواسيب – وذلك مثلاً من خلال شبكة مُسَخَّرة[222] – لاستطاع 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 المعيَّرة تتوافر بصورة واسعة على شبكة الإنترنت[223] – بعضها مجاناً لكن أشدها كفاءة قد تصل تكلفته بسهولة إلى عدة آلاف من الدولارات الأمريكية.[224] 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.[225]

تنامي دور حواسيب الأفراد باعتبارها هدفاً لهجمات القرصنة

لا يشكل النفاذ إلى النظام الحاسوبي في كثير من الأحيان الدافع الرئيسي للهجوم.[226] ولما كانت حواسيب الشركات تتمتع بوجه عام بحماية أفضل من حواسيب الأفراد، فمن الأصعب شن الهجمات على حواسيب الشركات باستخدام أدوات برمجياتية سابقة التشكيل.[227] 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 المسخّرة الخاضعة لهم فيستخدمون تلك الحواسيب في مزيد من الأنشطة الإجرامية.[228]

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.[229] 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؛[230] أو لمرتكب الفعل نوايا ضارة؛[231] إذا تم الحصول على بيانات أو تعديلها أو إتلافها. وثمة نظم قانونية أخرى لا تجرم النفاذ في حد ذاته بل تركز على الجرائم اللاحقة عليه.[232]

ويُظهر تحليل أكثر حداثة اتجاهاً نحو هجمات هادفة وأكثر تطوراً بالإضافة إلى الهجمات العارمة الواسعة النطاق التي هيمنت في العقود السابقة.[233] وبينما تتبع الهجمات الواسعة النطاق نهجاً انتهازياً ويمكن تنفيذها على نحو أسهل، فإن الهجمات الهادفة تتطلب المزيد من الطاقة من جانب الجاني ولكنها أكثر فعالية وضرراً[234] بشكل ملحوظ بالنسبة للضحية.[235]

2.5.2 حيازة البيانات بطريقة غير مشروعة (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.[236] ويتنامى استخدام الإنترنت للحصول على الأسرار التجارية.[237] وقيمة المعلومات الحساسة، والقدرة على النفاذ إليها عن بُعد، يجعلان التجسس

على البيانات محط اهتمام كبير. وفي ثمانينات 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 من بلدان مختلفة.[238]

ويستخدم الجُناة تقنيات مختلفة للنفاذ إلى حواسيب الضحايا،[239] تشمل برمجيات تمسح المنافذ غير المحمية،[240] أو برمجيات تتحايل على تدابير الحماية،[241] فضلاً عن "الهندسة الاجتماعية".[242] والنهج الأخير على وجه الخصوص، 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.[243] وفي سياق النفاذ غير القانوني، فإنه يصف كذلك التلاعب بالبشر بغرض النفاذ إلى النظم الحاسوبية.[244] وتعد الهندسة الاجتماعية عادةً ناجحة للغاية، لأن أضعف حلقة في أمن الحاسوب تتمثل أحياناً كثيرة في المستخدمين الذين يقومون بتشغيل النظام الحاسوبي. ومن ذلك مثلاً، "التصيُّد الاحتيالي" الذي أصبح مؤخراً من الجرائم الرئيسية التي ترتكب في الفضاء السيبراني،[245] 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 باستخدام الهندسة الاجتماعية. ونتيجة لذلك ينبغي لتوعية المستخدمين أن تشكل جزءاً جوهرياً في أي استراتيجية لمكافحة الجريمة السيبرانية.[246] وإضافة إلى ذلك، يمكن اتخاذ تدابير تقنية لمنع النفاذ غير القانوني. وتسلط منظمة التعاون والتنمية في الميدان الاقتصادي الضوء على أهمية التجفير بالنسبة للمستخدمين، لأن بمقدوره أن يساعد على تحسين حماية البيانات.[247] 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.[248] فنجاح الجناة في الحصول على معلومات حساسة يُعزى في أحيان كثيرة إلى غياب تدابير الحماية. ونظراً لزيادة تخزين المعلومات الهامة في النظم الحاسوبية، من الضروري تقييم ما إذا كانت تدابير الحماية التقنية التي يتخذها المستعملون كافية، أو ما إذا كان واضعو القوانين بحاجة إلى فرض حماية إضافية من خلال تجريم التجسس على البيانات.[249]

وعلى الرغم من أن الجناة يستهدفون عادةً الأسرار التجارية، فإن البيانات المخزنة في حواسيب الأفراد تُستهدف بدورها على نحو متزايد.[250] فالمستخدمون الأفراد كثيراً ما يخزنون المعلومات المتعلقة بالحسابات المصرفية وبطاقات الائتمان الخاصة بهم على حواسيبهم.[251] ويستطيع الجناة استخدام هذه المعلومات في أغراضهم الخاصة (كاستغلال بيانات الحسابات المصرفية في تحويل أموال) أو بيعها لطرف ثالث.[252] فسجلات بطاقات الائتمان مثلاً تباع بمبلغ يصل إلى 60 دولاراً أمريكياً.[253] وتركيز القراصنة على حواسيب الأفراد أمر لافت للنظر، لأن الأرباح التي يمكن جَنيها 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 الجيدة، فإن التجسس على البيانات المخزنة في حواسيب الأفراد يكون على الأرجح أعلى ربحاً.

وهناك نهجان للحصول على المعلومات. حيث يمكن للجناة النفاذ إلى نظام حاسوبي أو جهاز لتخزين البيانات واستخلاص المعلومات أو محاولة التلاعب بالمستعمل لحمله على الإفصاح عن المعلومات أو شفرات النفاذ التي تمكن الجناة من النفاذ إلى المعلومات ("التصيّد الاحتيالي").

ويستخدم الجناة في أحيان كثيرة الأدوات الحاسوبية المركبة في حواسيب الضحايا أو برمجيات خبيثة تُدعى برمجيات التجسس في نقل البيانات إليهم.[254] قد اكتشفت في السنوات الأخيرة أنواع مختلفة من برمجيات التجسس، مثل مسجلات النقرات على لوحة المفاتيح.[255] ومسجلات النقرات على لوحة المفاتيح هذه هي أدوات برمجياتية تسجل كل نقرة تُوقَّع على لوحة مفاتيح حاسوب مصاب.[256] 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[257]) كي لا تنقل إلا أهم البيانات المكتشفة. وتتوافر أيضاً أجهزة مماثلة في صورة أجهزة عَتادية توصَّل بين لوحة المفاتيح والنظام الحاسوبي لتسجيل النقرات الموقَّعة على لوحة المفاتيح. ومسجلات النقرات العتادية من الصعب تركيبها واكتشافها، لأنها تتطلب النفاذ المادي إلى النظام الحاسوبي.[258] ولذا، فإن أدوات مكافحة برمجيات التجسس والفيروسات تعجز إلى حد كبير عن اكتشافها.[259]

وإلى جانب النفاذ إلى النظم الحاسوبية، يستطيع الجناة أيضاً 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 باستعمال تقنيات الهندسة الاجتماعية.[260] وقد أصبح "التصيد الاحتيالي" مؤخراً واحدة من أهم الجرائم المتعلقة بالفضاء السيبراني.[261] 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.[262]

وقد غيرت التطورات من قبيل "البيانات الكبيرة"، حيث تجمع الشركات كميات كبيرة من البيانات من أجل إجراء تحليل متطور، من أهمية خرق البيانات في مسرح التهديدات. فإذا تمكن الجناة من النفاذ إلى قواعد بيانات كبيرة بما فيها من بيانات شخصية عن العملاء فإن مجرد خرق البيانات يمكن أن يسفر عن تحمل تكاليف كبيرة من جانب الشركة المتضررة – حتى لو لم يستخدم الجناة البيانات لارتكاب جرائم أخرى.[263] ويبلغ متوسط تكلفة خرق البيانات 136 دولار للفرد الواحد.[264] ونتيجة لهجوم قرصنة واحد تناول قاعدة بيانات العملاء، تكبدت شركة سوني تكاليف مباشرة بلغت حوالي 000 000 170 دولار أمريكي.[265]

وتشير البحوث التي نشرت في عام 2014 إلى أن كمية البيانات المتاحة في الأسواق السيبرانية السوداء، التي تم الحصول عليها من خلال خرق البيانات، تتضمن بيانات اعتماد عما يصل إلى 360 مليون حساب.[266]

3.5.2 الاعتراض غير القانوني

يستطيع الجناة أن يعترضوا الاتصالات بين المستخدمين[267] (مثل الرسائل الإلكترونية) أو أي أشكال أخرى من عمليات نقل البيانات (لدى قيام المستخدمين بتحميل البيانات على مُخدّم على الويب، أو النفاذ إلى وسائط للتخزين الخارجي معتمدة على الويب[268]) من أجل تسجيل البيانات التي يجري تبادلها. وفي هذا السياق، يستطيع الجناة بصورة عامة 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[269]).

وتتمتع معظم عمليات نقل البيانات بين موفري البنية التحتية للإنترنت أو مقدمي خدمة الإنترنت بحماية جيدة ومن الصعب اعتراضها.[270] غير أن الجناة يبحثون عن النقاط الضعيفة في النظام. وتتمتع التكنولوجيات اللاسلكية بشعبية أكبر، وتبين خبرة الماضي أنها قليلة المنعة.[271] 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.[272] وبمقدور الجناة الذين يريدون أن يعترضوا عملية لتبادل البيانات أن يقوموا بذلك من أي موقع داخل هذه الدائرة. وحتى عندما تكون الاتصالات اللاسلكية مجفرة، قد يستطيع الجناة أن يفكوا تجفير البيانات المسجلة.[273]

وكي ما يتمكن الجناة من النفاذ إلى المعلومات الحساسة، ينشئ بعضهم نقاط نفاذ بالقرب من المواقع التي يوجد بها طلب مرتفع على النفاذ اللاسلكي[274] (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.

ولا يمنع استخدام الخطوط الثابتة الجناة من اعتراض الاتصالات.[275] فعمليات نقل البيانات التي تمر عبر السلك تصدر عنها طاقة كهرمغنطيسية.[276] وإن استخدم الجناة المعدات الصحيحة، لكان باستطاعتهم أن يكشفوا ويسجلوا هذه الانبعاثات[277] وربما تمكنوا من تسجيل عمليات نقل البيانات بين حواسيب المستخدمين والشبكة الموصولين بها، وكذلك داخل النظام الحاسوبي.[278]

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.[279]

4.5.2 التدخل في البيانات

تتسم البيانات الحاسوبية بأهمية حيوية للمستخدمين الأفراد وللشركات والإدارات لأن هذه الأطراف تعتمد جميعاً على تكاملية البيانات وتيسُرها.[280] والعجز عن النفاذ إلى البيانات يمكن أن يسفر عن ضرر (مالي) كبير. ويستطيع المهاجمون أن ينتهكوا تكاملية البيانات وأن يتدخلوا فيها عن طريق[281] حذف البيانات أو حجبها أو تحويرها. ومن الأمثلة الشائعة لحذف البيانات الفيروس الحاسوبي.[282] ومنذ البدايات الأولى لاستحداث التكنولوجيا الحاسوبية، كانت الفيروسات الحاسوبية تهدد المستخدمين الذين لم يقوموا بتركيب وسائل الحماية السليمة.[283] ومنذ ذلك الحين، ما برح عدد الفيروسات الحاسوبية يتزايد بدرجة ملموسة.[284] ولم يتزايد عدد هجمات الفيروسات فقط وإنما تغيرت تقنيات الفيروسات ووظائفها أيضاً (الحمولة المؤثرة).[285]

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.[286] 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)[287] قد أصابت 90% من النظم الحاسوبية القليلة المنعة في غضون عشرة دقائق من توزيعها.[288] ويقدر الضرر المالي الذي تسببت فيه الهجمات الفيروسية في عام 2000 وحده بنحو 17 مليار دولار أمريكي.[289] وظل هذا الضرر كبيراً في عام 2003 إذ بلغ آنذاك ما يربو على 12 مليار دولار أمريكي.[290]

وتقوم معظم الفيروسات الحاسوبية المنتمية إلى الجيل الأول إما بحذف بيانات أو بعرض رسائل. وقد تنوعت الحمولات المؤثرة في الآونة الأخيرة.[291] فقد أصبحت الفيروسات الحديثة قادرة على تركيب أبواب خلفية تمكن الجناة من التحكم عن بُعد 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.[292]

واستناداً إلى تقارير نشرتها الشركات الأمنية فإن عدد فيروسات الحاسوب وغيرها من أشكال البرمجيات الخبيثة يتزايد بشكل مستمر بما يصل إلى 30 مليون سليلة برمجية خبيثة جديدة سنوياً.[293] وتُبلغ مختبرات كاسبيرسكي أنها كشفت في عام 2013 عن أكثر من 300 000 ملف خبيث جديد كل يوم.[294] وبما أن غالبية هذه الأرقام تنشرها شركات أمنية تبيع البرمجيات المضادة للفيروسات فهذا يمثل بالتأكيد تحدياً من حيث موثوقية هذه البيانات. ولكن التطور يشير إلى أنه بعد عقود من اكتشاف أول فيروس حاسوبي ما زالت البرمجيات الخبيثة تمثل تحدياً كبيراً لسلامة الإنترنت.

5.5.2 التدخل في النظم

لا تختلف الشواغل المتعلقة بالهجمات الموجهة ضد البيانات الحاسوبية عن شواغل 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.[295] وإذا نجح الجناة في منع النظم الحاسوبية من العمل بشكل سلس لألحق هذا خسائر مالية ضخمة بالضحايا.[296]

ويمكن شن الهجمات عن طريق القيام بهجمات مادية على النظم الحاسوبية.[297] ولو تمكن الجناة من النفاذ إلى النظام الحاسوبي لأصبح بمقدورهم أن يدمروا المعدات. وبالنسبة لمعظم النظم القانونية، لا تطرح حالات الهجوم المادي عن بُعد 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.[298]

وتطرح الخدع الاحتيالية مزيداً من التحديات على النظم القانونية. ومن أمثلة الهجمات المنفذة عن بُعد ضد النظم الحاسوبية ما يلي، الديدان الحاسوبية،[299] والهجمات الرامية إلى الحرمان من النفاذ إلى الخدمة (DoS).[300]

والديدان الحاسوبية[301] 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 عرقلة التشغيل السلس للنظام الحاسوبي باستخدام موارد النظام من أجل استنساخ ذاتها على الإنترنت، أو توليد 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.[302] فعن طريق استهداف نظام حاسوبي بطلبات تفوق قدرته على مناولتها، 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 وإباي (eBay) وأمازون.[303] وقد جرى التبليغ عن هجمات شبيهة في 2009 على مواقع إلكترونية حكومية وتجارية في الولايات المتحدة وكوريا الجنوبية.[304] وأسفر ذلك عن عدم تيسر بعض الخدمات لعدة ساعات بل ولعدة أيام.[305]

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،[306] 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.

على الرغم من تطور أدوات الوقاية التقنية واستراتيجيات التخفيف، ما زالت هجمات إنكار الخدمة تمثل تحدياً للشركات والمؤسسات الحكومية. وتشير بعض البحوث إلى أن خطر هذه الهجمات والتكاليف ذات الصلة في تزايد.[307]

6.2 الجرائم المتعلقة بالمحتوى

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

Victimization Study, 2005; *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/.

تغطي هذه الفئة المحتوى الذي يعتبر غير قانوني، ويشمل ذلك استغلال الأطفال في المواد الإباحية، والمواد الحاضّة على كراهية الأجانب، أو توجيه الإهانات إلى الرموز الدينية.[308] ووضع صكوك قانونية للتعامل مع هذه الفئة يعد أشد تأثراً إلى حد بعيد بالنُّهُج 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،[309] ولكنه يمكن أن يكون مشمولاً بالحماية بموجب مبدأ حرية التعبير[310] في الولايات المتحدة.[311] كما أن استخدام عبارات مسيئة للنبي أمر مجرم في كثير من البلدان العربية،[312] ولكن ليس في بعض البلدان الأوروبية.

وينبغي ألاّ تتعارض النهج القانونية لتجريم المحتوى غير المشروع مع الحق في حرية التعبير. ويُعرّف الحق في حرية التعبير على سبيل المثال بالمبدأ 1 (ب) من مبادئ جوهانسبرغ بشأن الأمن الوطني وحرية التعبير.[313] غير أن المبدأ 1 (ج) يوضح أن الحق في حرية التعبير يمكن أن يكون خاضعاً لقيود. وعلى الرغم من أن تجريم المحتوى غير المشروع ليس مستبعداً في حد ذاته، فإنه يجب أن يكون محدوداً للغاية. وتُناقش هذه القيود فيما يتعلق بتجريم التشهير بوجه خاص.[314] ويشير الإعلان المشترك لعام 2008 لمقرر الأمم المتحدة الخاص المعني بحرية الرأي والتعبير وما إلى ذلك إلى أنه ينبغي عدم تجريم مفاهيم غامضة مثل توفير الاتصالات وتمجيد الإرهاب أو التطرف والترويج لهما.[315]

وتُعدّ هذه التحديات القانونية مركبة، لأن المعلومات التي تستخدم في أحد البلدان يمكن النفاذ إليها من أي مكان آخر في العالم تقريباً.[316] 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.[317]

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.[318]

وتُتبع 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.[319] ويتمثل الحل الآخر في تركيب برمجيات ترشيح حواسيب المستعملين (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).[320]

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)[321] أن هذا النوع من الرقابة يمارس في الوقت الحاضر في أكثر من عشرين بلداً.[322]

1.6.2 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؛[323]
- النفاذ العالمي،[324] 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[325]) – وهذا الجانب يحظى بتقدير مستهلكي المواد الإباحية، بحكم الآراء الاجتماعية السائدة.

ووقفت بحوث أجريت مؤخراً على أن الإنترنت يتوافر عليها في أي وقت نحو 4,2 ملايين موقع إباحي.[326] وإلى جانب مواقع الويب، يمكن توزيع المواد الإباحية عن طريق التبادل باستخدام نظم تقاسم الملفات؛[327] وأنظمة الرسائل الفورية.

وتجرم مختلف البلدان 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،[328] ساعية بذلك إلى حماية القصر.[329] وتبين الدراسات أن نفاذ الأطفال إلى المواد الإباحية يمكن أن يؤثر تأثيراً سلبياً على تطورهم.[330] وامتثالاً لهذه القوانين، استحدثت "نظم للتحقق من بلوغ السن".[331] وتجرم بلدان أخرى أي تبادل للمواد الإباحية حتى بين الكبار،[332] مع التركيز على مجموعات بعينها (مثل القُصَّر).

ويمثل منع النفاذ إلى المواد الإباحية تحدياً أمام البلدان التي تجرم التعامل مع هذه المواد. وخارج الإنترنت تستطيع السلطات في كثير من الحالات 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 تمكّنها من إلزام مقدمي الخدمة بإزالة المحتوى المشين.

ومبدأ *السيادة الوطنية* لا يسمح بوجه عام لبلد من البلدان بأن يجري تحقيقات داخل أراضي بلد آخر، دون إذن من السلطات المحلية.[333] وحتى عندما تلتمس السلطات دعم البلدان التي تعمل انطلاقاً من مواقع الويب المشينة، فإن نجاح التحقيقات والعقوبات الجنائية قد يعوقه مبدأ "الإجرام المزدوج".[334]

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[335]) للحد من فرص النفاذ إلى مواقع معينة على الويب.[336]

2.6.2 استغلال الأطفال في المواد الإباحية

أصبحت شبكة الإنترنت قناة رئيسية لتوزيع المواد الإباحية التي يُستغل فيها الأطفال. وفي السبعينات والثمانينات من القرن الماضي، واجه الجناة الذين كانوا يقومون بتبادل المواد الإباحية التي يُستغل فيها الأطفال تهديدات خطيرة.[337] وفي ذلك الوقت، كانت السوق التجارية للمواد الإباحية التي يُستغل فيها الأطفال تركز أساساً على أوروبا والولايات المتحدة[338] وكانت المواد تُنتج محلياً وكانت باهظة الثمن ويصعب الحصول عليها.[339] وكانت نُهج شراء أو بيع المواد الإباحية التي يستغل فيها الأطفال تنطوي على عدد من المخاطر التي لم تعد موجودة اليوم بالمرة أو على الأقل ليست بالكثيرة. وفي الماضي، لم تكن للمنتجين القدرة على تطوير التصوير الفوتوغرافي والأفلام.[340] وكانوا يعتمدون على الخدمات المقدمة من الشركات، مما كان يزيد من الفرص المتاحة لوكالات إنفاذ القانون لتحديد المواد الإباحية التي يُستغل فيها الأطفال من خلال التقارير الواردة من الشركات القائمة بالتطوير.[341] وسمح توفر كاميرات الفيديو بتغيير هذا الوضع للمرة الأولى.[342] ولكن لم تتعلق المخاطر بالإنتاج فقط. وبالمثل كان الحصول على المواد الإباحية محفوفاً بالمخاطر بالنسبة للجناة. وكانت الطلبات تتم عن طريق الاستجابة للإعلانات المنشورة في الصحف.[343] وكانت وسائل الاتصال بين البائع والمحصِّل، ومن ثم السوق نفسها، محدودة.[344] وكانت المواد الإباحية التي يُستغل فيها الأطفال حتى منتصف التسعينات، تُنقل أساساً من خلال الخدمات البريدية، وأدت التحقيقات الناجحة إلى الكشف عن عدد كبير من الجناة.[345] وفي رأي الخبراء، كان إنفاذ القانون في ذلك الوقت قادراً على مواجهة التحديات.[346]

وقد تغير هذا الوضع تغييراً جذرياً مع توفر تطبيقات تبادل البيانات عبر شبكة الإنترنت. وبينما كان إنفاذ القانون في الماضي يتعامل مع مواد تماثلية، أصبحت الغالبية العظمى من المواد المكتشفة اليوم ذات طابع رقمي.[347] ومنذ منتصف التسعينات،

استخدم الجناة خدمات الشبكة على نحو متزايد لتوزيع هذه المواد.[348] وتم الاعتراف بالمشاكل الناجمة عن ذلك من حيث الكشف والتحقيق في القضايا المتعلقة بهذه المواد الإباحية.[349] وتُعد شبكة الإنترنت اليوم القناة الرئيسية للاتجار بالمواد الإباحية العادية،[350] فضلاً عن المواد الإباحية التي يُستغل فيها الأطفال.[351]

ويمكن تحديد عدة أسباب للانتقال من التوزيع التماثلي إلى التوزيع الرقمي. فشبكة الإنترنت تعطي للمستعملين الأقل مهارة من الناحية التقنية انطباعاً بقدرتهم على التصرف بشكل غير ظاهر للآخرين. وإذا كان مرتكب الجريمة لا يستعمل تكنولوجيا الاتصالات المجهولة المصدر، فإن هذا الانطباع خاطئ. ولكن استخدام وسائل متطورة للاتصالات المجهولة يمكن أن يعوق التعرف على الجاني، وهو أمر يدعو إلى القلق فيما يتعلق بتبادل المواد الإباحية على الخط.[352] وإضافة إلى ذلك، دُعم هذا التطور بانخفاض أسعار الأجهزة والخدمات التقنية التي تستخدم للإنتاج والاتجار في المواد الإباحية التي يُستغل فيها الأطفال، مثل أجهزة التسجيل وخدمات الاستضافة.[353] وحيث إن مواقع الويب وخدمات الإنترنت متاحة لحوالي مليارين من المستعملين، فإن عدد العملاء المحتملين ازداد أيضاً. وهناك مخاوف من أن سهولة النفاذ إلى الإنترنت تجتذب الناس الذين لم يكونوا ليخاطروا إلى الحصول على المواد الإباحية خارج الإنترنت.[354] ومع التحول من وسائط الإعلام التماثلية إلى وسائط الإعلام الرقمية، جرى التبليغ عن عدد متزايد من الصور الإباحية التي يُستغل فيها الأطفال تم كشفها من خلال التحقيقات.[355] والجانب الآخر الذي يرجح أن يكون قد دعم هذا التطور هو أن المعلومات الرقمية يمكن إنتاج نسخ كثيرة منها عموماً دون فقدان الجودة.[356] وبينما كان فقدان الجودة بسبب الاستنساخ يشكل عائقاً في الماضي أمام مستهلكي المواد الإباحية التي يُستغل فيها الأطفال الذين يرغبون في استنساخ المواد والاتجار بها، أصبح من الممكن اليوم أن يكون ملف تم تنزيله مصدراً للمزيد من عمليات الاستنساخ.[357] ومن نتائج هذا التطور هو أنه، حتى عندما يتم القبض على الجاني الذي أنتج هذه المواد في البداية ومصادرة ملفاته، يصبح من الصعب "إزالة" الملفات بعد أن تم تداولها عبر الإنترنت.[358]

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.[359] وتشارك منظمات دولية في مكافحة ما يُنشر على الخط من مواد إباحية يُستغل فيها الأطفال،[360] وطرحت في هذا الصدد عدة مبادرات قانونية دولية تشمل فيما تشمله: اتفاقية الأمم المتحدة لحقوق الطفل لعام 1989؛[361] والمقرر الإطاري لمجلس الاتحاد الأوروبي بشأن مكافحة الاستغلال الجنسي للأطفال واستخدام الأطفال في المواد الإباحية لعام 2003؛[362] واتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي لعام 2007.[363]

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.[364] 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 1 000 صورة؛ وأن 80% منهم كانوا يحتفظون في حواسيبهم بصور لأطفال تتراوح أعمارهم بين 6 أعوام و12 عاماً؛[365] وأن 19% منهم كان لديهم صور لأطفال تقل أعمارهم عن 3 أعوام؛[366] وأن 21% منهم كانت لديهم صور تُظهر مشاهد عنف.[367]

ويُدرُّ بيع المواد الإباحية التي يُستغل فيها الأطفال أرباحاً طائلة؛[368] إذ يكون جامعوها مستعدين لدفع مبالغ كبيرة للحصول على أفلام وصور تعرض مشاهد لأطفال في سياق جنسي.[369] وتعثر محركات البحث على هذه المواد بشكل سريع.[370] 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.[371]

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

1 استخدام العملات الافتراضية والسَّداد المجهول الهوية[372]

يُمكّن السَّداد 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.[373] 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.[374] ولكن عندما يُجري الجناة عملية سداد مجهول الهوية يكون من الصعب تعقبهم.[375] وإذا استخدم الجناة هذه العملات المجهولة فذلك يحد من قدرة وكالات إنفاذ القانون على تحديد المشتبه فيهم بتعقب التحويلات المالية[376] – مثلاً في القضايا المتصلة باستغلال الأطفال في المواد الإباحية التجارية.[377]

2 استخدام تكنولوجيا التجفير[378]

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،[379] مما يعوق التحقيقات الجنائية بصورة خطيرة.[380]

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.[381]

3.6.2 العنصرية والأقوال الحاضة على الكراهية، وتمجيد العنف

تستخدم الجماعات الراديكالية نظم الاتصالات الجماهيرية مثل الإنترنت لنشر دعايتها.[382] وقد ارتفع في السنوات الأخيرة عدد مواقع الويب التي تحتوي على مضمون عنصري وأقوال حاضة على الكراهية[383] – 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.[384] وفي عام 2006، كان يوجد بالإنترنت ما يزيد على 6 000 موقع ويب من هذا النوع.[385]

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.[386] 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.[387] 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.[388] ففي بعض البلدان، قد يتمتع مثل هذا المحتوى بالحماية بموجب مبادئ حرية التعبير .[389] 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.[390] 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.[391]

وتجلت التفاوتات بين البلدان بشأن هذه القضايا أثناء إعداد مشروع اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. وتسعى الاتفاقية بشأن الجريمة السيبرانية إلى تحقيق التواؤم بين القوانين المتعلقة بالجريمة السيبرانية لكفالة عدم تعويق التحقيقات الدولية

من جراء تعارض القوانين.[392] ولم 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 اتفاقية الجريمة السيبرانية وعولج، عوضاً عن ذلك، في البروتوكول الأول القائم بذاته.[393] ولولا ذلك لما كان بمقدور بعض البلدان (ومن بينها الولايات المتحدة) أن توقع اتفاقية الجريمة السيبرانية.

4.6.2 إهانة الأديان

يعرض عدد متزايد[394] من مواقع الويب مواد معينة تخضع في بعض البلدان للأحكام المتعلقة بإهانة الأديان، ومن هذه المواد مثلاً الكتابات المعادية للدين.[395] وعلى الرغم من أن بعض المواد توثق وقائع واتجاهات موضوعية (كانخفاض التردد على الكنائس في أوروبا مثلاً)، فإن هذه المعلومات قد تعتبر غير قانونية في بعض الولايات القضائية. وتشمل أمثلة أخرى الطعن في الأديان أو نشر رسوم كاريكاتورية.

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.[396] وتُعد حرية التعبير سبباً رئيسياً من نجاح الإنترنت، بما تتضمنه من بوابات تُستخدم تحديداً لنشر محتوى لا يُعده إلا المستخدمون.[397] وعلى الرغم من الأهمية الحيوية لحماية هذا المبدأ، فإن تطبيق مبادئ حرية التعبير تحكمها، حتى في أكثر البلدان ليبراليةً، 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.[398]

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[399] أو تدنيس نسخ القرآن الكريم،[400] في حين تتبع بلدان أخرى نهجاً أكثر ليبرالية وقد لا تجرم هذه الأفعال.

5.6.2 المقامرة غير القانونية والألعاب المتاحة على الخط

الألعاب والمقامرة على الإنترنت من أسرع المجالات نمواً على هذه الشبكة.[401] وتفيد شركة ليندن لابز Linden Labs، التي ابتكرت لعبة "حياة ثانية" (Second Life) المتاحة على الخط،[402] أن هذه اللعبة قد تُسجل فيها نحو عشرة ملايين حساب.[403] وتبين التقارير أن بعض هذه الألعاب قد استخدمت لارتكاب جرائم من بينها،[404] تبادل وعرض المواد الإباحية التي يستغل فيها الأطفال،[405] والاحتيال،[406] والمقامرة في كازينوهات القمار الافتراضية المتاحة على الخط،[407] والقذف (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[408] (غير أن هذه التقديرات ما زالت منخفضة نسبياً إذا قورنت بإيرادات المقامرة التقليدية[409]). وبالنسبة لعام 2015 تقدر الإيرادات بمبلغ 28 مليار.[410]

ويتباين تنظيم القمار على الإنترنت وخارجها بين البلدان[411] – 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).[412] ويعزى نجاح ماكاو إلى أن القمار يعتبر غير قانوني في الصين[413] ولذا يسافر آلاف المقامرين من أرض الصين القارية إلى ماكاو للعب القمار فيها.

وتسمح الإنترنت للناس بالالتفاف على القيود المفروضة على القمار.[414] وتنتشر كازينوهات القمار المتاحة على الخط على نطاق واسع، وتوجد معظمها في بلدان تطبق قوانين ليبرالية، أو لا تطبق أي لوائح، فيما يتعلق بالمقامرة على الإنترنت. فيستطيع المستخدمون فتح حسابات على الخط وتحويل الأموال والمشاركة في ألعاب الحظ.[415] كما يمكن استخدام كازينوهات القمار المتاحة على الخط في غسل الأموال وفي أنشطة تموّل الإرهاب.[416] 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.

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.[417] وقد بذلت عدة محاولات تشريعية لمنع المشاركة في المقامرة على الخط:[418] 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.[419]

6.6.2 القذف والمعلومات الزائفة

يمكن استخدام الإنترنت بغرض التضليل بنفس السهولة التي تستخدم بها للإعلام.[420] فمواقع الويب يمكن أن تعرض معلومات زائفة أو تشهيرية، ولا سيما في المنتديات وحجرات الدردشة، حيث يستطيع المستخدمون نشر رسائل لا تخضع لتحقق المشرفين.[421] ويستخدم القصر على نحو متزايد منتديات الويب ومواقع العلاقات الاجتماعية، حيث يمكن كذلك نشر هذا النوع من المعلومات.[422] ويمكن أن يشمل السلوك الإجرامي[423] (على سبيل المثال) نشر صوراً فوتوغرافية حميمة أو معلومات زائفة عن السلوك الجنسي.[424]

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.[425] 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. وهذه المزايا لم تَحُل دون استحداث مشروعات قيمة مثل موسوعة ويكيبديا،[426] التي يُعدِ محتواها المستخدمون على الخط والتي تطبق إجراءات صارمة لضبط المحتوى. غير أن هذه التكنولوجيا نفسها يمكن أن يستخدمها الجناة من أجل نشر معلومات زائفة (عن المنافسين مثلاً)،[427] أو كشف معلومات سرية (كنشر أسرار حكومية أو معلومات تجارية حساسة).

ومما يتّسم 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.[428] 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[429] يتعين موازنتها بحماية ضحايا القذف المحتملين.[430]

7.6.2 الرسائل الاقتحامية وما يتعلق بها من تهديدات

تعنى عبارة "الرسائل الاقتحامية" توجيه أعداد ضخمة من الرسائل الطفيلية.[431] 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،[432] اكتسبت موجة رسائل البريد الإلكتروني الاقتحامية أبعاداً هائلة.[433] واليوم، تفيد منظمات مقدمي خدمة البريد الإلكتروني أن الرسائل الاقتحامية تشكل نسبة تتراوح بين 85 و90 في المائة من جميع رسائل البريد الإلكتروني.[434] 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%).[435] وبعد ست سنوات ما زالت أولى ثلاثة مصادر للرسائل الاقتحامية هي ذاتها: جمهورية الصين الشعبية (22,97%) والولايات المتحدة (17,6% من المجموع المسجل) وجمهورية كوريا (12,67%).[436]

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.[437] وعلى الرغم من أن تكنولوجيا الترشيح تواصل تطورها، فإن مرسلي الرسائل الاقتحامية يجدون سُبلاً للالتفاف عليها – وذلك مثلاً 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.[438]

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[439])، فإن كثيراً من الجناة يستخدمون الشبكات المسخّرة[440] لتوزيع البريد الإلكتروني الطفيلي. فعن طريق استخدام الشبكات المسخّرة المعتمدة على الآلاف من النظم الحاسوبية،[441] 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 المسخّرة.[442] ويرى بعض الخبراء أن الحل الحقيقي الوحيد لمكافحة الرسائل الاقتحامية هو زيادة تكاليف الإرسال التي يتحملها الراسلون.[443] 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.[444] 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 50 000 دولار أمريكي عن طريق إرسال ما لا يقل عن 9 مليارات رسالة اقتحامية.[445]

وفي عام 2005، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي تقريراً حلل تأثير الرسائل الاقتحامية على البلدان النامية.[446] 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.[447] وتستهلك الرسائل الاقتحامية وقتاً قيماً وموارد ثمينة في البلدان التي تعد فيها موارد الإنترنت أكثر ندرة وأعلى تكلفة.

8.6.2 الابتزاز

لا يعتبر الابتزاز جريمة سيبرانية نمطية وإنما جريمة تقليدية. ومع ذلك، فإن الاستخدام الناشئ لتكنولوجيا المعلومات والاتصالات أدى إلى هجمات كثيراً ما يشار إليها باسم "الابتزاز السيبراني".[448] وفي السنوات الأخيرة استهدفت هذه الهجمات كلاً من الشركات الكبرى والشركات المبتدئة الصغيرة.[449] ويتزايد تواتر استفادة الجناة من المزايا العديدة التي تقدمها تكنولوجيا المعلومات والاتصالات بالمقارنة مع الأساليب التقليدية التي كانت ترتكب بها هذه الجريمة. وبالإضافة إلى استخدام تكنولوجيا الاتصالات المغفلة الهوية لتنفيذ الجريمة ثمة عدد متزايد من الجناة يستخدمون العملات الافتراضية بدلاً من المدفوعات النقدية بالتحويل البرقي.[450] وتشير البحوث إلى أن الشركات ما زالت تستخف بأهمية تهديد الابتزاز.[451]

وهناك شكل من أشكال الابتزاز على درجة أعلى من الأتمتة – ما يسمى "برمجية الفدية" — وهو برمجية خبيثة تصيب نظام الحاسوب وتغلقة، وتعرض رسالة مفادها أن جهاز الحاسوب لن يفتح ما لم تدفع الضحية فدية. وهو يعتبر مثار قلق متزايد.[452] وزيادة في الإقناع، غالباً ما يدّعي الجناة بأن سلطات إنفاذ القانون هي التي عطّلت الحاسوب بسبب أنشطة غير مشروعة من جانب المستخدم.[453]

9.6.2 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،[454] والبيع غير القانوني للمنتجات، وتقديم 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.[455] ويصدق الأمر نفسه على الأدوية – فالأدوية التي تتوافر بلا قيود في بعض البلدان قد تستوجب تذكرة طبية في بلدان أخرى.[456] وقد تجعل التجارة عبر الحدود من الصعب التأكد من أن النفاذ إلى منتجات معينة يبقى قاصراً على الأراضي المعنية.[457] 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،[458] وسهولة النفاذ إلى هذه المعلومات يزيد من احتمال وقوع الهجمات.

7.2 الجرائم المتعلقة بحقوق المؤلف والعلامات التجارية

Bibliography (selected): Androutsellis-Theotokis/Spinellis, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; Bakken, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf; Clarke/Sandberg/Wiley/Hong, Freenet: a distributed anonymous information storage and retrieval system, 2001; Cunard/Hill/Barlas, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; Fischer, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002; Johnson/McGuire/Willey, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf; Lohmann, Digital

Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf; Penn, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2; Rayburn, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001; Schoder/Fischbach/Schmitt, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Sifferd, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93.

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[459] لمشكلات قانونية تتصل بانتهاكات حقوق المؤلف. إذ قد يجري تنزيل منتجاتها واستنساخها وتوزيعها.

1.7.2 الجرائم المتعلقة بحقوق المؤلف

مع التحول من التكنولوجيا التماثلية إلى التكنولوجيا الرقمية،[460] أتاحت الرقمنة[461] 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.[462]

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 تبادل الأغاني والملفات والبرمجيات المحمية بحقوق المؤلف في نظم اقتسام الملفات،[463] الالتفاف على نظم إدارة الحقوق الرقمية(DRM).[464]

ونظم اقتسام الملفات هي خدمات شبكية تقوم على الاتصال بين النظراء[465] وتتيح للمستخدمين تقاسم الملفات،[466] مع ملايين المستخدمين الآخرين في كثير من الأحيان.[467] 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 (P2P) دوراً حيوياً في الإنترنت. ففي 2007 ولّدت شبكات الاتصال بين النظراء ما يزيد على 50% من حركة المستهلكين على الإنترنت.[468] 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،[469] وتسجل اتجاهات مماثلة في سائر بلدان المنظمة.[470] ويمكن استخدام نظم تقاسم الملفات لتبادل أي نوع من البيانات الحاسوبية، بما في ذلك الموسيقى والأفلام والبرمجيات.[471] ومن الزاوية التاريخية، كانت نظم تقاسم الملفات تستخدم أساساً لتبادل الموسيقى، لكن تبادل مواد الفيديو تتزايد أهميته أكثر فأكثر.[472]

والتكنولوجيا المستخدمة في خدمات تقاسم الملفات فائقة التطور وتتيح تبادل ملفات كبيرة في غضون فترات زمنية قصيرة.[473] 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 نابستر Napster.[474] وخلافاً للجيل الأول من نظم إنتاج الملفات (ولا سيما خدمة نابستر الشهيرة)، فإن الجيل الثاني من نظم تقاسم الملفات لم يعد يستند إلى مخدم مركزي يوفر قائمة بالملفات المتاحة بين

المستخدمين.[475] فالمفهوم اللامركزي للجيل الثاني من شبكة تقاسم الملفات يجعل من الأصعب منعها من العمل. ولكن يمكن، بفضل الاتصالات المباشرة، تعقب مستخدمي إحدى الشبكات عن طريق عنوان بروتوكول الإنترنت الخاص بهم.[476] 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.[477]

وتكنولوجيا تقاسم الملفات لا يستخدمها الأشخاص العاديون والمجرمون وحدهم بل تستخدمها أيضاً الشركات التجارية العادية.[478] والملفات التي يتم تبادلها بنظم تقاسم الملفات لا تنتهك كلها حقوق المؤلف. إذ تشمل أمثلة استخدامها المشروع ما يُؤذِن بتبادله في إطار الملك العام من نسخ ومصنفات فنية.[479]

ومع ذلك، فإن استخدام نظم تقاسم الملفات يطرح تحديات على صناعة الترفيه.[480] ومن غير الواضح إلى أي مدى يُعزى 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[481] وعن وجود مليارات الملفات التي تم تنزيلها.[482] وظهرت في نظم تقاسم الملفات أفلام يتم تبادلها قبل عرضها في دور العرض رسمياً[483] 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.[484]

وقد ردت صناعة الترفيه على ذلك بتطبيق تكنولوجيا ترمي إلى منع المستخدمين من استنساخ أقراص CD وDVD مثل نظم تخليط المحتوى (CSS)،[485] وهي تكنولوجيا تحفير تمنع استنساخ المحتوى على أقراص DVD.[486] 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 (DRM)"[487] 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.

ومن أكبر الصعوبات التي تصادفها هذه التكنولوجيات إمكانية الالتفاف على تكنولوجيا حماية حقوق المؤلف.[488] فقد استحدث الجناة أدوات برمجياتية تُمكّن المستخدمين من أن يتيحوا على الإنترنت ملفات محمية بحقوق المؤلف[489] 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 بتحفير 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 التحفير باستخدام أدوات برمجياتية.[490]

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.[491]

2.7.2 الجرائم المتعلقة بالعلامات التجارية

انتهاكات العلامات التجارية وهذا جانب معروف جيداً من جوانب التجارة العالمية، تماثل انتهاكات حقوق المؤلف. وقد انتقلت الانتهاكات المتعلقة بالعلامات التجارية إلى الفضاء السيبراني، وهي تخضع للتجريم بدرجات متباينة بموجب القوانين الجنائية الوطنية المختلفة.[492] وتشمل أخطر هذه الجرائم استخدام العلامات التجارية في أنشطة إجرامية بغرض تضليل المستعملين، والجرائم المتعلقة بأسماء الميادين.

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 التصيُّد الاحتيالي،[493] حيث ترسل إلى مستخدمي الإنترنت ملايين الرسائل الإلكترونية الشبيهة بالرسائل الصادرة عن الشركات المشروعة، تتضمن، على سبيل المثال، العلامات التجارية.[494]

وهناك قضية أخرى تتصل بانتهاكات العلامات التجارية الجرائم المتعلقة بالميدان[495] مثل الاستقطان السيبراني،[496] الذي يعني عملية غير قانونية لتسجيل اسم ميدان مطابق أو مماثل للعلامة التجارية لمنتج أو لشركة.[497] ويسعى الجناة، في معظم هذه الحالات، إلى بيع الميدان بسعر مرتفع إلى الشركة[498] أو يستخدمونه لبيع منتجات أو خدمات تضلل المستخدمين من خلال ارتباطها المفترض بالعلامة التجارية.[499] ومن الأمثلة الأخرى على الجرائم المتصلة بالميدان "اختطاف الميدان" أو تسجيل أسماء الميدان التي انقضت مدتها عرضاً.[500]

8.2 الجرائم المتعلقة بالحاسوب

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

تغطي هذه الفئة عدداً من الجرائم التي يستلزم ارتكابها نظاماً حاسوبياً. وخلافاً للفئات السابقة، فإن هذه الفئة الواسعة من الجرائم لا تُعد، في كثير من الأحيان، صارمة بنفس القدر من زاوية الحماية التي تكفلها المبادئ القانونية. وتشمل هذه الفئة الاحتيال الحاسوبي، والتزييف والتصيُّد الاحتيالي وانتحال الهوية باستخدام الحاسوب، وإساءة استخدام الأجهزة.

1.8.2 الاحتيال والاحتيال الحاسوبي

الاحتيال الحاسوبي من أكثر الجرائم شيوعاً على الإنترنت،[501] لأنه يمكن الجناة من استخدام الأتمتة[502] وأدوات برمجياتية لإخفاء هويتهم.

وتُمكّن الأتمتة الجناة من جني أرباح طائلة من عدد من الأفعال الصغيرة.[503] 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.[504] ومن أمثلة هذا النوع من الخدع الاحتيالية ما يُعرف باسم الخدعة النيجيرية ويقصد بها الاحتيال لتحصيل مبلغ من المال بزعم تقديم خدمة لاحقة وهمية.[505]

وعلى الرغم من أن هذه الجرائم ترتكب باستخدام تكنولوجيا الحاسوب، فإن معظم نظم القانون الجنائي تصنفها لا كجرائم متعلقة بالحاسوب بل كحالات احتيال عادي.[506] 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. وتشمل أهم جرائم الاحتيال ما يلي:

الاحتيال عن طريق المزادات المتاحة على الخط[507]

تُعد المزادات العامة المتاحة على الخط من أكثر خدمات التجارة الإلكترونية شعبية. وحتى في عام 2006، بيعت على موقع إيباي eBay، وهو أكبر سوق للمزادات المتاحة على الخط في العالم، سلع تزيد قيمتها على 20 مليار دولار أمريكي.[508] 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.[509] والصعوبة في التمييز بين البائعين الحقيقيين والجناة، جعلت من الاحتيال عن طريق المزادات واحدة من أكثر الجرائم السيبرانية انتشاراً.[510] وأوسع أسلوبين انتشاراً هما[511] عرض سلع غير موجودة للبيع، ومطالبة المشترين بدفع ثمنها قبل تسليمها،[512] وشراء 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[513] 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.[514] وبموجب هذه الخدعة المسماة "الاستيلاء على الحسابات"[515] 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.

الاحتيال لتحصيل مبلغ من المال بزعم تقديم خدمة لاحقة وهمية[516]

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[517] 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 بيانات حساباتهم المصرفية، فإن الجناة قد يستخدمونها في أنشطة احتيالية. وتوحي الأدلة بأن مثل هذه الرسائل الإلكترونية يرد عليها آلاف الضحايا[518] 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 من حيث عدد الضحايا وحجم الخسائر الإجمالية على السواء.[519]

2.8.2 التزييف الحاسوبي

يعني التزييف الحاسوبي التلاعب في الوثائق الرقمية[520] ويمكن أن تُرتكب الجريمة مثلاً عن طريق إنشاء وثيقة تبدو كما لو كانت صادرة عن مؤسسة موثوق بها، أو التلاعب في الصور الإلكترونية (ومن ذلك مثلاً الصور المستخدمة كدليل في المحاكم)، أو تحوير الوثائق النصية.

ويُعد تزوير الرسائل الإلكترونية عنصراً أساسياً للتصيد الاحتيالي الذي يشكل تحدياً خطيراً لوكالات إنفاذ القانون في جميع أنحاء العالم[521] ذلك أن "التصيد الاحتيالي" يسعى إلى جعل الأهداف يفصحون عن معلومات شخصية/سرية[522] فيرسل الجناة في كثير من الأحيان رسائل إلكترونية شبيهة بالرسائل الصادرة عن مؤسسات مالية مشروعة يتعامل معها الهدف[523] وتصمم هذه الرسائل الإلكترونية بطريقة تجعل من الصعب على الأهداف أن يكتشفوا زيفها[524] 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.[525]

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.

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[526] قد استخدمت من أجل حماية الوثيقة من التزييف.[527]

3.8.2 انتحال الهوية

يصف مصطلح انتحال الهوية – الذي لا يُعرّف ولا يُستخدم بطريقة متسقة – فعلاً إجرامياً يتمثل في الاحتيال لانتحال هوية شخص آخر واستخدامها.[528] ويمكن القيام بهذه الأفعال دون الاستعانة بوسائل تقنية[529] كما يمكن ارتكابها على الخط باستخدام تكنولوجيا الإنترنت.[530]

إن التغطية الإعلامية الواسعة[531] ونتائج مختلف الدراسات الاستقصائية التي تحلل مدى الخسارة الناجمة عن انتحال الهوية،[532] فضلاً عن تحليلات قانونية وتقنية[533] عديدة نشرت في السنوات الأخيرة يمكن أن يؤدي بسهولة إلى استنتاج مفاده أن الجرائم المتصلة بالهوية هي من ظواهر القرن الحادي والعشرين.[534] ولكن ليست الحالة كذلك، نظراً لأن الجرائم المتصلة بتقمّص الشخصية والتزوير وإساءة استعمال وثائق الهوية كانت موجودة منذ أكثر من قرن.[535] وفي الثمانينات بالفعل، أفادت الصحف بصورة مكثفة عن إساءة استخدام المعلومات المتعلقة بالهوية.[536] لم يُسفِر ظهور استخدام الهويات الرقمية وتكنولوجيا المعلومات سوى عن تغيير أساليب المجرمين وأهدافهم.[537] وأتاحت زيادة استخدام المعلومات الرقمية إمكانيات جديدة للمجرمين للنفاذ إلى المعلومات المتصلة بالهوية.[538] وهكذا، كان لعملية التحول من دول صناعية إلى مجتمعات معلومات[539] تأثير كبير على تطور جرائم انتحال الهوية. ومع ذلك، فعلى الرغم من العدد الكبير لحالات انتحال الهوية المتصلة بالإنترنت، فإن الرقمنة لم تغير الجريمة نفسها بشكل جذري، ولكن أدت إلى مجرد استحداث أهداف جديدة وتيسير وضع أساليب جديدة.[540] ويبدو أنه تم الإفراط في تقدير أثر زيادة استعمال تكنولوجيا الإنترنت. واستناداً إلى نتائج تحليل الأسلوب للجرائم المتعلقة بالهوية، ما زال انتحال الهوية تعتبر إلى حد كبير جريمة خارج الخط.[541] وفي عام 2007 كان 20 في المائة من الجرائم التي ارتكبت في الولايات المتحدة[542] كانت عبارة عن انتهاكات احتيالية[543] وخروقات خاصة بالبيانات على الخط. ورغم التطورات الحديثة ما زال انتحال الهوية خارج الخط على درجة عالية من الأهمية. ومما يبعث على الدهشة، الأهمية المستمرة للجرائم خارج الخط، حيث إن الرقمنة وكذلك عولمة الخدمات القائمة على الشبكة أدت إلى زيادة استخدام المعلومات الرقمية المتصلة بالهوية.[544] كما أن أهمية المعلومات المتصلة بالهوية آخذة في النمو، سواء في الاقتصاد أو على مستوى التفاعل الاجتماعي. وفي الماضي، كانت "السمعة الطيبة" والعلاقات الشخصية الطيبة تسيطر على الأعمال والمعاملات اليومية.[545] ومع الانتقال إلى التجارة الإلكترونية، أصبح التعرّف وجهاً لوجه شبه مستحيل، ونتيجة لذلك أصبحت المعلومات المتصلة بالهوية أكثر أهمية إلى حد كبير بالنسبة للناس الذين يشاركون في معاملات اجتماعية واقتصادية.[546] ويمكن وصف هذه العملية بالميكنة،[547] حيث تُحول الهوية إلى معلومات تتصل بالهوية يمكن تقديرها كمياً. وهذه العملية، جنباً إلى جنب مع التمييز بين الجانب الذي يطغى عليه الطابع الفلسفي لمصطلح "الهوية" بصورة أكبر (التي

تعرّف[548] بأنها مجموعة من السمات الشخصية)، والمعلومات المتعلقة بالهوية القابلة للتقدير الكمي التي تمكّن من التعرف على الشخص، تكتسي أهمية كبيرة. وعملية التحول ليست ذات صلة فقط بالسمات المتعلقة بالإنترنت الخاصة بانتحال الهوية، نظراً لأن أثر التطور يتجاوز بكثير شبكات الحاسوب. ففي أيامنا هذه، تهيمن متطلبات المعاملات غير المباشرة، مثل الثقة والأمن[549] على الاقتصاد بصورة عامة ولا تقتصر على الأعمال المتعلقة بالتجارة الإلكترونية. ومن أمثلة ذلك استخدام بطاقات الدفع بالرقم PIN (رقم التعريف الشخصي) لشراء السلع في المتاجر الكبرى.

وتشمل الجريمة التي توصف بأنها انتحال هوية ثلاث مراحل مختلفة بوجه عام،[550] 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.[551] ومن الأمثلة على ذلك بيع المعلومات المتعلقة بالهوية.[552] فسجلات بطاقات الائتمان تباع مثلاً بمبلغ يصل إلى 60 دولاراً أمريكياً،[553] 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.[554] 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.[555]

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"[556])، أو أن يسرق البريد.[557] 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 وصولاً إلى معلومات تتعلق بقضايا أمن الحاسوب وإلى معلومات شخصية يمكن استغلالها في الخدع الخاصة بانتحال الهوية. وقد يتمثل هدف الجاني مثلاً في البحث عن نظم لا تكفل حماية مأمونة لكلمة السر لاستقاء البيانات منها.[558] وتسلط التقارير الضوء على المخاطر التي ينطوي عليها الاستخدام القانوني لمحركات البحث في أغراض غير قانونية.[559] 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 انتحال الهوية.[560] 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،[561] أن أكثر من 35% من المجيبين يُعزون إلى الأطراف الداخلية نسبة تزيد على 20% من خسائر منظمتهم. وفي عام 2013، أظهرت دراسة استقصائية أن 23 في المائة من الجرائم السيبرانية مرتبطة بعارفين من داخل الشركة و53 في المائة من المجيبين يعتقدون أن هجمات العارفين من الداخل أكثر ضرراً من الهجمات من الخارج.[562] 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.[563]

ويتباين نوع البيانات التي يستهدفها الجناة.[564] وتتمثل أهم هذه البيانات في رقم الضمان الاجتماعي أو رقم جواز السفر، تاريخ الميلاد، العنوان، أرقام الهاتف وكلمات السر.

رقم الضمان الاجتماعي (SSN) أو رقم جواز السفر

رقم الضمان الاجتماعي الذي يستخدم مثلاً 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.[565] ويستطيع الجناة استخدام هذا الرقم، ومعلومات عن جوازات السفر، لفتح حسابات مالية، أو الاستيلاء على الحسابات المالية القائمة، أو الحصول على ائتمانات، أو أخذ قروض.[566]

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).[567] 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[568] وإما بأن تنشر نزولاً على متطلبات قانونية وذلك مثلاً لدى تسجيل العلامات على مواقع الويب.[569]

كلمة السر للحسابات غير المالية

النفاذ إلى كلمات السر الخاصة بالحسابات يتيح للجناة أن يغيروا بيانات تهيئة الحساب وأن يستخدمونه في الأغراض الخاصة بهم.[570] 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.[571]

كلمة السر الخاصة بالحسابات المالية

تُعد المعلومات المتعلقة بالحسابات المالية هدفاً مفضلاً لهجمات انتحال الهوية شأنها شأن أرقام الضمان الاجتماعي. وهذا يشمل الحسابات الجارية وحسابات الادخار، وبطاقات الائتمان وبطاقات الخصم، والمعلومات المتعلقة بالتخطيط المالي. وتُعد هذه المعلومات مصدراً هاماً لانتحال الهوية من أجل ارتكاب جرائم مالية سيبرانية.

وانتحال الهوية مشكلة خطيرة ومتنامية.[572] ففي النصف الأول من عام 2004، وقعت 3% من الأسر في الولايات المتحدة ضحية لانتحال الهوية.[573] وفي عام 2012 أعلن مكتب إحصاءات العدل أن 7 في المائة من جميع الأشخاص ممن بلغ 16 سنة أو تجاوزها في الولايات المتحدة تعرض لحادث انتحال هوية واحد على الأقل في عام 2012.[574] وفي المملكة المتحدة، تشير الحسابات إلى أن التكلفة التي يتحملها الاقتصاد البريطاني نتيجة انتحال الهوية تصل إلى 1,3 مليار جنيه إسترليني كل عام.[575] وتتراوح تقديرات الخسائر الناجمة عن انتحال الهوية في أستراليا بين ما يقل عن مليار دولار أمريكي وأكثر من 3 مليارات دولار أمريكي كل عام.[576] وتقدر الدراسة الاستقصائية لانتحال الهوية لعام 2006 خسائر الولايات المتحدة في عام 2005 بمقدار 56,6 مليار دولار أمريكي.[577] ويقدر تقرير انتحال الهوية لعام 2013 الخسائر في عام 2012 بمبلغ 20,9 مليار دولار. وقد لا تكون الخسائر مالية فحسب، بل هي تشمل أيضاً الإضرار بالسمعة.[578] والواقع أن كثيراً من الضحايا لا يبلغون عن هذه الجرائم، كما أن المؤسسات المالية لا تودّ في أحيان كثيرة الإعلان عن تجارب عملائها السيئة. ومن المرجح أن يفوق الانتشار الفعلي لانتحال الهوية من بعيد عدد الحالات المبلغ عنها.[579]

ويستند انتحال 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 المعلومات البيومترية) مكلفة وغير مستخدمة على نطاق واسع. ونظراً لقلة القيود المفروضة على الأنشطة التي تمارس على الخط، فإن انتحال الهوية يصبح سهلاً ومربحاً.[580]

وثمة ظاهرة مرتبطة على نحو وثيق بالتطور نحو "البيانات الكبيرة" وهي العدد المتزايد من المعلومات المتعلقة بالهوية والمتاحة في "الأسواق السوداء". فإذا تمكن الجناة من النفاذ إلى قواعد البيانات التي تضم سجلات الملايين من العملاء فقد يباع عدد كبير منها بعد ذلك. وتشير البحوث التي نشرت في عام 2014 على سبيل المثال إلى أن كمية المعلومات المتعلقة بالهوية المتاحة في الأسواق السيبرانية السوداء التي يتم الحصول عليها من خلال خرق البيانات، تتضمن مثلاً بيانات الاعتماد لما يصل إلى 360 مليون حساب.[581]

4.8.2 إساءة استخدام الأجهزة

يمكن ارتكاب الجريمة السيبرانية بغير أن تستخدم في ذلك إلا معدات أساسية نسبياً.[582] 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،[583] ومجاناً في كثير من الأحيان. أما الأدوات الأكثر تطوراً، فتكلف عدة آلاف من الدولارات.[584] ويستطيع الجناة، باستخدام هذه الأدوات البرمجياتية، مهاجمة نظم حاسوبية أخرى بمجرد الضغط على أحد الأزرار. 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.[585] وتتوافر أدوات برمجياتية تتيح[586] شن هجمات تستهدف الحرمان من النفاذ إلى الخدمة،[587] وتصميم فيروسات حاسوبية، وفك تجفير الرسائل المجفرة، أو النفاذ إلى النظم الحاسوبية بطريقة غير قانونية.

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.[588] 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 هذه – وذلك مثلاً بتجريم إنتاجها وبيعها وحيازتها.[589]

9.2 الجرائم المجتمعة

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

يُستخدم العديد من المصطلحات لوصف الخدع المعقدة التي تجمع بين عدد من الجرائم المختلفة. ومن أمثلة ذلك استخدام الإرهابيين للإنترنت، وغسل الأموال السيبراني، والتصيُّد الاحتيالي.

1.9.2 استخدام الإرهابيين للإنترنت

ركّز نقاش جرى في تسعينات القرن الماضي حول استخدام المنظمات الإرهابية للشبكة، على الهجمات المعتمدة على الشبكة والموجهة ضد بُنى تحتية حاسمة مثل النقل وإمدادات الطاقة ("الإرهاب السيبراني")، كما كان يركز على استخدام تكنولوجيا المعلومات في الصراعات المسلحة ("الحرب السيبرانية").[590] وقد أوضح نجاح الهجمات التي تستخدم فيها الفيروسات والبرمجيات الروبوتية، على نحو جليّ، أوجه الضعف في أمن الشبكة. وقيام الإرهابيين بشن هجمات ناجحة بالاعتماد على الإنترنت أمر ممكن،[591] لكن من الصعب تقييم دلالة التهديدات.[592] وكانت درجة التوصيل البيني آنذاك محدودة مقارنة بالوقت الحاضر، ومن المرجّح للغاية أن يكون هذا الأمر – إلى جانب حرص الدول على تكتّم 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.[593]

غير أن هذه الحالة قد تبدّلت بعد هجمات الحادي عشر من سبتمبر التي عجلت بدء مناقشة مكثفة بشأن استخدام الإرهابيين لتكنولوجيا المعلومات والاتصالات.[594] ومما سهّل هذه المناقشة التقارير[595] التي أفادت أن الجناة قد استخدموا الإنترنت في التحضير للهجوم.[596] وعلى الرغم من أن الهجمات لم تكن هجمات سيبرانية، لأن الجماعة التي شنّت هجوم الحادي عشر من سبتمبر لم تقُم بهجوم معتمد على الإنترنت، فإن الإنترنت قد أدّت دوراً في التحضير للاعتداء.[597] وضمن هذا السياق، اكتُشفت طرق مختلفة تستخدم بها المنظمات الإرهابية الإنترنت.[598] ومن المعروف اليوم أن الإرهابيين يستخدمون تكنولوجيا المعلومات والاتصالات والإنترنت من أجل:

- الدعاية؛
- جمع المعلومات؛
- التحضير للهجمات في العالم الحقيقي؛
- نشر المواد التدريبية؛
- الاتصال؛
- تمويل الإرهاب؛
- شن الهجمات ضد البُنى 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 بُنى تحتية حاسمة ينبغي ألاّ يخرج عن محور دائرة النقاش. فقلّة المنعة وتنامي الاعتماد[599] على تكنولوجيا المعلومات يجعلان من الضروري مراعاة الهجمات المعتمدة على الإنترنت والموجهة ضد البُنى التحتية الحاسمة في الاستراتيجيات الرامية إلى منع الإرهاب السيبراني ومكافحته.

لكن مكافحة الإرهاب السيبراني تبقى عسيرة على الرغم من تزايد كثافة ما يضطلع به من بحوث. وتبين المقارنة بين مختلف النُّهُج الوطنية العديد من أوجه التماثل في الاستراتيجيات.[600] ومن أسباب هذا التطور أن المجتمعات الدولية قد أقرت بأن تهديدات الإرهاب الدولي تستوجب حلولاً عالمية.[601] ولكن من غير المعروف على وجه اليقين في الوقت الحاضر ما إذا كان هذا النهج يُعدّ ناجحاً أو ما إذا كانت النظم القانونية والخلفيات الثقافية المتباينة تستوجب حلولاً متباينة. وتقييم هذه القضية يحمل في طياته تحديدات 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 قِبَل المنظمات الإرهابية. فالمعلومات المتعلقة بهذه المسألة تُعد في كثير من الأحيان معلومات سرية ولذا لا تتوافر إلا لقطاع الاستخبارات،[602] وإلى الآن لم تتوافق الآراء بعد حتى على المقصود بمصطلح "الإرهاب".[603] 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 دليل على أن الإرهابيين يستخدمون الإنترنت في التحضير لهجماتهم.[604] وتبدو هذه الحجة 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.[605] 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.[606] كما بدأ الإرهابيون في استخدام جمهور مواقع الفيديو (مثل يوتيوب YouTube) لتوزيع رسائل ومواد دعائية عن طريق الفيديو.[607] واستخدام مواقع الويب والمنتديات الأخرى دليل على أن الجماعة المخرّبة باتت تركز على العلاقات العامة بطريقة ذات طابع مهني أوضح.[608] فتستخدم مواقع الويب والوسائط الأخرى لنشر المواد الدعائية،[609] ولوصف أنشطتها وتبريرها،[610] ولتجنيد أعضاء ومانحين جدد[611] والاتصال بالحاليين منهم.[612] وقد استخدمت مواقع الويب مؤخراً في توزيع لقطات فيديو عن عمليات إعدام.[613]

جمع المعلومات

تتوافر على الإنترنت معلومات كثيرة عن الأهداف المحتملة.[614] ومن ذلك مثلاً، أن المهندسين المشاركين في بناء المباني العمومية كثيراً ما ينشرون الرسومات الهندسية لتلك المباني على مواقع الويب الخاصة بهم. 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.[615] كما تم الوقوف على إرشادات تبين كيفية صنع القنابل، بل وحتى على مخيمات تدريب افتراضية تقدم إرشادات عن كيفية استخدام الأسلحة بنهج التعلّم الإلكتروني.[616] وتم الوقوف أيضاً على معلومات حساسة لا توفر لها روبوتات البحث حماية كافية، ويمكن النفاذ إليها عن طريق محركات البحث.[617] 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.[618] وفي عام 2006، أفادت جريدة النيويورك تايمز أن موقع ويب حكومياً قد نشر، في إطار سَوقِه لأدلة على النُّهج التي يتبعها العراق لاستحداث أسلحة نووية، معلومات أساسية تتعلق بصنع الأسلحة النووية.[619] وأُبلغ عن حادثة مماثلة في أستراليا حيث نُشرت على مواقع ويب حكومية معلومات عن أهداف محتملة للهجمات الإرهابية.[620] 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.[621]

التحضير لهجمات تُنفّذ 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. وتناقش هنا 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.[622] إذ تتوافر على الخط ألعاب مختلفة تحاكم العالم الحقيقي. ويستطيع ممارس 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.[623]

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.[624] وفي عام 2008، اكتشفت دوائر غربية مخدّماً على الإنترنت يوفر قاعدة لتبادل مواد تدريبية وتيسير الاتصالات.[625] وأُبلغ عن مواقع ويب مختلفة تشغلها منظمات إرهابية لتنسيق أنشطتها.[626]

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 من أجل التنسيق لهجماتهم.[627] ونقلت الصحافة أخباراً عن استخدام البريد الإلكتروني في تبادل إرشادات تفصيلية عن الأهداف وعدد المهاجمين.[628] وعن طريق استخدام تكنولوجيا التجفير ووسائل الاتصالات المجهولة الهوية، يستطيع أطراف الاتصال أن يزيدوا من صعوبة تحديد الاتصالات الإرهابية ورصدها.

تمويل الإرهاب

تعتمد معظم المنظمات الإرهابية على الموارد المالية التي تتلقاها من أطراف ثالثة. وقد أصبح تتبّع هذه المعاملات المالية من النُّهُج الرئيسية المتّبعة في مكافحة الإرهاب بعد هجمات الحادي عشر من سبتمبر. ومن أهم الصعوبات المصادفة في هذا الصدد أن الموارد المالية المطلوبة لشن الهجمات لا تُعدّ مرتفعة بالضرورة.[629] 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.[630] 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.[631] ويتمثل نهج آخر في تحصيل التبرعات على الخط عن طريق بطاقات الائتمان. وكان الجيش الجمهوري الآيرلندي (IRA) من أولى المنظمات الإرهابية التي جمعت التبرعات عن طريق بطاقات الائتمان.[632] ويجازف كلا النهجين باحتمال أن تكتشف المعلومات المنشورة وأن يُستعان بها لتتبّع المعاملات المالية. ولذا، فإن من المرجَّح أن تصبح نظم الدفع الإلكتروني المجهول الهوية أكثر انتشاراً. وتحاول المنظمات الإرهابية، تجنّباً لاكتشافها، أن تُخفي 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. وليس من السهل تماماً إثبات أن المعاملات المالية التي تجري على هذه المواقع ليس عمليات شراء عادية بل تبرعات. وسيكون من الضروري التحقيق في كل معاملة، وهو أمر قد يكون صعباً إذا كان المتجر الموجود على الخط يعمل في ولاية قضائية مختلفة أن يستخدم نظماً للدفع المجهول الهوية.[633]

الهجمات ضد البُنى التحتية الحرجة

بالإضافة إلى الجرائم الحاسوبية العادية مثل الاحتيال وانتحال الهوية، يمكن أن تصبح الهجمات ضد البُنى التحتية الحرجة للمعلومات هدفاً للإرهابيين. وتنامي الاعتماد على تكنولوجيا المعلومات يجعل البُنى التحتية الحرجة أكثر عِرضة للهجمات.[634] ويصدُق هذا بوجه خاص على الهجمات الموجهة ضد النظم الموصولة بينياً عن طريق شبكات الحواسيب والاتصالات.[635] وفي تلك الحالات يتجاوز الخلل الذي يسببه هجوم معتمد على الشبكة مجرد تعطّل نظام واحد. فحتى الانقطاعات القصيرة في الخدمات يمكن أن تُلحِق ضرراً مالياً ضخماً بالأعمال التجارية الإلكترونية – ولا يصدق هذا الخدمات المدنية وحدها بل ويصدق أيضاً على البُنى التحتية والخدمات العسكرية.[636] ويطرح التحقيق في مثل هذه الهجمات أو حتى الوقاية منها تحديات فريدة.[637] فخلافاً للهجمات المادية، لا يتعيّن على الجُناة أن يكونوا موجودين في مكان وقوع

الهجوم.[638] ويستطيع الجناة، إبان قيامهم بالهجوم، استخدام وسائل الاتصال المجهول الهوية وتكنولوجيا التجفير لإخفاء هويتهم.[639] وكما سَلَفَتْ الإشارة، يقتضي التحقيق في هذه الهجمات صكوكاً إجرائية خاصة، والتكنولوجيا اللازمة للتحقيق، والموظفين والمدرّبين.[640]

ومن المعترف به على نطاق واسع أن البُنى التحتية الحرجة تشكل هدفاً محتملاً لهجمات إرهابية، لأنها تُعدّ بحكم التعريف ذات أهمية حيوية لاستدامة دولة من الدول واستقرارها.[641] وتعتبر البنية التحتية حرجة إذا كان من شأن تعطيلها أو تدميرها أن يُضعِف الأمن الدفاعي أو الاقتصادي للدولة.[642] وهذه البُنى 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 الناجم عن اضطراب الخدمات من جراء إعصار كاترينا الذي أصاب الولايات المتحدة مدى اعتماد المجتمع على تيسُّر تلك الخدمات.[643] وتؤكد برمجية "ستوكسنت" (Stuxnet) الخبيثة التهديد الناشئ الذي تشكله الهجمات المعتمدة على الإنترنت والتي تركز على البُنى التحتية الحرجة[644] وفي سنة 2010، اكتشفت شركة أمنية في بيلاروس برمجية خبيثة جديدة.[645] ومازال يجري البحث بشأن التلاعبات التي تسببها البرمجية وبشأن مصممها ودوافعه وحتى الآن لم تُكتشف جميع الحقائق، لا سيما فيما يتعلق بمن وراءها ودوافع مصممها.[646] لكن، وفيما يخص وظائف البرمجية بالتحديد، يبدو أن هناك الآن أساساً قوياً بالأحرى من الحقائق.

وحسب ما جاء في التقارير، فإن البرمجية المعقدة، ذات أكثر من 4 000 وظيفة،[647] تستهدف أنظمة المراقبة الصناعية (ICS) [648] – لا سيما الأنظمة التي تنتجها شركة سيمنس التكنولوجية (Siemens).[649] وقد نُشرت البرمجية عن طريق وسائط تخزين البيانات القابلة للنقل ولجأت إلى استغلال الأيام رباعية الأصفار لإلحاق الضرر بالأنظمة الحاسوبية.[650] ووردت تقارير عن تضرر أنظمة حاسوبية بالأساس من إيران وإندونيسيا وباكستان، بل ومن الولايات المتحدة وبلدان أوروبية أيضاً.[651] ورغم وصف البرمجية الخبيثة مراراً وتكراراً كبرمجية عالية التطور، فإن هناك تقارير تُثير جدلاً بشأن درجة تطوّرها.[652]

ومثلما ذُكر أعلاه، فإن تحديد من وراء البرمجية ودوافعه أمر أصعب ومازال يشوبه عدم اليقين إلى حد كبير. وقد ذهبت تقارير إخبارية ودراسات إلى القول بأن البرمجية ربما كانت تستهدف مرافق تخصيب اليورانيوم في إيران وبأن من الممكن أنها تسببت في تأخير البرنامج النووي للبلد.[653]

ويمكن استخلاص استنتاجين من اكتشاف هذه البرمجية الخبيثة. أولاً، يؤكد هذا الحدث أن البُنى التحتية الحرجة تعتمد اعتماداً كبيراً على التكنولوجيا الحاسوبية وأن من الممكن تعرُّضها للهجمات. ثانياً، يؤكد نشر البرمجية عن طريق وسائط تخزين البيانات القابلة للنقل، من بين طرق أخرى، أن مجرد قطع اتصال الأنظمة الحاسوبية بالإنترنت لا يمنع الهجمات.

ويتعدى اعتماد البُنى التحتية الحرجة على تكنولوجيا المعلومات والاتصالات قطاع الطاقة والصناعة النووية. ويمكن إيضاح هذا بتسليط الضوء على بعض الحوادث المتعلقة بالنقل الجوي الذي يعتبر أيضاً جزءاً من البُنى التحتية الحرجة في معظم البلدان. ويشكل نظام التسجيل للسفر أحد الأهداف المحتملة للهجمات. وتستند أنظمة التسجيل للسفر في معظم مطارات العالم بالفعل إلى نظم حاسوبية موصولة بينياً.[654] وفي عام 2004 أصابت دودة ساسر (Sasser) الحاسوبية[655] ملايين الحواسيب حول العالم، ومن بينها النظم الحاسوبية للخطوط الجوية الكبرى، مما فرض إلغاء الرحلات.[656]

ويتمثل هدف آخر من الأهداف المحتملة في أنظمة إصدار البطاقات على الخط. فاليوم يُشترى عدد كبير من بطاقات السفر على الخط. وتستخدم الخطوط الجوية تكنولوجيا المعلومات في عمليات متنوعة. وتسمح جميع الخطوط 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 (DoS).[657] وفي عام 2000، شُنّت عدة هجمات من هذا النوع، في غضون فترة وجيزة، ضد شركات شهيرة مثل الـ سي إن إن (CNN) إي باي (e-Bay) وأمازون.[658] وأسفر ذلك عن عدم توافر بعض الخدمات لعدة

ساعات بل ولعدة أيام.[659] كما تضررت الخطوط الجوية بدورها من تلك الهجمات. وفي عام 2001 كان موقع لوفتهانزا على الويب هدفاً لإحدى الهجمات.[660]

وأخيراً، فإن نظم المراقبة الجوية من الأهداف المحتملة الأخرى للهجمات المعتمدة على الإنترنت والموجهة ضد البُنى التحتية للنقل الجوي التي تتسم بأهمية حاسمة. وقد تجلّت قلة منعةِ نظم المراقبة الجوية الحاسوبية إبان هجوم قرصنة تعرض له مطار وورسستر في الولايات المتحدة في عام 1997[661] ففي أثناء هذا الهجوم، عطّل الجناةُ الخدمات الهاتفية الداخلة إلى برج المراقبة وأغلقوا نظام المراقبة التي يدير إضاءة مهابط الطائرات.[662]

2.9.2 *الحرب السيبرانية*

بعد الهجمات التي شُنَّت ضد الأنظمة الحاسوبية في إستونيا في سنة 2007 وجورجيا في سنة 2008 وبعد اكتشاف الفيروس الحاسوبي "ستوكسنت" (Stuxnet)[663]، استُخدم مصطلح الحرب السيبرانية مراراً وتكراراً لوصف الحالة رغم أن استخدام هذا المصطلح مثير للجدل – مثلما يتضح ذلك أدناه بمزيد من التفصيل.

المصطلح والتعاريف

ليس هناك أي مصطلح متّسق ولا أي تعريف مقبول على نطاق واسع للحرب السيبرانية. والمصطلحات الأخرى المستخدمة هي حرب المعلومات والحرب الإلكترونية والحرب السيبرانية وحرب الشبكة والعمليات المعلوماتية.[664] وتستعمل هذه المصطلحات عموماً استعمال تكنولوجيا المعلومات والاتصالات في شن حرب باستخدام الإنترنت. أما التعريفات الأكثر تقييداً، فتعرف هذه الأنشطة كنهج للنزاع المسلح يرتكز على إدارة واستخدام المعلومات في جميع أشكالها وعلى جميع المستويات لتحقيق فائدة عسكرية حاسمة لا سيما في البيئة المشتركة والمختلفة.[665] وتغطي تعاريف أخرى أوسع أي نزاع إلكتروني تكون في المعلومات ميزة استراتيجية تستحق الانقضاض عليها أو تدميرها.[666]

تطوّر النقاش

كان هذا الموضوع مسألة نقاش مثيرة للجدل على مدى عقود.[667] وتركّز الانتباه في البداية على استبدال الحرب الكلاسيكية بالهجمات المستخدِمة للحاسوب أو المعتمدة عليه.[668] وفي هذا الصدد، كانت القدرة على إضعاف أي عدو كان دون الدخول في نزاع عنصراً من العناصر الجوهرية التي شُكِّلت منذ البداية صميم النقاش.[669] كما أن الهجمات المعتمدة على الشبكة أزهد تكلفة بوجه عام من العمليات العسكرية التقليدية[670] ويمكن أن تقوم بها حتى الدول الصغيرة. وعلى الرغم من بعض الحالات الملموسة التي يُستشهد بها غالباً، تبقى الجوانب الأساسية من النقاش افتراضية إلى حد كبير.[671] والحالتان اللتان يُستشهد بهما في أغلب الأحيان هما الهجمات الحاسوبية التي شُنّت ضد إستونيا وجورجيا. بيد أن تصنيف هجوم كفعل من الأفعال الحربية يتطلّب استيفاء بعض المعايير.

ففي سنة 2007، شهدت إستونيا نقاشاً صاخباً بشأن إزالة نصب تذكاري للحرب العالمية الثانية، بما في ذلك أعمال شغب في شوارع العاصمة.[672] وفضلاً عن أشكال الاحتجاج التقليدية، اكتشفت إستونيا آنذاك عدة موجات من الهجمات المتصلة بالحاسوب والموجهة ضد المواقع الشبكية والخدمات على الخط الحكومية والتجارية الخاصة،[673] بما في ذلك تشويه المواقع الشبكية،[674] وشن هجمات ضد مخدّمات أسماء الميادين وهجمات موزعة للحرمان من النفاذ إلى الخدمات (DDoS)، من خلال استخدام البرمجيات الروبوتية.[675] وفيما يخص هذا النوع الأخير من الهجمات أوضح الخبراء لاحقاً أن وقوع الهجمات الناجحة ضد المواقع الشبكية للمنظمات الحكومية في إستونيا لم يكن ليحدث لولا عدم كفاية تدابير الحماية.[676] كما كان أثر الهجمات ومصدرها موضوع مناقشة مثيرة للجدل.[677] وفي حين أفادت التقارير[678] والمقالات[679] الإخبارية بأن الهجمات كادت أن توقف البنية التحتية الرقمية للبلد، تظهر بحوث أكثر موثوقية أن أثر الهجمات كان محدوداً سواء فيما يتعلق بالأنظمة الحاسوبية المتضررة أو المدة التي توقف فيها الخدمات.[680] ودار نقاش مماثل فيما يتعلق بتحديد مصدر الهجمات.[681] فبينما قيل خلال الهجمات إن أراضي الاتحاد الروسي هي مصدرها،[682] أظهر تحليل الهجمات أنها متصلة في الواقع بأكثر من 170 بلداً.[683] وحتى

وإن كانت الدوافع وراء الهجوم سياسية، فإنه لا يشكل بالضرورة عملاً حربياً. ونتيجة لذلك، يتعين استبعاد حالة إستونيا من القائمة. وعلى الرغم من أن الهجمات كانت متصلة بالحاسوب وموجهة ضد مواقع شبكية وخدمات على الخط حكومية وتجارية خاصة، بما فيها تشويه المواقع الشبكية[684] وشن هجمات موزعة للحرمان من النفاذ إلى الخدمات،[685] لا يمكن تصنيف هذه الهجمات (DDoS) كحرب سيبرانية لأنها لم تشكل عملاً عدائياً ولم تحدُث أثناء نزاع بين دولتين تتمتعان بالسيادة.

ومن بين الهجومين المذكورين أعلاه، يُعد هجوم سنة 2008 على الأنظمة الحاسوبية في جورجيا الأقرب إلى هجوم متصل بالحرب. ففي سياق نزاع مسلح تقليدي[686] بين الاتحاد الروسي وجورجيا، اكتُشفت عدة هجمات متصلة بالحاسوب وموجهة ضد مواقع شبكية وشركات حكومية جورجية[687] (بما فيها تشويه المواقع الشبكية وشن هجمات موزعة للحرمان من النفاذ إلى الخدمات).[688] ومثلما كان الأمر في الحادث الذي شهدته إستونيا، نُوقش مصدر الهجوم ضد جورجيا نقاشاً مستفيضاً في وقت لاحق. وعلى الرغم من أن بعض التقارير الإخبارية[689] حددت على ما يبدو المصدر الجغرافي للهجوم، فإن البحوث القائمة على التكنولوجيا تشير إلى استخدام البرمجيات الروبوتية، مما يزيد إلى حد كبير من صعوبة تحديد المصدر.[690] ومن شأن عدم القدرة على تحديد مصدر الهجمات إلى جانب اختلاف الأفعال المكتشفة اختلافاً كبيراً عن الحرب التقليدية أن يجعلا من الصعب وصف الهجمات كحرب سيبرانية.

وبقدر ما يكتسي النقاش حول هذه الظاهرة أهمية كبيرة، تجدر الإشارة إلى أن هذه الهجمات ليست ظاهرة غير مسبوقة. فالدعاية تُنشر عن طريق الإنترنت والهجمات ضد الأنظمة الحاسوبية الخاصة بالتحالفات العسكرية باتت مفهوماً شائعاً بالأحرى. وقد اكتُشفت بالفعل خلال الحرب في يوغوسلافيا هجمات ضد الأنظمة الحاسوبية لحلف الناتو آتية من صربيا.[691] ورداً على تلك الهجمات، شاركت الدول الأعضاء في حلف الناتو حسب التقارير في هجمات مشابهة ضد الأنظمة الحاسوبية في صربيا.[692] كما استُخدمت استخداماً مكثفاً أشكال أخرى من الدعاية المتصلة بالحاسوب وغيرها من أشكال عمليات الحرب النفسية (PSYOPS) الرامية إلى خفض الروح المعنوية للطرف الآخر.[693]

أهمية التمييز

يتجلى في الأفعال المحتمل اتصالها بالحرب العديد من أوجه التشابه مع أشكال أخرى من أشكال سوء استخدام تكنولوجيا المعلومات والاتصالات، من قبيل الجريمة السيبرانية واستخدام الإرهابيين للإنترنت. ونتيجة لذلك تستخدم في أغلب الأحيان مصطلحات "الجريمة السيبرانية" و"استخدام الإرهابيين للإنترنت" و"الحرب السيبرانية" كمترادفات. لكن التمييز بينها مهم للغاية بما أن الأُطُر القانونية المطبّقة تختلف اختلافاً كبيراً. وفي حين يجري التصدي عموماً للجريمة السيبرانية من خلال إجراءات تجرّم هذا الفعل، فإن القواعد والإجراءات المتصلة بالحرب تخضع إلى حد كبير للقانون الدولي، ولا سيما ميثاق الأمم المتحدة.

3.9.2 غسل الأموال السيبراني

في عام 2013، تصدّر عناوين الصحف نبأ إغلاق مورّد العملات الإلكترونية "Liberty Reserve".[694] وقد تمثل هذه القضية، التي انطوت على ما يقدر بمبلغ 6 مليارات دولار أمريكي، أكبر قضية غسل أموال سيبراني في التاريخ.[695] وفي عام 2013، نشرت وزارة الخزانة الأمريكية تفاصيل الاستنتاجات فيما يتعلق بالقضية.[696] وقد بدّلت الإنترنت ملامح عملية غسل الأموال. وإذا كانت التقنيات التقليدية لغسل الأموال مازالت توفر عدداً من المزايا فيما يخص المبالغ الكبيرة، فإن الإنترنت توفر من جهتها مزايا جمّة. فالخدمات المالية المتاحة على الخط تتيح إجراء معاملات مالية متعددة على النطاق العالمي بسرعة بالغة. وأسهمت الإنترنت في التغلّب على الاعتماد على المعاملات النقدية المادية. وحلّت 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 الجُناة على ابتكار تقنيات جديدة. ويستند كشف المعاملات المشتبه فيها في إطار مكافحة غسل الأموال إلى التزامات المؤسسات المالية المشاركة في عملية التحويل.[697]

وينقسم غسل الأموال بوجه عام إلى ثلاث مراحل هي: الاستثمار والترقيد والإدماج.

وفيما يتعلق باستثمار كميات كبيرة من النقد قد لا يوفر استخدام الإنترنت مزايا ملموسة جمّة.[698] غير أن الإنترنت تُعدّ مفيدة بوجه خاص للجناة في مرحلة الترقيد (أو الإخفاء). وفي هذا السياق، يُعدّ تقصّي غسل الأموال صعباً بوجه خاص عندما يلجأ غاسلو الأموال إلى كازينوهات القمار المتاحة على الخط لترقيد أموالهم.[699]

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

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 0,10 دولار أمريكي أو أقل)، حيث يكون من الصعب استخدام بطاقات الائتمان. ومع تنامي الطلب على المدفوعات البالغة الصِّغر، ابتُكرت 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 إن بعض موفري هذه الحسابات يتيحون التحويل المباشر بين النظراء (من شخص لآخر) أو سحب مبالغ نقدية.[700] ويستطيع الجناة أن يفتحوا حسابات ذهبية إلكترونية في بلدان مختلفة وأن يجمعوا بينها، مما يُعقد سُبُل استخدام الأدوات المالية في غسل الأموال وتمويل الإرهاب. وقد يستخدم أيضاً أصحاب الحسابات معلومات غير دقيقة أثناء التسجيل لإخفاء هويتهم.[701]

وإلى جانب العملات الافتراضية البسيطة، توجد أيضاً عملات تجمع بين الجانب الافتراضي وعدم الكشف عن الهوية. ومن أمثلتها عملة *Bitcoin*، وهي عملة افتراضية تستخدم تكنولوجيا الاتصال بين النظراء.[702] ورغم أنها نظام لا مركزي لا يستلزم وسطاء مركزيين لضمان صحة الهيئات المعنية بإجراء الصفقات، فإن هجمات ناجحة وقعت في سنة 2011 تؤكد أوجه الضعف/المخاطر المتصلة بهذه العملات الافتراضية اللامركزية.[703] وفي حالة إذا استخدم مجرمون هذه العملات المجهولة المصدر، فإن هذا سيحدّ من قدرة سلطات إنفاذ القانون على تحديد المشتبه فيهم من خلال تعقّب التحويلات النقدية[704] – في الحالات المتعلقة مثلاً بالاستغلال التجاري للأطفال في المواد الإباحية.[705]

استخدام كازينوهات القمار على الخط

خلافاً لكازينوهات القمار الحقيقية، لا يقتضي الأمر توظيف استثمارات مالية كبيرة لإنشاء كازينوهات القمار على الخط.[706] وبالإضافة إلى ذلك، فإن الأنظمة المتعلقة بكازينوهات القمار المتاحة على الخط وخارج الخط تتفاوت في كثير من الأحيان فيما بين البلدان.[707] 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، تنبُع الصعوبات الناشئة عن الأنظمة من التحديات المصادفة في التحقق من الزبائن، لأنه قد يكون من الصعب إجراء تحقق دقيق إذا كان مقدم الخدمة المالية والزبون لا يلتقيان أبداً.[708] وإلى جانب هذا، فإن الافتقار إلى الاتصال الشخصي يجعل من الصعب تطبيق الإجراءات التقليدية القاضية بالتعرف على الزبون. كما أن تحويلات الإنترنت تنطوي في أغلب الأحيان على مشاركة من مقدمي الخدمة في بلدان مختلفة عبر الحدود. وأخيراً، من الصعب بوجه خاص رصد الصفقات عندما يسمح مقدمو الخدمة للزبائن بنقل القيمة وفقاً لنموذج التعامل بين النظراء.

4.9.2 التصيُّد الاحتيالي

استحدثت الجناة تقنيات تتيح لهم الحصول على معلومات شخصية من المستخدمين، تتراوح من برمجيات التجسس[709] إلى هجمات "التصيّد الاحتيالي".[710] ويُقصد بمصطلح "التصيّد الاحتيالي" أفعالاً تنفذ لجعل الضحايا يفصحون عن معلومات شخصية/سرية.[711] وهناك أنواع مختلفة من برمجيات التصيّد الاحتيالي[712] 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") تتطلّب من الضحايا القيام بإجراءات الدخول العادية، مما يمكّن 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،[713] مما يُسفر في كثير من الأحيان عن انتهاكات للعلامات التجارية.[714] وتطلب الرسائل المزيفة من متلقيها تسجيل بيانات الدخول من أجل إجراء عمليات تحديث أو عمليات للتحقق الأمني، وقد تلجأ أحياناً إلى التهديد (بإقفال الحساب مثلاً) في حالة عدم تعاون المستخدمين. وتحتوي الرسائل المزيفة عادة على وصل ينبغي أن يتبعها الضحية تقوده إلى الموقع الإيهامي، كي لا يدخل المستخدمون يدوياً إلى عنوان الويب الصحيح للبنك المشروع. وقد استحدث الجناة تقنيات متقدمة تمنع المستخدمين من تبيّن أنهم ليسوا في موقع الويب الحقيقي.[715]

وبمجرّد 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 التصيّد الاحتيالي.[716] ففي أبريل 2007، أُبلغ فريق العمل المعني بمكافحة التصيّد الاحتيالي[717] بأكثر من 55 000 موقع اصطياد قائم بذاته.[718] وفي يناير 2014 ارتفع عدد مواقع التصيد الاحتيالي وكاد يبلغ 43 000 موقع.[719] ولا تقتصر تقنيات التصيّد 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 تُعدّ هامة بوجه خاص في الولايات المتحدة ويمكن استخدامها في ارتكاب جرائم "انتحال الهوية".[720]

---

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

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

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

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

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

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

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

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

95 Article 1, Definitions and Use of Terms,

For the purposes of this Convention:

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

[…]

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

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

98 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq.*

99 Universal serial bus (USB)

100 Article 4 – Data Interference:

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

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

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

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

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

104 *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-

in-france-overview; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

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

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

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

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

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

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

111 See below: § 2.5.

112 See below: § 2.6.

113 See below: § 2.7.

114 See below: § 2.8.

115 See below: Chapter 2.8.1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

138 Third Interpol Symposium on International Fraud, France 1979.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

162 German Crime Statistics 2009, available at www.bka.de. As this number also includes traditional crimes that involved Internet technology at any stage of the offence, the increase of cases cannot necessarily be used to determine the specific development in the typology-based crime fields.

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

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

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

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

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

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

169 The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise

News, 27.10.2007, – available at: www.heise-security.co.uk/news/80152. See also: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, page 660.

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

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

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

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

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

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

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

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

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

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

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

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

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

183 2010 CSO CyberSecurity Watch Survey, 2010.

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

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

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

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

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

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

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

191 See 2005 FBI Computer Crime Survey, page 10.

192 See: § 2.4.

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

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

195 Computer Security Institute (CSI), United States.

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

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

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

199 See below: § 2.4.

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

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

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

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

204 See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61; *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

232 One example of this is the German Criminal Code, 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

293 Annual Report, Pandalabs, 2013.

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

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

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

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

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

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

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

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

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

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

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

305 *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;

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

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

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

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

(1) Whoever: 1. domestically distributes or publicly uses, in a meeting or in writings (Section 11 subsection (3)) disseminated by him, symbols of one of the parties or organizations indicated in Section 86 subsection (1), nos. 1, 2 and 4; or 2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use domestically or abroad, in the manner indicated in number 1, shall be punished with imprisonment for not more than three years or a fine.

(2) Symbols, within the meaning of subsection (1), shall be, in particular, flags, insignia, uniforms, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in sentence 1 shall be deemed to be equivalent thereto.

(3) Section 86 subsections (3) and (4), shall apply accordingly.

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

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

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

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

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

315 International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, and the ACHPR (African Commission on Human and Peoples Rights) Special Rapporteur on Freedom of Expression and Access to Information, 2008.

316 See below: §§ 3.2.6 and 3.2.7.

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

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

Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

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

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

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

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

323 Depending on the availability of broadband access.

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

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

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

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

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

Section 184 Dissemination of Pornographic Writings

(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

378 See below: § 3.2.14.

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

380 See below: § 3.2.14.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

402 www.secondlife.com.

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

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

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

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

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

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

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

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

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

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

413 See Art. 300 China Criminal Code:

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

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

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

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

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

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

419 See § 5367 Internet Gambling Prohibition Enforcement Act.

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

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

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

423 Regarding the controversial discussion about the criminalization of defamation, see: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: 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: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf.

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

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

426 See: www.wikipedia.org

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

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

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

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

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

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

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

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

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

436 Kaspersky Security Bulletin. Spam Evolution 2013.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

451 KPMG E-Crime Study 2013, page 7.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

493 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions. See *Gecko*, The criminalization of Phishing and Identity Theft, Computer und Resht, 2005, 606; *Ullman*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: § 2.9.4.

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

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

496 Another term used to describe the phenomenon is "domain grabbing". Regarding cybersquatting, see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from cybersquatters, Virginia Journal of Law and Technology, Vol. 10,

Issue 6; *Binomial*, Cyberspace Technological Standardization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 *et seq.*; *Struve/Wagner*, Real space Sovereignty in Cyberspace: Problems with the Ant cybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 *et seq.*; *Travis*, The Battle for Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003.

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

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

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

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

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

502 Regarding the related challenges, see below.

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

504 Regarding the related automation process: § 3.2.8.

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

506 For more information, see below: § 6.2.14.

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

508 See www.ebay.com.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

530 Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15 per cent obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

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

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

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

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

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

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

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

538 *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270.

539 Unlike in the industrial society, members of the information society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society, see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

540 *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 51.

541 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 6.

542 35 per cent of the overall number of cases.

543 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 6.

544 Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07_935T, page 4.

545 *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

546 See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 555.

547 *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science Technology Society, 2007, Vol. 27, 2008, page 20.

548 See Encyclopaedia Britannica 2007.

549 *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, 533.

550 *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

551 In some cases perpetrators used the data they obtained to hide their real identity. Regarding this aspect, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

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

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

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

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

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

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

558 For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

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

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

561 The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of cybercrime businesses. It is based on the responses of 494 computer security practitioners from in US corporations, government agencies and financial institutions. The survey is available at: www.gocsi.com/

562 2013 US State of Cybercrime Survey, How Bad is the Insider Threat, Carnegie Mellon University, 2013.

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

564 For more details, see: *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

565 *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

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

567 *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005, page 6; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

568 Examples is the online community Facebook, available at www.facebook.com.

569 See for example Art. 5 of the Directive 2000/31/Ec Of The European Parliament And Of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

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

571 Regarding forensic analysis of e-mail communication, see: *Gupta*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

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

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

574 Press release from the Bureau of Justice Statistics, 12.12.2013, available at: www.bjs.gov/content/pub/press/vit12pr.cfm .

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

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

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

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

579 The United States Federal Bureau of Investigation (FBI) requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. The Head of the FBI office in New York is quoted as saying: "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack". See: Heise News, available at: www.heise-security.co.uk/news/80152.

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

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

582 The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: § 3.2.3.

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

584 For an overview about the tools used, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (USD 200-500), see: *Paget*, Identity Theft, White Paper, McAfee, 2007, available at: www.mcafee.com/us/threat_center/white_paper.html.

585 See above: § 2.5.1.

586 For more examples, see: The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 23 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law-enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

587 DoS is an acronym for denial-of-service attack. For more information, see above: § 2.5.5.

588 These generally contain two elements: Software that automates the process of sending out e-mails by avoiding techniques that enable e-mail providers to identify spam e-mails and a database with thousands or even millions of e-mail addresses. For more information, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 25, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

589 For more details, see below: § 6.2.14.

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

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

592 The CIA pointed out in 2002 that attacks against critical infrastructure in the United States will become an option for terrorists. Regarding the CIA position, see: *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007, page 13, available at: 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 cyberterrorism 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.

593 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.

594 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 seq*., 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 seq.; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: 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 seq.*; 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.

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

596 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; *Zeller*, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;

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

598 For an overview, see: *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*

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

600 Regarding different international approaches as well as national solutions, see: *Sieber* in Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007

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

602 Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyberattacks During the War on Terrorism, page 14ff.; *Clark*, Computer Security Officials Discount Chances of "Digital Pearl Harbour", 2003; USIP Report, Cyberterrorism, How real is the threat, 2004, page 2; *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats; Wilson in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

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

604 *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

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

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

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

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

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

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

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

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

613 Videos showing the execution of American citizens Berg and Pearl were made available on websites. See *Weimann* in the USIP Report: How Terrorists use the Internet, 2004, page 5.

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

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

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

617 For more information regarding the search for secret information with the help of search engines, see: *Long, Skoudis, van Eijkelenborg*, Google Hacking for Penetration Testers.

618 "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy." For further information, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information & Security, 2006, page 17.

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

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

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

622 See US Commission on Security and Cooperation in Europe Briefing, 15.05.2008, available at: http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecordType=B&CFID=18849146&CFTOKEN=53; *O'Brian*, Virtual Terrorists, The Australian, 31.07.2007, available at: http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html*; O'Hear*, Second Life a terrorist camp?, ZDNet.

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

624 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008, page 215 *et seq.*

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

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

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

628 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=.

629 The Commission analysing the 9/11 attacks calculated that the costs for the attack could have been between USD 400 000 and 500 000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved, the cost per person was relatively small. Regarding the related challenges, see also: *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

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

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

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

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

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

635 *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats, Center for Strategic and International Studies, December 2002.

636 *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf.

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

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

639 CERT Research 2006 Annual Report, page 7 *et seq.*, available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

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

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

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

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

644 Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

645 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

646 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

647 Cybersecurity Communique, American Gas Association, 2010, available at: https://www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

648 *Falliere/Murchu/Chien*, W32.Stuxnet Dossier, Symantec, November 2010, page 1; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

649 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

650 Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

651 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1; Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

652 See for example: *Leyden*, Lame Stuxnet Worm: "Full of Errors" says Security Consultant, The Register, 19.02.2011.

653 *Albright/Brannan/Walrond*, Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 22.12.2010; *Broad/Markoff/Sanger*, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times, 15.01.2011; *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 2; *Timmerman*, Computer Worm Shuts Down Iranian Centrifuge Plant, Newsmax, 29.11.2010.

654 *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: www.pp.bme.hu/tr/2003_1/pdf/tr2003_1_03.pdf; *Merten/Teufel*, Technological Innovations in the Passenger Process of the Airline Industry: A Hypotheses Generating Explorative Study in O'Conner/Hoepken/Gretzel, Information and Communication Technologies in Tourism 2008.

655 Sasser B Worm, Symantec Quick reference guide, 2004, available at: http://eval.symantec.com/mktginfo/enterprise/other_resources/sasser_quick_reference_guide_05-2004.en-us.pdf.

656 *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; The Sasser Event: History and Implications, Trend Micro, June 2004, available at: http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp02sasserevent040812us.pdf.

657 *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP, 1997; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

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

659 *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html.

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

661 Improving our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center, Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary United States Senate One Hundred Seventh Congress First Session, July 2001, Serial No. J–107–22, available at: http://cipp.gmu.edu/archive/215_S107FightCyberCrimeNICPhearings.pdf.

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

663 Regarding the Stuxnet software, see: *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1.000 Centrifuges at the Nataz Enrichment Plant? Preliminary Assessment, Institute for Science and International Security, 2010.

664 *Wilson*, Information Operations and Cyberwar, Capabilities and related Policy Issues, CRS Report for Congress, RL21787, 2006; *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996..

665 *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

666 *Schwartau*, Information Warfare: Chaos on the Electronic Superhighway, 1994, page 13.

667 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

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

669 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

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

671 *Libicki*, Sub Rosa Cyberwar, COEP, 2010.

672 *Myers*, Estonia removes Soviet-era war memorial after a night of violence, The New York Times, 27.04.2007; Estonia removes Soviet memorial, BBC News, 27.04.2007; *Tanner*, Violence continues over Estonia's removal of Soviet war statue, The Boston Globe, 28.04.2007.

673 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

674 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

675 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

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

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

678 See for example: *Landler/Markoff*, Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007.

679 *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27, page 193.

680 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18-20.

681 Estonia hit by Moscow cyberwar, BBC News, 17.05.2007; *Traynor*; Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17.05.2007.

682 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

683 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

684 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007..

685 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

686 Regarding the background to the conflict, see: Council of Europe Parliamentary Assembly Resolution 1633 (2008), The consequences of the war between Georgia and Russia.

687 *Tikk/Kaska/Rünnimeri/Kert/Talihärm/Vihul*, Cyberaattacks Against Georgia: Legal Lessons Identified, 2008, page 4; *Hart*, Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar, Washington Post, 14.08.2008; Cybersecurity and Politically, Socially and Religiously Motivated Cyberattacks, European Union, Policy Department External Policies, 2009, page 15; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

688 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

689 See for example: *Partitt,* Georgian blogger Cyxymu blames Russia for cyberattack, The Guardian, 07.08.2009.

690 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 75; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

691 See *Walker*, Information Warfare and Neutrality, *Vanderbilt Journal of Trans-national Law* 33, 2000; *Banks*, Information War Crimes: Mitnick meets Milosevic, 2001, AU/ACSC/019/2001-04.

692 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyberforce, Alb. Law Journal of Science and Technology, Vol. 18, page 315.

693 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 61.

694 *Rushton*, Liberty Reserve shut down in $6bn money laundering case, The Telegraph, 28.05.2013.

695 Santora/Rashbaum/Perlroth, Online Currency Exchange Accused of Laundering $ 6 Billion, NYT.

696 Notice of Finding, Departement of the Treasury, 2013, available at: www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf .

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

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

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

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

701 Regarding the related challenges, see below: § 3.2.I.

702 Regarding the fundermental concept see: Nakamoto (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

703 Regarding the attacks see: Cohen, Speed Bumps on the Road to Virtual Cash, NYT, 3.7.2011, available at: www.nytimes.com/2011/07/04/business/media/04link.html.

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

705 Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at: http://www.missingkids.com/en_US/documents/FCACPTrendsInOnlineCrimePaper2011.pdf

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

707 Regarding approaches to the criminalization of illegal gambling, see below: § 6.2.12.

708 See: Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000-2001, 2001, page 2.

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

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

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

712 The following section describes e-mail-based phishing attacks, compared to other phishing scams, which may, for example, be based on voice communications. See: *Gonsalves*, Phishers Snare Victims with VoIP, 2006, available at: www.techweb.com/wire/security/186701001..

713 "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organized crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see above: § 2.6.7.

714 Regarding related trademark violations, see above: § 2.7.2.

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

716 In some phishing attacks, as many as 5 per cent of victims provided sensitive information on fake websites. See *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, page 1, that refers to *Loftesness*, Responding to "Phishing" Attacks, Glenbrook Partners (2004).

717 Anti-Phishing Working Group. For more details, see: www.antiphishing.org.

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

719 Phishing Activitiy Trends Report, 1st Quarter 2014, WPWG, 2014.

720 See above: § 2.8.3.

3 تحديات مكافحة الجريمة السيبرانية

Bibliography (selected): *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV; *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142; *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 291 *et seq.*; *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2; *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19; *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*; *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001; *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago. edu/Papers/PickerCyber.200.pdf; *Putnam/Elliott*, International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004; *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003; *Wallsten*, Regulation and Internet Use in Developing Countries, 2002.

أسفرت التطورات التي استُجدّت 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 التعرّف عليهم ولتعويق التحقيقات. ويركّز هذا الفصل على التحديات المصادفة في مكافحة الجريمة السيبرانية.

1.3 الفرص

على الرغم من أن تطور بعض خدمات تكنولوجيا المعلومات والاتصالات، مثل مخدمات الاتصالات المغفلة الهوية أو الأدوات المقاومة للتحقيقات الجنائية، من شأنه أن يعيق بجدية التحقيقات، فقد أفادت التطورات التقنية بمثابة عوامل تمكين لمزيد من التحقيقات المتقدمة.

1.1.3 الأتمتة العامة للتحقيقات

كان البحث في الماضي عن الأدلة ذات الصلة بحاسوب شخص مشتبه به يجري أساساً يدوياً. وقد غيّر تطور أدوات التحقيق الجنائي المتقدمة هذا الوضع جذرياً. وبمقدور وكالات إنفاذ القانون الآن أن تستخدم القوة المتزايدة للنظم الحاسوبية وبرمجيات الأدلة الجنائية المعقدة للإسراع بالتحقيقات ولأتمتة إجراءات البحث.[721] ومع ذلك لا يمكن أتمتة كل طرائق 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 النُّهُج المعتمدة على قيمة الفرم ناجحة إلا إذا كانت الصور قد سبق تصنيفها، وكانت قيمة الفرم قد خُزّنت في قاعدة بيانات، ولم تكن الصورة التي حُللت قد تم تعديلها.[722]

وتتسم برمجيات الأدلة الجنائية بالقدرة على البحث آلياً عن صور المواد الإباحية التي يُستغل فيها الأطفال وذلك عن طريق مقارنة الملفات الموجودة في الأقراص الصلبة للمشتبه فيهم مع المعلومات عن الصور المعروفة. ومن ذلك مثلاً، 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. وتمكن خبراء الأدلة الجنائية الحاسوبية من تفكيك التعديلات وإعادة بناء وجه المشتبه فيه.[723] 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 يُستغل فيها الأطفال. فلو كان الجاني قد غطى ببساطة وجهه بنقطة بيضاء لكان اكتشاف هويته أمراً مستحيلاً.

2.1.3 استحداث البيانات في الخدمات على الخط

كما أشير أعلاه، تلقى الخدمات المتصلة بتكنولوجيا المعلومات والاتصالات رواجاً كبيراً. وما الفيسبوك ويوتيوب وتويتر وإينستاغرام سوى بعض الأمثلة لخدمات تضم الملايين من المستعملين[724] ومعظمها يتعقب على نحو مكثف أنشطة مستعمليها،[725] بل هو جزء من نموذج أعمال تلك الشركات. وفي نفس الوقت قد تكون هذه البيانات ذات أهمية كبيرة بالنسبة للمحققين. فإذا كان من الممكن قانونياً طلب الحصول على هذه المعلومات واستخدامها، يستطيع المحققون إجراء تحقيق متطور للغاية ويمكنهم مثلاً التحقق من هوية المشتبه به قبل ارتكاب جريمة يكاد لا يستطيع أن يقوم بها شخص واحد. والمعلومات الموقعية التي تستحدثها شركات الهاتف الخليوي يمكن أن تكون على قدر مماثل من الأهمية، حيث يمكن أن تكشف هذه البيانات عما إذا كان الهاتف الخليوي للشخص المشتبه في مكان قريب من مسرح الجريمة وقت ارتكابها.[726]

3.1.3 استحداث البيانات ضمن عمليات الرقمنة خارج الخط

أصبحت تكنولوجيا المعلومات والاتصالات تستخدم ضمن العمليات اليومية بشكل مكثف. وهذا يؤدي إلى استحداث المزيد من البيانات التي يمكن أن تستخدمها – تبعاً للتصريح بالنفاذ إلى هذه البيانات واستخدامها في التحقيقات الجنائية – الوكالات المكلفة بإنفاذ القانون. ولا يقتصر ذلك على الخدمات الجديدة الرقمية البحتة، مثل الشبكات الاجتماعية التي تجتذب اهتمام المستعملين وتخزن البيانات، بل يشمل الخدمات التقليدية خارج الخط التي تضطلع بمراحل من عملية الرقمنة. مثال ذلك زيادة استخدام تكنولوجيا المعلومات والاتصالات في الخدمات البريدية.[727] حيث تستخدم الماسحات الضوئية عالية السرعة لمسح العنوان وتحويله إلى بيانات إلكترونية.[728] وقد أخذ بتقنية من هذا القبيل في الولايات المتحدة في وقت مبكر في ثمانينيات القرن الماضي.[729]

وفي عام 2013 جاء في الصحف أن الخدمات البريدية الأمريكية تسجل كل البريد لأغراض تحقيقات إنفاذ القانون. وفي إطار برنامج عزل البريد والتحكم فيه وتقصيه (MICT) الذي استحدث في عام 2011 بعد هجمات الجمرة الخبيثة في الولايات المتحدة، يتم الاحتفاظ بصورة من كل رسالة وطرد يرسل في الولايات المتحدة.[730] وقد استخدمت هذه المعلومات في التحقيقات الجنائية.[731]

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.[732] وتُعدّ تكنولوجيا المعلومات والاتصالات مسؤولة الآن عن مراقبة وإدارة الوظائف في المباني،[733] والسيارات، وخدمات الطيران.[734] كما تعتمد إمدادات الطاقة والمياه ومرافق الاتصالات على تكنولوجيا المعلومات والاتصالات. ومن المرجّح أن يستمر تغلغل هذه التكنولوجيا بقدر أكبر في الحياة اليومية.[735] وتزايد الاعتماد على تكنولوجيا المعلومات والاتصال يجعل النظم والخدمات أكثر عُرضة للهجمات الموجهة ضد البُنى التحتية الحاسمة.[736] فحتى الانقطاعات القصيرة في الخدمات يمكن أن تسبب أضراراً مالية ضخمة لشركات التجارة الإلكترونية.[737] فالهجمات ليس بمقدورها أن تعطل الاتصالات المدنية وحدها؛ ذلك أن الاعتماد على تكنولوجيا المعلومات والاتصالات يشكل خطراً كبيراً على الاتصالات العسكرية أيضاً.[738]

وتعاني البُنى 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 مايكروسوفت،[739] ولذا فإن الجناة يستطيعون أن يصمموا هجمات ناجعة بالتركيز على هذا الهدف الواحد.[740]

واعتماد المجتمع على تكنولوجيا المعلومات والاتصالات لا يقتصر على البلدان الغربية.[741] فالبلدان النامية تواجه أيضاً تحديات فيما يتعلق بدرء الهجمات الموجهة ضد بُناها التحتية وضد المستخدمين الموجودين بها.[742] واستحداث بُنى تحتية تكنولوجية أزهد تكلفة مثل واي ماكس WiMAX[743] (قابلية التشغيل على الصعيد العالمي فيما يخص النفاذ بالموجات الصِّغرية) قد يُمكّن البلدان النامية من توفير خدمات الإنترنت لعدد أكبر من الناس. وتستطيع البلدان النامية أن تتجنّب أخطاء بعض البلدان الأوروبية التي ركزت أساساً على تعظيم فرص النفاذ دون توظيف استثمارات ذات شأن في مجال الحماية. وأوضح خبراء من الولايات المتحدة أن الهجمات الناجحة ضد موقع الويب الرسمي للمنظمات الحكومية في إستونيا[744] لم يكن ليحدُث لولا عدم كفاية تدابير الحماية[745] 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.[746]

ويجب وضع استراتيجيات لدرء هذه الهجمات ولاستحداث تدابير مضادة، تشمل استنباط وتعزيز السبل التقنية للحماية، بالإضافة إلى وضع قوانين مناسبة وكافية تمكّن وكالات إنفاذ القانون من مكافحة الجريمة السيبرانية على نحو فعال.[747]

2.2.3 عدد المستخدمين

تنمو شعبية الإنترنت وخدماتها نمواً سريعاً، إذ يزيد عدد مستخدميها على ملياري نسمة على الصعيد العالمي في سنة 2010.[748] وتركز شركات الحاسوب ومقدمو خدمة الإنترنت على البلدان النامية التي توجد بها أعظم الإمكانات للنمو الإضافي.[749] وفي عام 2005، تجاوز عدد مستخدمي الإنترنت في البلدان النامية عددهم في البلدان الصناعية،[750] في حين سيُمكّن استحداث الأجهزة الرخيصة وتنمية فرص النفاذ اللاسلكي مزيداً من الناس من النفاذ إلى الإنترنت.[751]

ومع تنامي عدد الأشخاص الموصولين بالإنترنت، يتزايد عدد الأهداف وعدد الجناة.[752] ومن الصعب تقدير عدد من يستخدمون الإنترنت في أنشطة إجرامية. فحتى لو لم تزِد 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 تُعد أكثر انخفاضاً في البلدان النامية، فإن تعزيز الأمن السيبراني ليس أكثر سهولة فيها، لأن الجناة يستطيعون ارتكاب جرائمهم من أي مكان في العالم.[753]

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 أشدّ صعوبة. فالنُّهُج المعتمدة على قيمة الفرم مثلاً لا تكون ناجحة إلا إذا كانت الصور قد سَبق تصنيفها، وكانت قيمة الفرم قد خُزّنت في قاعدة بيانات، ولم تكن الصورة التي حُلِّلت قد تمّ تعديلها.[754]

3.2.3 توفر الأجهزة وفرص النفاذ

لا تلزم إلا معدات أساسية لارتكاب الجرائم الحاسوبية. فما يتطلبه ارتكاب جريمة هو المعدات والبرمجيات والنفاذ إلى الإنترنت.

وفيما يتعلق بالمعدات، تتنامى قوة الحواسيب باطّراد.[755] وهناك عدد من المبادرات التي تُمكّن الناس في البلدان النامية من استخدام تكنولوجيا المعلومات والاتصالات على نطاق واسع.[756] 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 البرمجياتية المتخصصة أن تجعل ارتكاب الجريمة السيبرانية أكثر سهولة. ويستطيع الجناة أن يقوموا بتنزيل أدوات برمجياتية[757] مصممة كي تُعين موضع المنافذ المفتوحة أو كي تخترق حماية كلمة السر.[758] ومن الصعب تقييد الانتشار الواسع لهذا النوع من الأجهزة بسبب تقنيات المحاكاة والتبادل بين النظراء.[759]

والعنصر الحيوي الأخير هو النفاذ إلى الإنترنت. وعلى الرغم من أن تكلفة النفاذ إلى الإنترنت[760] تُعدّ أعلى في معظم البلدان النامية عن نظيرتها في البلدان الصناعية، فإن عدد مستخدمي الإنترنت في البلدان النامية يتزايد بسرعة.[761] 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 السُّبُل النموذجية للنفاذ إلى الشبكات ما يسمّى بـ "التجول الحربي" ويُقصد بهذا المصطلح التجوّل بحثاً عن شبكات لا سلكية يمكن النفاذ إليها.[762] وأكثر الأساليب انتشاراً التي يمكن أن يستخدمها المجرمون للنفاذ إلى الشبكة بصفة مجهولة إلى حد ما هي الوحدات المطرافية العمومية للإنترنت، والشبكات (اللاسلكية) المفتوحة،[763] والشبكات التي أخضعتها القرصنة، والخدمات المدفوعة الثمن مقدماً دون تطبيق متطلبات تسجيل.

وتتخذ وكالات إنفاذ القانون إجراءات لتقييد النفاذ بلا ضوابط إلى خدمات الإنترنت تجنّباً لاستخدام هذه الخدمات في ارتكاب الجرائم. ففي إيطاليا والصين، على سبيل المثال، يتطلّب استخدام الوحدات المطرافية للإنترنت تعريف المستخدمين لأنفسهم.[764] غير أن هناك حججاً تعارض تطبيق متطلبات التعريف هذه.[765] فعلى الرغم من أن تقييد النفاذ يمكنه أن يمنع ارتكاب الجرائم وييسّر التحقيقات التي تجريها وكالات إنفاذ القانون، فإن هذه التشريعات يمكن أن تعوق نمو مجتمع المعلومات وتنمية التجارة الإلكترونية.[766]

وقد أُشير إلى أن تقييد النفاذ إلى تقييد النفاذ إلى الإنترنت على هذا النحو يمكن أن يشكل انتهاكاً لحقوق الإنسان.[767] 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،[768] 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 توفر المعلومات

تضمُّ الإنترنت الملايين من صفحات الويب[769] التي تحتوي على أحدث المعلومات. ويمكن أن يشارك في ذلك أي شخص ينشر أو يتعهد صفحة ويب. ومن الأمثلة على نجاح المواقع التي يُعدُّها المستخدمون موسوعة ويكيبيديا،[770] المتاحة على الخط والتي يستطيع أي إنسان أن ينشر فيها.[771]

كما يعتمد نجاح الإنترنت أيضاً على محركات بحث قوية تمكِّن 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.[772] وقد سلَّطت التقارير الضوء على احتمال استخدام محركات البحث في أغراض غير قانونية.[773] 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.[774] وعلى الرغم من أن مثل هذه المعلومات كانت متاحة قبل استحداث الإنترنت، فإن النفاذ إليها كان أشدَّ صعوبة. أما اليوم فقد أصبح باستطاعة أي مستخدم للإنترنت أن يَنْفذ إلى هذه المعلومات.

كما يستطيع المجرمون استخدام محركات البحث لتحليل الأهداف.[775] وقد وُجد أثناء التحقيقات مع أعضاء جماعة إرهابية دليل تدريبي يثبت مدى فائدة الإنترنت في جمع المعلومات عن الأهداف المحتملة.[776] 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).[777]

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 حَوكَمَة الإنترنت أن الإنترنت لا تختلف عن البُنى التحتية للاتصالات الوطنية بل وحتى عبر الوطنية.[778] ويتعين أيضاً أن تخضع الإنترنت لحكم القانون والمشرعين، وقد بدأت وكالات إنفاذ القانون في وضع معايير تستلزم درجة معينة من التحكم المركزي.

وقد صُمِّمَت الإنترنت في الأصل كشبكة عسكرية[779] تستند إلى معمار الشبكة اللامركزية، وهو معمار يسعى إلى الحفاظ على التشغيل الأساسي سليماً ومستمراً حتى لو تعرَّضت بعض مكونات الشبكة للهجوم. ونتيجة لذلك، تقاوم البنية التحتية للإنترنت محاولات التحكم الخارجي. فهي لم تُصمَّم أصلاً لتيسير التحقيقات الجنائية أو لمنع هجوم آتٍ من داخل الشبكة.

واليوم، تُستخدَم الإنترنت بشكل متزايد في الخدمات المدنية. ومع الانتقال من الخدمات العسكرية إلى الخدمات المدنية، تغيَّرت طبيعة الطلب على أدوات التحكم. فلما كانت الشبكة تعتمد على بروتوكولات مصمّمة 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.[780]

ومن أمثلة المشكلات الناجمة عن غياب أدوات التحكم أن المستخدمين يستطيعون الالتفاف على تكنولوجيا الترشيح[781] باستخدام مخدّمات اتصالات مجهولة مجفّرة.[782] 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 تجنّبه إذا استخدم الزبائن مخدم اتصالات مجهولاً يجفّر 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.

6.2.3 الأبعاد الدولية

تطالُ كثير من عمليات نقل البيانات أكثر من بلد واحد.[783] وتستند البروتوكولات المستخدمة لنقل البيانات على الإنترنت إلى مسار أمثل، في حال سد الوصلات المباشر بصفة مؤقتة.[784] وحتى عندما تكون عمليات النقل المحلي داخل بلد المصدر

محدودة، فإن البيانات يمكن أن تغادر هذا البلد فتنقل عبر مسارات خارج أراضيه ثم يُعادُ توجيهها إليه نحو المقصد النهائي فيه.[785] وعلاوةً على ذلك، فإن كثيراً من خدمات الإنترنت تستند إلى خدمات من الخارج،[786] فقد يؤجر مثلاً مقدم الخدمة المضيف مساحة على الويب في أحد البلدان بالاعتماد على معدات موجودة في بلد آخر.[787]

وإذا كان الجناة والأهداف موجودين في بلدان مختلفة، ستحتاج التحقيقات في الجريمة السيبرانية إلى تعاون وكالات إنفاذ القانون في كل البلدان المتضررة.[788] ولا تسمح السيادة الوطنية بإجراء تحقيقات داخل أراضي بلدان مختلفة دون إذن من السلطات المحلية.[789] 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.[790] إذ تنفذ التحقيقات في كثير من الأحيان ضمن أُطُر زمنية قصيرة للغاية.[791] والبيانات الحيوية لتعقّب 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.[792] كما يطرح مبدأ الإجرام المزدوج[793] صعوبات إذا كان الفعل المعني غير مُجرّم في أحد البلدان المشاركة في التحقيق.[794] وقد يدرج الجناة عن عَمد بلداناً ثالثة في هجماتهم لجعل التحقيق أكثر صعوبة.[795]

وقد يختار المجرمون عن عَمد أهدافاً تقع خارج بلدهم، ويأتون بأفعالهم انطلاقاً من بلدان تعاني من عدم كفاية التشريعات المتعلقة بالجريمة السيبرانية.[796] 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،[797] والأحكام المتعلقة بالتعاون الدولي الواردة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[798]

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 تُعد جرائم عبر وطنية. وتتطلب الجرائم السيبرانية الدولية كثيراً من الجهد والوقت. ويسعى مرتكبو هذه الجرائم إلى تجنّب البلدان التي تُطبّق فيها تشريعات قوية لمكافحة الجريمة السيبرانية.[799]

ويُعدُّ منع "الملاذات الآمنة" من التحديات الرئيسية المصادفة في مجال مكافحة الجريمة السيبرانية.[800] فما دامت هناك "ملاذات آمنة"، فإن الجناة سيستخدمونها لتعويق التحقيق. والبلدان النامية التي لم تنفذ بعد تشريعات تتعلق بالجريمة السيبرانية قد تصبح معرّضة لها، لأن المجرمين قد يختارون أن يتخذوها مقراً لنشاطهم لتجنّب 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 لسنّ التشريعات اللازمة. ومن الأمثلة على ذلك الدودة الحاسوبية المسماة "لف بغ" (Love Bug) التي استنبطها شخص مشتبه فيه بالفلبين في عام 2000،[801] والتي أصابت ملايين الحواسيب في جميع أنحاء العالم.[802] وكان مما أعاق التحقيقات المحلية أن استحداث ونشر برمجيات خبيثة لم يكن جرماً في ذلك الوقت بصورة كافية في الفلبين.[803] ومن الأمثلة الأخرى نيجيريا التي تعرضت لضغوط لاتخاذ إجراء ضد خِدع الاحتيال المالي الموزعة عن طريق البريد الإلكتروني.

8.2.3 الأتمتة

من أكبر مزايا تكنولوجيا المعلومات والاتصالات قدرتها على أتمتة عمليات معينة. وللأتمتة عدة نتائج كبرى هي: أنها تزيد من سرعة العمليات، كما أنها تزيد من نطاق وتأثير العمليات، وأخيراً، فإنها تحدّ من التدخل البشري.

وتقلل الأتمتة من الحاجة إلى أيدي عاملة كثيفة التكلفة، مما يتيح لمقدمي الخدمات أن يوفرها بأسعار أقل.[804] ويستطيع الجناة أن يستخدموا الأتمتة لتعظيم نطاق أنشطتهم – إذ يمكنهم إرسال ملايين عديدة من الرسائل الاقتحامية جملة واحدة[805] عن

طريق الأتمتة.[806] وباتت هجمات القرصنة مؤتمتة الآن هي الأخرى،[807] إذ يصل عدد ما يشن من هجماتها كل يوم إلى 80 مليون هجوم[808] بسبب استخدام أدوات برمجياتية[809] تستطيع أن تهاجم آلاف النظم الحاسوبية في غضون ساعات.[810] ويستطيع الجناة، عن طريق أتمتة العمليات، جني أرباح طائلة بتصميم خدع احتيالية تستند إلى عدد كبير من الأفعال الإجرامية التي تُلحِق بكل ضحية خسارة منخفضة نسبياً.[811] وكلما انخفضت الخسارة الواحدة زاد احتمال عدم إبلاغ الضحية عن الجريمة.

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.[812] 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

تُعد النظم الحاسوبية الحديثة المتداولة الآن في السوق نُظماً قوية ويمكن استخدامها لتوسيع نطاق الأنشطة الإجرامية. لكن تزايد قوّة[813] 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 شنّت مؤخراً على المواقع الحكومية في إستونياً.[814] إذ يوحي تحليل الهجمات بأنها ارتكبت من قبل آلاف الحواسيب المنضوية ضمن "برمجية روبوتية"،[815] أو من قِبَل مجموعة من الحواسيب المستغلة التي تُشغل برامج معينة عن طريق التحكم الخارجي.[816] وفي معظم الحالات، تُصاب الحواسيب ببرمجيات خبيثة تُركّب فيها أدوات تسمح بسيطرة الجناة عليها. وتستخدم البرمجيات الروبوتية لجمع معلومات عن الأهداف أو للقيام بهجمات عالية المستوى.[817]

وخلال السنوات الأخيرة، أصبحت البرمجيات الروبوتية تشكل خطراً جسيماً على الأمن السيبراني.[818] ويتفاوت حجم البرمجية الروبوتية، من عدة حواسيب إلى أكثر من مليون حاسوب.[819] ويفيد التحليل الراهن أن نسبة تصل إلى ربع كل الحواسيب الموصولة بالإنترنت يمكن أن تصيبها برمجيات تجعلها جزءاً من برمجية روبوتية.[820] ويمكن استخدام البرمجيات الروبوتية في أنشطة جنائية مختلفة تشمل الهجمات التي تستهدف الحرمان من النفاذ إلى الخدمات،[821] وإرسال الرسائل الاقتحامية،[822] والقيام بهجمات القرصنة؛ وتبادل ملفات محميّة بموجب حق المؤلف.

وتوفر البرمجيات الروبوتية 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[823] كما تزيد البرمجيات الروبوتية من صعوبة تتبّع الجاني الأصلي، لأن الآثار الأولية لن تقود إلا إلى عضو في البرمجيات الروبوتية. 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 ثواني 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.[824]

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. فكي يتسنّى للمحققين تتبّع المشتبه فيهم وكشفهم، يتعيّن عليهم في كثير من الأحيان النفاذ إلى بيانات قد تُحذف بعد النقل بفترة قصيرة.[825] ولذا، فإن قدرة سلطات التحقيق على الاستجابة خلال فترة قصيرة للغاية تُعدُّ 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.[826]

وتُعدُّ "إجراءات التجميد السريع"[827] ومراكز شبكة 24/7[828] من أمثلة الأدوات التي يمكن أن تعجّل بالتحقيقات. كما تستهدف التشريعات المتعلقة باحتجاز البيانات زيادة الوقت المتاح لوكالات إنفاذ القانون لإجراء التحقيقات. فلو تسنّى حفظ البيانات اللازمة لتتبُّع الجناة لفترة معقولة، لأُتيح لوكالات إنفاذ القانون فرصة أفضل للنجاح في كشف المشتبه فيه.

11.2.3 سرعة التطوّر

تشهد الإنترنت تطوراً مستمراً. وكان ابتكار السطح البيني البياني الخاص بالمستخدم (WWW[829]) هو بداية ما طرأ عليها من توسّع مثير، إذ كان استعمال المخدّمات السابقة المعتمدة على الأوامر أقل يُسراً وسهولة. وأتاح إنشاء الشبكة العالمية تطبيقات جديدة، مثلما أتاح كذلك ارتكاب جرائم جديدة.[830] وتكافح وكالات إنفاذ القانون في سبيل مواكبة التطورات. وتستجد بصفة مستمرة تطورات أخرى، ولاسيما من خلال الألعاب المتاحة على الخط، والاتصالات عن طريق نقل الصوت باستخدام بروتوكول الإنترنت (VoIP).

وتتزايد باطّراد 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.[831]

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.[832] ولذا يستلزم الأمر تقنيات جديدة.[833]

كما تشهد المعدات الحاسوبية الجديدة وتكنولوجيا الشبكات تطوراً سريعاً. وتحوّل 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.[834] وأدمجت في الساعات والأقلام ومدى الجيب أجهزة ذاكرة مزوّدة 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 ملمّين بأحدث التكنولوجيات ويستطيعوا تحديد المعدات ذات الصلة والأجهزة المحددة التي تعيّن مصادرتها.

ويتمثل تحدّ آخر في استخدام نقاط النفاذ اللاسلكية. ويشكل التوسع في النفاذ اللاسلكي إلى الإنترنت في البلدان النامية فرصة سانحة، كما يشكل تحدياً لوكالات إنفاذ القانون.[835] فإذا استخدم الجناة نقاط نفاذ لا سلكية لا تتطلّب تسجيلاً، يصبح من الأصعب على وكالات إنفاذ القانون أن تتتبّع الجناة لأن التحقيقات لن تقود إلا إلى نقاط النفاذ هذه.

12.2.3 الاتصالات المجهولة الهوية

يشكل تحديد مصدر الاتصال في أغلب الأحيان عنصراً جوهرياً من عناصر التحقيق في جريمة سيبرانية. لكن بسبب الطابع الموزّع للشبكة،[836] وتوافر بعض خدمات الإنترنت، التي لا يمكن معها التأكد من المصدر، يصعب كشف الجناة.[837]

وقد تكون الاتصالات مجهولة الهوية إما نتيجة فرعية لخدمة ما، أو مقدَّمة بنيّة تجنيب المستخدم بعض العيوب. ومن الأساسي مراعاة عدم اليقين الذي يشوب المصدر لمنع التوصل إلى استنتاجات غير صحيحة.[838] ومن أمثلة هذه الخدمات – التي يمكن حتى الجمع بينها ما يلي:

- الوحدات المطرافية العمومية للإنترنت (مثل الوحدات المطرافية في المطارات أو مقاهي الإنترنت)؛[839]
- أجهزة ترجمة عنوان الشبكة (NAT) والشبكات التقديرية الخاصة (VPN)؛[840]
- الشبكات اللاسلكية؛[841]
- الخدمات المتنقلة المدفوعة الثمن مقدماً التي لا تتطلب تسجيلاً؛
- قدرات التخزين لصفحات الاستقبال الموفرة دون تسجيل؛
- مخدّمات الاتصالات المجهولة الهوية؛[842]
- المواقع المجهولة الهوية التي تعيدُ إرسال البريد الإلكتروني.[843]

ويستطيع الجناة إخفاء هوياتهم بأن يستخدموا مثلاً عناوين زائفة للبريد الإلكتروني.[844] ويوفر كثير من مقدمي الخدمات عناوين بريد إلكترونية مجانية. وحتى إذا كان يجب 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 مثلاً إذا ما أراد المستخدمون الانضمام إلى جماعات النقاش السياسي دون كشف هويتهم. وقد تؤدي الاتصالات المجهولة الهوية إلى شيوع سلوك اجتماعي، ولكنها يمكن أن تسمح أيضاً للمستخدمين بالصرّف بحرية أكبر.[845]

وبما أن المستخدمين يتركون وراءهم آثاراً تدل عليهم، فإن هناك حاجة إلى وسائل لحماية المستخدمين من الأنشطة التي تستهدف تصنيفهم على أساس خصائصهم.[846] ولذا تؤيد دول ومنظمات شتى مبدأ الاستخدام المجهول الهوية لخدمات البريد الإلكتروني عن طريق الإنترنت. ويرد هذا المبدأ، على سبيل المثال، في توجيه الاتحاد الأوروبي المتعلق بالخصوصية والاتصالات الإلكترونية.[847] كما يمكن العثور على نموذج للنهج القانوني الرامي إلى حماية خصوصية المستخدمين في المادة 37 من لائحة الاتحاد الأوروبي المتعلقة بحماية البيانات.[848] غير أن بعض البلدان تتصدى لتحديات الاتصالات المجهولة الهوية بتطبيق قيود قانونية.[849] وعلى سبيل المثال، تلزم إيطاليا مقدمي خدمة النفاذ العمومي إلى الإنترنت بالتعرُّف على هوية المستخدمين، قبل أن يبدأوا في استخدام الخدمة.[850]

وتستهدف هذه التدابير مساعدة وكالات إنفاذ القانون على كشف هويات المشتبه فيهم، غير أنه من السهل تجنّبها. 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.[851]

13.2.3 إخفاق وسائل التحقيق التقليدية

يتطلب التحقيق في الجريمة السيبرانية وملاحقة مرتكبيها أدوات ووسائل خاصة بالإنترنت تحديداً لتمكين السلطات المختصة من إجراء التحقيقات.[852] وتعتبر وسائل الكشف عن الجاني وجمع الأدلة اللازمة للإجراءات الجنائية وسائل أساسية في هذا السياق.[853] ويمكن أن تكون هذه الوسائل مماثلة لتلك التي تُستخدم في التحقيقات الإرهابية التقليدية غير المتصلة بالتكنولوجيا الحاسوبية. لكن في عدد متزايد من القضايا المتصلة بالإنترنت (VoIP)، لا تكفي وسائل التحقيق التقليدية للكشف عن الجاني. ومثال على ذلك اعتراض اتصالات الصوت عبر بروتوكول الإنترنت.[854] وفي العقود الأخيرة، طورت الدول وسائل للتحقيق مثل التنصُّت تمكّنها من اعتراض اتصالات الخطوط الثابتة والهواتف المتنقلة على السواء.[855] ويجري اعتراض المكالمات الصوتية التقليدية عادةً عن طريق موردي الاتصالات.[856] وعند تطبيق المبدأ نفسه على اتصالات نقل الصوت بواسطة بروتوكول الإنترنت، سيكون على وكالات إنفاذ القانون الاستعانة بموردي خدمات الإنترنت (ISP) وموردي

الخدمات الذين يوفرون خدمات نقل الصوت بواسطة بروتوكول الإنترنت. لكن إذا كانت الخدمة قائمة على تكنولوجيا الاتصال بين النظراء، فقد لا يستطيع موردو الخدمات عموماً اعتراض الاتصالات، بما أن البيانات المعنية تُنقل مباشرة بين الشركاء في الاتصال.[857] ولهذا، فإن الحلول التقنية والصكوك القانونية ذات الصلة ضرورية.

14.2.3 تكنولوجيا التجفير

من العوامل الأخرى التي يمكن أن تعقّد التحقيق في الجريمة السيبرانية تكنولوجيا التجفير،[858] التي تحمي المعلومات من أن ينفذ إليها أشخاص غير مخوّلين والتي تُعد حلاً تقنياً رئيسياً في مكافحة الجريمة السيبرانية.[859] والتجفير تقنية تحوّل النص الصريح إلى نسق غامض باستخدام خوارزمية.[860] والتجفير ليس بالأمر الجديد،[861] شأنه شأن عدم الكشف عن الهوية، لكن التكنولوجيا الحاسوبية أدخلت تغييرات على هذا المجال. وقد خضع مدة طويلة للسرية. لكن في بيئة موصولة بينياً، بات من الصعب الحفاظ على هذه السرية.[862]

وبسبب انتشار الأدوات البرمجية سهلة الاستعمال وإدماج تكنولوجيا التجفير في أنظمة التشغيل[863] أصبح من الممكن الآن تجفير البيانات الحاسوبية بمجرّد النقر على الفأرة مما يزيد بالتالي من احتمال أن تواجه وكالات إنفاذ القانون مواد مجفَّرة.[864] وهناك منتجات برمجية متنوعة متاحة تمكّن المستخدمين من حماية الملفات من النفاذ غير المخول[865] لكن من غير المعروف على وجه اليقين إلى أيّ مدى يستخدم الجُناة بالفعل تكنولوجيا التجفير لإخفاء أنشطتهم.[866] وتفيد دراسة استقصائية عن المواد الإباحية التي يستغل فيها الأطفال أن 6 في المائة فقط من الحائزين على هذه المواد يستخدمون تكنولوجيا التجفير،[867] لكن الخبراء يسلّطون الضوء على التهديد المتمثل في تزايد استخدام تكنولوجيا التجفير في قضايا الجريمة السيبرانية.[868]

وتوجد استراتيجيات تقنية مختلفة لمعالجة البيانات المجفَّرة وعدة أدوات برمجية لأتمتة هذه العمليات.[869] وتتراوح هذه الاستراتيجيات بين تحليل مواطن الضعف في الأدوات البرمجية المستخدمة لتجفير الملفات، والبحث عن عبارات السر الخاصة بالتجفير،[870] وتجريب كلمات السر النمطية،[871] وصولاً إلى شن الهجمات الطويلة التي تشمل كافة الاحتمالات. ويُستخدم مصطلح "هجوم شامل لجميع الاحتمالات" لوصف عملية الكشف عن شفرة من خلال تجريب جميع التركيبات الممكنة.[872] وتِبعاً لتقنيات التجفير وحجم المفتاح قد تستغرق هذه العملية عقوداً من الزمن.[873] ومن ذلك مثلاً أنه إذا استخدم أحد الجناة برمجيات تجفير لها قدرة تجفير تبلغ 20 بتة، فإن حجم مساحة المفتاح تناهِز 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 بتة،[874] فإن المدة اللازمة لاختراق التجفير قد تصل إلى أسبوعين.[875] وفي سنة 2002، استطاعت جريدة وول ستريت جورنال، على سبيل المثال، أن تفك بنجاح تجفير ملفات مجفرة بقدرة 40 بتة، وُجدت على حاسوب لتنظيم القاعدة.[876] وباستخدام قدرة تجفير تبلغ 56 بتة، سيحتاج الحاسوب الواحد إلى 2 852 سنة لاختراق التجفير. أما إذا استخدم الجناة قدرة تجفير تبلغ 128 بتة، فإن مليار نظام حاسوبي تعمل حصراً على فك التجفير قد تأخذ آلافاً من مليارات السنين لاختراقه.[877] ويلاحظ أن أحدث نسخة من برمجيات التجفير الشائعة بي جي بي (PGP) تسمح بتجفير قدرته 1 024 بتة.

وتتجاوز قدرة برمجيات التجفير الحالية مجرد تجفير آحاد الملفات. فأحدث نسخة من نظم تشغيل ميكروسوفت، على سبيل المثال، تسمح بتجفير قرص صلب برمّته.[878] ويستطيع المستخدمون أن يركّبوا بسهولة برمجيات التجفير. وعلى الرغم من أن بعض خبراء الأدلة الجنائية الحاسوبية يعتقدون أن هذه الوظيفة لا تهددهم،[879] فإن تيسّر هذه التكنولوجيا على نطاق واسع لأي مستخدم يمكن أن تؤدي إلى التوسع في استخدام التجفير. وتتوافر أيضاً أدوات لتجفير الاتصالات – ومن ذلك مثلاً رسائل البريد الإلكتروني والمكالمات الهاتفية[880] التي يمكن إرسالها عن طريق نقل الصوت باستخدام بروتوكول الإنترنت.[881] ويستطيع الجناة، عن طريق تكنولوجيا مجفرة لنقل الصورة باستخدام بروتوكول الإنترنت، حماية المحادثات الصوتية من محاولات اعتراضها.[882]

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).[883] ومن الصعب على سلطات التحقيق أن تميّز بين التبادل البريء لصور العطل والإجازات، وتبادل صور تحتوي على رسائل خفية مجفّرة.[884]

ويتمثل توافر تكنولوجيات التجفير واستخدامها من قِبَل المجرمين تحدياً لوكالات إنفاذ القانون. وتناقش في الوقت الحاضر نهج قانونية متنوعة لمعالجة المشكلة،[885] تشمل: احتمال فرض التزامات على مطوّري البرمجيات تقضي بتركيب باب خلفي لوكالات إنفاذ القانون؛ وفرض حدود على قوة المفاتيح؛ وفرض التزامات بالإفصاح عن المفاتيح، في حالة التحقيقات الجنائية.[886] لكن تكنولوجيا التجفير لا يستخدمها المجرمون وحدهم – فثمة سُبُل 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،[887] تُعدّ الحماية الذاتية عنصراً هاماً في الأمن السيبراني.

15.2.3 الخلاصة

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.

3.3 التحديات القانونية

1.3.3 التحديات المصادفة لدى إعداد القوانين الجنائية الوطنية

التشريع السليم هو الأساس الذي يُستند 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 أوّل نفاذ غير مأذون به إلى الشبكات الحاسوبية قد وقع بعد إنشاء تلك الشبكات في سبعينات القرن الماضي بفترة قصيرة.[888] وبالمثل، ظهرت أول جرائم تتعلق بالبرمجيات بعد استحداث الحواسيب الشخصية في ثمانينات القرن الماضي بفترة قصيرة، حيث استخدمت هذه النظم آنذاك لاستنساخ المنتجات البرمجياتية.

وتحديث القانون الجنائي الوطني من أجل الملاحقة القضائية للأشكال الجديدة من الجريمة السيبرانية التي تُرتكب على الخط أمر يستغرق وقتاً. وفي الواقع، فإن بعض البلدان لم تفرغ بعد من عمليات التكيّف هذه. ويتعين استعراض وتحديث الأفعال التي يجرِّمها القانون الجنائي الوطني. ومن ذلك مثلاً أن المعلومات الرقمية يجب أن تتمتّع بمركز مكافئ لمركز التوقيعات والمستخرجات التقليدية.[889] فبغير إدراج الأفعال المتعلقة بالجريمة السيبرانية، لن يتسنّى ملاحقة الانتهاكات قضائياً.

ويتمثّل التحدي الرئيسي الذي يواجهه النظم القانونية الجنائية الوطنية في التأخر الزمني الذي يفصل بين الاعتراف بصور إساءة الاستخدام المحتملة للتكنولوجيات الجديدة، والتعديلات التي يلزم إدخالها على القانون الجنائية الوطني. ويظل هذا التحدي هاماً وآنياً أكثر من أي وقت مضى، بحكم السرعة التي يطّرد بها تجدد الشبكات. وتسعى بلدان كثيرة بصورة جادة إلى اللحاق بعمليات التكيف التشريعي.[890] وتنطوي عملية التكيف، بوجه عام، على ثلاث خطوات: التكيف مع القانون الوطني، وتحديد الثغرات في القانون الجنائي، وصوغ تشريعات جديدة.

يجب أن يبدأ التكيف مع القانون الوطني بالاعتراف بإساءة استخدام التكنولوجيا الجديدة

يتعين أن تضم وكالات إنفاذ القانون الوطنية إدارات محددة مؤهلة للتحقيق في الجرائم السيبرانية المحتملة. وقد تحسّنت الحالة بفضل إنشاء أفرقة الاستجابة للطوارئ الحاسوبية (CERT)،[891] وأفرقة الاستجابة للحوادث الحاسوبية (CIRT)، وأفرقة الاستجابة لحوادث الأمن الحاسوبي (CSIRT)، ومرافق بحثية أخرى.

تحديد الثغرات الموجودة في القانون الجنائي

من 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 مثلاً أن القوانين التي تتناول التزييف يمكن أن تنطبق بنفس القدر من السهولة على الوثائق الإلكترونية). فتقتصر الحاجة إلى التعديلات الشرعية عندئذ على الجرائم التي أغفلها القانون الوطني أو لم يغطّيها بصورة كافية.

صوغ تشريعات جديدة

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 ولتعقُّد بُناها.[892] 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، تتّسم المحاولات الرامية إلى تحقيق التواؤم بين القوانين الجنائية الوطنية المختلفة بأهمية متزايدة.[893] وتستطيع القوانين أن تنتفع بدرجة كبيرة من خبرة البلدان ومن المشورة القانونية الدولية المتخصصة.

2.3.3 الجرائم الجديدة

لا تُعد الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات، في معظم الحالات، جرائم جديدة، بل تُعدّ خِدعاً احتيالية طُوِّرَت كي تمارس على الخط. والاحتيال هو أحد الأمثلة على ذلك – إذ لا يوجد فارق كبير بين شخص يبعث رسالة بنيّة تضليل شخص آخر وبين شخص يبعث رسالة إلكترونية مُضمراً النيّة نفسها.[894] فإذا كان الاحتيال يشكّل 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 تطبّق 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.

وإلى جانب التكيُّف 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 تجرّم بعد في البلدان كلها السرقة والاحتيال في الألعاب الحاسوبية والألعاب التي تُنظم على الخط.[895] وقد ركزت المناقشات بشأن الألعاب المنظمة على الخط، لفترة طويلة، على قضايا حماية الشباب (مثل اشتراك 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).[896] وتُكشف بصفة مستمرة أنشطة إجرامية جديدة. فقد "تسرق" عملات افتراضية في ألعاب على الخط ويتم تداولها في مواقع المزادات.[897] وتنطوي بعض العملات الافتراضية على قيمة منسوبة إلى العملات الحقيقية (استناداً إلى سعر صرف معلوم)، مما يعطي الجريمة بُعداً "حقيقياً".[898] وقد لا يتسنّى ملاحقة هذه الجرائم قضائياً في البلدان جميعاً. وعملاً على الحيلولة دون توفير ملاذات آمنة للجُناة، من الحيوي رصد التطورات المستجدّة 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.[899] وتحتاج وكالات إنفاذ القانون إلى أدوات كافية للتحقيق في الأعمال الإجرامية المحتملة. وبعض هذه الأدوات (مثل احتجاز البيانات[900]) يمكن أن يتعارض مع حقوق مستخدمي الإنترنت الأبرياء.[901] وإذا كانت خطورة الفعل الإجرامي لا تتناسب مع شدة التدخل، فإن استخدام أدوات التحقيق قد لا تكون مبرّرة أو قانونية. وهذا ما جعل بعض الأدوات التي يمكنها أن تحسّن التحقيق لم تطبّق 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 المحدِق يسوّغ التغيير المطلوب. وكان الأخذ بأدوات جديدة يُبرَّر، 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،[902] بالقياس إلى تكاليف تخزين الوثائق المادية، إلى تزايد مطّرد في عدد الوثائق الرقمية.[903] وكان للرقمنة والاستخدام الناشئ لتكنولوجيا المعلومات والاتصالات تأثير كبير على الإجراءات المتعلقة بجمع الأدلة واستخدامها في المحكمة.[904] ونتيجة لهذا التطور بدأ الأخذ بالدليل الرقمي كمصدر جديد من مصادر الأدلة.[905] وهو يُعرَّف بأنه أي بيانات تُخزّن أو تُنقل باستخدام تكنولوجيا حاسوبية تؤيد النظرية الخاصة بكيفية حدوث جريمة ما.[906] وتقترن مناولة الدليل الرقمي بتحديات فريدة وتتطلب إجراءات خاصة.[907] ومن أصعب الجوانب في هذا الصدد الحفاظ على تكاملية الدليل الرقمي.[908] فالبيانات الرقمية بالغة الهشاشة ويمكن بسهولة حذفها[909] أو تعديلها. ويصدق هذا بوجه خاص على المعلومات المخزّنة في ذاكرة النظام RAM التي تُحذف آلياً عند إقفال النظام[910] ولذا تتطلّب تقنيات حفظ خاصة.[911] بالإضافة إلى ذلك، قد يكون للتطورات الجديدة تأثير كبير على التعامل مع الدليل الرقمي. ومن الأمثلة على ذلك معالجة المعلومات عن طريق الإنترنت (التي تُعرف باسم معالجة المعلومات في السحاب cloud-computing). وكان المحققون يستطيعون في الماضي التركيز على مقار المشتَبه فيهم لدى بحثهم عن البيانات الحاسوبية. أما اليوم فعليهم أن يأخذوا في اعتبارهم أن المعلومات الرقمية قد تُخزّن في الخارج ويمكن النفاذ إليها عن بُعد، عند الضرورة.[912]

ويؤدي الدليل الرقمي دوراً هاماً في شتى مراحل التحقيقات بشأن الجريمة السيبرانية. ومن الممكن بوجه عام التمييز[913] بين أربع مراحل.[914] فالأولى هي تحديد الأدلة ذات الصلة.[915] والثانية هي جمع الأدلة وصونها. وتشمل المرحلة الثالثة تحليل التكنولوجيا الحاسوبية والأدلة الرقمية. وفي المرحلة الأخيرة، يتعيّن تقديم الأدلّة إلى 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. ويُقصد بمصطلح "الأدلة الجنائية الحاسوبية "التحليل المنهجي لمعدات تكنولوجيات المعلومات بغرض البحث عن أدلة رقمية.[916] والتزايد المطّرد لحجم البيانات المخزّنة في صورة رقمية يُسلط الضوء على التحديات اللوجستية التي تنطوي عليها هذه التحقيقات.[917] ولذا، فإن النُّهُج الرامية إلى أتمتة إجراءات الأدلة الجنائية، باللجوء مثلاً إلى استخدام عمليات البحث عن صور المواد الإباحية التي يستغلّ فيها الأطفال بالاعتماد على قيمة الفرم[918] أو باستخدام الكلمات المفتاحية،[919] تؤدي دوراً هاماً بالإضافة إلى التحقيقات اليدوية.[920]

وتِبعاً لمتطلبات التحقيق المعني، يمكن أن تشمل الأدلة الجنائية الحاسوبية، على سبيل المثال، تحليل المعدات والبرمجيات التي يستخدمها المشتَبه فيه،[921] ودعم المحققين في تعيين الأدلة ذات الصلة،[922] واسترجاع الملفات المحذوفة،[923] وتجفير الملفات،[924] والكشف عن هوية مستخدمي الإنترنت عن طريق تحليل بيانات الحركة.[925]

721 See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf ; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

722 Regarding hash-value based searches for illegal content, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

723 For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp

724 In 2014 Facebook alone reported 829 million daily active users and 1.32 billion monthly active user. Source: http://newsroom.fb.com/company-info/ .

725 See for example: *Chaabane/Kaafar/Boreli*, Big Friend is Watching You: Analyzing Online Social networks Tracking Capabilities, Proceedings of the 2012 ACM workshop on online social networks, page 7 et seq.

726 See in this regard: *Daniel*, Cellular Location Evidence for Legal Professionals, 2014.

727 Regarding the development see: The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

728 Regarding the process see: *Rlamondon/Srihari*, On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey, ICC Transactions on pattern Analysis and machine Intelligence, Vol. 22, No. 1, 2000, page 63 et seq.

729 The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

730 *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

731 *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

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

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

734 See *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

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

736 Regarding the impact of attacks, see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

737 A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

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

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

740 Regarding the discussion on the effect of the monoculture of operating systems on cybersecurity, see *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; Warning: Microsoft 'Monoculture', Associated Press, 15.02.2004, available at

www.wired.com/news/privacy/0,1848,62307,00.html; *Geer and others*, CyberInsecurity: The Cost of Monopoly, available at: http://cryptome.org/cyberinsecurity.htm

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

742 Regarding the integration of developing countries in the protection of network infrastructure, see: Chairman's Report on ITU Workshop On creating trust in Critical Network Infrastructures, available at: www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

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

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

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

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

747 See below: § 4.

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

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

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

751 An example for new technology in this area is WiMAX (Worldwide Interoperability for Microwave Access), a standards-based wireless technology that provides broadband connections over long distances. Each WiMAX node could enable high-speed Internet connectivity in a radius of up to 50 km. For more information, see: The WiMAX Forum at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

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

753 The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: § 2.9.4.

754 Regarding hash-value based searches, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

755 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law). For more information, see *Moore*, Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law, available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.

756 "World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr/

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

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

759 In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime. See below: § 6.2.15.

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

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

762 For more information, see: *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

763 With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

764 One example of an approach to restrict the use of public terminals for criminal offences is Art. 7 of the Italian Decree-Law No. 144. Decree-Law 27 July 2005, No. 144 – "Urgent measures for combating international terrorism". For more information about the Decree-Law, see for example the article "Privacy and data retention policies in selected countries", available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

765 See below: § 6.5.13.

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

767 Regarding the question whether access to the Internet is a human right, see: *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; Regarding the declaration of Internet Access as a human right in Estonia, see: Information and Communications Technology, in UNDP Annual Report 2001, page 12, available at: www.undp.org/dpa/annualreport2001/arinfocom.pdf; Background Paper on Freedom of Expression and Internet Regulation, 2001, available at: www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

768 Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument.

769 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 a total of nearly 130 million websites at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

770 http://www.wikipedia.org

771 In the future development of the Internet, information provided by users will become even more important. "User generated content" is a key trend among the latest developments shaping the Internet. For more information, see: *O'Reilly*, What Is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software, 2005, available at: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

772 For more information, see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

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

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

775 See *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003, page 112 *et seq.*, available at: www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf; *Brown/Carlyle/Salmerón/Wood*, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530, available at: www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

776 "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 per cent of all information required about the enemy". Reports vary as to the source of the quotation: The British High Commissioner Paul Boateng mentioned in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: *Boateng*, The role of the media in multicultural and multifaith societies, 2007, available at: www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624. The United States Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites, see: *Knezo*, "Sensitive but Unclassified" Information and Other Controls: Policy & Options for Scientific and Technical Information, 2006, page 24, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

777 See Telegraph.co.uk, news from 13 January 2007.

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

779 For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff*, A Brief History of the Internet, available at: www.isoc.org/internet/history/brief.shtml.

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

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

782 For more information regarding anonymous communications, see below: § 3.2.l2.

783 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

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

785 See *Kahn/Lukasik*, Fighting Cyber Crime and Terrorism: The Role of Technology, presentation at the Stanford Conference, December 1999, page 6 *et seq.*; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

786 One example of the international cooperation of companies and delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system of the mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, page 429 *et seq.* (with notes *Sieber*)

787 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

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

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

790 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

791 See below: § 3.2.10.

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

793 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

794 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, page 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

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

796 Regarding the extend of cross-border cases related to computer fraud, see: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 9, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

797 See below: § 6.6.12.

798 See below: § 6.6.

799 One example is phishing. Although most sites are still stored in the United States (32%), which has strong legislation in place, countries such as China (13%), Russia (7%) and the Republic of Korea (6%), which may have less effective instruments in the field of international cooperation in place, are playing a more important role. Apart from the United States, none of them has yet signed and ratified cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

800 This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: § 5.1.

801 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU. Regarding the effect of the worm on critical information infrastructure protection, see: *Brock*, ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: www.gao.gov/archive/2000/ai00181t.pdf.

802 BBC News, Police close in on Love Bug culprit, 06.05.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. Regarding the technology used, see: http://radsoft.net/news/roundups/luv/20000504,00.html.

803 See for example: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

804 One example of low-cost services that are automated is e-mail. The automation of registration allows providers to offer e-mail addresses free of charge. For more information on the difficulties of prosecuting cybercrime involving e-mail addresses, see: § 3.2.l2.

805 The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

806 For more details on the automation of spam mails and the challenges for law-enforcement agencies, see: *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

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

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

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

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

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

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

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

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

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

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

817 See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, available at: www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, An Inside Look at Botnets, available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, BotNets: Detection and Mitigation.

818 See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf.

819 *Keizer*, Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, 21.10.2005, available at: www.techweb.com/wire/172303160

820 See *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

821 E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

822 "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: www.ic3.gov/media/initiatives/BotRoast.pdf.

823 *Staniford/Paxson/Weaver*, How to Own the Internet in Your Space Time, 2002, available at: www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

824 *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International, 2006, page 142.

825 *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

826 Regarding the necessary instruments, see below: § 6.5. One solution that is currently being discussed is data retention. Regarding the possibilities and risks of data retention, see: *Allitsch*, Data Retention on the Internet – A measure with one foot offside?, Computer Law Review International 2002, page 161 *et seq.*

827 The term "quick freeze" is used to describe the immediate preservation of data on request of law-enforcement agencies. For more information, see below: § 6.5.4.

828 The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country. For more information, see below: § 6.6.8.

829 The graphical user interface called World Wide Web (WWW) was created in 1989.

830 The development of the graphical user interface supported content-related offences in particular. For more information, see above: § 2.6.

831 For more information see above: § 2.6.5.

832 Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

833 With regard to the interception of peer-to-peer based VoIP communications, law-enforcement agencies need to concentrate on carrying out the interception by involving the access provider.

834 Regarding the implications of the use of cell phones as storage media for computer forensics, see: *Al-Zarouni*, Mobile Handset Forensic Evidence: a challenge for Law Enforcement, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Al-Zarouni%20-%20Mobile%20Handset%20Forensic%20Evidence%20-%20a%20challenge%20for%20Law%20Enforcement.pdf.

835 On the advantages of wireless networks for the development of an IT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries", 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

836 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

837 Regarding the challenges related to anonymous communication, see: *Sobel*, The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity, Virginia Journal of Law and Technology, Symposium, Vol. 5, 2000, available at: www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

838 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

839 Regarding legislative approaches requiring identification prior to the use of public terminals, see Art. 7 of the Italian Decree-Law No. 144. For more information, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.* and below: § 6.5.14.

840 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

841 Regarding the difficulties that are caused if offenders use open wireless networks, see above: § 3.2.3.

842 Regarding technical approaches in tracing back users of anonymous communication servers based on the TOR structure, see: *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

843 See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

844 Regarding the possibilities of tracing offenders using e-mail headers, see: *Al-Zarouni*, Tracing Email Headers, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

845 *Donath*, Sociable Media, 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

846 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Regarding the benefits of anonymous communication see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf..

847 "(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services [...]". Source: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

848 Article 37 – Traffic and billing data "1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection". – Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

849 See below: § 6.5.13.

850 Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

851 Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

852 This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

853 Regarding user-based approaches in the fight against cybercrime, see: *Goerling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

854 The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols. For more information, see: *Swale*, Voice Over IP: Systems and Solutions, 2001; *Black*, Voice Over IP, 2001.

855 Regarding the importance of interception and the technical solutions, see: *Karpagavinayagam/State/Festor*, Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection – ICIMP 2007. Regarding the challenges related to interception of data communication, see*: Swale/Chochliouros/Spiliopoulou/Chochliouros*, Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response, in *Janczewski/Colarik*, Cyber Warfare and Cyber Terrorism, 2007, page 424..

856 Regarding the differences between PSTN and VoIP communication, see: *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq.*

857 Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq*.

858 Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the mathematical background, see: *Menezes*, Handbook of Applied Cryptography, 1996, page 49 *et seq.*

859 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: 2006 E-Crime Watch Survey, page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

860 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

861 *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

862 *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58, page 143.

863 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

864 Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital

Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

865 Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see www.truecrypt.org).

866 Regarding the use of cryptography by terrorists, see: *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

867 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

868 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

869 Regarding the most popular tools, see: *Frichot*, An Analysis and Comparison of Clustered Password Crackers, 2004, page 3, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf. Regarding practical approaches in responding to the challenge of encryption see: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

870 See: Data Encryption, Parliament Office for Science and Technology No. 270, UK, 2006, page 3, available at: www.parliament.uk/documents/upload/postpn270.pdf.

871 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

872 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

873 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf

874 *Schneier*, Applied Cryptography, page 185; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005, page 36, available at: www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

875 1 099 512 seconds.

876 *Usborne*, Has an old computer revealed that Reid toured world searching out new targets for al-Qaida?, The Independent, 18.01.2002, available at: http://www.independent.co.uk/news/world/americas/has-an-old-computer-revealed-that-reid-toured-world-searching-out-new-targets-for-alqaida-663609.html; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf. With further reference to the case: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

877 Equivalent to 10790283070806000000 years.

878 This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.

879 See *Leyden*, Vista encryption 'no threat' to computer forensics, The Register, 02.02.2007, available at: www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

880 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, Skype Security Evaluation, 2005, available at: www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

881 Phil Zimmermann, the developer of the encryption software PGP, developed a plug-in for VoIP software that can be used to install added encryption, in addition to the encryption provided by the operator of the communication services. The difficulty arising from the use of additional encryption methods is the fact that, even if the law-enforcement agencies intercept the communications between two suspects, the additional encryption will hinder the analysis. For more

information on the software, see: *Markoff*, "Voice Encryption may draw US Scrutiny", New York Times, 22.05.2006, available at: 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.

882 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

883 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; *Labs*, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

884 For practical detection approaches, see: *Jackson/Grunsch/Claypoole/Lamont*, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, page 1 *et seq.*; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001.

885 See below: § 6.5.11.

886 See below: § 6.5.11.

887 See above: § 3.2.8.

888 See BBC News, Hacking: A history, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

889 An example of the integration of digital sources is Section 11, Subsection 3 of the German Penal Code: "Audio & visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection."

890 Within this process, the case-law based Anglo-American law system has advantages in terms of reaction time.

891 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 per cent of Internet systems to a halt in November 1988. For more information on the history of the CERT CC, see: www.cert.org/meet_cert/; *Goodman*, Why the Police don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.

892 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and UN Resolution 55/63.

893 See below: § 5.

894 See above: § 2.8.1.

895 Regarding the offences recognized in relation to online games, see above: § 2.6.5.

896 Regarding the trade of child pornography in Second Life, see for example BBC, Second Life "child abuse" claim, 09.05.2007, at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: http://secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy/.

897 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 *et seq.*

898 *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

899 Regarding the use of ICTs by terrorist groups, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16; *Hutchinson*, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf; *Gercke*, Cyberterrorism, Computer Law Review International 2007, page 64.

900 Data retention describes the collection of certain data (such as traffic data) through obliged institutions, e.g. access providers. For more details, see below: § 6.5.5.

901 Relating to these concerns, see: Advocate General Opinion, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

902 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

903 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

904 *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

905 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historic development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

906 *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

907 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq*.

908 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1.

909 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

910 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

911 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

912 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

913 Regarding the different models of cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also: *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

914 This includes the development of investigation strategies.

915 The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

916 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

917 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

918 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

919 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

920 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

921 This includes for example the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

922 This includes for example the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

923 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

924 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

925 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq*.

4 بناء القدرات

Bibliography (selected): *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141*; Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf*; Henten/Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1; *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003*; Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf; *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et seq.*; *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

دفع تزايد عدد الجرائم السيبرانية التي تم الوقوف عليها وتزايد عدد الضحايا، حتى في البلدان النامية الأقل توصيلاً، بموضوعي الأمن السيبراني والجريمة السيبرانية إلى مرتبة أعلى في جدول أعمال كل من القطاع الخاص والحكومات على السواء. ولما كانت تكنولوجيا المعلومات والاتصالات تتطور بسرعة بالغة، وخاصة في البلدان النامية، فقد أصبح وضع وتنفيذ التدابير الفعالة لمكافحة الجريمة السيبرانية مسألة هامة. ويعطي الفصل التالي لمحة عامة عن القضايا التي غالباً ما تتناولها البلدان عندما تعكف على وضع تدابير المكافحة.

1.4 الأمن السيبراني والجريمة السيبرانية

من أولى الأسئلة التي كثيراً ما تطرح عندما تشرع الدول في التصدي لجرائم الإنترنت: هل يكون ذلك في إطار إنفاذ القانون أم في إطار الأمن السيبراني؟ والتمييز بين الموضوعين ليس بالأمر اليسير.[926] ومن الواضح أن الموضوعين مترابطان، كما يدل على ذلك قرار الجمعية العامة للأمم المتحدة عام 2010 بشأن الأمن السيبراني[927] الذي يتناول الجريمة السيبرانية بمثابة تحد رئيسي كبير. ومن ثم يمكن النظر إلى الجريمة السيبرانية كعنصر متأصل[928] في أي نهج لتعزيز الأمن السيبراني، ومع ذلك فهي بالتأكيد عنصر واحد فقط في استراتيجية الأمن السيبراني. ومن شأن أخذ ذلك في الاعتبار أن يبرز الطابع المتعدد التخصصات لكلا الموضوعين، وبالتالي الحاجة إلى إشراك مختلف أصحاب المصلحة داخل الحكومة في هذه العملية. وغالباً ما ينطوي وضع الاستجابة الوطنية للجريمة السيبرانية على إشراك هيئات مختلفة (مثل النيابة العامة ووزارة الاتصالات ووزارة التربية والتعليم، وغيرها).

2.4 منهجية بناء القدرات

يكشف تحليل لمختلف المناهج لبناء القدرات الوطنية اللازمة في مكافحة الجريمة السيبرانية في كل بلد عن بعض العناصر الرئيسية التي يمكن اعتبارها بمثابة عناصر أساسية لنهج أفضل الممارسات.

1.2.4 إطار العمل

نقطة البداية هي مناقشة مركزة داخل البلد (ومع المنظمات الدولية الداعمة) للتوصل إلى فهم كامل للمطالب وللتمكن من صوغ مشروع خطة/اقتراح يقابلها. وتغطي هذه المناقشة مواضيع مختلفة – من ذلك مثلاً: هل يجب أن يتضمن المشروع استراتيجية أم تشريعات سياسة عامة أم مجرد عناصر منها؟ هل هنالك هياكل قائمة ينبغي الانطلاق منها؟ ما هي المعايير الوطنية أو الإقليمية أو الدولية التي ينبغي أن تستخدم كمعايير لتحليل مقارن؟ ما هي المواضيع التي ينبغي تغطيتها (من قبيل حماية الأطفال على الخط، وحماية البيانات، والجريمة السيبرانية، وحماية البيانات والمعاملات الإلكترونية)؟ هل يجب أن يتضمن المشروع أيضاً تدريب الخبراء و/أو وضع المواد التدريبية؟ هي يتلقى البلد حالياً شكلاً آخر من أشكال الدعم؟ ولفهم حالة مختلف الأنشطة أهمية كبيرة من أجل تنسيق مختلف أنشطة الدعم.

2.2.4 وضع خطة مشروع

استناداً إلى نتائج المناقشة الأولية يمكن العمل على وضع مسوّدة خطة مشروع تصف بمزيد من التفصيل الأنشطة والخبراء المعنيين والنتائج المتوقعة والجدول الزمني.

3.2.4 التقييم كنقطة بداية

يمثل بدء المشروع بعملية تقييم ملائم عامل نجاح رئيسياً. ولا يمكن التماس الدعم الذي يلبي الغرض ما لم يكن كل المسؤولين والخبراء المشاركين على علم بحالة المكونات القائمة (من قبيل السياسات أو التشريعات) والتفاصيل، مثل تفاصيل الصياغة القانونية في البلد المعني. وينبغي أن يشمل هذا التقييم القدرات المؤسسية فضلاً عن تحديد أصحاب المصلحة الرئيسيين (مثل الخبراء الحكوميين، وجمعيات أصحاب الأعمال، وجماعات المصالح، مثل جماعات الحريات المدنية).

4.2.4 التحليل المقارن

تُظهر نتائج التقييم الوضع الحالي كما هو – ولكن التقييم لا يمكنه تصوير أين يقف البلد إزاء بعض معايير المقارنة. ويستند التحليل المقارن إلى نتائج التقييم ولكنه يمكن أن يضيف عنصراً تحليلياً. وأساس المقارنة هو المعايير المستخدمة لتحديد الثغرات المحتملة وتسليط الضوء على أفضل الممارسات. فإذا كان البلد المستفيد جزيرة صغيرة في المحيط الهادئ وجزءاً من الكومنولث عندئذ يمكن مقارنة التشريع الوطني القائم أو مشروع القانون المتوخى بقانون الكومنولث النموذجي بشأن الجرائم الحاسوبية والجرائم المتصلة بالحاسوب وكذلك بهيكل النموذج الإقليمي لمشروع تكنولوجيا المعلومات والاتصالات لبلدان المحيط الهادئ (ICB4PAC). وثمة معايير أخرى يمكن أن تضاف إلى القائمة، مثل توجيه الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات أو اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. وتكون النتيجة عبارة عن تقرير معقد يقارن أو يدرج العناصر الوطنية المحددة، والعناصر المماثلة في المعايير، ويشير إلى أوجه الشبه والاختلاف ويضع التوصيات.

5.2.4 التشاور مع أصحاب المصلحة

ثمة ممارسة أخرى في نُهُج أفضل الممارسات في بناء القدرات وهي استضافة المشاورات مع أصحاب المصلحة. وقد أثبتت خبرة سنوات عديدة لبناء القدرات في مجال الاستراتيجية والسياسات والتشريعات أن التشاور مع أصحاب المصلحة ينطوي على إمكانية تعزيز عملية الصياغة بشكل ملحوظ. وهو يتطلب بالتأكيد الكثير من الجهد لمناقشة عناصر سياسة وطنية ومشروع قانون مع طائفة واسعة من أصحاب المصلحة. ومع ذلك، فإن العملية التشريعية السلسة التي أعقبت المشاورات مع أصحاب المصلحة في تلك البلدان التي مرت بالفعل بعملية التبديل دليل على جدوى عقد مناقشات مكثفة في إطار عملية الصياغة بغية التأكد من معالجة مختلف الشواغل.

وفي أثناء هذه المشاورات على مستوى البلد، يدعى مختلف أصحاب المصالح الوطنية (ومنهم مثلاً الجمهور العام والعاملون في السياسة والمسؤولون الحكوميون ودوائر الصناعة والأعمال ومقدمو خدمات الإنترنت ودعاة الحريات المدنية) لحضور مختلف

الاجتماعات التشاورية التي تناقش فيها نتائج التحليل والطريق المقترح المضي فيها. وتؤخذ في الحسبان المدخلات من أصحاب المصلحة وتندرج في عملية صوغ السياسات والتشريعات.

6.2.4 عملية الصياغة

من الممكن، استناداً إلى التحليل المقارن والمشاورات مع أصحاب المصلحة، وضع أو تعديل الاستراتيجيات والسياسات والتشريعات ذات الصلة. وتشمل عملية الصياغة عادة أيضاً صوغ المذكرات التفسيرية وغيرها من الوثائق (من قبيل وثائق الإحاطة لمجلس الوزراء).

7.2.4 أنشطة التدريب والتعليم والمتابعة

إن أفضل الاستراتيجيات والسياسات والتشريعات لا تكفي وحدها لمحاربة الجريمة السيبرانية بشكل فعال. ولا تقل عنها أهمية التدابير الأخرى، مثل تدريب المهنيين وتثقيف الجمهور عموماً. وتتراوح أنشطة التدريب الممكنة من التدريب على منع الجريمة في سن معينة في المدارس إلى عمليات محاكاة الحوادث السيبرانية في الوقت الفعلي لكبار المسؤولين الحكوميين لمساعدتهم على تجنب الهجمات. وتشمل أنشطة المتابعة أيضاً في كثير من الأحيان عملية تقييم المشروع.

3.4 الاستراتيجية كنقطة انطلاق

يؤدي الأمن السيبراني،[929] كما سلفت الإشارة، دوراً هاماً في التطور الجاري لتكنولوجيا المعلومات ولخدمات الإنترنت.[930] وأصبح تعزيز أمان الإنترنت (وحماية مستخدمي الإنترنت) أمراً جوهرياً لاستحداث الخدمات الجديدة ولوضع السياسات الحكومية.[931] 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.[932]

وينبغي أن تكون استراتيجية مكافحة الجريمة السيبرانية عنصراً جوهرياً في استراتيجية الأمن السيبراني. والبرنامج العالمي للأمن السيبراني،[933] 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.[934]

1.3.4 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.

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 مثلاً بالتركيز على مسائل الحماية التقنية التي تُعد كثيفة التكلفة بقدر أكبر.

وثمة عدة مسائل أخرى يتعين أن تراعيها البلدان النامية التي تعتمد الاستراتيجيات القائمة لمكافحة الجريمة السيبرانية، من بينها: مدى توافق الأنظمة القانونية المعنية وحالة المبادرات المساندة (مثل توعية المجتمع) ونطاق تدابير الحماية الذاتية المطبقة، وكذلك نطاق الدعم المقدم من القطاع الخاص (وذلك مثلاً من خلال الشراكات بين القطاعين العام والخاص).

2.3.4 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.[935] ولذا يتعين إدراج العوامل والاختلافات الإقليمية لدى تنفيذ هذه الاستراتيجيات في أماكن أخرى.

3.3.4 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.

4.3.4 التوسع في الاستراتيجيات إلى ما هو أبعد من الخطط المستقبلية

وضعت البلدان، في السنوات الأخيرة، استراتيجيات تشمل الأمن السيبراني والجريمة السيبرانية.[936] وينطبق ذلك أيضاً على المنظمات الدولية والمؤسسات الحكومية الدولية.[937] وتكشف مقارنة تلك المناهج المختلفة عن قدر كبير من أوجه التشابه.

وغالبية استراتيجيات الأمن السيبراني والجريمة السيبرانية وثائق قصيرة نسبياً (10-20 صفحة) لا توفر درجة عالية من التفصيل. وينصب التركيز فيها على إبراز أهمية الموضوع وتأكيد الإرادة على العمل وتحديد قرارات عامة عما ينبغي القيام به لتحسين الأمن السيبراني. وغالبية الاستراتيجيات لا تقدم حلولاً وتدابير ملموسة. وفكرة الاستراتيجية هي أنها توفر حلاً لتحدٍّ ما أو لمشكلة ما. ولا حاجة لأن تكون خاصة بحالة محددة، وإنما ينبغي أن توفر التوجيه عند مواجهة التحديات.[938] فاستراتيجية الأمن السيبراني الألمانية[939] مثلاً تحدد أن لدى الحكومة خططاً لتنظيم المبادرات وللمضي في دراسة مسؤوليات مقدمي الخدمات. ولكن الاستراتيجية لا تحدد الجهة التي ستأخذ زمام المبادرة ولا كيف ينبغي لها تحقيق الأهداف.

ومن مزايا الاستراتيجية المقتضبة أنها تتطلب وقتاً قصيراً لوضعها. ومن شأن اقتصار التعريف على مبادئ عامة جداً أن يقلل أيضاً إلى حد كبير الحاجة إلى تحديثات منتظمة.[940] ومن الممكن أن تبقى استراتيجية عامة جداً سارية لسنوات عديدة قبل أن تتطلب التحديث. ولكن هذا النهج ينطوي أيضاً على تحديات. ومن المؤكد أن وضع نهج شامل لا يتطلب جمع التدابير والأنشطة في وثيقة واحدة. ولكن وجود وثائق مختلفة يؤدي إلى احتمال عدم توافق مختلف التدابير. وتبين التجربة أنه نظراً لتعقيد التهديدات فإن مجرد وجود تناقضات بسيطة داخل مختلف التدابير يمكن أن تنال إلى حد كبير من فعالية كل من الوقاية من الحوادث والاستجابة لها. ولا يمكن لأي استراتيجية أن تعزز فعاليتها ما لم تضمن اتساق جميع مكوناتها وترابطها.

وثمة حل وسط ممكن أن يتمثل في الجمع بين استراتيجية عامة للغاية وخطط عمل ملموسة (وبالتالي أكثر تفصيلاً) من أجل المتابعة. ومن شأن هذا النهج أن يمكّن من الإفصاح علناً عن الجهود التي تبذل لنشر استراتيجية تتناول الجريمة السيبرانية والأمن السيبراني ولكنه يضمن في الوقت ذاته سرية التدابير الملموسة. وقد تكون الحاجة إلى تقديم لمحة عامة عن الأنشطة في مجال الجريمة السيبرانية والأمن السيبراني حاجة ملحة بالنسبة للحكومات، كما أن وجود استراتيجية وطنية للأمن السيبراني يمكن أن يكون ضرورياً لكي تتمكن البلدان من اجتذاب المستثمرين. وفي نفس الوقت قد لا يكون الكشف عن تفاصيل التدابير المتخذة لتعزيز الأمن السيبراني لتحديد هوية المجرمين مقبولاً في كل الحالات إذ من شأنه أن يزود المهاجمين بالمعلومات التي يمكن استخدامها لاستبانة مواطن الضعف.

4.4 أهمية وضع سياسة عامة

يعتبر وضع تشريعات تجرّم بعض السلوكيات أو استحداث وسائل لتحري عملية غير مألوفة في أغلب البلدان. ويتمثل الإجراء الاعتيادي بادئ ذي بدئ في استحداث سياسة عامة[941] وتشبه السياسة العامة الاستراتيجية التي ترمي إلى تحديد مختلف الوسائل المستعملة لمعالجة القضية. وعلى خلاف استراتيجية أكثر شمولاً للجريمة السيبرانية قد تتناول مختلف أصحاب المصلحة، يتمثل دور السياسة العامة في تحديد الاستجابة الحكومية العامة لقضية معينة.[942] ولا تنحصر هذه الاستجابة بالضرورة في وضع التشريعات حيث تمتلك الحكومات وسائل مختلفة يمكن استعمالها لتحقيق أهداف السياسة العامة. وحتى عندما يتخذ قرار بأن هناك حاجة لتنفيذ تشريع ما، لا يتعين بالضرورة التركيز على القانون الجنائي بل يمكن أيضاً أن تناول تشريعات تركز بشكل أكبر على منع الجريمة. وفي هذا الصدد، من شأن وضع سياسة عامة لتمكين أي حكومة من أن تحدد بشكل شامل استجابتها للمشكلة. وحيث إن مكافحة الجريمة السيبرانية لا يمكن بالقطع قصره على استحداث تشريعات فحسب، بل تتضمن استراتيجيات مختلفة مع اتخاذ تدابير مختلفة، حيث تضمن السياسة العامة ألاّ ينتج عن هذه التدابير المختلفة أوجه تضارب.

وفي إطار النهج المختلفة الرامية إلى تحقيق تواؤم تشريعات الجريمة السيبرانية تم إيلاء أولوية منخفضة جداً ليس فقط لدمج التشريعات ضمن الإطار القانوني الوطني ولكن لإدراجها أيضاً ضمن سياسة عامة قائمة أو استحداث هذه السياسة العامة لأول مرة. ونتيجة لذلك، واجهت بعض البلدان التي قامت باستحداث تشريعات للجريمة السيبرانية فقط دون وضع استراتيجية لمكافحة الجريمة السيبرانية فضلاً عن وضع سياسات على المستوى الحكومي صعوبات بالغة. نتجت هذه الصعوبات بشكل رئيسي بسبب غياب تدابير لمنع الجريمة فضلاً عن التداخل بين مختلف التدابير.

1.4.4 *المسؤولية داخل الحكومة*

تمكن السياسة العامة من مواءمة الكفاءات لتوافق موضوع من المواضيع داخل الحكومة. ووجود تداخل بين مختلف الوزارات أمر عادي – وفيما يتعلق بالجريمة السيبرانية، فذلك أمر يحدث غالباً بما أنها موضوع يهم عدة تخصصات.[943] ويمكن أن تتصل جوانب متعلقة بمكافحة الجريمة السيبرانية بولاية وزارة العدل أو وزارة الاتصالات أو وزارة الأمن القومي، وذلك على سبيل الذكر لا الحصر. في إطار عملية وضع سياسة عامة معينة، يمكن تحديد دور مختلف المؤسسات الحكومية الضالعة.

وهو ما تم التعبير عنه من خلال مشروع سياسة عامة نموذجية بشأن الجريمة السيبرانية لمشروع البلدان الجزرية في المحيط الهادئ ICB4PAC:[944]

> *من الأهمية بمكان في هذا الصدد أن تحدد بوضوح المسؤوليات التي يضطلع بها مختلف أصحاب المصلحة. ويعتبر ذلك ملائماً بصورة خاصة لأن الجريمة السيبرانية هي موضوع مشترك بين القطاعات يمكن أن تتصل بولايات مؤسسات مختلفة مثل المدعي العام ووزارة الاتصالات وآخرين.*

2.4.4 *تحديد مختلف المكونات*

كما ذكر آنفاً، يمكن استعمال السياسة العامة لتحديد مختلف مكونات النهج. ويمكن أن يتراوح ذلك من تقوية القدرات المؤسسية (مثل مؤسسة الشرطة وجهة الادعاء) إلى إجراء تعديلات ملموسة على التشريعات (مثل وضع تشريعات أكثر تقدماً).

وهذه مسألة أخرى تم تناولها في مشروع سياسة عامة نموذجية بشأن الجريمة السيبرانية لمشروع البلدان الجزرية في المحيط الهادئ ICB4PAC:[945]

> *تتطلب معالجة التحديات متعددة الأبعاد لمكافحة الجريمة السيبرانية نهجاً شاملاً يشمل السياسات العامة والتشريعات والتعليم وإذكاء الوعي وبناء القدرات والبحوث فضلاً عن النهج التقنية.*

وينبغي على نحو مثالي استعمال السياسة العامة لتنسيق الأنشطة المختلفة – حتى ولو كانت تنفذها وزارات وهيئات حكومية مختلفة. بيد أن حقيقة أن هذه السياسات تتطلب موافقة مجلس الوزراء عادةً، لا تسمح فقط بتحديد مختلف الهيئات الحكومية والوزارات الضالعة في موضوع ما بل تسمح أيضاً بتحقيق التواؤم في الأنشطة.[946]

3.4.4 تحديد أصحاب المصلحة

يمكن للسياسة العامة أن تحدد ليس فقط المؤسسات الحكومية الضالعة بل أيضاً أصحاب المصلحة الذين ينبغي التعامل معهم. وقد يكون من الضروري، على سبيل المثال وضع مبادئ توجيهية تتعلق بإشراك القطاع الخاص.

وتم التعبير عن قضية أصحاب المصلحة الذين ينبغي إشراكهم والتعامل معهم في إطار، على سبيل المثال، مشروع سياسة عامة نموذجية بشأن الجريمة السيبرانية لمشروع البلدان الجزرية في المحيط الهادئ ICB4PAC.[947]

وعلاوةً على ذلك، ينبغي لهذا النهج أن يشرك مختلف أصحاب المصلحة مثل الحكومة والوزارات والوكالات الحكومية والقطاع الخاص والمدارس والجامعات والزعماء العرفيين والمجتمع المحلي والهيئات الدولية والإقليمية وجهات إنفاذ القانون والقضاة والجمارك والمدعين العامين والمحامين والمجتمع المدني والمنظمات غير الحكومية.

4.4.4 تحديد نقاط مرجعية

كما يتم التأكيد عليه أدناه، تحدد منظمات اقليمية مختلفة أهمية تحقيق التواؤم بين التشريعات كأحد الأولويات الرئيسية.[948] بيد أن ضرورة تحقيق التواؤم لا تقتصر على التشريعات – فهي تشمل قضايا مثل الاستراتيجية وتدريب الخبراء.[949] ويمكن استعمال السياسة العامة لتحديد المجالات التي ينبغي تحقيق التواؤم فيها فضلاً عن تحديد المعايير الإقليمية و/أو الدولية التي ينبغي تنفيذها.

وتم التعبير عن أهمية تحقيق التواؤم على سبيل المثال في مشروع سياسة نموذجية بشأن الجريمة السيبرانية لمشروع البلدان الجزرية في المحيط الهادئ ICB4PAC.[950]

ونظراً للبعد العالمي للجريمة السيبرانية وفضلاً عن ضرورة حماية مستخدمي الإنترنت في المنطقة من أن يصبحوا ضحايا للجريمة السيبرانية، ينبغي إيلاء اتخاذ تدابير لزيادة القدرة على مكافحة الجريمة السيبرانية أولوية عالية. وينبغي أن تتماشى الاستراتيجيات ولا سيما التشريعات التي وضعت لمواجهة تحديات الجريمة السيبرانية مع المعايير الدولية من جهة، ومن جهة أخرى ينبغي أن تعكس الخاصيات الفريدة للمنطقة.

وهناك مثال آخر يتمثل في سياسة نموذجية بشأن الجريمة السيبرانية لمشروع منطقة الكاريبي HIPCAR.[951]

ويجب أن تكون هناك أحكام تشمل أكثر أشكال الجريمة السيبرانية شيوعاً وانتشاراً على نطاق واسع فضلاً عن تلك الجرائم التي لها أهمية محددة بالنسبة للمنطقة (على سبيل المثال الرسائل الاقتحامية).

وبغية ضمان القدرة على التعاون مع وكالات إنفاذ القانون في بلدان المنطقة وكذلك خارج المنطقة ينبغي للتشريعات أن تكون متوافقة مع المعايير وأفضل الممارسات الدولية على حد سواء وكذلك (إلى أقصى حد ممكن) مع المعايير وأفضل الممارسات الإقليمية القائمة.

5.4.4 تحديد المواضيع الرئيسية للتشريعات

يمكن أن تستعمل السياسة العامة لتحديد المجالات الرئيسية التي ينبغي أن تتناولها التشريعات. ويمكن أن يشمل ذلك على سبيل المثال قائمة الجرائم التي ينبغي التطرق إليها. ويمكن أن تشمل درجة التفصيل التعرض إلى تفاصيل الأحكام التي ينبغي إدراجها ضمن قانون الجريمة السيبرانية.

ويعتبر السياسة النموذجية بشأن الجريمة السيبرانية لمشروع منطقة الكاريبي HIPCAR.[952]

ينبغي وجود حكم يجرّم الانتاج المتعمد وغير المشروع للمنتجات التي تستغل الأطفال في المواد الإباحية وبيعها والتصرفات المتعلقة بذلك. وينبغي في هذا الصدد مراعاة المعايير الدولية بوجه خاص. وينبغي أن تشمل التشريعات بالإضافة إلى ذلك تجريم حيازة المواد الإباحية المتعلقة بالأطفال والنفاذ إلى المواقع الإلكترونية المرتبطة بهذه المواد. وينبغي إدراج بند استثناء يخوّل وكالات إنفاذ القانون تنفيذ التحقيقات.

6.4.4 تحديد الأطر القانونية التي تتطلب تعديلات أو تحديثات أو تغييرات

إن استحداث تشريعات تخص الجريمة السيبرانية ليس بالأمر الهين ذلك أن هناك مجالات متنوعة تستلزم تنظيماً. وبالإضافة إلى القانون الجنائي الموضوعي والقانون الإجرائي، يمكن أن تشمل تشريعات الجريمة السيبرانية قضايا متعلقة بالتعاون الدولي والأدلة الإلكترونية ومسؤولية مقدم خدمة الإنترنت. وفي معظم البلدان قد توجد بالفعل عناصر لهذه التشريعات – غالباً في شكل أُطر قانونية مختلفة. ولا تحتاج الأحكام المتعلقة بالجريمة السيبرانية بالضرورة أن تنفذ من خلال نص تشريعي واحد. وقد أن يكون ضرورياً بالنسبة إلى الهياكل القائمة تحديث مواد مختلفة من التشريعات (مثل تعديل قانون الأدلة لضمان قابلية تطبيقه فيما يخص مقبولية الأدلة الإلكترونية في الدعاوى الجنائية) أو حذف حكم من قانون أقدم (على سبيل المثال فيما يخص قانون الاتصالات) ضمن عملية استحداث تشريع جديد.

وبلا شك يعتبر هذا النهج في تنفيذ تشريعات الجريمة السيبرانية من خلال عملية مراعاة الهياكل القائمة أكثر صعوبة من مجرد تنفيذ معيار إقليمي أو تطبيق أفضل الممارسات الدولية حرفياً داخل نص تشريعي قائم بذاته. غير أنه فيما يتعلق بعملية تكييف تشريعات تسمح بالحفاظ على التقاليد القانونية الوطنية، تشجع بلدان عديدة مثل هذا النهج.

ويمكن استعمال السياسة العامة لتحديد مختلف المكونات التي ينبغي دمجها فضلاً عن تحديد القوانين القائمة التي تتطلب تحديثات.

7.4.4 أهمية منع الجريمة

رغم أنه يحتمل أن تساعد التهديدات بالعقاب على منع اقتراف الجرائم، فإن تركيز التشريع الجنائي لا ينصب على منع الجريمة بل معاقبتها. ورغم ذلك، يعتبر منع الجريمة أحد المكونات الرئيسية في المكافحة الفعالة للجريمة السيبرانية.[953] ويمكن أن تتراوح التدابير المتخذة بدءاً من إيجاد الحلول التقنية (مثل وضع جدران حامية تمنع النفاذ غير المشروع لنظام الحاسوب وتركيب برمجيات مضادة للفيروسات تعرقل تركيب برمجيات ضارة) إلى منع النفاذ إلى المحتويات غير المشروعة.[954]

وتم التعبير عن أهمية منع الجريمة السيبرانية على سبيل المثال في مشروع البلدان الجزرية في المحيط الهادئ ICB4PAC وهو مشروع سياسة نموذجية بشأن الجريمة السيبرانية:[955]

وبالإضافة إلى تجريم الجريمة السيبرانية وتحسين قدرة وكالات إنفاذ القانون على مكافحة الجريمة السيبرانية، هناك ضرورة لوضع تدابير لمنع الجريمة. وفي إطار عملية وضع هذه التدابير والتي قد تتراوح من ايجاد الحلول التقنية إلى زيادة وعي المستخدم، من المهم تحديد هذه الجماعات التي تتطلب اهتماماً خاصاً مثل الشباب والأشخاص المعاقين من الناحية التكنولوجية (مثل الأشخاص المقيمين في القرى النائية الذين لا علم لهم بالتكنولوجيا) والنساء. بيد أنه، ينبغي كذلك تطبيق تدابير منع الجريمة على المستخدمين الذين لهم دراية كبيرة والأطراف الفاعلة من المؤسسات التكنولوجية مثل موردي البُنى التحتية الحرجة (مثل قطاع السياحة والقطاع المالي). وينبغي أن تشمل المناقشة بشأن التدابير اللازمة مجموعة واسعة من الرسائل مثل إذكاء الوعي وإتاحة وسائل الحماية التكنولوجية بالمجان وتشجيعها (مثل البرمجيات المضادة للفيروسات) وتنفيذ حلول تمكن الآباء من تقييد النفاذ إلى بعض المحتويات الإلكترونية في الإنترنت. ووجود هذه التدابير بطريقة مثالية عند إدخال خدمة/تكنولوجيا رعايتها إلى أن يتم تشغيلها. وبغية ضمان تغطية على هذه التدابير لنطاق أوسع ينبغي إشراك مجموعة واسعة من أصحاب المصلحة تتراوح من موردي خدمات الإنترنت إلى الهيئات الحكومية والإقليمية والتماس مصادر متنوعة للتمويل.

5.4 دور الهيئات التنظيمية في مكافحة الجريمة السيبرانية

خلال عقود مضت، انصبّ تركيز الحلول التي جرى مناقشتها لمكافحة الجريمة السيبرانية على وضع التشريعات. وكما ورد آنفاً في الفصل الذي تناول استراتيجية مكافحة الجريمة السيبرانية، تظل المكونات الضرورية لنهج شامل لمكافحة الجريمة السيبرانية أكثر تعقيداً. وسلطت الأضواء مؤخراً على الدور الذي يمكن أن تضطلع به الهيئات التنظيمية في مكافحة الجريمة السيبرانية.

1.5.4 من تنظيم الاتصالات إلى تنظيم تكنولوجيا المعلومات والاتصالات

يعترف بالدور الذي تضطلع به الهيئات التنظيمية في سياق الاتصالات على نطاق واسع.[956] ولأن الإنترنت أضعفت النماذج القديمة لتقسيم المسؤوليات بين الحكومة والقطاع الخاص، يمكن ملاحظة تحول للدور التقليدي الذي تقوم به الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات مع تغيير على مستوى التركيز بشأن تنظيم تكنولوجيا المعلومات والاتصالات.[957] وتجد بالفعل السلطات التنظيمية لتكنولوجيا المعلومات والاتصالات نفسها اليوم ضالعة في مجموعة من الأنشطة المرتبطة لمكافحة الجريمة السيبرانية. ويصدق ذلك بوجه خاص على مجالات مثل تنظيم المحتوى وسلامة الشبكات وحماية المستهلك لأن المستخدمين أصبحوا في موقف ضعف.[958] ولذلك تعتبر مشاركة الهيئات التنظيمية ناتجة عن كون الجريمة السيبرانية تقوض تطور صناعة تكنولوجيا المعلومات والاتصالات والمنتجات والخدمات ذات الصلة.

ويمكن النظر إلى الواجبات والمسؤوليات الجديدة التي تضطلع بها الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات في مكافحة الجريمة السيبرانية كجزء من الاتجاه الأوسع لتحويل النماذج المركزية لتنظيم الجريمة السيبرانية إلى بنيات هياكل. وفي بعض البلدان، قامت الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات بالفعل باستكشاف إمكانية نقل نطاق الواجبات التنظيمية من قضايا المنافسة والتخويل داخل صناعة الاتصالات إلى حماية المستهلك على نطاق أوسع وتطوير الصناعة والسلامة السيبرانية والمشاركة في وضع السياسات المتعلقة بالجريمة السيبرانية وتنفيذها والتي تشمل استعمالاً أوسع لتكنولوجيا المعلومات والاتصالات وبالتالي القضايا المتصلة بالجريمة السيبرانية. وفي حين تشكلت بعض الهيئات التنظيمية الجديدة بولايات ومسؤوليات تشمل الجريمة السيبرانية،[959] وسعت الهيئات التنظيمية الأقدم القائمة لتكنولوجيا المعلومات والاتصالات من نطاق المهام القائمة الملقاة على عاتقها لتشمل أنشطة مختلفة تهدف إلى مكافحة التهديدات السيبرانية ذات الصلة.[960] ورغم ذلك، ما زال نطاق هذه المشاركة وحدودها قيد المناقشة.

2.5.4 نماذج لتوسيع نطاق مسؤولية الهيئة التنظيمية

هناك نموذجان مختلفان لتحديد ولاية الهيئات التنظيمية في مكافحة الجريمة السيبرانية، وهما ممارسة الولاية القائمة على نحو واسع أو إنشاء ولايات جديدة.

وهناك مجالان تقليديان لمشاركة الهيئات التنظيمية وهما حماية المستهلك وسلامة الشبكات. وقد تغير التركيز على حماية المستهلك مع التحول من خدمات الاتصالات إلى الخدمات المتصلة بالإنترنت. فبالإضافة إلى التهديدات التقليدية يتعين مراعاة أثر الرسائل الاقتحامية والبرمجيات الضارة والبرامج الروبوتية. ونستمد مثالاً على توسيع نطاق ولاية الهيئة التنظيمية من الهيئة الهولندية المستقلة للبريد والاتصالات (OPTA). وتشمل ولاية[961] الهيئة التنظيمية حظر الرسائل الاقتحامية ومنع نشر البرمجيات الضارة.[962] وخلال مناقشة ولاية الهيئة الهولندية المستقلة للبريد والاتصالات،[963] أعربت المنظمة عن رأيها بمد الجسور بين الأمن السيبراني كمجال تقليدي للنشاط والجريمة السيبرانية من أجل مواجهة هاتين القضيتين معاً بشكل فعال.[964] وإذا كان ينظر إلى الجريمة السيبرانية كرمز لإخفاق الأمن السيبراني، فبالتالي يتسع نطاق ولاية الهيئات التنظيمية تلقائياً.

وتتوقف إمكانية توسيع نطاق ولاية الهيئة التنظيمية لتشمل قضايا الجريمة السيبرانية أيضاً على التصميم المؤسسي للهيئة التنظيمية، وما إذا كانت متعددة القطاعات (مثل لجان المرافق العامة) أو هيئة تنظيم للاتصالات تختص بقطاع محدد أو هيئة تنظيمية متقاربة. وبينما يتمتع كل نموذج خاص بالتصميم المؤسسي بمزاياه وعيوبه من منظور تنظيم صناعة تكنولوجيا المعلومات والاتصالات،[965] فإنه ينبغي مراعاة التصميم المؤسسي عند تقييم كيفية إشراك هيئات تنظيم تكنولوجيا المعلومات والاتصالات والمجالات التي يتعيّن إشراكها فيها. وتواجه الهيئات التنظيمية المتقاربة بوجه عام، التي تضطلع بمسؤولية تنظيم الوسائط والمحتوى الإنترنت فضلاً عن خدمات تكنولوجيا المعلومات والاتصالات، تحدياً من حيث تعقيد أعباء العمل.[966] ومع ذلك، يمكن أن تشكل ولايتهم الشاملة ميزة في التعامل مع القضايا المتعلقة بالمحتوى مثل المواد الإباحية المستغلة للأطفال أو المحتويات غير المشروعة أو الضارة. وفي إطار بيئة متقاربة تكافح فيها الهيئات التنظيمية التقليدية للاتصالات لإيجاد حلول لبعض القضايا مثل الجمع بين موردي خدمات محتوى وسائط الإعلام وموردي خدمات الاتصالات، وتبدو الهيئات التنظيمية المتقاربة في وضع أفضل لمعالجة قضايا شبكات المحتوى. وعلاوةً على ذلك، يمكن للهيئات التنظيمية المتقاربة أن تساعد في تجنّب عدم الاتساق وعدم التيقن بشأن التنظيم والتدخل التنظيمي غير المتساوي فيما يتعلق بمختلف المحتويات المنقولة عبر مختلف المنصات.[967] ورغم ذلك، لا ينبغي أن تقوض مناقشة مزايا هيئات التنظيم المتقاربة أهمية أنشطة هيئات التنظيم المختصة بقطاع وحيد. ففي حين لم يكن لدى الاتحاد الأوروبي، على سبيل المثال، حتى نهاية عام 2009 إلا أربع هيئات تنظيم متقاربة لتكنولوجيا المعلومات والاتصالات،[968] كان عدد أكبر يشارك في مواجهة الجريمة السيبرانية.

وعند التفكير في توسيع نطاق استعمال الولايات القائمة، يجب أن يؤخذ في الاعتبار قدرة هيئة التنظيم وضرورة تجنب التداخل مع ولايات المنظمات الأخرى. ويمكن حل مثل هذه النزاعات المحتملة بصورة أسهل إذا تم تحديد ولايات جديدة بوضوح.

ويتمثل النهج الثاني في استحداث ولايات جديدة. ونظراً لاحتمال وقوع نزاعات، قررت بلدان مثل ماليزيا إعادة تحديد الولايات لتفادي الالتباس والتداخل. وأنشأت اللجنة الماليزية للاتصالات ووسائط الإعلام (MCMC)، بوصفها هيئة تنظيم متقاربة، إدارة خاصة[969] تتناول أمن المعلومات واعتمادية الشبكات وسلامة الاتصالات والبُنى التحتية الحرجة للاتصالات.[970] ويمكن ملاحظة نهج مماثل في كوريا الجنوبية حيث أنشئت لجنة كوريا للاتصالات (KCC) في عام 2008 من خلال دمج الوزارة السابقة للمعلومات والاتصالات واللجنة الكورية للإذاعة. وتضطلع لجنة كوريا للاتصالات، من بين الواجبات الملقاة على عاتقها بمسؤولية حماية مستعملي الإنترنت من المحتويات الضارة أو غير القانونية.[971]

3.5.4 أمثلة على مشاركة الهيئات التنظيمية في مكافحة الجريمة السيبرانية

لم يتم بعد تعريف النموذج الذي سيحدد بوضوح ولاية الهيئات التنظيمية فحسب، بل أيضاً مجال عمل الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات في هذا الميدان. وتمتع عدد قليل فقط من هيئات تنظيم تكنولوجيا المعلومات والاتصالات بسلطات فعلية تتجاوز تنظيم الاتصالات وتعالج قضايا قطاع تكنولوجيا المعلومات والاتصالات الأوسع نطاقاً. ويعرض العمل في قطاع يتغير و يتطور بسرعة الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات لمجالات جديدة والتي كانت تعتبر تقليدياً من مجالات عمل إدارات ووكالات حكومية أخرى، بل ليست مجال عمل أي جهة على الإطلاق.[972] وحتى ولو كانت هيئة

التنظيم تمتلك في *الواقع* كفاءة كافية وخبرة في الصناعة للمشاركة في معالجة قضايا محددة متعلقة بالجريمة السيبرانية، فإن تحديد ولاية واضحة تتضمن المجالات الفعلية التي تتم فيها المشاركة يُعدّ أمراً رئيسياً لكي تؤدي الهيئات التنظيمية دورها بفعالية. ويُسلط الضوء فيما يلي على المجالات المحتملة لمشاركة الهيئات التنظيمية:

الاستراتيجيات العالمية للسياسة

يفصل مبدأ تقسيم السلطة داخل الدولة[973] ما بين صنع السياسة العامة وتنفيذها. ورغم أهمية هذا المفهوم، قد يقتضي ما تتسم به القضية من تعقيد من الهيئات التنظيمية المشاركة في إسداء المشورة بشأن السياسات.[974] وتقوم الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات في عدة بلدان، بسبب خبرتها الصناعية وقنوات اتصالها القائمة مع أصحاب مصلحة آخرين، بدور مهم في تحديد السياسات والاستراتيجيات لتطوير صناعة تكنولوجيا المعلومات والاتصالات.[975] ففي بعض البلدان، فإن مهمة تقديم مدخلات إلى صانعي السياسات في مجال تكنولوجيا المعلومات والاتصالات يعد بالتالي واحدة من المهام الرئيسية لتكنولوجيا المعلومات والاتصالات.[976] وبينما تركز هذه الممارسة الشائعة على إسداء المشورة بشأن قضايا الاتصالات، يمكن توسيع نطاق الولاية إلى الجريمة السيبرانية.[977] وفي فنلندا، شكلت الحكومة لجنة استشارية معنية بأمن المعلومات (ACIS) تحت إشراف السلطة الفنلندية التنظيمية للاتصالات (FICORA) بهدف تطوير استراتيجيتها الوطنية للمعلومات.[978] ويحدد المقترح الذي صدر عن اللجنة الاستشارية المعنية بأمن المعلومات عام 2002 أهداف وإجراءات النهوض باستراتيجية أمن المعلومات. ويمكن اعتبار عدة تدابير بأنها متعلقة بالجريمة السيبرانية والتأكيد على أهمية وضع وتحسين التشريعات الملائمة وتوطيد التعاون الدولي وزيادة الوعي بأهمية أمن المعلومات بين المستعملين النهائيين.[979]

المشاركة في وضع تشريعات الجريمة السيبرانية

تعتبر السلطة التشريعية المختصة باعتماد التشريعات وليست السلطة التنظيمية. ومع ذلك، يمكن أن تقوم هيئة تنظيم تكنولوجيا المعلومات والاتصالات بدور مهم في عملية وضع تشريعات الجريمة السيبرانية. ونظراً للخبرة التي تمتلكها الهيئات التنظيمية في مجال حماية البيانات وسرية تداولها ومنع انتشار البرمجيات الضارة والجوانب الأخرى المتعلقة بحماية المستهلك ومسؤوليات موردي خدمات الإنترنت فقد تمت مناقشة مشاركتها في هذه الميادين، على نحو خاص. وبالإضافة إلى ذلك، لا يعتبر القانون الجنائي مجالاً تجهله الهيئات التنظيمية لأنه في العديد من البلدان يمكن أن تخضع الانتهاكات الخطيرة للالتزامات المتعلقة بالمجال التقليدي للعمل التنظيمي لعقوبات جنائية.[980] وبالإضافة إلى الدور الاستشاري الذي تتمتع به الهيئات التنظيمية فيما يتعلق بالاستراتيجيات العامة كما تم التأكيد عليه آنفاً، فإنها يمكن أن تشارك في عملية صياغة التشريعات. وشاركت اللجنة الأوغندية للاتصالات، على سبيل المثال، كهيئة استشارية في عملية صياغة تشريعات الجريمة السيبرانية.[981] وعلاوةً على ذلك، تعتبر الآن اللجنة الأوغندية للاتصالات[982] من خلال فريق المهام الوطني الأوغندي المعني بالتشريعات السيبرانية جزءاً من مبادرة إقليمية يطلق عليها اسم فريق مهام بلدان شرق إفريقيا[983] المعني بالقوانين السيبرانية كلف بعملية مستمرة لتطوير وتنسيق قوانين الجريمة السيبرانية في منطقة شرق إفريقيا. وفي زامبيا، طُلب من السلطة المعنية بالاتصالات أن تساعد في صياغة تشريع جديد متعلق بالجريمة السيبرانية،[984] وهو تحديداً القانون المعني بالاتصالات والمعاملات الإلكترونية لعام 2009. وهناك مثال آخر في بلجيكا حيث ساعدت الهيئة البلجيكية لتنظيم تكنولوجيا المعلومات والاتصالات (BIPT) عام 2006[985] في عملية صياغة التشريعات المتعلقة بالجريمة السيبرانية. وتم وضع مشروع هذه التشريعات بالتعاون مع الخدمة الفدرالية العامة للعدل والوحدة الفدرالية للجرائم الحاسوبية.[986]

اكتشاف الجريمة السيبرانية والتحقيق بشأنها

تقوم أفرقة الاستجابة للحوادث الحاسوبية (CIRT) بدور مهم في رصد التهديدات والحوادث السيبرانية واكتشافها ودراستها والتحقيق بشأنها.[987] وبسبب الطبيعة المتعددة القطاعات لمشكلة الجريمة السيبرانية، أنشأت مجموعة من أصحاب المصلحة بما فيهم الحكومات والشركات التجارية ومشغلو الاتصالات والهيئات الأكاديمية أفرقة مختلفة للاستجابة للحوادث الحاسوبية لتنفيذ وظائف مختلفة.[988] وفي بعض البلدان، تضطلع الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات بمسؤولية إنشاء أفرقة

الاستجابة الوطنية للحوادث الحاسوبية وإدارتها. ولا تُعدّ هذه الأفرقة أحد أهم الكيانات المسؤولة عن اكتشاف حوادث الجريمة السيبرانية والتحقيق بشأنها على الصعيد الوطني فحسب، ولكن أيضاً أحد أهم المشاركين في إجراءات تعزيز التعاون بشأن الجريمة السيبرانية على الصعيد الدولي. وكان الفريق الفنلندي الوطني للاستجابة لحالات الطوارئ الحاسوبية من أوائل هذه الأفرقة التي أُنشئت كمبادرة تحت إشراف الهيئة التنظيمية لتكنولوجيا المعلومات والاتصالات وتم إطلاقه في يناير 2002 برعاية السلطة الفنلندية لتنظيم الاتصالات (FICORA)[989]. ويمكن العثور على أمثلة أخرى في السويد[990] والإمارات العربية المتحدة[991] وقطر.[992]

تيسير إنفاذ القانون

يمكن للهيئة التنظيمية لتكنولوجيا المعلومات والاتصالات أن تتولى فقط القيام بالتحقيقات وتتصرف في هذا الصدد كهيئة لإنفاذ القانون على أساس ولاية صريحة تُمنح للهيئة التنظيمية لممارسة أحكام قانونية معيّنة وإنفاذها. وقامت بعض البلدان بالترخيص للهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات بأن تتصرف كوكالة لإنفاذ القانون في المجالات المتعلقة بالجريمة السيبرانية مثل التدابير الرامية لمكافحة الرسائل الاقتحامية وتنظيم المحتوى أو التدابير المتعلقة بإنفاذ التنظيم المشترك. وفيما يخص الرسائل الاقتحامية، تعتبر الهيئات الأوروبية التنظيمية لتكنولوجيا المعلومات والاتصالات بالفعل جزءاً من شبكة الاتصال لسلطات تنفيذ مكافحة الرسائل الاقتحامية التي أنشأتها المفوضية الأوروبية عام 2004 لمكافحة الرسائل الاقتحامية على الصعيد الأوروبي.[993] ويعرض فريق المهام التابع لمنظمة التعاون والتنمية في الميدان الاقتصادي والمعني بالرسائل الاقتحامية كذلك قائمة الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات التي تعمل كجهات اتصال لوكالات إنفاذ القانون.[994] وتوجد اتفاقات تعاون بين الهيئات التنظيمية لتكنولوجيا المعلومات والاتصالات ووحدات الجريمة السيبرانية على صعيد الشرطة في هولندا ورومانيا.[995]

4.5.4 *التدابير القانونية*

لعل التدابير القانونية هي، من بين الركائز الخمس للبرنامج العالمي للأمن السيبراني، أهم التدابير لاستراتيجية مكافحة الجريمة السيبرانية.

القانون الجنائي الموضوعي

وهذا يتطلب أولاً أن تجرم كل أحكام القانون الجنائي الموضوعية اللازمة أعمالاً مثل الاحتيال الحاسوبي، والنفاذ غير القانوني، والتداخل في البيانات، وانتهاك حقوق المؤلف، واستغلال الأطفال في المواد الإباحية.[996] ووجود أحكام في القانون الجنائي تنطبق على أعمال مماثلة ترتكب خارج شبكة لا يعني أنها يمكن أن تنطبق على الأعمال المرتكبة على الإنترنت أيضاً.[997] ولذا، فإن من الحيوي إجراء تحليل شامل للقوانين الوطنية الراهنة للوقوف على أي ثغرات محتملة.[998]

القانون الجنائي الإجرائي

وإلى جانب الأحكام الموضوعية للقانون الجنائي،[999] تحتاج وكالات إنفاذ القانون إلى الأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية.[1000] وتطرح هذه التحقيقات نفسها عدداً من التحديات.[1001] فالجناة يستطيعون أن يقوموا بعملهم من أي مكان تقريباً في العالم وأن يتخذوا تدابير لإخفاء هويتهم.[1002] وقد تكون الأدوات والصكوك اللازمة للتحقيق في الجريمة السيبرانية مختلفة إلى حد كبير عن تلك المستخدمة للتحقيق في الجرائم العادية.[1003] وبالنظر إلى البعد الدولي[1004] للجريمة السيبرانية، فمن الضروري، بالإضافة إلى ذلك، تطوير الإطار القانوني الوطني ليكون قادراً على التعاون مع وكالات إنفاذ القانون في الخارج.[1005]

الأدلة الإلكترونية

تحتاج سلطات التحقيق المختصة وكذلك المحاكم عند معالجة الجريمة السيبرانية إلى التعامل مع الأدلة الإلكترونية. ويطرح التعامل مع هذه الأدلة عدداً من التحديات[1006] غير أنه يفتح كذلك المجال أمام إمكانيات جديدة للتحقيق ولعمل خبراء

الأدلة الجنائية والمحاكم[1007]. وفي الحالات التي لا تتوفر فيها أي مصادر أخرى للأدلة، قد تتوقف القدرة على تحديد ومقاضاة مجرم معين بنجاح على التجميع والتقييم الصحيح للأدلة الإلكترونية.[1008] ويؤثر هذا على الطريقة التي تتعامل بها وكالات إنفاذ القانون والمحاكم مع هذه الأدلة.[1009] وبينما تعرض الوثائق التقليدية عن طريق عرض الوثيقة الأصلية على المحكمة، تتطلب الأدلة الرقمية في بعض الحالات إجراءات خاصة لا تسمح بتحويلها إلى أدلة تقليدية، على سبيل المثال عن طريق تقديم نسخة مطبوعة من الملفات وغيرها من البيانات المكتشفة.[1010] ولذلك يعتبر وجود على تشريعات تتناول قبول هذه الأدلة أمراً حيوياً لمكافحة الجريمة السيبرانية.

التعاون الدولي

نظراً للبُعد الدولي للإنترنت وعولمة الخدمات[1011] يتميز عدد متزايد من الجرائم السيبرانية ببعد دولي. وتحتاج البلدان التي ترغب في التعاون مع البلدان الأخرى للتحقيق في الجريمة عبر الحدود إلى استعمال صكوك التعاون الدولي.[1012] وإذا أخذنا في الاعتبار تنقل المجرمين، يبين عدم الارتباط بين حضور المجرم وأثر الجريمة التحدي القائم والحاجة للتعاون بين وكالات إنفاذ القانون والسلطات القضائية.[1013] وبسبب الاختلافات الموجودة في القانون الوطني ومحدودية الصكوك، يعتبر التعاون الدولي أحد التحديات الرئيسية لعولمة الجريمة.[1014] وتحتاج البلدان في إطار نهج شامل لمواجهة الجريمة السيبرانية إلى النظر في تعزيز قدرتها للتعاون مع البلدان الأخرى وأن تكون الإجراءات أكثر فعالية.

مسؤولية مورّد الخدمة

يصعب ارتكاب الجريمة السيبرانية دون استعمال خدمات مورد خدمات الإنترنت. وترسل الرسائل الإلكترونية ذات المحتوى المهدد باستعمال خدمة مورد بريد إلكتروني ويتضمن تحميل المحتوى غير المشروع من موقع إلكتروني من جملة أمور خدمة لمورد مستضيف ومورد للنفاذ ونتيجة لذلك غالباً ما يكون موردو خدمات الإنترنت في مركز التحقيقات الجنائية التي تشمل المجرمين الذين يستعملون خدمات موردي خدمات الإنترنت لارتكاب الجريمة.[1015] وإذا أخذنا في الاعتبار أن ارتكاب الجريمة السيبرانية لا يمكن أن يتم دون مشاركة موردي خدمة الإنترنت من جهة، وأن موردي خدمات الإنترنت لا يستطيعون غالباً منع هذه الجرائم من جهة أخرى، فإن ذلك يفضي إلى مسألة ما إذا كان يتعين تقييد مسؤولية موردي خدمات الإنترنت.[1016] ويمكن معالجة هذه القضية ضمن نهج قانوني شامل لمواجهة الجريمة السيبرانية.

5.5.4 التدابير التقنية والإجرائية

تنطوي التحقيقات المتعلقة بالجريمة السيبرانية، في كثير من الأحيان، على مكون تقني قوي.[1017] 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 تطوير 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 (مثلاً بالانتقال من نظام تان TAN[1018] إلى النظام آيتان ITAN[1019]) قد أزال كثيراً من المخاطر الناشئة عن هجمات "التصيّد الاحتيالي" الراهنة، مما يبين الأهمية الحيوية للحلول التقنية.[1020] 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)، وموردو الخدمات وشركات البرمجيات.

وقد يكون من الأسهل، من الناحية اللوجستية، التركيز على حماية البنى التحتية الأساسية (مثل الشبكات الرئيسية، والمسيّرات، والخدمات الأساسية)، بدلاً 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، بدلاً 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.

ويؤدي موردو خدمات 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).[1021]

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.

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.[1022]

وبالإضافة إلى بناء القدرات يقتضي الأمر توعية المستخدمين.[1023] 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 الوعي من جانب الضحايا.[1024] وهناك برمجيات متنوعة يمكن أن تكشف آلياً عن مواقع الويب الاحتيالية،[1025] 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.[1026] 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.[1027] فإذا كان المستخدمون مثلاً 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 والدروس المنظمة في المدارس والمكتبات ومراكز تكنولوجيا المعلومات والجامعات إضافة إلى الشراكات بين القطاعين العام والخاص (PPP).

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 التوالي، يتأثرون بتهديدات الجريمة السيبرانية، تجنباً لفقدان ثقتهم بخدمات الاتصالات المتاحة على الخط. وقد طلب مكتب التحقيقات الفيدرالي بالولايات المتحدة صراحة من الشركات أن تتغلب على نفورها من الدعاية السلبية وأن تبلغ عن الجريمة السيبرانية.[1028] وعملاً على تحديد مستويات التهديد، وإعلام المستخدمين، من الحيوي تحسين جمع المعلومات ذات الصلة ونشرها.[1029]

التعاون الدولي

تمر عمليات نقل البيانات على الإنترنت، في الكثير من الحالات، بأكثر من بلد واحد.[1030] ويعزى هذا إلى تصميم الشبكة وكذلك إلى البروتوكولات التي تضمن إمكانية إجراء عمليات النقل بنجاح، حتى إذا كانت الخطوط المباشرة مسدودة بصفة مؤقتة.[1031] وبالإضافة إلى ذلك، فإن عدداً كبيراً من خدمات الإنترنت (ومنها مثلاً خدمات الاستضافة) توفره شركات تقع مقارها في الخارج.[1032]

وفي الحالات التي لا يكون الجاني موجوداً فيها بنفس بلد الضحية، يقتضي التحقيق التعاون بين وكالات إنفاذ القانون في جميع البلدان المتضررة.[1033] 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.[1034] 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. ويُعزى 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.

6.4 تجارب بناء القدرات في مجموعة دول إفريقيا والكاريبي والمحيط الهادئ (ACP)

تشارك الاتحاد الدولي للاتصالات والاتحاد الأوروبي، في الفترة 2008-2013، في تمويل مشروع[1035] يهدف إلى دعم وضع السياسات والتشريعات في بلدان المجموعة، كجزء من برنامج "تكنولوجيا المعلومات والاتصالات" وصندوق التنمية الأوروبي التاسع. وتم تقديم الدعم لمنطقة إفريقيا جنوب الصحراء في إطار "مواءمة سياسات تكنولوجيا المعلومات والاتصالات في إفريقيا جنوب الصحراء" (HIPSSA). وتم بالنسبة لبلدان الكاريبي تنفيذ مشروع "تعزيز القدرة التنافسية في منطقة الكاريبي من خلال مواءمة سياسات تكنولوجيا المعلومات والاتصالات، والإجراءات التشريعية والتنظيمية لدعم بلدان الكاريبي" (HIPCAR).[1036] وتلقت بلدان المحيط الهادئ الدعم أيضاً ضمن مشروع "بناء القدرات وسياسة تكنولوجيا المعلومات والاتصالات والأطر التنظيمية والتشريعية لدعم البلدان الجزرية في المحيط الهادئ" (ICB4PAC). وقد وضع الاتحاد منهجية محددة وأحرز تقدماً هاماً في بناء القدرات ذات الصلة في تلك السنوات الست.

1.6.4 المنهجية

كان من أهم إنجازات المشاريع وضع منهجية شاملة لبناء القدرات في مجال الاستراتيجية/السياسة/التشريعات. وكان جزء من التحضير لذلك دراسة أمثلة لأفضل الممارسات في المنهجيات القائمة للمواءمة الإقليمية للسياسات والتشريعات. ومع ذلك، فإن تفرّد المشروع من حيث عدد البلدان المعنية (أكثر من 70 بلداً من ثلاث مناطق)، ومجالات العمل (ما يصل إلى تسعة) والوقت (ست سنوات) جعل من الضروري وضع نهج جديدة.

وخلال أولى المرحلتين وضعت سياسات إقليمية نموذجية وتشريعات نموذجية. وبدأت هذه المرحلة بتقييم السياسات والتشريعات القائمة في البلدان المستفيدة. وللتأكد من استبانة كل القوانين المعمول بها، تمت عملية التقييم على يد خبراء دوليين وإقليميين بدعم من النظراء المتفرغين في كل بلد. وفي التقرير الذي لخص الاستنتاجات، تمت مقارنة المعايير القائمة المستبانة مع أفضل الممارسات الإقليمية والدولية – مع إيلاء الأولوية لتلك القابلة للتطبيق مباشرة على الأقل في بعض البلدان المستفيدة (مثل التشريع النموذجي لدول الكومنولث). ومع ذلك، أضيفت أيضاً أفضل الممارسات من مناطق أخرى، مثل الاتحاد الأوروبي. وتضمنت تقارير التقييم[1037] لمحة عامة عن التشريعات القائمة، فضلاً عن التحليل القانوني المقارن للتشريعات القائمة مع أفضل الممارسات الإقليمية والدولية. ومن أجل إعداد تحليل للثغرات، حدد تقرير التقييم أيضاً مطالب إقليمية معينة لم تتناولها بالضرورة أفضل الممارسات الدولية. ثم نوقش تقرير التقييم مع أصحاب المصلحة الرئيسيين من جميع البلدان

المستفيدة. وبعد التشاور مع أصحاب المصلحة، وُضعت سياسات وقوانين نموذجية وملاحظات تفسيرية لجميع مجالات العمل ذات الصلة. وقاد هذه العملية خبراء إقليميون (من جميع البلدان المستفيدة) للتأكد من أن النواتج لا تتماشى مع أفضل الممارسات الإقليمية والدولية فحسب بل يمكن أيضاً تنفيذها بسهولة.

وكانت المرحلة الثانية مكرسة لإمكانية التنفيذ على الصعيد الوطني. وهنا كان من الضروري أيضاً وضع منهجية إفرادية. وقد استدعى الإطار الزمني المحدود وعدد مجالات العمل منهجية تسمح بدعم على درجة عالية من الكفاءة داخل كل بلد. وبعد تحديد ماهية مجموعة الأعمال اللازمة يتلقى كل بلد خطة مشروع تتناول الدعم الإفرادي الخاص به. ولضمان أقصى قدر من الدعم من أصحاب المصلحة في البلد شملت عملية تكييف السياسات والتشريعات النموذجية مشاورات واسعة مع أصحاب المصلحة. وفي إطار تلك المشاورات دعي مختلف أصحاب المصلحة الوطنيين (ومنهم عامة الناس والعاملون في السياسة وموظفو الحكومة ودوائر الصناعة والأعمال ومقدمو خدمات الإنترنت ودعاة الحريات المدنية) للمشاركة في مختلف الاجتماعات التشاورية حيث نوقشت علناً عملية النقل والسياسات والتشريعات النموذجية. وقد شملت عملية الصياغة المدخلات من أصحاب المصلحة وأدرجتها فيها. كما شارك في عملية الصياغة خبراء محليون وإقليميون/دوليون. وبالإضافة إلى ذلك عقدت ورش عمل لبناء القدرات لمختلف مجموعات المصالح (مثل التدريب المخصص لأفراد الشرطة ودورات منفصلة للقضاة والمدعين العامين ومحاضرات في المدارس والجامعات، وورش عمل لعامة الناس وحملات بالتعاون مع الصحافة المحلية).

2.6.4 *الدروس المستخلصة*

أدى العمل المكثف مع أكثر من 70 بلداً إلى استبانة لأفضل الممارسات مختلفة يمكن أن تكون مفيدة لمشاريع بناء القدرات في المستقبل.

بالإضافة إلى التشريعات يحتاج الأمر إلى سياسة

إن وضع التشريعات هو شرط أساسي لتوفير بيئة موثوقة لاستخدام تكنولوجيا المعلومات والاتصالات.[1038] ولكن من غير المعتاد الشروع في هذه العملية بوضع التشريعات قبل وضع استراتيجية وسياسة عامة. ومعظم البلدان تبدأ بوضع سياسة عامة. ودور هذه السياسة هو تحديد استجابة الحكومة لقضية معينة.[1039] والسياسة تمكن الحكومة من تحديد استجابة شاملة لمشكلة ما. وبالإضافة إلى التشريعات، قد يشمل ذلك استجابات أخرى يمكن استخدامها لتحقيق أهداف السياسة. وخلافاً للنهج الإقليمية الأخرى التي تركز على مواءمة التشريعات – مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية[1040] — شملت مشاريع دعم بلدان إفريقيا جنوب الصحراء (HIPSSA) وبلدان الكاريبي (HIPCAR) والبلدان الجزرية في المحيط الهادئ (ICB4PAC) وضع مثل هذه السياسات. وكنتيجة ملموسة، يسّر ذلك تعاون مختلف أصحاب المصلحة (وخاصة الوزارات) ذوي الاختصاصات المتداخلة في مجال تكنولوجيا المعلومات والاتصالات. ومن المرجح أن من شأن الجمع بين السياسات والتشريعات اختصار الوقت اللازم في بلد ما لإدخال تشريع جديد.

فوارق محدودة بين التشريعات النموذجية

تكشف مقارنة مختلف النهج الإقليمية (مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية،[1041] والقرار الإطاري للاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات،[1042] ومشروع اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني[1043] ومشاريع دعم بلدان إفريقيا جنوب الصحراء (HIPSSA) وبلدان الكاريبي (HIPCAR) والبلدان الجزرية في المحيط الهادئ (ICB4PAC) التي تتناول الجرائم الملموسة (مثل النفاذ غير المشروع) عن درجة كبيرة من الاتساق في النهج والمنهجية المعمول بها. وكلها تتبع أفضل الممارسات الدولية ومن ثم يمكن استخدام القانون النموذجي الذي وضعه فريق من خبراء الكاريبي كأساس لوضع إطار نموذجي لمشروعي بلدان إفريقيا جنوب الصحراء والبلدان الجزرية في المحيط الهادئ.

معايير عالية في البلدان النامية

يُبرز المشروع أن المعايير التي تضعها البلدان الصغيرة والنامية لا ينبغي أن تكون أدنى من المعايير الموضوعة في أوروبا. بل هنالك في الواقع عناصر مختلفة من الأطر القانونية تفوق المعايير الأوروبية. مثال ذلك استغلال الأطفال في المواد الإباحية حيث تشير المادة 9 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية فقط إلى "مواد تصور بصرياً" طفلاً ما وبالتالي لا تغطي المواد السمعية، على الرغم من أنه من المعروف على نطاق واسع أن المجرمين يتبادلون أيضاً ملفات صوتية لاستغلال الأطفال في مواد إباحية.[1044] وقد اعتمدت مشاريع بلدان إفريقيا جنوب الصحراء وبلدان الكاريبي والبلدان الجزرية في المحيط الهادئ نهجاً مختلفاً وهي تتجنب مصطلح "بصرياً"، ومن ثم تشمل الملفات الصوتية.

ميزة مشاركة واسعة من جانب الخبراء وعقد المشاورات مع أصحاب المصلحة

ثمة جانبان تبين أن لهما قيمة كبيرة أثناء المرحلة الانتقالية وهما إشراك خبراء من كل البلدان المستفيدة تقريباً في صوغ السياسات والتشريعات النموذجية فضلاً عن المشاركة الواسعة من أصحاب المصلحة الوطنيين في العملية الانتقالية.

وقد أظهر التقييم أن المشاركة الواسعة من جانب الخبراء من جميع البلدان المستفيدة في عملية وضع المعايير الإقليمية لقيت نجاحاً كبيراً. مثال ذلك أن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية وضعها خبراء من 14 دولة عضواً فقط[1045] من أصل 47 دولة وأربعة خبراء من دول غير أعضاء[1046]. وعلى النقيض من ذلك، فإن السياسات والتشريعات النموذجية لمشاريع بلدان إفريقيا جنوب الصحراء وبلدان الكاريبي والبلدان الجزرية في المحيط الهادئ وضعها خبراء من جميع البلدان المستفيدة تقريباً.

وثمة تجربة إيجابية أخرى بشأن استضافة المشاورات مع أصحاب المصلحة. فقد اتفقت جميع الأطراف المعنية على أن الأمر يتطلب القدر الكبير من الطاقة اللازمة لمناقشة عناصر سياسة وطنية ولصوغ تشريعات مع طائفة واسعة من أصحاب المصلحة مقارنة بمناقشات داخلية فقط. لكن العملية التشريعية السلسة التي أعقبت مشاركة أصحاب المصلحة مؤشر على ميزة عقد مناقشات مكثفة في إطار عملية الصياغة للتأكد من معالجة مختلف الشواغل.

---

926 Regarding a clear distinction see for example: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1, page 3.

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

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

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

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

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

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

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

934 See below: § 4.4.

935 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arab regions.

936 See for example: Austria: National ICT Security Strategy Austria, available at: www.ccdcoe.org/strategies/Austrian_Cyber_Security_Strategy.pdf ; Estonia: Cyber Security Strategy, available at: www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf ; Germany: Cybersecurity Strategy for Germany, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile ; United Kingdom: UK Cyber Security Strategy, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf ; New Zealand: www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf ; For more examples see: National Cyber Security Framework Manual, NATO CCD, 2012, page 53 et seq.

937 See for example the EU Cybersecurity Strategy: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1. Regarding the activities of the UN in relation to Cybersecurity see: *Maurer*, Cyber Norm Emergence at the United Nations, An Analysis of the Activities at the UN regarding Cyber-Security, 2011.

938 See: National Cyber Security Framework Manual, NATO CCD, 2012, page 46.

939 Cybersecurity Strategy for Germany, 2011, page 7, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

940 With regard to the need of updates see below III.5.c.

941 This issue was for example taken into consideration within the EU/ITU co-funded projects HIPCAR and ICB4PAC. The model policy, as well as the model legislation, are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

942 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

943 Regarding the need for an interdisciplinary approach see: *Schjolberg/Ghernaouti-Helie*, A Global Treaty on Cybersecurity and Cybercrime, Second Edition, 2011, page 17, available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

944 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

945 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

946 .See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

947 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

948 See below: § 5.

949 The harmonization of training is one of the main objectives for the EU Cybercrime Centers of Excellence Network (2Centre). Information is available at: www.2centre.eu. Other examples are the European Cybercrime Training & Education Group (ECTEG) as well as the Europol Working Group on the Harmonization of Cybercrime Training (EWGHCT).

950 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

951 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

952 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

953 See for example: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, 2007, page 5, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf; *Pladna*, The Lack of Attention in the Prevention of Cyber Crime and How to improve it, University of East Carolina, ICTN6883, available at: www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf.

954 Regarding blocking of websites with illegal content see: *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008.

955 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

956 Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary, page 7, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf; see also ITU, World Summit on Information Society, The Report of the Task Force on Financial Mechanisms for ICT for Development, December, 2004, available at: www.itu.int/wsis/tffm/final-report.pdf; ITU/infoDEV ICT Regulation Toolkit, Chapter 4.1. What is the Role of Regulators?, available at: www.ictregulationtoolkit.org/en/Section.3109.html

957 See GSR09 – Best Practice Guidelines on innovative regulatory approaches in a converged world to strengthen the foundation of a global information society, available at www.itu.int; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009 // available at: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf

958 *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf; *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

959 E.g. Korea Communications Commission, established in February 2008 (formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission), announced among other core regulatory duties protection of Internet users from harmful or illegal content. Korea Communications Commission: http://eng.kcc.go.kr.

960 E.g. Swedish ICT Regulator PTS addresses cyberthreats and cybercrime under user protection mandate and network security mandate. See: *PTS*. Secure communications, available at www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

961 *OPTA*. Regulatory areas, available at: www.opta.nl/en/about-opta/regulatory-areas/.

962 The Dutch regulator is granted the mandate to monitor any contravention of the prohibition of unsolicited communication under its duties to provide Internet safety for consumers.

963 OPTA has the power to take action against anyone contravening the prohibition of spam and unsolicited software by imposing fines.

964 OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

965 *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Henten/ Samarajiva/ Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; infoDev/ITU ICT regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

966 See the discussions on regulation, illegal content and converged regulators: *Van Oranje et al,* Responding to Convergence: Different approaches for Telecommunication regulators TR-700-OPTA, 30 September 2008, available at: www.opta.nl/download/convergence/convergence-rand.pdf; *Millwood Hargrave, et al,* Issues facing broadcast content regulation, Broadcasting Standards Authority, New Zealand, 2006, available at: www.bsa.govt.nz/publications/IssuesBroadcastContent-2.pdf. See also: *ITU*, Case Study: Broadband, the Case of Malaysia, Document 6, April 2001, available at: www.itu.int/osg/spu/ni/broadband/workshop/malaysiafinal.pdf.

967 See*: infoDev/ITU* ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html. See also: *Henten/ Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; *Singh/Raja*, Convergence in ICT services: Emerging regulatory responses to multiple play, June 2008, available at: http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/Convergence_in_ICT_services_Emerging_regulatory_responses_to_multiple_play.pdf; *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1.

968 The four states which have regulators that can be regarded as converged regulatory authorities are: Finland, Italy, Slovenia and the United Kingdom. See: infoDev/ITU ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html.

969 Information and network security (INS).

970 See: *MCMC*, What do we Do. Information Network Security, available at: www.skmm.gov.my/what_we_do/ins/feb_06.asp.

971 Korea Communications Commission: Important Issues, available at: http://eng.kcc.go.kr.

972 Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary. 2009, P. 11, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

973 See: *Haggard/McCubbins*, Presidents, Parliaments, and Policy. University of California, San Diego, July 1999, available at: http://mmccubbins.ucsd.edu/ppp.pdf. For the discussion with regard to regulatory agencies, see: *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making: a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf.

974 The rationale for separating the ICT regulator from the policy-making body is to have an independent regulator that maintains a distance from the ministry or other government bodies which could remain as the major shareholder of the incumbent. An independent regulator can avoid conflict of interest that can happen if the regulator is also responsible for industry promotion. See: *OECD*, Telecommunications Regulatory Structures and Responsibilities, DSTI/ICCP/TISP(2005)6/FINAL, January, 2006, available at: www.oecd.org/dataoecd/56/11/35954786.pdf.

975 InfoDev ITU ICT Regulation toolkit. Section 6.3. Separation of Power and Relationship of Regulator with Other Entities, available at: www.ictregulationtoolkit.org/en/Section.1269.html.

976 Public Consultation Processes. InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; *Labelle*, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

977 One example is the Botswana Telecommunications Authority, which is required to provide the input to government policy-making efforts. See: Case Study Single Sector Regulator: Botswana Telecommunications Authority (BTA). InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/PracticeNote.2031.html.

978 International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich, 2009, available at www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663, P. 133.

979 National Information Security Strategy Proposal, November, 2002 // available at: www.mintc.fi/fileserver/national_information_security_strategy_proposal.pdf..

980 *Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

981 See: *Uganda Communications Commission*, Recommendations on Proposed Review of the Telecommunications Sector Policy, 2005, available at: www.ucc.co.ug/UgTelecomsSectorPolicyReview_31_Jan_2005.pdf; *Blythe*, The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control in Repositioning African Business and Development for the 21st Century, Simon Sigué (Ed.), 2009, available at: www.iaabd.org/2009_iaabd_proceedings/track16b.pdf; Uganda Computer Misuse Bill 2004, available at: www.sipilawuganda.com/files/computer%20misuse%20bill.pdf.

982 See, for example: Report of the Second EAC Regional Taskforce Meeting on Cyber Laws. June 2008, Kampala, Uganda, available at: http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf.

983 Now: Zambia Information and Communications Technology Authority.

984 *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis, Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf; *Hatyoka*, ZICTA Corner – Defining ZICTA's new mandate. Times of Zambia, 2009 // available at: www.times.co.zm/news/viewnews.cgi?category=12&id=1262768483.

985 Zambia Electronic Communications and Transactions Act 2009, available at: www.caz.zm/index.php?option=com_docman&Itemid=75. See also ZICTA. Cybercrime Penalties (Part 1), available at: www.caz.zm/index.php?option=com_content&view=article&id=76:cyber-crime-penalties-part-1&catid=34:column&Itemid=38.

986 Annual report 2008 Belgian Institute for postal service and telecommunication, BIPT, 2009, available at: http://bipt.be/GetDocument.aspx?forObjectID=3091&lang=en.

987 See: *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003, available at: www.cert.org/archive/pdf/03hb001.pdf.

988 *Scarfone/Grance/Masone,* Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61, 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf, pp. 2-2.

989 www.ficora.fi/.

990 .Sweden's IT Incident Centre (Sitic) is located in the ICT regulator PTS.See: PTS. Secure communications, available at: www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

991 aeCERT created as an initiative of the UAE Telecommunications Regulatory Authority to detect, prevent and respond to current and future cybersecurity incidents in the UAE*: Bazargan*, A National Cybersecurity Strategy aeCERT Roadmap. Presentation at Regional Workshop on Frameworks for Cybersecurity and CIIP 18 – 21 Feb 2008 Doha, Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

992 The national CERT (qCERT) was established by the Qatari ICT regulator (ictQatar) and acts on behalf of ictQatar; *Lewis*, Q-CERT. National Cybersecurity Strategy Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incid ent-management-brisbane-july-08.pdf.

993 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf.

994 E.g. ICT regulators are involved in law-enforcement efforts with regard to combating spam in the following countries: Australia, Finland, Greece, Hungary, Japan, Malaysia, Mexico, Netherlands, Portugal, Turkey. See: *OECD* Task Force on Spam. Enforcement authorities contact list, available at: www.oecd-antispam.org/countrycontacts.php3.

995 .*Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

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

997 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et. seq*.

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

999 See below: § 6.2.

1000 See below: § 6.2.

1001 For an overview of the most relevant challenges in the fight against cybercrime, see above: § 3.1.

1002 One possibility to mask identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems, see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

1003 Regarding legal responses to the challenges of anonymous communication, see below: §§ 6.5.10 and 6.3.11.

1004 See above: § 3.2.6.

1005 See in this context below: § 6.6.

1006 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

1007 *Vaciago*, Digital Evidence, 2012.

1008 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

1009 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

1010 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

1011 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1012 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

1013 See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

1014 *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

1015 See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

1016 For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

1017 *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

1018 Transaction authentication number – for more information, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

1019 The ITAN system improves the TAN system. The financial institutions provide the customer with a number of TAN-indexed identity numbers. With regard to each relevant transaction, the online banking system requires a specific ITAN number selected at random from the list of supplied TAN. For more information, see: *Bishop*, Phishing & Pharming: An investigation into online identity theft, 2005, available at: http://richardbishop.net/Final_Handin.pdf.

1020 Regarding various authentication approaches in Internet banking, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

1021 Regarding approaches to coordinate the cooperation of law-enforcement agencies and Internet service providers in the fight against cybercrime, see the results of the working group established by Council of Europe in 2007. For more information, see: www.coe.int/cybercrime/.

1022 Capacity building is in general defined as the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation (of women in particular), human resources development and strengthening of managerial systems. In addition, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations, user groups, professional associations, academics and others).

1023 At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect". Regarding user-education approaches in the fight against phishing, see: Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, Technical Trends in Phishing Attacks, available at: www.cert.org/archive/pdf/Phishing_trends.pdf. Regarding sceptical views on user education, see: *Görling*, The Myth Of User Education, 2006, available at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

1024 Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: www.cert.org/archive/pdf/Phishing_trends.pdf.

1025 *Shaw*, Details of anti-phishing detection technology revealed in Microsoft Patent application, 2007, available at: http://blogs.zdnet.com/ip-telephony/?p=2199; Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers – Cyota Inc., Internet Identity and MarkMonitor to provide phishing Web site data for Microsoft Phishing Filter and SmartScreen Technology services, 2005, available at: www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

1026 For a different opinion, see: *Görling*, The Myth Of User Education, 2006, at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

1027 At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

1028 "The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack, explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, available at: www.heise-security.co.uk/news/80152.

1029 Examples of the publication of cybercrime-related data include: Symantec Government Internet Security Threat Report Trends for July–December 06, 2007, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf; Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

1030 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1031 The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: Tanebaum, Computer Networks; Comer, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1032 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network-storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

1033 Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1034 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

1035 Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/

1036 For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

1037 The assessment reports are available on the HIPCAR website and will be on the HIPSSA and ICB4PAC website shortly.

1038 With regard to the relevance of legislation related to the specific topic cybercrime see: *Gercke*, CRi 2012, 81.

1039 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf .

1040 Council of Europe Convention on Cybercrime (CETS No. 185); *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225,; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, CRi 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, page 7 *et seq.*; *Gercke*, 10 years Convention on Cybercrime, Cri 2011, 142 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

1041 Art. 2: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

1042 Art. 2 (1) :Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

1043 Art. III-2: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system.

1044 Regarding the relevance of audio files see: *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf .

1045 Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Netherlands, Portugal, Sweden and "The Former Yugoslav Republic of Macedonia".

1046 The decision to establish the working group was made during the 583rd Meeting of the Minister's, Decision No. CM/Del/Dec(97)583.

5 لمحة عامة عن أنشطة المنظمات الإقليمية والدولية

Bibliography (selected): *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009; Committee II Report, 11th UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007; *Nilsson* in *Sieber*, Information Technology Crime, page 576; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001; Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, 2001; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07.

يقدم الفصل التالي لمحة عامة عن النُّهُج التشريعية الدولية[1047] وعلاقتها بالنُّهج الوطنية.

1.5 النّهج 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 السبعة (الثمانية سابقاً)[1048]

في عام 1997، أنشأت مجموعة الثمانية (G8) "اللجنة الفرعية[1049] المعنية بجرائم التكنولوجيا الراقية" التي تهتم بمكافحة الجريمة السيبرانية.[1050] 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.[1051] وأيد رؤساء مجموعة الثمانية في وقت لاحق هذه المبادئ التي جاء فيها أنه:

- يجب ألا تكون هناك ملاذات آمنة لمن يسيؤون 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، عُقد في موسكو بالاتحاد الروسي.[1052] وأعربت بلدان مجموعة الثمانية عن شواغلها إزاء بعض الجرائم (مثل استغلال الأطفال في المواد الإباحية)، وكذلك إزاء إمكانية تتبُّع 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.[1053]

وكان من الإنجازات العملية التي أسفر عنها عمل فريق الخبراء إنشاء شبكة دولية لجهات الاتصال تُدعى شبكة 24/7، التي تستلزم من البلدان المشاركة أن تعيّن جهات اتصال للتحقيقات عبر الوطنية يمكن النفاذ إليها 24 ساعة في اليوم و7 أيام في الأسبوع.[1054]

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 ("اتفاقية الجريمة السيبرانية").[1055] وفي عام 2001، ناقشت مجموعة الثمانية الأدوات الإجرائية لمكافحة الجريمة السيبرانية في ورشة عمل عُقدت في طوكيو،[1056] ركزت على ما إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات أو ما إذا كان حفظ البيانات يُعد حلاً بديلاً.[1057]

وفي عام 2004، أصدر وزراء العدل والداخلية في مجموعة الثمانية بياناً تناولوا فيه ضرورة إنشاء قدرات عالمية في مجال مكافحة الاستخدامات الإجرامية للإنترنت[1058] وأحاطت مجموعة الثمانية، مرة أخرى، علماً بالاتفاقية.[1059]

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.[1060] وفي أعقاب اجتماع وزراء العدل والداخلية في مجموعة الثمانية، عُقدت في موسكو قمة مجموعة الثمانية حيث كانت قضية الإرهاب السيبراني[1061] محل نقاش.[1062]

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.[1063] ولم يُشر هذا الاتفاق إلى أفعال محددة ينبغي أن تجرمها الدول.

وفي اجتماع وزراء العدل والداخلية المنعقد في عام 2009 في روما، إيطاليا، نُوقشت عدة قضايا متعلقة بالجريمة السيبرانية. وجاء في البيان الختامي أنه، من وجهة نظر مجموعة الثمانية، ينبغي حجب المواقع الإباحية التي يُستغل فيها الأطفال، بالاستناد إلى قوائم سوداء تحدثها وتنشرها منظمات دولية.[1064] وفيما يخص الجريمة السيبرانية بوجه عام، سلط البيان الختامي الضوء على وجود تهديد متنام وأشار إلى أن التعاون الأوثق بين موردي الخدمات والجهات المعنية بإنفاذ القانون أمر ضروري وأنه لا بد من تعزيز أشكال التعاون القائمة، مثل جهات الاتصال التابعة لمجموعة الثمانية والمعنية بجرائم التقنيات العالية والتي تعمل يومياً على مدار الساعة.[1065]

وفي قمة مجموعة الثمانية المنعقدة في ماسكوكا، كندا، لم تناقَش الجريمة السيبرانية إلا بشكل مختصر. ويشير إعلان ماسكوكا فقط إلى أنه في سياق الأنشطة الإرهابية، تشعر مجموعة الثمانية بالقلق إزاء التهديد المتنامي الذي تشكله الجريمة السيبرانية وسوف تكثف أعمالها من أجل إضعاف الشبكات الإرهابية والإجرامية.[1066]

وقد نوقش موضوعا الجريمة السيبرانية والأمن السيبراني في المنتدى الإلكتروني لمجموعة الثمانية، الذي ناقشت خلاله الوفود مواضيع متصلة بالإنترنت مع قادة الأعمال التجارية،[1067] وكذلك في قمة مجموعة الثمانية في دوفيل، فرنسا. لكن على الرغم

من الاهتمام الكبير الذي حظي به موضوع الجريمة السيبرانية، لم يتضمن البيان الختامي للقمة أي توصيات محددة، خلافاً للسنوات السابقة. واتفقت مجموعة الثمانية فقط على مبادئ عامة مثل أهمية الأمن والحماية من الجريمة، بما يعزز من وجود إنترنت قوية ومزدهرة.[1068]

2.1.5 الأمم المتحدة ومكتب الأمم المتحدة المعني بالمخدرات والجريمة[1069]

اعتمدت الأمم المتحدة عدة نُهُج مهمة لكي تتصدى لتحدي الجريمة السيبرانية. وفي حين حصرت المنظمة استجابتها في البداية في مبادئ توجيهية عامة، فقد عالجت في الآونة الأخيرة التحديات والاستجابة القانونية المتعلقة بهذا الأمر معالجة مكثفة على نحو أكبر.

اتفاقية الأمم المتحدة لحقوق الطفل

تتضمن اتفاقية الأمم المتحدة لحقوق الطفل، التي اعتُمدت في عام 1989،[1070] عدة أدوات ترمي إلى حماية الأطفال. ولا تعرِّف هذه الاتفاقية استغلال الأطفال في المواد الإباحية، كما أنها لا تتضمن أحكاماً تنسق تجريم نشر المواد الإباحية التي يُستغل فيها الأطفال على الخط. بيد أن المادة 34 تدعو الدول الأعضاء إلى منع استغلال الأطفال في العروض الإباحية.

قرار الجمعية العامة للأمم المتحدة 121/45

بعد المؤتمر الثامن للأمم المتحدة المعني بمنع الجريمة ومعاملة المجرمين (الذي عُقد في هافانا بكوبا في الفترة من 27 أغسطس إلى 7 سبتمبر 1990)، اعتمدت الجمعية العامة للأمم المتحدة قراراً يتناول التشريعات المتعلقة بالجرائم الحاسوبية.[1071] وفي عام 1994 نشرت الأمم المتحدة، بناءً على قرار الجمعية العامة 45/121 (1990)، دليلاً بشأن منع ومكافحة الجريمة المتعلقة بالحاسوب.[1072]

البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية

لا يعالج البروتوكول الاختياري مسألة استغلال الأطفال في المواد الإباحية بصفة عامة فحسب، بل إنه يشير بعبارة صريحة إلى دور الإنترنت في نشر هذه المواد.[1073] ويعرَّف استغلال الأطفال في المواد الإباحية بأنه أي تمثيل لطفل، بأي وسيلة كانت، يشارك مشاركة حقيقية أو بالمحاكاة في أنشطة جنسية صريحة أو أي تمثيل للأعضاء الجنسية للطفل لأغراض جنسية بالأساس.[1074] وتلزم المادة 3 الأطراف بتجريم بعض السلوك – بما في ذلك الأفعال المتصلة باستغلال الأطفال في المواد الإباحية.

> **المادة 3**
>
> *1 تكفل كل دولة طرف أن تغطي، كحد أدنى، الأفعال والأنشطة التالية تغطية كاملة بموجب قانونها الجنائي أو قانون العقوبات فيها سواء أكانت هذه الجرائم ترتكب محلياً أم دولياً أو كانت ترتكب على أساس فردي أو منظم:*
>
> *[...]*
>
> *ج) إنتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالطفل على النحو المعرَّف في المادة 2.*
>
> *[...]*

مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين

خلال مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، الذي عُقد في فيينا في عام 2000، دار النقاش حول أثر الجرائم المتصلة بالإنترنت في ورشة عمل خاصة.[1075] وركز النقاش بالأخص على فئات الجريمة والتحرّي عنها عبر الحدود، وكذلك على الاستجابة القانونية لهذه الظاهرة.[1076] وتتضمن استنتاجات ورشة العمل عناصر أساسية من النقاش الذي

لا يزال جارياً، وهي: أن التجريم ضروري، وأنه لا بد أن تشمل التشريعات موادَّ إجرائية، وأن التعاون الدولي أساسي، وأنه ينبغي تعزيز الشراكة بين القطاعين العام والخاص.[1077] وإلى جانب هذا، سُلِّط الضوء على أهمية بناء القدرات – وهو موضوع جرى تناوله من جديد في السنوات التالية.[1078] ودعا إعلان فيينا لجنة منع الجريمة والعدالة الجنائية إلى الاضطلاع بالعمل في هذا الشأن:

> *18 تقرر وضع توصيات بسياسات ذات توجه عملي بشأن منع ومكافحة الجرائم المتعلقة بالحواسيب، وندعو لجنة منع الجريمة والعدالة الجنائية إلى الاضطلاع بالعمل في هذا الشأن، آخذة في الاعتبار الأعمال الجارية في منتديات أخرى. ونعلن التزامنا أيضاً بالعمل على تعزيز قدرتنا على منع الجرائم المرتبطة بالتكنولوجيا الراقية والحواسيب والتحري عن تلك الجرائم وملاحقتها قضائياً.*

قرار الجمعية العامة للأمم المتحدة 55/63

في العام نفسه، اعتمدت الجمعية العامة قراراً بشأن إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية يعرض عدداً من أوجه التماثل مع خطة العمل المؤلفة من عشر نقاط التي اعتمدتها مجموعة الثمانية في عام 1997.[1079] 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؛*
>
> *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 يمكّنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية؛*

ويدعو القرار 55/63 الدول إلى اتخاذ التدابير اللازمة لمكافحة الجريمة السيبرانية على الصعيدين الإقليمي والدولي. ويشمل ذلك سَنّ تشريعات محلية للقضاء على أي ملاذات آمنة لإساءة استعمال التكنولوجيا لأغراض إجرامية، وتحسين قدرات الجهات المعنية بإنفاذ القانون من أجل التعاون عبر الحدود في مجال التحقيق والملاحقة القضائية بشأن القضايا الدولية المتعلقة بإساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وتحسين تبادل المعلومات، وتعزيز أمن البيانات والأنظمة الحاسوبية، وتدريب الموظفين المكلفين بإنفاذ القانون على التعامل بشكل خاص مع التحديات المرتبطة بالجريمة السيبرانية، وإنشاء أنظمة للمساعدة المتبادلة، وزيادة الوعي العام بالتهديد الذي تشكله الجريمة السيبرانية.

قرار الجمعية العامة للأمم المتحدة 56/121

في عام 2002، اعتمدت الجمعية العامة قراراً آخر بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.[1080] ويشير القرار إلى النُّهُج 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 تقرّر إرجاء النظر في هذا الموضوع ريثما تنجَز الأعمال المتوخاة في خطة عمل لجنة منع الجريمة والعدالة الجنائية بشأن مكافحة الجريمة المتصلة بالتكنولوجيات الرفيعة والتطبيقات الحاسوبية.

ويؤكد القرار 56/121 على ضرورة التعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية. ويسلط الضوء على الدور الذي يمكن أن تضطلع به الأمم المتحدة وغيرها من المنظمات الدولية والإقليمية. كما يدعو القرار الدول إلى مراعاة التوجيهات المقدمة من لجنة منع الجريمة والعدالة الجنائية عند سن التشريعات الوطنية.

قرارا الجمعية العامة للأمم المتحدة 57/239 و58/199

يشكل القراران 57/239 و58/199 القرارين الرئيسيين للجمعية العامة للأمم المتحدة اللذين يعالجان موضوع الجريمة السيبرانية. ودون الدخول في التفاصيل ذات الصلة بالجريمة السيبرانية، يذكِّر القراران المذكوران بالقرارين 55/06 و56/121. والقراران معاً يشددان أيضاً على ضرورة التعاون الدولي في مكافحة الجريمة السيبرانية من خلال إقرارهما بأن الثغرات الموجودة في نفاذ الدول إلى تكنولوجيا المعلومات واستخدامها لها يمكن أن تضعِف فعالية التعاون الدولي في مجال مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.[1081]

مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية

نُوقشت الجريمة السيبرانية خلال مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية ("مؤتمر الأمم المتحدة المتعلق بالجريمة") في بانكوك، تايلاند، في عام 2005. وتناولت ورقة المعلومات الأساسية[1082] وورش العمل[1083] معاً العديد من التحديات المرتبطة بالاستخدام الناشئ للأنظمة الحاسوبية في ارتكاب الجرائم، وبالبُعد العابر للحدود الوطنية وبهذا النوع من الجرائم. وفي إطار الاجتماعات التحضيرية التي عُقدت قبل المؤتمر، دعت بعض البلدان الأعضاء مثل مصر إلى وضع اتفاقية جديدة للأمم المتحدة بشأن مكافحة الجريمة السيبرانية، ودعا الاجتماع التحضيري الإقليمي لغرب آسيا إلى التفاوض بشأن هذه الاتفاقية.[1084] وقد أُدرجت إمكانية التفاوض بشأن اتفاقية كهذه في دليل المناقشة الخاص بمؤتمر الأمم المتحدة الحادي عشر المتعلق بالجريمة.[1085] لكن الدول الأعضاء لم تستطع في ذلك الوقت أن تقرر الشروع في تنسيق التشريعات. وبالتالي، فإن إعلان بانكوك يحيل إلى النهج القائمة، دون ذكر صك معين.

16 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.

قرار الجمعية العامة للأمم المتحدة 60/177

وبعد مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، الذي عُقد في بانكوك بتايلاند في عام 2005، اعتُمد إعلان يسلط الضوء على ضرورة التنسيق التواؤم لدى مكافحة الجريمة السيبرانية.[1086] ويتطرق، من بين ما يتطرق إليه، إلى 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، صاحَبتهما 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. ونسلّم 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.

وقد أيد قرار الجمعية العامة للأمم المتحدة 60/177 إعلان بانكوك لعام 2005، الذي يشجع جهود المجتمع الدولي الرامية إلى تعزيز واستكمال التعاون القائم لمنع الجرائم المتصلة بالحاسوب، داعياً إلى مواصلة بحث إمكانية تقديم المساعدة إلى الدول الأعضاء في مجال التصدي للجرائم المتصلة بالحاسوب تحت رعاية الأمم المتحدة، وبشراكة مع منظمات أخرى ذات مجال تركيز مشابه.

مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية

لقد نُوقش موضوع الجريمة السيبرانية أيضاً في مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية الذي عُقد في البرازيل في عام 2010.[1087] وخلال الاجتماعات التحضيرية الإقليمية الأربعة للمؤتمر، لأمريكا اللاتينية ومنطقة الكاريبي،[1088] ومنطقة غرب آسيا،[1089] ومنطقة آسيا والمحيط الهادئ،[1090] وإفريقيا،[1091] دعت البلدان إلى وضع اتفاقية دولية بشأن الجريمة السيبرانية. وصدرت دعوات مماثلة في الأوساط الأكاديمية.[1092]

وفي المؤتمر نفسه، اتخذت الدول الأعضاء خطوة مهمة من أجل إشراك الأمم المتحدة بنشاط أكبر في النقاش المتعلق بمسألة الجريمة الحاسوبية والجريمة السيبرانية. ولعل مناقشة الوفود للموضوع على مدى يومين وتنظيم أحداث جانبية إضافية يؤكدان أهمية الموضوع، الذي نُوقش بكثافة أكبر مقارنة بالمؤتمرات السابقة بشأن الجريمة.[1093] وركزت المداولات على موضوعين أساسيين هما: كيف يمكن تحقيق تنسيق المعايير القانونية، وكيف يمكن للبلدان النامية أن تحصل على الدعم في مكافحة الجريمة السيبرانية؟ والموضوع الأول يتعلق بأن تضع الأمم المتحدة معايير قانونية شاملة وأن تقترح أن تطبق الدول الأعضاء اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. وعند التحضير لمؤتمر الأمم المتحدة المتعلق بالجريمة، أعرب مجلس أوروبا عن بواعث قلق بشأن النهج المتّبع من جانب الأمم المتحدة،[1094] ودعا إلى دعم اتفاقيته المتعلقة بالجريمة السيبرانية. وبعد نقاش مكثف، نوقش خلاله بالأخص المدى المحدود لاتفاقية الجريمة السيبرانية، قررت الدول الأعضاء ألاّ تقترح التصديق على هذه الاتفاقية بل أن تعزز دور الأمم المتحدة في مجالين مهمين، يتجليان في إعلان سلفادور:

41 نوصي بأن يقوم مكتب الأمم المتحدة المعني بالمخدرات والجريمة، عند الطلب، وبالتعاون مع الدول الأعضاء والمنظمات الدولية المعنية والقطاع الخاص، بتقديم المساعدة التقنية إلى الدول وتوفير التدريب لها من أجل تحسين التشريعات الوطنية وبناء قدرات السلطات الوطنية، من أجل التصدي للجريمة الإلكترونية، بما في ذلك منع هذه الجريمة بكل أشكالها والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها، وتحسين أمن الشبكات الحاسوبية.

42 ندعو لجنة منع الجريمة والعدالة الجنائية إلى النظر في دعوة فريق خبراء حكومي دولي مفتوح باب العضوية إلى الانعقاد من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لتلك الجريمة، بما يشمل تبادل المعلومات عن التشريعات الوطنية وأفضل الممارسات والمساعدة التقنية والتعاون الدولي، بغية دراسة الخيارات المتعلقة بتعزيز التدابير القانونية أو التدابير الأخرى القائمة على الصعيدين الوطني والدولي للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن.

وأوصت الدول الأعضاء بالتالي بأن يضطلع مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) بدور قوي في العمل على بناء القدرات العالمية حسب الطلب. بالنظر إلى خبرة هذا المكتب في مجال بناء القدرات المتصلة بالتشريعات الجنائية وأنه، خلافاً لمجلس أوروبا، يتوفر له شبكة عالمية من المكاتب الإقليمية، من المرجح أن تضطلع الأمم المتحدة عن طريقه بدور أكثر أهمية في هذا المجال مستقبلاً.

وتؤكد التوصية الثانية أنه في وقت انعقاد مؤتمر الأمم المتحدة المتعلق بالجريمة لم يتسنَّ للدول الأعضاء أن تقرر ما إذا كانت ستضع نصاً قانونياً أم لا. ويعكس ذلك النقاش المثير للجدل الذي دار أثناء المؤتمر، حيث أعربت خلاله البلدان الأوروبية التي صدّقت بالفعل على اتفاقية الجريمة السيبرانية بالأخص عن دعمها لهذا الصك في حين دعا عدد من البلدان النامية إلى وضع اتفاقية للأمم المتحدة. بيد أن ردّ فعل الدول الأعضاء اختلف عما كان في المؤتمر الحادي عشر للجريمة، حيث أشارت فيه إلى صكوك قائمة. ولم تُشِر هذه المرة إلى صكوك قائمة بل إنها، والأهم من ذلك، لم تقرر التوصية باعتماد اتفاقية الجريمة السيبرانية كمعيار عالمي، بل أوصت الدول الأعضاء بدعوة لجنة منع الجريمة والعدالة الجنائية إلى إجراء دراسة شاملة، ينبغي أن تشمل، من بين ما تشمل، بحث الخيارات المتعلقة بتعزيز التدابير القانونية أو التدابير الأخرى القائمة على الصعيدين الوطني والدولي للتصدي للجريمة السيبرانية واقتراح تدابير جديدة في هذا الشأن.

قرار الجمعية العامة للأمم المتحدة 64/211

في مارس 2010، أصدرت الجمعية العامة للأمم المتحدة قراراً جديداً[1095] كجزء من مبادرة "إرساء ثقافة عالمية للأمن السيبراني". ويحيل القرار 64/211 إلى قرارين مهمين بشأن الجريمة السيبرانية[1096] وأيضاً إلى قرارين رئيسيين بشأن الأمن السيبراني.[1097] وتدعو أداة التقييم الذاتي الطوعي للجهود الوطنية الرامية إلى حماية البُنى التحتية الحرجة للمعلومات، المقدمة كمرفق للقرار، البلدان إلى استعراض وتحديث الهيئات القانونية (بما فيها تلك المتصلة بالجرائم السيبرانية والخصوصية وحماية البيانات والقانون التجاري والتوقيعات الرقمية والتجفير) التي قد تكون قد تجاوزها الزمن أو فات أوانها بسبب سرعة الأخذ بالجديد من تكنولوجيات المعلومات والاتصالات والاعتماد عليها. كما يدعو القرار الدول إلى الاستعانة بالاتفاقيات والترتيبات والسوابق الإقليمية والدولية في عمليات الاستعراض هذه.

13 استعرِض النصوص القانونية المرجعية (بما في ذلك النصوص المرجعية التي لها علاقة بجرائم الفضاء الإلكتروني والسرية وحماية البيانات والقانون التجاري والتوقيعات الرقمية والتشفير) واستكمِل ما قد يكون متقادماً منها أو فات أوانه بسبب سرعة الأخذ بالجديد من تكنولوجيات المعلومات والاتصالات والاعتماد عليها، واستَعِن بالاتفاقيات والترتيبات والسوابق الإقليمية والدولية في عمليات الاستعراض هذه. وتحقق مما إذا كان بلدك قد وضع التشريعات الضرورية للتحقيق في جرائم الفضاء الإلكتروني ومحاكمة مرتكبيها، مع ملاحظة الأطر القائمة، مثل قراري الجمعية العامة 55/63 و56/121 بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، والمبادرات الإقليمية، بما في ذلك اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الإلكتروني.

14 حدِّد الوضع الحالي للسلطات والإجراءات الوطنية المعنية بجرائم الفضاء الإلكتروني، بما في ذلك السلطات القانونية والوحدات الوطنية المعنية بجرائم الفضاء الإلكتروني، ومستوى فهم المدعين العامين والقضاة والمشرعين للقضايا المتعلقة بجرائم الفضاء الإلكتروني.

15 قيِّم مدى كفاية القوانين والنصوص القانونية المرجعية القائمة للتصدي للتحديات المتعلقة بجرائم الفضاء الإلكتروني حالياً ومستقبلاً وبالفضاء الإلكتروني بصفة أعم.

16 تحرَّ مدى المشاركة الوطنية في الجهود الدولية الرامية إلى مكافحة جرائم الفضاء الإلكتروني، من قبيل شبكة نقاط الاتصال المعنية بجرائم الفضاء الإلكتروني العاملة على مدار الساعة.

17 حدِّد متطلبات وكالات إنفاذ القوانين الوطنية من أجل التعاون مع الجهات النظيرة الدولية للتحقيق في جرائم الفضاء الإلكتروني العابرة للحدود الوطنية في الحالات التي تكون فيها الهياكل الأساسية واقعة في أراضي بلدك أو التي يكون فيها الجناة مقيمين في تلك الأراضي، في حين يقيم الضحايا في أماكن أخرى.

وإن ارتباط أربعة مواضيع من بين 18 موضوعاً تتضمنها أداة التقييم الذاتي، بالجريمة السيبرانية يؤكد أهمية قدرة الجهات المعنية بإنفاذ القانون على مكافحة الجريمة السيبرانية بشكل فعال حفاظاً على الأمن السيبراني.

الدراسة العالمية بشأن الجريمة السيبرانية

بعد مناقشات مكثفة[1098] حول موضوعات ومنهجية[1099] دراسة شاملة لمكتب الأمم المتحدة المعني بالمخدرات والجريمة فيما يتعلق بالجريمة السيبرانية، تلقت الدول الأعضاء في الأمم المتحدة استبياناً في أوائل عام 2012. وفي الوقت ذاته تم إنشاء بوابة إلكترونية على الخط.[1100] ويحتوي الاستبيان المعقد على أسئلة شتى تتناول مختلف مجالات التشريع بشأن الجريمة السيبرانية، مثل التعاريف والتجريم والصكوك الإجرائية. وقد طُلب من الدول الأعضاء توفير معلومات عن حالة تشريعاتها فضلاً عن تنفيذ مختلف المعايير الإقليمية (مثل اتفاقية الجرائم السيبرانية). وفي عام 2013 قدمت هذه النتائج[1101] إلى لجنة منع الجريمة والعدالة الجنائية.[1102]

وفي عام 2013، نشر المكتب المعني بالمخدرات والجريمة النتائج الأولى للدراسة.[1103] وهذه الدراسة هي الأكثر تعقيداً حتى الآن وهي تحتوي على نتائج من 69 دولة عضواً ردت عليها.[1104] وبالإضافة إلى الردود من الدول الأعضاء، تشمل الدراسة نتائج استعراض 500 وثيقة ومعلومات متاحة للجمهور تقدمت بها أكثر من 40 شركة و16 مؤسسة أكاديمية. وتبرز الدراسة أن مدى شمول صكوك المواءمة الإقليمية – مثل اتفاقية مجلس أوروبا بشأن الجرائم السيبرانية – محدود. وبالإضافة إلى ذلك تظهر الدراسة أن صكوكاً إقليمية أخرى لا تقل أهمية.[1105] واجتمع فريق الخبراء العامل في فبراير 2013 ورفع المسألة إلى لجنة منع الجريمة والعدالة الجنائية.[1106]

وفي أبريل 2013، ناقشت لجنة منع الجريمة والعدالة الجنائية لأول مرة نتائج الدراسة.[1107] ويناقش القرار 22/7 العمل المنجز دون الخوض في التفاصيل.[1108] وبدلاً من ذلك تدعو اللجنة الدول الأعضاء إلى استعراض النتائج، وتطلب من فريق الخبراء مواصلة العمل وتطلب إلى الأمانة ترجمة الدراسة إلى جميع لغات الأمم المتحدة. وخلال الاجتماع الثالث والعشرين تناول عدد من المشاركين موضوع الجريمة السيبرانية.[1109] وعلى الرغم من النداءات المختلفة التي تدعو إلى المواءمة على الصعيد العالمي، لم تتخذ اللجنة قراراً في هذا الصدد. وبدلاً من ذلك فهي تركز بشكل أكبر على بناء القدرات بالتشديد على برنامج بناء القدرات العالمي الذي يديره المكتب المعني بالمخدرات والجريمة.[1110]

فريق الخبراء الحكوميين

في عام 2013، تقدم فريق خبراء حكوميين ضم خبراء من بلدان أوروبية، وهي إستونيا وفرنسا وألمانيا والمملكة المتحدة، تقريراً عن "التنمية في مجال المعلومات والاتصالات في سياق الأمن الدولي".[1111] وكان موضوع الأمن السيبراني/أمن المعلومات محور اهتمام الفريق العامل. وبالإضافة إلى ذلك – وعلى الرغم من مناقشة المعايير – ركز الفريق العامل على جانب واحد معين من جوانب الأمن السيبراني: ألا وهو تدخل الدولة.[1112]

فريق الخبراء الحكومي الدولي المعني بالجريمة السيبرانية

طبقاً لقرار الدول الأعضاء بدعوة مكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى إنشاء فريق عمل حكومي دولي، عقد هذا الفريق اجتماعه الأول في فيينا في يناير 2011.[1113] ويضم فريق الخبراء ممثلين عن الدول الأعضاء والمنظمات الحكومية الدولية والمنظمات الدولية والوكالات المتخصصة والقطاع الخاص والأوساط الأكاديمية. وناقش أعضاء فريق الخبراء خلال هذا

الاجتماع مشروع بنية دراسة شاملة لتحليل موضوع الجريمة السيبرانية، وسُبل التصدي لها.[1114] وفيما يخص المعالجة القانونية، أكد عدد من الأعضاء فائدة الصكوك القانونية الدولية القائمة، بما فيها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (UNTOC) واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، وأن من المحبّذ إعداد صك قانوني عالمي لمعالجة مشكلة الجريمة السيبرانية بالتحديد. واتُفق على أن يُتخذ القرار بشأن ما إذا كان ينبغي وضع صك عالمي أم لا بعد إجراء الدراسة.

قرارات ونشاطات أخرى

بالإضافة إلى ذلك، يتناول عدد من مقررات منظومة الأمم المتحدة وقراراتها وتوصياتها قضايا تتعلق بالجريمة السيبرانية. ومن أهمها ما يلي: اعتمد مكتب الأمم المتحدة للمخدرات والجريمة (UNODC) ولجنة منع الجريمة والعدالة الجنائية[1115] قراراً بشأن المنع الفعال للجريمة واستجابات العدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال.[1116] وفي عام 2004، اعتمد المجلس الاقتصادي والاجتماعي للأمم المتحدة[1117] 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.[1118] وأُنشئ فريق عمل في عام 2005.[1119] كما شُكّل فريق أساسي من الخبراء معني بالجرائم ذات الصلة بالهوية لكي يُجري دراسة شاملة بشأن الموضوع. وفي عام 2007، اعتمد المجلس قراراً بشأن التعاون الدولي على منع جرائم الاحتيال الاقتصادي والجرائم ذات الصلة بالهوية والتحري عنها وملاحقة مرتكبيها قضائياً ومعاقبتهم.[1120] ولا يتناول أي من القرارين صراحة التحديات المتعلقة بجرائم الإنترنت[1121] ولكنهما ينطبقان على هذه الجرائم أيضاً. وبالاستناد إلى القرار 2004/26[1122] والقرار 2007/20[1123] للمجلس الاقتصادي والاجتماعي، شكّل مكتب الأمم المتحدة المعني بالمخدرات والجريمة في عام 2007 فريقاً أساسياً من الخبراء لتبادل الآراء بشأن المسار الأفضل للعمل.[1124] وأجرى الفريق الأساسي العديد من الدراسات التي شملت جوانب الجرائم المتصلة بالإنترنت.[1125] وفي عام 2004، اعتمد المجلس الاقتصادي والاجتماعي قراراً بشأن بيع المخدرات المشروعة عن طريق الإنترنت، تناول صراحة ظاهرة تتعلق بجريمة حاسوبية.[1126]

مذكرة التفاهم بين مكتب الأمم المتحدة المعني بالمخدرات والجريمة والاتحاد الدولي للاتصالات

في عام 2011، وقّع مكتب الأمم المتحدة المعني بالمخدرات والجريمة والاتحاد الدولي للاتصالات (ITU) على مذكرة تفاهم بشأن الجريمة السيبرانية.[1127] وتغطي هذه المذكرة التعاون (لا سيما فيما يخص بناء القدرات والمساعدة التقنية لصالح البلدان النامية) والتدريب وورش العمل المشتركة. وفيما يخص أنشطة بناء القدرات، يمكن للمنظمتين الرجوع إلى شبكة واسعة من المكاتب الميدانية في جميع القارات. وفضلاً عن ذلك، اتفقت المنظمتان على نشر المعلومات والمعارف وتحليل البيانات على نحو مشترك.

3.1.5 الاتحاد الدولي للاتصالات[1128]

يؤدي الاتحاد الدولي للاتصالات (ITU)، بوصفه وكالة متخصصة داخل منظومة الأمم المتحدة، دوراً ريادياً في تقييس الاتصالات وتنميتها وكذلك فيما يخص قضايا الأمن السيبراني.

القمة العالمية لمجتمع المعلومات

واضطلع الاتحاد الدولي للاتصالات، من بين أنشطته الأخرى، بدور الوكالة الرائدة للقمة العالمية لمجتمع المعلوما (WSIS) التي عُقدت 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*.

وتسلّط خطة عمل جنيف الضوء على أهمية التدابير الرامية إلى مكافحة الجريمة السيبرانية:[1129]

جيم 5. 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 عُولجت قضية الجريمة السيبرانية في المرحلة الثانية من القمة العالمية لمجتمع المعلومات التي عُقدت في تونس في عام 2005. ويُسلط برنامج عمل تونس لمجتمع المعلومات[1130] الضوء على ضرورة التعاون الدولي في مكافحة الجريمة السيبرانية ويشير إلى النُّهج التشريعية الراهنة مثل قرارات 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 الأُطر 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.

البرنامج العالمي للأمن السيبراني

وكان من نتائج القمة العالمية لمجتمع المعلومات، أن اختير الاتحاد الدولي للاتصالات الميسِّر الوحيد لخط العمل جيم5 المكرَّس لبناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.[1131] وفي اجتماع التيسير الثاني لخط العمل جيم5 للقمة العالمية لمجتمع المعلومات، الذي عُقد في عام 2007، سلّط الأمين العام للاتحاد الدولي للاتصالات الضوء على أهمية التعاون الدولي في مكافحة الجريمة السيبرانية وأعلن استهلال *البرنامج العالمي للأمن السيبراني*[1132] ويتوخى البرنامج العالمي للأمن السيبراني سبعة أهداف رئيسية،[1133] ويستند إلى خمس ركائز استراتيجية،[1134] بما في ذلك وضع استراتيجيات وإعداد تشريعات نموذجية بشأن الجريمة السيبرانية. وهذه الأهداف السبعة هي:

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.

ومن أجل تحليل ووضع تدابير واستراتيجيات بشأن الأهداف السبعة للبرنامج العالمي للأمن السيبراني، شكّل الأمين العام للاتحاد الدولي للاتصالات فريق خبراء رفيع المستوى (HLEG) يضم ممثلين عن الدول الأعضاء والصناعة والمجتمع العلمي.[1135] وفي عام 2008، استكمل فريق الخبراء المفاوضات ونشر "التقرير الاستراتيجي العالمي".[1136] والتدابير الأكثر ملاءمة للجريمة السيبرانية هي التدابير القانونية التي يتضمنها الفصل 1. ويقدم هذا الفصل، إلى جانب لمحة عامة عن النُّهج الإقليمية والدولية المختلفة لمكافحة الجريمة السيبرانية،[1137] فكرة عامة عن أحكام القوانين الجنائية،[1138] والصكوك الإجرائية،[1139] واللوائح التي تحدد مسؤولية موردي خدمة الإنترنت،[1140] والضمانات التي تحمي الحقوق الأساسية لمستعملي الإنترنت.[1141]

بناء القدرات

في إطار البرنامج العالمي للأمن السيبراني التابع للاتحاد الدولي للاتصالات، يعمل قطاع تنمية الاتصالات من أجل مساعدة البلدان على تنفيذ أنشطة متسقة بشأن الأمن السيبراني على المستويات الوطنية والإقليمية والدولية. وقد جاء تأكيد لولاية الاتحاد في مجال بناء القدرات في القرار 130 (المراجَع في غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين. وبناء على هذا القرار، يضطلع الاتحاد بولاية مساعدة الدول الأعضاء، لا سيما البلدان النامية، في إعداد تدابير قانونية مناسبة وعملية فيما يخص الحماية من التهديدات السيبرانية.

وتشمل هذه الولاية أنشطة بناء القدرات في مجال وضع استراتيجيات وتشريعات هياكل للإنفاذ وهياكل تنظيمية على الصعيد الوطني (مثل الرصد والإنذار والتصدي للحوادث)، من بين مجالات أخرى. ونظم الاتحاد عدة مؤتمرات إقليمية تناولت بالتحديد، من بين المواضيع التي تناولتها، موضوع الجريمة السيبرانية.[1142] واستحدث قطاع تنمية الاتصالات، مع شركاء من القطاعين العام والخاص، أدوات الأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات (CIIP) لمساعدة الدول الأعضاء على إذكاء الوعي على المستوى الوطني، وإجراء تقييمات ذاتية للأمن السيبراني الوطني، ومراجعة التشريعات وتطوير قدرات

الرصد والإنذار والتصدي للحوادث. وتشمل هذه الأدوات دليل فهم الجرائم السيبرانية، وأداة الاتحاد للتقييم الوطني الذاتي للأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات، ومجموعة أدوات الاتحاد للتخفيف من حدة البرمجيات الروبوتية.

القرارات

لقد اعتمد الاتحاد الدولي للاتصالات العديد من القرارات بشأن الأمن السيبراني وذات الصلة بالجريمة السيبرانية، في حين لم يعالج الموضوع على نحو مباشر بأحكام للقانون الجنائي.

- القرار 130 (المراجَع في غوادالاخارا، 2010) لمؤتمر المندوبين المفوضين، بشأن تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.
- القرار 149 (أنطاليا، 2006) لمؤتمر المندوبين المفوضين، بشأن دراسة التعاريف والمصطلحات المتعلقة ببناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.
- القرار 45 (الدوحة، 2006) للمؤتمر العالمي لتنمية الاتصالات (WTDC)، بشأن آليات لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتحامية وتقرير *الاجتماع الخاص بآليات التعاون في مجال الأمن السيبراني ومكافحة الرسائل الاقتحامية* (31 أغسطس– 1 سبتمبر 2006).
- القرار 50 (المراجَع في جوهانسبرغ، 2008) للجمعية العالمية لتقييس الاتصالات (WTSA)، بشأن الأمن السيبراني.
- القرار 52 (المراجَع في جوهانسبرغ، 2008) للجمعية العالمية لتقييس الاتصالات (WTSA)، بشأن مكافحة الرسائل الاقتحامية والتصدي لها.
- القرار 58 (المراجَع في جوهانسبرغ، 2008) للجمعية العالمية لتقييس الاتصالات، بشأن تشجيع إنشاء أفرقة استجابة وطنية في حالات الحوادث المعلوماتية، خاصة للبلدان النامية.

المشاريع التي يشارك في تمويلها الاتحاد الدولي للاتصالات والاتحاد الأوروبي في مجموعة بلدان إفريقيا والكاريبي والمحيط الهادئ

سعياً لدعم وضع السياسات والتشريعات في بلدان المجموعة، قرر الاتحاد الدولي للاتصالات والاتحاد الأوروبي المشاركة في تمويل مشروع[1143] كجزء من برنامج "تكنولوجيا المعلومات والاتصالات" في بلدان المجموعة وصندوق التنمية الأوروبي التاسع. وفيما يتعلق بمختلف التطورات والأولويات السابقة في بلدان إفريقيا والكاريبي والمحيط الهادئ جرى تقسيم المشروع إلى ثلاثة برامج فرعية إقليمية. وتم دعم منطقة إفريقيا جنوب الصحراء ببرنامج "مواءمة سياسات تكنولوجيا المعلومات والاتصالات في إفريقيا جنوب الصحراء" (HIPSSA). وبالنسبة لبلدان منطقة البحر الكاريبي تم تنفيذ مشروع "تعزيز القدرة التنافسية في منطقة البحر الكاريبي من خلال مواءمة السياسات والتشريعات والإجراءات التنظيمية لتكنولوجيا المعلومات والاتصالات" (HIPCAR).[1144] وأخيراً تلقت بلدان المحيط الهادئ الدعم ضمن مشروع "دعم بناء القدرات وسياسات تكنولوجيا المعلومات والاتصالات والأطر التنظيمية والتشريعية في البلدان الجزرية في المحيط الهادئ" (ICB4PAC).

وتألف كل من المشاريع الثلاثة من مرحلتين رئيسيتين. وتم خلال المرحلة الأولى تقييم إقليمي للتشريعات القائمة ومقارنة بأفضل الممارسات الدولية. وبناءً على التقييم والمشاورات المكثفة وضعت سياسات وتشريعات نموذجية. وخلال المرحلة الثانية تلقت البلدان الدعم لوضع السياسات والتشريعات النموذجية على الصعيد الوطني.

مواءمة سياسات تكنولوجيا المعلومات والاتصالات في إفريقيا جنوب الصحراء (HIPSSA)

في وقت يرجع إلى عام 2004، أطلق الاتحاد الدولي للاتصالات والاتحاد الأوروبي مشروعاً إقليمياً رائداً لدعم إنشاء سوق متكاملة لتكنولوجيا المعلومات والاتصالات في غرب إفريقيا (مواءمة سوق تكنولوجيا المعلومات والاتصالات لبلدان الجماعة الاقتصادية لدول غرب إفريقيا (ECOWAS) والاتحاد الاقتصادي والنقدي لغرب إفريقيا (UEMOA)[1145]. وفي عام 2005

اعتمد مبدأ توجيهي لأفضل الممارسات،[1146] ومتابعة لذلك اعتمد وزراء تكنولوجيا المعلومات والاتصالات في بلدان ECOWAS القرارات التنظيمية لمواءمة تكنولوجيا المعلومات والاتصالات في عام 2006[1147] وفي عام 2007 اعتمدت هيئة رؤساء دول وحكومات ECOWAS القرارات كعمل تكميلي.[1148]

وتقرر توسيع المشروع الرائد المذكور أعلاه ليشمل مجموعة بلدان إفريقيا جنوب الصحراء. وقد شمل المشروع 42 من البلدان المستفيدة في إفريقيا جنوب الصحراء.[1149] والهدف من المشروع هو وضع وتعزيز سياسات ومبادئ توجيهية متوائمة لتكنولوجيا المعلومات والاتصالات لإيجاد بيئة سوق مستدامة[1150] وكذلك بناء القدرات البشرية والمؤسسية في مجال تكنولوجيا المعلومات والاتصالات من خلال طائفة من تدابير التدريب والتعليم وتبادل المعارف.

تعزيز القدرة التنافسية في منطقة الكاريبي (HIPCAR)

في عام 2008، أطلق مشروع HIPCAR الذي شمل 15 من بلدان منطقة البحر الكاريبي.[1151] ويهدف المشروع إلى مساعدة بلدان منتدى الكاريبي (CARIFORUM)[1152] على مواءمة سياسات تكنولوجيا المعلومات والاتصالات والأطر القانونية. وحُددت، في إطار الإعداد، تسعة مجالات عمل[1153] وضعت فيها، أثناء المرحلة الأولى من المشروع، نصوص سياسات وتشريعات نموذجية لتسهيل وضع ومواءمة التشريعات في المنطقة. وهذه المجالات هي: المعاملات الإلكترونية (التجارة)، والأدلة الإلكترونية، والخصوصية وحماية البيانات، واعتراض الاتصالات، والجرائم السيبرانية، والنفاذ إلى المعلومات العامة/حرية المعلومات، والنفاذ الشامل، والتوصيل البيني، وأخيراً الترخيص. وفي المرحلة الثانية تلقى عدد من البلدان (من بينها بربادوس وغرينادا وسانت كيتس ونيفيس وسانت لوسيا وترينيداد) الدعم في عملية التنفيذ على الصعيد الوطني.[1154]

بناء القدرات وأطر سياسة تكنولوجيا المعلومات والاتصالات والأطر التنظيمية والتشريعية لدعم البلدان الجزرية في المحيط الهادئ (ICB4PAC)

بناءً على طلب البلدان الجزرية في المحيط الهادئ، قدم المشروع الشقيق (ICB4PAC)[1155] بناء القدرات في مجال سياسات ولوائح تكنولوجيا المعلومات والاتصالات. وركز المشروع على بناء القدرات البشرية والمؤسسية في مجال تكنولوجيا المعلومات والاتصالات من خلال تدابير التدريب والتعليم وتبادل المعارف من أجل 15 بلداً من بلدان المحيط الهادئ.[1156] وشملت مجالات العمل على سبيل المثال الترخيص والترقيم والنفاذ الشامل والتوصيل البيني ونمذجة التكاليف وكذلك الجرائم السيبرانية.

2.5 النُّهُج الإقليمية

بالإضافة إلى المنظمات الدولية التي تضطلع بدور نشط على الصعيد العالمي، فإن عدداً من المنظمات الدولية التي تركز في عملها على مناطق محددة تمضي قُدماً في تنفيذ أنشطة تتناول قضايا متصلة بالجريمة السيبرانية.

1.2.5 مجلس أوروبا[1157]

يضطلع مجلس أوروبا بدور نشط في التصدي لتحديات الجريمة السيبرانية.

الأنشطة حتى عام 1995

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 مُدرجاً على جدول أعمال مجلس أوروبا منذ ذلك الحين.[1158] وفي عام 1985 عيّن مجلس أوروبا لجنة خبراء[1159] لمناقشة الجوانب القانونية للجرائم الحاسوبية.[1160] وفي عام 1989، اعتمدت اللجنة الأوروبية لمشكلات الجرائم "تقرير الخبراء بشأن الجريمة المتعلقة بالحاسوب"،[1161] الذي حلل الأحكام القانونية الجنائية الموضوعية اللازمة لمكافحة الأشكال الجديدة للجرائم السيبرانية، بما فيها الاحتيال والتزييف الحاسوبيين. واعتمدت لجنة الوزراء في عام 1989 توصية[1162] 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 سَن تشريعات جديدة، التقرير الخاص بالجريمة المتعلقة بالحاسوب الذي أعدته اللجنة الأوروبية لمشكلات الجرائم، وبوجه خاص المبادئ التوجيهية المقدمة إلى المشرِّعين 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.*

وفي عام 1995، اعتمدت لجنة الوزراء توصية أخرى تتناول المشكلات الناشئة عن الجرائم الحاسوبية عبر الوطنية.[1163] وتضمنت التوصية تذييلاً يلخص المبادئ التوجيهية لصوغ التشريعات المناسبة.[1164]

اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية والبروتوكول الإضافي الأول

قررت اللجنة الأوروبية لمشكلات الجرائم (CDPC) في عام 1996 أن تنشئ لجنة خبراء لمعالجة الجريمة السيبرانية.[1165] 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.[1166] 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 المتعلقة بالجريمة السيبرانية في الجزء الثاني من جلستها العامة المعقودة في أبريل 2001.[1167] وقُدم مشروع الاتفاقية، الموضوع في صيغته النهائية، إلى اللجنة الأوروبية لمشكلات الجريمة للموافقة عليه، وإلى لجنة الوزراء لاعتماده وفتح باب التوقيع على الاتفاقية.[1168] وفتح باب التوقيع على الاتفاقية المتعلقة بالجريمة السيبرانية في حفل توقيع عُقد في بودابست في 23 نوفمبر 2001، وقع خلاله 30 بلداً على الاتفاقية المتعلقة بالجريمة السيبرانية (من بينها أربعة بلدان غير أعضاء في مجلس أوروبا شاركت في المفاوضات هي كندا والولايات المتحدة واليابان وجنوب إفريقيا). وبحلول يونيو 2014، كانت 47 دولة[1169] قد وقعت على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية وكانت 42 دولة[1170] قد صدّقت عليها[1171] — ومنها أربع دول[1172] لم توقع الاتفاقية من قبل. وفي المجموع دُعيت 12 دولة[1173] إلى الانضمام إلى الاتفاقية المتعلقة بالجريمة السيبرانية، لكنها لم تنضم.[1174] واليوم يُعترف بالاتفاقية المتعلقة بالجريمة السيبرانية بوصفها صكاً إقليمياً هاماً في مكافحة الجريمة السيبرانية وتحظى بدعم منظمات دولية مختلفة.[1175]

بعد الاتفاقية المتعلقة بالجريمة السيبرانية تمّ وضع البروتوكول الإضافي الأول لهذه لاتفاقية.[1176] فخلال المفاوضات حول نص الاتفاقية المتعلقة بالجريمة السيبرانية، تبين أن تجريم العنصرية وتوزيع المواد الحاضة على كراهية الأجانب مسألتان مثيرتان للجدل بوجه خاص.[1177] إذ أعربت بعض البلدان التي يحظى فيها مبدأ حرية التعبير[1178] بحماية قوية عن خشيتها من ألاّ تستطيع التوقيع على الاتفاقية المتعلقة بالجريمة السيبرانية في حالة تضمينها أحكاماً تنتهك حرية التعبير.[1179] وفي مشروع النسخة الرابعة لعام 1998، كانت الاتفاقية لا تزال تتضمن حكماً يلزم الأطراف بتجريم المحتوى غير القانوني الذي "يتعلق بقضايا معينة مثل استغلال الأطفال في المواد الإباحية والكراهية القائمة على العنصرية".[1180] ولتفادي أي حالة تكون فيها البلدان غير قادرة على التوقيع على الاتفاقية لأسباب تتعلق بحرية التعبير، أُزيلت المسألتان المذكورتان من الاتفاقية المتعلقة بالجريمة السيبرانية خلال عملية الصياغة تمّ إدراجهما في بروتوكول منفصل. وبحلول يونيو 2014، كانت 38 دولة[1181] قد وقعت على البروتوكول الإضافي وكانت 20 دولة [1182] قد صدقت عليه.

النقاش حول اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية

ما زالت اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية الصك الذي يحظى بأوسع مدى في الوقت الراهن وبدعم منظمات دولية مختلفة.[1183] لكن النقاش الذي دار خلال المؤتمر الثاني عشر المتعلق بالجريمة أكد أن أثر الاتفاقية بات محدوداً بعد مرور عشر سنوات على فتح باب التوقيع عليها.[1184]

المدى المحدود لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية

حتى يناير 2011، كانت الولايات المتحدة الأمريكية البلد الوحيد غير الأوروبي الذي صدق على الصك. وصحيح أن أثر الاتفاقية لا يمكن أن يُقاس فقط بعدد التوقيعات أو التصديقات، بما أن بلداناً مثل الأرجنتين[1185] وباكستان،[1186] والفلبين،[1187] ومصر،[1188] وبوتسوانا[1189]، ونيجيريا،[1190] استخدمت الاتفاقية كنموذج وصاغت أجزاء من تشريعاتها وفقاً للاتفاقية المتعلقة بالجريمة السيبرانية دون أن تنضم إليها رسمياً. لكن حتى في حالة هذه البلدان، ليس من المعروف على وجه اليقين إلى أي حد استخدمت هذه البلدان الاتفاقية المتعلقة بالجريمة السيبرانية كنموذج. فبعضها استخدم أيضاً نصوصاً قانونية أخرى، مثل توجيه الاتحاد الأوروبي المتعلق بالهجمات على أنظمة المعلومات والقانون النموذجي للكومنولث. ولأن هذه القوانين تبرز عدداً من أوجه التشابه مع الاتفاقية المتعلقة بالجريمة السيبرانية، وكذلك لأن الأحكام لم تُنقل كلمة بكلمة إلا في حالات نادرة جداً، بل كُيِّفت مع احتياجات البلدان، يكاد يكون من المستحيل تحديد ما إذا كان بلد من البلدان استخدم هذه الاتفاقية أو إلى أي مدى استخدمها كمبدأ توجيهي. وعلى الرغم من ذلك، يدعي مجلس أوروبا أن أكثر من 100 بلد إما وقّع على الاتفاقية أو صدق عليها أو استخدمها أثناء صياغة التشريعات المحلية.[1191] بيد أن من غير الممكن التحقق من هذا العدد. ولا يكشف الاتحاد الأوروبي عن أسماء البلدان المعنية، ويشير فقط إلى "قائمة داخلية". كما أنه لا يكشف حتى عن العدد الدقيق لهذه البلدان. وحتى إذا تسنى إثبات أن 100 بلد قد استخدم الاتفاقية المتعلقة بالجريمة السيبرانية، فإن هذا لا يعني بالضرورة أن هذه البلدان قد واءمت تشريعاتها مع الاتفاقية. كما أن المعلومات الغامضة التي نشرها مجلس أوروبا تترك بالأحرى السؤال مطروحاً بشأن ما إذا كانت جميع الأحكام المأخوذة من الاتفاقية المتعلقة بالجريمة السيبرانية قد نُفذت أو أن التنفيذ يقتصر على واحد منها.

سرعة عملية التصديق

لم يكن المدى الجغرافي المحدود الأمر الشاغل الوحيد الذي نوقش في مؤتمر الأمم المتحدة الثاني عشر المتعلق بالجريمة. وظلت سرعة التوقيع والتصديق بدون شك مسألة من المسائل الهامة. وبعد تسع سنوات من التوقيع الأولي من جانب 30 دولة في 23 نوفمبر 2001، لم توقّع سوى 17 دولة أخرى على الاتفاقية المتعلقة بالجريمة السيبرانية. وهذه المرة، لم تنضم أي دولة غير عضو في مجلس أوروبا إلى الاتفاقية، على الرغم من دعوة ثمانية بلدان.[1192] وتطور عدد التصديقات على النحو التالي: 2002 (2[1193])، و2003 (2[1194])، و2004 (4[1195])، و2005 (3[1196])، و2006 (7[1197])، و2007 (3[1198])، و2008 (2[1199])، و2009 (3[1200])، و2010 (4[1201])، و2011 (2[1202]) و2012 (6[1203]) و2013 (3[1204]). كما أن عملية التنفيذ بطيئة بقدر بطء عملية التصديق. وفي المتوسط، يستغرق أي بلد بين التوقيع على الاتفاقية والتصديق عليها أكثر من 5 سنوات. والاختلافات بين البلدان كبيرة. ففي حين لم تستغرق ألبانيا إلا أكثر من نصف عام بقليل للتصديق على الاتفاقية، احتاجت ألمانيا إلى 10 سنوات تقريباً من أجل ذلك.

ما من تقييم للتصديق

حتى الآن لم يقيِّم مجلس أوروبا أبداً ما إذا كانت تلك البلدان التي قدمت صك تصديقها على الاتفاقية المتعلقة بالجريمة السيبرانية قد نفّذت الاتفاقية على أرض الواقع وفقاً للشروط المطلوبة. وفي حالة البلدان الأولى بالأخص التي صدقت على الاتفاقية، هناك بواعث قلق كبيرة بشأن تنفيذها الكامل. وحتى في البلدان الكبيرة مثل ألمانيا والولايات المتحدة، من غير المرجح أن تكون الاتفاقية قد نُفّذت تنفيذاً كاملاً. فألمانيا على سبيل المثال، على عكس ما ترمي إليه المادة 2 من الاتفاقية

المتعلقة بالأمن السيبراني، لا تجرم النفاذ غير القانوني إلى الأنظمة الحاسوبية، لكنها تجرم فقط النفاذ غير القانوني إلى البيانات الحاسوبية.[1205] ويبين الموجز القطري لتشريعات الولايات المتحدة المتعلقة بالجريمة السيبرانية والمنشورة على الموقع الشبكي لمجلس أوروبا أن الفصل 1030(أ) (1)-(5) من العنوان 18 من قانون الولايات المتحدة يقابل المادة 2.[1206] لكن على عكس المادة 2 من الاتفاقية المتعلقة بالجريمة السيبرانية، لا تجرّم الفقرة 1030(أ) من العنوان 18 حتى النفاذ إلى نظام حاسوبي. وإلى جانب "النفاذ" إلى نظام حاسوبي، يقتضي هذا الفصل وقوع أفعال أخرى (من قبيل "الحصول" على معلومات).[1207]

نقاش عالمي

أحد جوانب الاتفاقية المتعلقة بالجريمة السيبرانية الذي انتُقد مراراً وتكراراً هو التمثيل غير الكافي للبلدان النامية في عملية الصياغة.[1208] ورغم البُعد العابر للحدود الذي تتسم به الجريمة السيبرانية، يختلف تأثيرها في شتى مناطق العالم. وينطبق هذا بالأخص على البلدان النامية.[1209] ولم يقتصر الأمر خلال التفاوض بشأن الاتفاقية على عدم وجود مشاركة واسعة للبلدان النامية في آسيا و إفريقيا وأمريكا اللاتينية، بل إن الاتفاقية تضع أيضاً شروطاً تقييدية بشأن مشاركة البلدان غير الأعضاء في مجلس أوروبا، على الرغم من أنها صُممت لتكون مفتوحة للبلدان غير الأعضاء. وبناء على المادة 37 من الاتفاقية، يقتضي الانضمام إلى الاتفاقية التشاور مع الدول المتعاقدة في الاتفاقية والحصول على موافقتها بالإجماع. وإلى جانب هذا، فإن المشاركة في المداولات بشأن إمكانية إجراء تعديلات مستقبلية تقتصر على الأطراف في الاتفاقية.[1210] وقد أظهر النقاش الذي دار في إطار التحضير لمؤتمر الأمم المتحدة الثاني عشر المتعلق بالجريمة أن البلدان النامية بالأخص مهتمة بنهج دولي وليس بالانضمام إلى مبادرات إقليمية. وخلال الاجتماعات التحضيرية الإقليمية لمؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، لأمريكا اللاتينية ومنطقة الكاريبي،[1211] ومنطقة غرب آسيا،[1212] ومنطقة آسيا والمحيط الهادئ،[1213] وإفريقيا،[1214] دعت البلدان إلى وضع اتفاقية دولية بشأن الجريمة السيبرانية. وصدرت دعوات مماثلة في الأوساط الأكاديمية.[1215]

عدم التجاوب مع الاتجاهات الجديدة

إن الجريمة السيبرانية مجال يتغير باستمرار.[1216] وفي التسعينات، عندما وُضعت الاتفاقية المتعلقة بالجريمة السيبرانية، لم يكن استخدام الإرهابيين للإنترنت،[1217] وهجمات البرمجيات الروبوتية[1218] والتصيُّد الاحتيالي[1219] أموراً معروفة أو ذات دور مهم بقدر أهمية دورها اليوم،[1220] ولذا لا يمكن معالجتها بحلول معينة. وحتى مجلس أوروبا نفسه أقر بأن الاتفاقية المتعلقة بالجريمة السيبرانية أصبحت قديمة جزئياً. ويمكن توضيح ذلك من خلال مقارنة الأحكام المتصلة باستغلال الأطفال في المواد الإباحية في الاتفاقية المتعلقة بالجريمة السيبرانية لعام 2001 مع المادة 20 (1)(و) من الاتفاقية المتعلقة بحماية الأطفال التي تجرم "الوصول عن علم إلى مواد إباحية يستغل فيها الأطفال، باستخدام تكنولوجيات المعلومات والاتصالات". ولا تجرم الاتفاقية المتعلقة بالجريمة السيبرانية هذا الفعل، على الرغم من أن الإحالة إلى تكنولوجيات المعلومات والاتصالات تؤكد أنه جريمة يمكن وصفها كجريمة سيبرانية. وعلى أساس الدوافع المقدمة في التقرير التوضيحي، قرر واضعو نص الاتفاقية إدراج هذا الحكم لتغطية الحالات التي يشاهد فيها الجناة صوراً للأطفال على الخط من خلال النفاذ إلى مواقع المواد الإباحية التي يُستغل فيها الأطفال، لكن دون تنزيل المواد. ويعني هذا، كنتيجة، أن الاتفاقية المتعلقة بالجريمة السيبرانية لا تشمل هذه الأفعال وبالتالي فإنها لا تستجيب في هذا الصدد حتى للمعايير الحالية الخاصة بمجلس أوروبا.

وينطبق الأمر نفسه على الصكوك الإجرائية. فاعتراض الاتصالات الصوتية القائمة على بروتوكول الإنترنت (VoIP)، ومقبولية الأدلة الرقمية وإجراءات التصدي للاستخدام الناشئ لتكنولوجيا التجفير ووسائل الاتصالات مجهولة الهوية أمور ذات أهمية كبيرة بالنسبة للاتفاقية المتعلقة بالجريمة السيبرانية، لكن الاتفاقية لم تتطرق إليها. وخلال عمر الاتفاقية البالغ عشر سنوات، لم تُدخل عليها أي تعديلات بالمرة، وباستثناء البروتوكول الإضافي المتعلق بالمواد المحرضة على كراهية الأجانب، لم تُضف أي أحكام أو صكوك إضافية إلى الاتفاقية.

ومع التكنولوجيات المتغيرة والسلوك الإجرامي، لا بد من تكييف القانون الجنائي. ومثلما ذُكر سالفاً، فإن الاحتياجات في مجال التشريعات المتعلقة بالجريمة السيبرانية تغيرت في السنوات العشر الأخيرة. ولذا، سيكون من الضروري جداً تحديث الاتفاقية المتعلقة بالجريمة السيبرانية. وقد راجعت منظمات إقليمية أخرى، مثل الاتحاد الأوروبي، للتوّ صكوكها القانونية التي تتصدى للجريمة السيبرانية، والتي وُضعت بعد الاتفاقية المذكورة، منذ حوالي خمس سنوات. ورغم الحاجة الماسة إلى عملية تحديث، فإن من غير المرجح أن تجري هذه العملية. فقد أعلن الاتحاد الأوروبي مؤخراً، وهو مؤيد قوي للاتفاقية المتعلقة بالجريمة السيبرانية، أنه يرى أن "تحديث الاتفاقية [المتعلقة بالجريمة السيبرانية] [...] لا يمكن أن يُعتبر خياراً مجدياً".[1221]

التركيز على انضمام البلدان التي توفر بُنى تحتية بدلاً من البلدان النامية

خلال السنوات العشر الماضية، لم ينجح مجلس أوروبا في الحصول على منضمين جُدد من البلدان الصغيرة والنامية. وأحد أسباب ذلك هو أن التفاوض بشأن الاتفاقية جرى بتمثيل غير كاف للبلدان النامية.[1222] وكانت آسيا و إفريقيا بالأخص ممثلتين تمثيلاً ضعيفاً في حين لم تكن أمريكا اللاتينية ممثلة بالمرة. ورغم أن مجلس أوروبا يدعو ممثلين من البلدان النامية إلى مؤتمره الرئيسي بشأن الجريمة السيبرانية، فإنه لا يسمح لهذه البلدان بالمشاركة في المداولات بشأن أي تعديلات محتملة في المستقبل، حيث إن تلك المداولات تقتصر على البلدان الأطراف في الاتفاقية.[1223]

وعند مقارنة الاتفاقية مع صكوك دولية بالفعل مثل اتفاقيات الأمم المتحدة، يمكن ملاحظة اختلافات أيضاً فيما يتعلق بعملية الانضمام. فخلال عملية الانضمام إلى الاتفاقية – المصممة كاتفاقية مفتوحة للبلدان غير الأعضاء – تطبق شروط تقييدية على هذه البلدان. وخلافاً لأي اتفاقية من اتفاقيات الأمم المتحدة، يقتضي الانضمام إلى الاتفاقية المتعلقة بالجريمة السيبرانية التشاور مع الدول المتعاقدة في الاتفاقية والحصول على موافقتها بالإجماع.[1224] ونتيجة لهذا، بدأت الدول النامية بالأخص تدعو إلى الأخذ بنهج دولي (أكثر) خلال التحضير لمؤتمر الأمم المتحدة الثاني عشر المعني بالجريمة. وفي إطار الاجتماعات التحضيرية الإقليمية للمؤتمر لأمريكا اللاتينية ومنطقة الكاريبي،[1225] ومنطقة غرب آسيا،[1226] ومنطقة آسيا والمحيط الهادئ،[1227] وإفريقيا،[1228] دعت البلدان المشاركة إلى وضع هكذا صك دولي.

ورغم أن استراتيجية مجلس أوروبا التي تركز على البلدان الغربية تبدو منطقية لأن هذه البلدان تضم البُنى التحتية، فإن إشراك البلدان النامية أساسي إذا كان التركيز سيشمل الضحايا المحتملين. ففي عام 2005، تجاوز عدد مستعملي الإنترنت في البلدان النامية العدد المسجل في البلدان الصناعية.[1229] وفي استبعاد البلدان النامية والتركيز في المقابل على البلدان المتقدمة التي تقدم (حالياً) معظم البُنى التحتية والخدمات، إغفال لجانبين مهمين، هما: أهمية حماية (أغلبية) مستعملي خدمات الإنترنت، والتأثير المتنامي بشدة للبلدان الناشئة مثل الهند والصين والبرازيل. وبدون دعم البلدان النامية في سن تشريعات تمكّنها من التحقيق بشأن الحالات التي يتضرر فيها مواطنوها والتعاون أيضاً على الصعيد الدولي مع وحدات إنفاذ القانون الأخرى فيما يتعلق بالكشف عن هوية الجناة، ستزداد صعوبة التحقيقات في الجرائم السيبرانية في الحالات التي تتصل بهذه البلدان. ويُظهر عدم انضمام أي بلد من البلدان النامية إلى الاتفاقية أو عدم تصديقه عليها، خلال السنوات العشر المنصرمة، محدودية نهج إقليمي كهذا. وبالنظر أيضاً إلى أن مجلس أوروبا لم يدع سوى ثمانية بلدان (من بين 146 دولة عضواً في الأمم المتحدة لم توقع على الاتفاقية) إلى الانضمام إلى الاتفاقية خلال العقد الأخير، يتجلى الجهد المحدود المستثمر في هذا الصدد. ويرتبط هذا بدون شك بكون احتياجات البلدان النامية فيما يخص التشريعات وبناء القدرات والمساعدة التقنية بشكل عام تتجاوز آليات الاتفاقية. وحتى اليوم، يركز مجلس أوروبا على مساعدة البلدان في مواءمة تشريعاتها مع الاتفاقية، لكنه لا يقدم أي مساعدة في صياغة التشريعات التي تتجاوز نطاق الاتفاقية (على سبيل المثال، من أجل سد الثغرات المذكورة أعلاه). وإلى جانب هذا، ربما تكون البلدان في حاجة بالفعل إلى المساعدة في صياغة التشريعات الوطنية لأن الأحكام التي تتضمنها الاتفاقية تتطلب إجراء تكييف خلال مرحلة التنفيذ. وعلى سبيل المثال، لا بد للبلدان أن تحدد الجهة المرخص لها بالأمر بإجراء تحقيق معين (القاضي/المدعي العام/مكتب الشرطة) والأسس التي يُستند إليها (أدلة مشفوعة بحلف اليمين/إقرار كتابي مشفوع بيمين/معلومات).

وقد نُوقش هذا الموضوع مناقشة مفصلة خلال مؤتمر الأمم المتحدة الثاني عشر للجريمة، وبناءً على هذه المناقشة قررت الدول الأعضاء في الأمم المتحدة تعزيز ولاية بناء القدرات لمكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) في مجال الجريمة السيبرانية.[1230] وحصلت مؤخراً منظمات أخرى في منظومة الأمم المتحدة مثل الاتحاد الدولي للاتصالات (ITV) على ولايات مماثلة.[1231]

الاتفاقية غير مصمّمة من أجل البلدان الصغيرة والنامية

تواجه البلدان الصغيرة والنامية صعوبات في تنفيذ المعايير التي تتضمنها الاتفاقية. وإن عدم تصديق أصغر الدول الأعضاء في مجلس أوروبا[1232] على الاتفاقية في السنوات العشر الماضية يؤكد بوضوح أن الاتفاقية لا تنطوي على صعوبات فقط بالنسبة للبلدان الصغيرة خارج أوروبا بل أيضاً بالنسبة للبلدان الأوروبية الصغيرة.

وأحد الأحكام الذي يسبب صعوبات في مرحلة التنفيذ في البلدان الصغيرة هو الحكم المتعلق بضرورة إنشاء جهة اتصال تعمل كل أيام الأسبوع على مدار الساعة. ويمكن أن يكون لجهة الاتصال هذه تأثير إيجابي للغاية في سرعة إجراء التحقيقات ولهذا فإن المادة 35 أداة من أهم الأدوات التي تتيحها الاتفاقية.[1233] ومع ذلك، من الجدير الإشارة إلى أن مجلس أوروبا قد نشر مؤخراً دراسة تحلل فعالية التعاون الدولي لمكافحة الجريمة السيبرانية[1234] ودراسة تتناول سير عمل جهات الاتصال التي تعمل على مدار الساعة لمكافحة الجريمة السيبرانية[1235]. وخلاصة هاتين الدراستين هي أن البلدان التي صدقت على الاتفاقية لم تستحدث جميعها جهة الاتصال هذه وحتى البلدان التي أتاحت جهة اتصال من هذا القبيل لم تستخدمها إلا لأغراض محدودة في أغلب الأحيان.

والمشكلة الرئيسية بالنسبة للبلدان النامية هي أن إنشاء جهة الاتصال هذه أمر إلزامي. في حين لا يطرح إنشاء وتسيير جهة اتصال كهذه على الأغلب أي صعوبات بالنسبة للبلدان المتقدمة التي تستخدم قوات شرطة متخصصة في التصدي للجريمة السيبرانية بالمناوبة ليلاً ونهاراً، فإن الأمر يشكل مع ذلك تحدياً بالنسبة للبلدان التي تتألف فيها قوات الشرطة المتخصصة في التصدي للجريمة السيبرانية من رجل شرطة واحد. وفي هذه الحالات سيتطلب هذا الالتزام استثمارات كبيرة. وبالتالي فإن القول بأن الانضمام إلى الاتفاقية وتنفيذها لا يسفران عن تكاليف بالنسبة للبلدان، مثلما صرح بذلك مؤخراً ممثل عن مجلس أوروبا في مؤتمر في منطقة المحيط الهادئ،[1236] هو قول صحيح فقط في حالة استبعاد التكاليف غير المباشرة، مثل تكاليف الإبقاء على جهة اتصال على مدار الساعة أو تكاليف تنفيذ التكنولوجيات الخاصة بتسجيل بيانات الحركة في الوقت الفعلي.

ليس هنالك نهجٌ شامل

كان أحد الأهداف الرئيسية المتوخاة من الاتفاقية هو تقديم نهج قانوني شامل لمعالجة جميع مجالات الجريمة السيبرانية ذات الصلة.[1237] لكن مقارنة الاتفاقية مع نهج أخرى، لا سيما القانون النموذجي لكومنولث الدول المستقلة المتعلق بالحاسوب والجرائم الحاسوبية[1238] وصكوك الاتحاد الأوروبي مثل التوجيه المتعلق بالتجارة الإلكترونية[1239]، تبين أن الاتفاقية تفتقر إلى جوانب مهمة. ومن أمثلة ذلك الأحكام التي تتناول مقبولية الأدلة الإلكترونية[1240] أو مسؤولية موردي خدمات الإنترنت(ISP). وينجم عن الافتقار بوجه خاص إلى حكم ينص على الأقل على إطار تنظيمي أساسي بشأن مقبولية الأدلة الإلكترونية تبعات خطيرة لأن الأدلة الإلكترونية أصبحت توصف على نطاق واسع كفئة جديدة من الأدلة.[1241] وإذا لم يكن لدى أي بلد صكوك أخرى سارية أو لم تكن المحاكم فيه هذه تعتبر هذه الأدلة مقبولة، فقد لا يستطيع هذا البلد الحكم على أي جناة على الرغم من أنه ينفذ الاتفاقية تنفيذاً كاملاً.

اتفاقية حماية الأطفال

استحدث مجلس أوروبا، في إطار نهجه الرامي إلى تحسين حماية القُصَّر من الاستغلال الجنسي، اتفاقية جديدة في عام 2007.[1242] وفي اليوم الأول لفتح باب التوقيع على اتفاقية حماية الأطفال وقعت عليها 23 دولة. وبحلول يونيو 2014، بلغ عدد الدول الموقعة عليها 47 دولة[1243]، وصدّقت 31 من هذه الدول على الاتفاقية[1244]. ويتمثل أحد

الأهداف الرئيسية لاتفاقية حماية الأطفال في تحقيق التوازن بين أحكام القانون الجنائي الرامية إلى حماية الأطفال من الاستغلال الجنسي.[1245] 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 يُستغل فيها الأطفال (المادة 20) وإغواء الأطفال لأغراض جنسية (المادة 23).

المفاوضات المتصلة ببروتوكول إضافي آخر

في عام 2012، اعتمدت لجنة اتفاقية الجرائم السيبرانية[1246] تقريراً يتناول النفاذ عبر الحدود والولاية القضائية.[1247] وعلى الرغم من الشواغل الهامة فيما يتعلق بالنفاذ عبر الحدود، اقترح التقرير اعتماد بروتوكول إضافي مخصص.[1248] وعلى النقيض من المناقشة المغلقة بشأن اتفاقية الجريمة السيبرانية يقترح التقرير عملية تشاور أكثر انفتاحاً.[1249] وفي يونيو 2013 استضاف مجلس أوروبا المشاورات العامة المتعلقة بالنفاذ عبر الحدود. واستناداً إلى تقارير المشاركين أعرب جميع الخبراء تقريباً عن انتقادات – بين المنظمات غير الحكومية والشركات والدول الأعضاء في مجلس أوروبا والمفوضية الأوروبية وخبراء حماية البيانات من مجلس أوروبا.[1250]

وفي عام 2013، نشر تقرير صدر عن الفريق العامل المعني بالنفاذ عبر الحدود.[1251] ويسرد التقرير المكونات المحتملة في بروتوكول إضافي. وهي تتراوح من النفاذ عبر الحدود مع الموافقة إلى أشكال شتى من النفاذ دون موافقة.[1252] وفي نوفمبر 2013 نشرت مذكرة إرشادية تتصل بالنفاذ عبر الحدود.[1253]

2.2.5 الاتحاد الأوروبي[1254]

على مدى العقد الأخير، استحدث الاتحاد الأوروبي (EU) عدة صكوك قانونية تتصدى لجوانب الجريمة السيبرانية. وفي حين أن هذه الصكوك ليست ملزمة بصفة عامة إلا للدول الأعضاء البالغ عددها 27 دولة، تستخدم عدة بلدان وأقاليم معايير الاتحاد الأوروبي كنقاط مرجعية في مناقشاتها الوطنية والإقليمية بشأن مواءمة التشريعات.[1255]

الحالة حتى ديسمبر 2009

حتى عام 2009، كانت ولاية الاتحاد الأوروبي في مجال القانون الجنائي محدودة ومثيرة للخلاف.[1256] فإلى جانب التحدي الخاص بمحدودية الولاية، لم يكن معروفاً على وجه اليقين إن كانت الولاية المتعلقة بأي تشريعات جنائية، بما فيها التشريعات المتصلة بالجريمة السيبرانية، في يد ما يُسمى "الركيزة الأولى" (الجماعة الأوروبية) أو "الركيزة الثالثة" (الاتحاد الأوروبي).[1257] وبما أن الرأي السائد كان هو أن الركيزة الثالثة هي المسؤولة، فإن التنسيق لم يكن ممكناً بالتالي إلا على أساس التعاون الحكومي الدولي في إطار الركيزة الثالثة للاتحاد الأوروبي المعنية بالتعاون بين الشرطة والهيئات القضائية في المسائل الجنائية.[1258] وعندما أعلنت محكمة العدل في عام 2005 أن إحدى أدوات الركيزة الثالثة في مجال القانون الجنائي (المقرر الإطاري للمجلس بشأن حماية البيئة من خلال القانون الجنائي[1259]) غير قانونية[1260]، أُثير الخلاف لأول مرة حول توزيع الصلاحيات. وقررت المحكمة أن المقرر الإطاري، غير القابل للتقسيم، يخرق المادة 47 من معاهدة الاتحاد الأوروبي بما أنه يتعدى على الصلاحيات التي تخولها المادة 175 من معاهدة الجماعة الأوروبية للجماعة. وكان لهذا القرار تأثير كبير على النقاش المتعلق بتنسيق القانون الجنائي داخل الاتحاد الأوروبي. وأوضحت المفوضية الأوروبية (EC)، المسؤولة عن النهوض بمعاهدات الاتحاد، أنه نتيجة للحكم المذكور، فإن عدداً من المقررات الإطارية المتعلقة بالقانون الجنائي غير صحيحة جزئياً أو بالكامل، بما أن جميع أحكامها أو بعضاً منها قد اعتُمد على أساس قانوني غير سليم.[1261] وعلى الرغم من الإقرار بالإمكانيات الجديدة لتقييم ولاية في إطار الركيزة الأولى، ظلت المبادرات التي اتخذتها المفوضية الأوروبية مع ذلك محدودة بسبب عدم تغطية الموضوع في الركيزة الأولى. وفي عام 2007، أكدت محكمة العدل الممارسة القانونية في قرار ثان للمحكمة.[1262]

الحالة بعد التصديق على معاهدة لشبونة

غيّرت معاهدة لشبونة (معاهدة "الإصلاح")،[1263] التي دخلت حيّز النفاذ في ديسمبر 2009، وظيفة الاتحاد الأوروبي إلى حد كبير. فإلى جانب إلغاء التمييز بين "الركيزة الأولى" و"الركيزة الثالثة"، منحت الاتحاد الأوروبي لأول مرة ولاية قوية في مجال

الجريمة الحاسوبية. وتمنح المواد من 82 إلى 86 من المعاهدة المتعلقة بسير عمل الاتحاد الأوروبي ولاية للاتحاد الأوروبي (TFEU) بشأن تنسيق تشريعات القانون الجنائي (القانون الجنائي الموضوعي والقانون الإجرائي). والمادة الأكثر ملاءمة للجريمة السيبرانية هي المادة 83 من المعاهدة المتعلقة بسير عمل الاتحاد الأوروبي.[1264] وتخول هذه المادة للاتحاد الأوروبي صلاحية وضع قواعد دنيا بشأن تعريف المخالفات الجنائية والعقوبات المتصلة بالجرائم الجسيمة ذات الطابع العابر للحدود. ويُشار إلى الجريمة السيبرانية بالتحديد كمجال من مجالات الجريمة ذات الصلة في الفقرة 1 من المادة 83. وبما أن مصطلح الجريمة الحاسوبية أوسع من مصطلح الجريمة السيبرانية، فإن هذه المادة تسمح للاتحاد الأوروبي بتنظيم المجالين معاً. وبناءً على الفقرة 2ي من المادة 4، تخضع التشريعات المتعلقة بالجريمة الحاسوبية للاختصاص المشترك بين الاتحاد الأوروبي والدول الأعضاء. ويمكّن هذا الأمر الاتحاد الأوروبي من اعتماد وثائق ملزمة قانونياً (الفقرة 2 من المادة 2) ويحدّ من قدرة الدول الأعضاء على ممارسة اختصاصها بالدرجة التي تمنع الاتحاد الأوربي من ممارسة اختصاصه.

وفي "برنامج إستوكهولم" ، الذي اعتمده مجلس أوروبا في عام 2009، أكد الاتحاد الأوروبي أنه سيستخدم الولاية الجديدة.[1265] وهذا البرنامج تعريف لمحور عمل الاتحاد الأوروبي في مجال العدالة والشؤون الداخلية خلال فترة خمس سنوات، ويلي برنامج لاهاي الذي وصل إلى نهايته في عام 2009.[1266] كما يؤكد البرنامج نية الاتحاد الأوربي في استخدام الولاية، من خلال الإشارة إلى مجالات الجريمة المذكورة في الفقرة 1 من المادة 83 من المعاهدة المتعلقة بسير عمل الاتحاد الأوروبي، ومنح الأولوية لمجالي استغلال الأطفال في المواد الإباحية والجريمة السيبرانية.[1267]

لمحة عامة عن صكوك الاتحاد الأوروبي ومبادئه التوجيهية

على الرغم من التغييرات الأساسية التي شهدتها بنية الاتحاد الأوروبي، ما زالت الصكوك المعتمدة في الماضي سارية. وبناءً على المادة 9 من البروتوكول المتعلق بالأحكام الانتقالية، يُحتفظ بالصكوك المعتمدة على أساس معاهدة الاتحاد الأوروبي قبل دخول معاهدة لشبونة حيّز النفاذ، إلى حين إلغاء أو إبطال أو تعديل هذه الصكوك تطبيقاً للاتفاقيات. ولهذا، يقدم الفصل التالي لمحة عامة عن جميع صكوك الاتحاد الأوروبي ذات الصلة.

السياسات العامة

لقد تصدى الاتحاد الأوروبي في عام 1996 سلفاً للمخاطر المتصلة بالإنترنت في بيان يتعلق بالمحتوى غير القانوني والضار المتاح على الإنترنت.[1268] وسلط الاتحاد الأوروبي الضوء على أهمية التعاون بين الدول الأعضاء من أجل مكافحة المحتوى غير القانوني على الخط.[1269] وفي عام 1999، اعتمد البرلمان والمجلس الأوروبيان خطة عمل للنهوض باستخدام أكثر أماناً للإنترنت ومكافحة المحتوى غير القانوني والضار على الشبكات العالمية.[1270] وتركز خطة العمل هذه على التنظيم الذاتي وليس على التجريم. وفي عام 1999 أطلق الاتحاد الأوروبي أيضاً مبادرة "أوروبا الإلكترونية"، باعتماده بيان المفوضية الأوروبية المعنون "أوروبا الإلكترونية – مجتمع معلومات للجميع".[1271] وتحدد هذه المبادرة الأهداف الجوهرية، لكنها لا تتناول تجريم الأفعال غير القانونية المرتكبة باستخدام تكنولوجيا المعلومات. وفي عام 2001، أصدرت المفوضية الأوروبية (EC) بياناً معنوناً "إنشاء مجتمع معلومات أكثر سلامة عن طريق تحسين أمن البُنى التحتية للمعلومات ومكافحة الجريمة المتعلقة بالحاسوب".[1272] وفي هذا البيان، حللت المفوضية الأوروبية وعالجت مشكلة الجريمة السيبرانية وأشارت إلى ضرورة الاضطلاع بعمل فعال للتصدي للتحديات المحدقة بتكاملية نظم وشبكات المعلومات وتيسّرها وإمكانية الاعتماد عليها.

أصبحت البُنى 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.[1273]

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.[1274]

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.[1275]

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.[1276]

وبالإضافة إلى البيان المتعلق بالجريمة الحاسوبية، نشرت المفوضية الأوروبية بياناً بشأن "أمن الشبكات والمعلومات"[1277] في عام 2001 حول المشاكل 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. وسلّما 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.[1278]

وفي عام 2007، نشرت المفوضية بياناً معنوناً نحو وضع سياسة عامة بشأن مكافحة الجريمة السيبرانية.[1279] ويلخص البيان الوضع الراهن ويؤكد 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 في مكافحة الجريمة السيبرانية؛
- تحسين تنسيق الدعم المالي للأنشطة التدريبية؛
- تنظيم اجتماع لخبراء إنفاذ القانون؛
- تعزيز الحوار مع الصناعة؛
- رصد التهديدات المتنامية للجريمة السيبرانية من أجل تقييم الحاجة إلى مزيد من التشريعات.

التوجيه المتعلق بالتجارة الإلكترونية (2000)

ويعالج التوجيه المتعلق بالتجارة الإلكترونية[1280]، من بين مسائل أخرى، مسؤولية مورد خدمة الإنترنت (ISP) عن أفعال ترتكبها أطراف ثالثة (المادة 12 *والمواد التالية لها*). وبمراعاة التحديات الناتجة عن البُعد الدولي للشبكة، قرر محررو التوجيه وضع معايير قانونية لتوفير إطار من أجل التنمية العامة لمجتمع المعلومات ودعم التنمية الاقتصادية بوجه عام وكذلك عمل وكالات إنفاذ القانون.[1281] ويقوم التوجيه على اعتبار أن تنمية خدمات مجتمع المعلومات متعثرة بسبب عدد من الحواجز القانونية أمام سير عمل السوق الداخلية على النحو الصحيح، مما يمنح الجماعة الأوروبية ولايتها.[1282] ويقوم تنظيم المسؤولية على مبدأ المسؤولية المتدرجة.[1283] وعلى الرغم من أن التوجيه يؤكد أنه ليست هناك أي نية لتحقيق اتساق في مجال القانون الجنائي في حد ذاته، فإنه ينظم المسؤولية كذلك بموجب القانون الجنائي.[1284]

قرار المجلس بشأن مكافحة استغلال الأطفال في المواد الإباحية على الإنترنت (1999)

في عام 2000، اعتمد مجلس الاتحاد الأوروبي نهجاً من أجل التصدي لاستغلال الأطفال في المواد الإباحية على الإنترنت. ويمثل القرار الذي اعتُمد متابعة لبيان عام 1996 بشأن المحتوى غير القانوني والضار على الإنترنت[1285] وخطة العمل ذات الصلة لعام 1999 بشأن النهوض باستخدام أكثر أماناً للإنترنت ومكافحة المحتوى غير القانوني والضار على الشبكات العالمية.[1286] غير أن القرار لا يتضمن التزامات بشأن اعتماد أحكام محددة في مجال القانون الجنائي.

القرار الإطاري بشأن مكافحة الاحتيال (2001)

في عام 2001، اعتمد الاتحاد الأوروبي الإطار القانوني الأول الذي يتصدى بشكل مباشر لجوانب الجريمة السيبرانية. ويتضمن القرار الإطاري للاتحاد الأوروبي بشأن مكافحة الاحتيال وتزوير وسائل الدفع[1287] غير النقدية التزامات بتنسيق تشريعات القانون الجنائي فيما يخص جوانب محددة من الاحتيال المتصل بالحاسوب وإنتاج الأدوات، مثل البرامج الحاسوبية، التي تُعتمد خصيصاً لغرض ارتكاب جريمة من الجرائم المذكورة في المقرر الإطاري.[1288]

> ***المادة 3 – الجرائم المتصلة بالحواسيب***
>
> *تتخذ كل دولة عضو التدابير اللازمة لضمان تجريم السلوك التالي عند ارتكابه عمداً: إجراء أو التسبب في إجراء تحويل للأموال أو قيم نقدية والتسبب بالتالي لشخص آخر في خسارة غير مسموح بها لأملاكه، وذلك بهدف تحقيق فائدة مالية غير مرخص بها لصالح الشخص الذي ارتكب الجريمة أو لصالح الغير، من خلال ما يلي:*
>
> - *تقديم أو تغيير أو إلغاء بيانات حاسوبية، لا سيما المتعلقة بتحديد الهوية، بدون حق، أو*
> - *التدخل في سير عمل برنامج أو نظام حاسوبي، بدون حق.*

وتماشياً مع الرأي السائد آنذاك ونتيجة لانعدام الولاية في الركيزة الأولى، وُضع الصك في إطار الركيزة الثالثة، مؤكداً بالتالي أنه بالنظر إلى البُعد الدولي للظاهرة المعنية، لا يمكن معالجة هذه القضايا بالشكل المناسب على يد الدول الأعضاء نفسها.

القرار الإطاري بشأن الهجمات ضد أنظمة المعلومات (2005)[1289]

بعد نشر السياسة العامة في عام 2001، قدمت المفوضية الأوروبية مقترحاً بشأن قرار إطاري يتعلق بالهجمات على أنظمة المعلومات.[1290] وقد عدّله واعتمده المجلس في عام 2005.[1291] وقد استعيض عن هذا الصك إبان ذلك بالتوجيه لعام 2012 (انظر أدناه). ورغم أنه يراعي اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية،[1292] فهو يركز على تنسيق الأحكام الجوهرية للقانون الجنائي المصممة من أجل حماية عناصر البنية التحتية. ولم تُدمج في هذا القرار الإطاري جوانب القانون الإجرائي

الجنائي (لا سيما تنسيق المواد اللازمة للتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها) والمواد المتصلة بالتعاون الدولي. ويسلّط القرار الإطاري الضوء على الثغرات والاختلافات في الأطر القانونية للدول الأعضاء وعلى التعاون الفعال بين الشرطة والسلطة القضائية في مجال الهجمات على أنظمة المعلومات.[1293]

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 ألاّ تجرم السلوك المشار إليه في الفقرة 1 إلا حيثما يُرتكب 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 يُرتكب دون حق، على الأقل في الحالات التي لا تكون طفيفة.

التوجيه المتعلق بالاحتفاظ بالبيانات (2005)

في عام 2005، اعتمد المجلس توجيه الاتحاد الأوروبي المتعلق بالاحتفاظ بالبيانات.[1294] ويتضمن هذا التوجيه التزاماً على مورّدي خدمة الإنترنت بأن يخزنوا بعض بيانات الحركة اللازمة للكشف عن هوية الجناة في الفضاء السيبراني. وفي عام 2014، أعلنت محكمة العدل الأوروبية أن التوجيه باطل.[1295]

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 تُولَّد فيه هذه البيانات أو تُعالج 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 تُعالج أو تُخزن (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 يُفضي إلى إعادة النظر في التوجيه وفي تنفيذه على يد المحاكم الدستورية.[1296] وفي مذكرة بشأن قضية منتجي الموسيقى في إسبانيا *(Promusicae)* ضد شركة الاتصالات الإسبانية *(Telefónica de España)*،[1297] أشار مستشار محكمة العدل الأوروبية، النائب العام جوليان كوكوت، إن من المثير للجدل ما إذا كان بالإمكان تنفيذ واجب الاحتفاظ بالبيانات دون انتهاك الحقوق الأساسية.[1298] وفي سنة 2001، سلطت مجموعة الثمانية الضوء بالفعل على احتمال مواجهة صعوبات بشأن تنفيذ هذه اللوائح.[1299]

وقد ارتكز التوجيه على ولاية الجماعة الأوروبية فيما يخص السوق الداخلية (المادة 95).[1300] وأكد محررو التوجيه أن المعايير القانونية والتقنية المختلفة في مجال الاحتفاظ بالبيانات لغرض التحقيق في الجريمة السيبرانية تشكل عوائق بالنسبة للسوق الداخلية للاتصالات الإلكترونية، طالما أن موردي الخدمة يواجهون متطلبات مختلفة تستوجب استثمارات مالية مختلفة.[1301] وطلبت أيرلندا، بتأييد من سلوفاكيا، من محكمة العدل الأوروبية إلغاء التوجيه لأنه لم يُعتمد على أساس قانوني سليم. واحتج البلَدان بأن المادة 95 ليست أساساً كافياً بما أن الصك لا يركز على سير السوق الداخلية بل بالأحرى على التحقيق في الجرائم والكشف عنها وملاحقة مرتكبيها. ورفضت محكمة العدل الأوروبية هذا الطلب باعتباره لا يستند إلى أي أسس، مشيرة إلى أن من شأن الاختلافات المتصلة بالالتزامات المتعلقة بالاحتفاظ بالبيانات أن تؤثر تأثيراً مباشراً في سير السوق الداخلية.[1302] وأكدت المحكمة أيضاً أن وضعاً كهذا يبرر سعي الهيئة التشريعية للجماعة الأوروبية من أجل تحقيق الهدف المتمثل في حماية سير السوق الداخلية على نحو سليم من خلال اعتماد قواعد متسقة.

وفي عام 2014، أعلنت محكمة العدل الأوروبية أخيراً أن التوجيه باطل[1303] وبناءً على رأي المحكمة فإنه يفضي إلى تدخل واسع النطاق وخطير بشكل خاص في الحقوق الأساسية في احترام الحياة الخاصة وحماية البيانات الشخصية، دون أن يقتصر التدخل على ما هو ضروري قطعاً. ونتيجة لذلك، لم تعد الدول الأعضاء مرتبطة بالتوجيه. ولكن القوانين الوطنية التي نفذت وفقاً للتوجيه ليست باطلة تلقائياً. ومن غير المؤكد اليوم ما إذا كان الاتحاد الأوروبي سوف يقدم ويعتمد توجيهاً جديداً.

تعديل القرار الإطاري المتعلق بمكافحة الإرهاب (2007)

في عام 2007، بدأ الاتحاد الأوروبي نقاشاً بشأن مشروع تعديل القرار الإطاري المتعلق بمكافحة الإرهاب.[1304] وفي مقدمة مشروع التعديل، سلّط الاتحاد الأوروبي الضوء على أن الإطار القانوني القائم يجرّم المساعدة أو التحريض ولكنه لا يجرّم نشر الخبرات الإرهابية عن طريق الإنترنت.[1305] 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 القرار 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.

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 تُرتكب بالفعل جريمة إرهابية للمعاقبة على أي فعل منصوص عليه في الفقرة 2."

واستناداً إلى الفقرة 1 (ج) من المادة 3[1306] من المقرر الإطاري، تُعدّ الدول الأعضاء مُلزمة 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 تحدّ 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 ستُستخدم بها بعد ذلك. ولذا يتعين أن يؤخذ سياق النشر في الاعتبار (كأن تكون قد نُشرت مثلاً في موقع ويب تديره منظمة إرهابية).

التوجيه المتعلق باستغلال الأطفال في المواد الإباحية (2011)

كان أول مشروع إطار قانوني متصل بالجريمة السيبرانية قُدّم بعد التصديق على معاهدة لشبونة هو المقترح المتعلق بوضع توجيه بشأن الاعتداء الجنسي على الأطفال واستغلالهم جنسياً واستغلالهم في المواد الإباحية،[1307] وقد اعتُمد هذا التوجيه في عام 2011.[1308] وأشار محررو التوجيه إلى أن تكنولوجيا المعلومات تمكّن الجناة من إنتاج وتوزيع المواد الإباحية التي يُستغل فيها الأطفال بسهولة أكبر[1309] وأكدوا أهمية التصدي للتحديات الناجمة عن ذلك من خلال وضع أحكام محددة. ويطبّق التوجيه معايير دولية، مثل اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال والاعتداء الجنسيين.[1310]

المادة 5 – الجرائم المتصلة باستغلال الأطفال في المواد الإباحية

1 تتخذ الدول الأعضاء التدابير اللازمة لضمان المعاقبة على السلوك المتعمّد المشار إليه في الفقرات من 2 إلى 6، عند ارتكابه دون وجه حق.

2 يُعاقب على حيازة أو امتلاك مواد إباحية يُستغل فيها الأطفال بالسجن لفترة قصوى لا تقل عن سنة واحدة.

3 يُعاقب على النفاذ عن علم إلى مواد إباحية يُستغل فيها الأطفال، باستخدام تكنولوجيا المعلومات والاتصالات، بالسجن لفترة قصوى لا تقل عن سنة واحدة.

4 يُعاقب على توزيع أو نشر أو إرسال مواد إباحية يُستغل فيها الأطفال بالسجن لفترة قصوى لا تقل عن سنتين.

5 يُعاقب على تقديم أو توريد أو إتاحة مواد إباحية يُستغل فيها الأطفال بالسجن لفترة قصوى لا تقل عن سنتين.

6 يُعاقب على إنتاج مواد إباحية يُستغل فيها الأطفال بالسجن لفترة قصوى لا تقل عن 3 سنوات.

7 يُترك لتقدير الدول الأعضاء تقرير ما إذا كانت هذه المادة تنطبق على حالات تتعلق باستغلال الأطفال في المواد الإباحية مثلما يُشار إليها في المادة 2(ج) ('3')، ويكون فيها عمر الشخص الذي يبدو أنه طفل 18 عاماً أو أكثر في الواقع وقت التصوير.

8 يُترك لتقدير الدول الأعضاء تقرير إن كانت الفقرتان 2 و6 من هذه المادة تنطبقان على حالات يثبت فيها أن المواد الإباحية مثلما يشار إليها في المادة 2(ج) ('4') من إنتاج المنتج وحده وملك له هو فقط من أجل استعماله الشخصي طالما لم تستعمل أي مواد إباحية مثلما يشار إليها في المادة 2(ج) ('1') أو ('2') أو ('3') لغرض إنتاجها وشريطة ألا ينطوي الفعل على أي احتمال لنشر المواد.

ويُقترح التوجيه، شأنه شأن الاتفاقية، تجريم النفاذ إلى المواد الإباحية التي يُستغل فيها الأطفال، باستخدام تكنولوجيا المعلومات والاتصالات.[1311] ويمكّن هذا وكالات إنفاذ القانون من ملاحقة الجناة في الحالات التي تستطيع فيها إثبات أن الجاني فتح مواقع إلكترونية فيها مواد إباحية يُستغل فيها الأطفال، لكن دون أن تستطيع إثبات تنزيل الجاني لمواد إباحية. وتنشأ مثل هذه الصعوبات في جمع الأدلة، على سبيل المثال، عندما يستخدم الجاني تكنولوجيا التجفير لحماية الملفات المنزَّلة على وسائط التخزين لديه.[1312] ويشير التقرير التوضيحي للاتفاقية المتعلقة بحماية الأطفال إلى ضرورة تطبيق الحكم أيضاً في الحالات التي يشاهد فيه الجاني فقط صور الأطفال المستغلين في المواد الإباحية على الخط دون تنزيلها.[1313] وعموماً، فإن فتح موقع على الإنترنت لا يؤدي تلقائياً إلى بدء عملية التنزيل – دون علم المستعمل.[1314] وكنتيجة لذلك، فإن الحكم مناسب بالأساس في الحالات التي يمكن فيها استهلاك المواد الإباحية التي يُستغل فيها الأطفال دون تنزيل المواد. وقد يكون الأمر كذلك، على سبيل المثال، إذا كان الموقع إلكتروني يتيح بثّ التسجيلات الفيديوية، ولا يحفظ المعلومات الواردة بل يستبعدها مباشرة بعد إرسالها، وذلك بسبب التشكيلة التقنية لعملية البثّ.[1315]

المادة 25 – تدابير مكافحة المواقع الإلكترونية التي تتضمن أو تنشر المواد الإباحية التي يُستغل فيها الأطفال

1 تتخذ الدول الأعضاء التدابير اللازمة من أجل ضمان الإزالة الفورية لصفحات الويب التي تتضمن أو تنشر المواد الإباحية التي يُستغل فيها الأطفال والمستضافة في أراضيها، والسعي من أجل الحصول على حق إزالة مثل هذه الصفحات المستضافة خارج أراضيها.

2 تتخذ الدول الأعضاء التدابير اللازمة لمنع النفاذ إلى صفحات الويب التي تتضمن أو تنشر المواد الإباحية التي يُستغل فيها الأطفال وتستهدف مستعملي الإنترنت داخل أراضيها. ويجب وضع هذه التدابير من خلال إجراءات شفافة وتقديم ضمانات كافية، لا سيما من أجل ضمان أن التقييد يقتصر على ما هو ضروري ومتناسب، وإفادة المستعملين بسبب التقييد. وتشمل هذه الضمانات أيضاً إمكانية التعويض القضائي.

وإلى جانب تجريم الأفعال المتصلة باستغلال الأطفال في المواد الإباحية، تضمن المشروع الأولي حكماً يُلزم الدول الأعضاء بتنفيذ إجراء حجب المواقع الإلكترونية التي تتضمن المواد الإباحية التي يُستغل فيها الأطفال.[1316] وتستخدم هذا النهج عدة بلدان أوروبية[1317] وأيضاً بلدان غير أوروبية مثل الصين[1318] وإيران[1319] وتايلاند[1320]. وتأتي بواعث القلق من عدم ثبوت فعالية أي من المفاهيم التقنية،[1321] كما أن النهج المذكور ينطوي على احتمال ملازم بأن يكون هناك إفراط في الحجب.[1322] وكنتيجة لذلك، جرى تغيير الحجب الإلزامي وتُركت للدول الأعضاء مسألة تقرير إن كان ينبغي تنفيذ التزامات الحجب على المستوى الوطني.

التوجيه المتعلق بالهجمات على نظم المعلومات (2013)

في سبتمبر 2010، قدم الاتحاد الأوروبي مقترحاً بتوجيه بشأن الهجمات على نظم المعلومات.[1323] وقد اعتمد في عام 2013.[1324] ومثلما شُرح أعلاه بمزيد من التفصيل، فقد اعتمد الاتحاد الأوروبي في عام 2005 قراراً إطارياً بشأن الهجمات على نظم المعلومات.[1325] وتؤكد المذكرة التوضيحية للمقترح أن هدف محرري التوجيه هو تحديث وتعزيز الإطار القانوني لمكافحة الجريمة السيبرانية في الاتحاد الأوروبي عن طريق التصدي للأساليب الجديدة التي ترتكب بها الجرائم.[1326] وإلى جانب تجريم النفاذ غير القانوني (المادة 3) والتدخل غير القانوني في نظم (المادة 4) والتدخل غير القانوني في البيانات (المادة 5)، الذي جاء مسبقاً في القرار الإطاري لعام 2005، يتضمن مشروع توجيه عام 2010 جريمتين إضافيتين.

> ***المادة 6 – الاعتراض غير القانوني***
>
> *تتخذ الدول الأعضاء التدابير اللازمة لضمان المعاقبة على الاعتراض، المقصود وبغير حق، باستخدام الوسائل التقنية، للإرسالات غير العمومية للبيانات الحاسوبية إلى نظام معلومات أو منه أو داخله، بما فيها الإرسالات الكهرمغنطيسية من نظام معلومات يحمل مثل هذه البيانات الحاسوبية، وذلك باعتبار هذا الاعتراض جريمة جنائية، على الأقل في الحالات غير البسيطة.*
>
> ***المادة 7 – الأدوات المستخدمة لارتكاب الجرائم***
>
> *تتخذ الدول الأعضاء التدابير اللازمة لضمان أن إنتاج أي من الأدوات التالية أو بيعها من أجل الاستعمال أو استيرادها أو توزيعها أو إتاحتها بشكل من الأشكال، عن قصد ودون وجه حق لغرض استخدامها في ارتكاب أي جريمة من الجرائم المشار إليها في المواد من 3 إلى 6، يعاقب عليه بمثابة جريمة جنائية، على الأقل في الحالات غير البسيطة:*
>
> *أ) برنامج حاسوبي، جرى تصميمه أو تكييفه بالأساس لغرض ارتكاب أي جريمة من الجرائم المشار إليها في المواد من 3 إلى 6؛*
>
> *ب) كلمة سر أو شفرة نفاذ أو بيانات مشابهة خاصة بحاسوب يمكن بواسطتها النفاذ إلى نظام حاسوبي بكامله أو إلى أجزاء منه.*

ويتماشى الحكمان إلى حد كبير مع الأحكام المقابلة لهما في الاتفاقية المتعلقة بالجريمة السيبرانية.

العلاقة باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية

مثلما ذُكر أعلاه، فقد جرى التفاوض بشأن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بين عامي 1997 و2000. وفي عام 1999، أعرب الاتحاد الأوروبي عن وجهة نظره بشأن الاتفاقية المتعلقة بالجريمة السيبرانية بصورة مشتركة.[1327] ودعا الدول الأعضاء إلى دعم صياغة مشروع اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.[1328] وفي ذلك الوقت، لم يكن لدى الاتحاد الأوروبي نفسه أي ولاية لوضع إطار قانوني مماثل. وقد غيّر التصديق على معاهدة لشبونة الوضع. لكن الاتحاد الأوروبي لم يقرر حتى الآن أن يغير موقفه بشأن الاتفاقية المتعلقة بالجريمة السيبرانية. وفي برنامج استوكهولم، يتم التأكيد على أن الاتحاد الأوروبي لا يدعو الدول الأعضاء فقط إلى التصديق على الاتفاقية المتعلقة بالجريمة السيبرانية، بل إنه يبين أيضاً أنه، حسب رأي الاتحاد الأوروبي، ينبغي أن تصبح هذه الاتفاقية الإطار القانوني المرجعي لمكافحة الجريمة السيبرانية على الصعيد العالمي.[1329] بيد أن هذا لا يعني أن الاتحاد الأوروبي لن يضع نهجاً شاملاً بشأن الجريمة السيبرانية، حيث توفر نهج الاتحاد الأوروبي مزيتين مهمتين. الأولى أن توجيهات الاتحاد الأوروبي يجب أن تُنفذ ضمن إطار زمني محدد وقصير، في حين أن مجلس أوروبا لا يمتلك أي وسيلة للإلزام بالتوقيع أو التصديق على الاتفاقيات غير الضغط السياسي.[1330] والمزية الثانية هي أن لدى الاتحاد الأوروبي ممارسة تتمثل في التحديث المستمر لصكوكه، في حين أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية لم تخضع لأي تحديث خلال السنوات الثلاث عشرة الأخيرة.

3.2.5 منظمة التعاون والتنمية في الميدان الاقتصادي[1331]

في عام 1983، استهلت منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) دراسة عن إمكانية تحقيق التواؤم بين القوانين الجنائية على الصعيد الدولي من أجل معالجة مشكلة الجريمة الحاسوبية.[1332] وفي عام 1985، نشرت المنظمة تقريراً حول التشريعات الراهنة وقدم اقتراحات بشأن مكافحة الجريمة السيبرانية.[1333] 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 (ICCP) 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.[1334] وتشمل المبادئ التوجيهية جوانب شتى من بينها القضايا المتعلقة بالعقوبات:

> *تُعد 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 تحديث 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.[1335] وتتضمن المبادئ التوجيهية تسعة مبادئ متكاملة هي:

> *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.[1336] وأظهر التقرير أن الرسائل الاقتحامية تشكل مشكلة أشد خطراً في البلدان النامية عنها في البلدان المتقدمة لأن الموارد في البلدان النامية أقل حجماً وأعلى تكلفة.[1337] وفي عام 2007، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي،[1338] 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.[1339] وفي عام 2008، نشرت المنظمة ورقة استكشافية حول انتحال الهوية على الخط.[1340] وتعرض الورقة نظرة عامة عن سمات انتحال الهوية وأشكالها المختلفة والمسائل المرتبطة بالضحايا فضلاً عن خطط إنفاذ القانون. وتشدد الورقة على أن أغلب بلدان المنظمة لا تعالج المسألة بحد ذاتها بواسطة أحكام محددة وأنه من الضروري النظر في مسألة تجريم انتحال الهوية كجريمة مستقلة. [1341] وفي عام 2009، نشرت منظمة التعاون والتنمية في الميدان الاقتصادي تقريراً عن البرمجيات الضارة. ورغم أن التقرير يتناول بإيجاز جوانب التجريم، فإنه يركز على نطاق البرمجيات الضارة وآثارها الاقتصادية.

4.2.5 مجموعة التعاون الاقتصادي في آسيا والمحيط الهادئ[1342]

اعتبر منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) الجريمة السيبرانية مجالاً هاماً للنشاط ودعا قادة المنتدى إلى توثيق التعاون بين المسؤولين المعنيين بمكافحة الجريمة السيبرانية.[1343] وسلط الإعلان الصادر عن الاجتماع الذي عقده وزراء الاتصالات والمعلومات في بلدان المنتدى في بانكوك في عام 2008، الضوء على أهمية مواصلة التعاون لمكافحة الجريمة السيبرانية.[1344] ولم يضع المنتدى إلى الآن إطاراً قانونياً بشأن الجريمة السيبرانية ولكنه يحيل إلى المعايير الدولية مثل اتفاقية بودابست بشأن الجرائم السيبرانية. وبالإضافة إلى ذلك درس المنتدى عن كثب التشريعات الوطنية المعنية بالجريمة السيبرانية في بلدان مختلفة[1345] في إطار دراسة استقصائية للتشريعات المتعلقة بالجريمة السيبرانية وأعد قاعدة بيانات للنهج الكفيلة بمساعدة الاقتصادات على وضع التشريعات ومراجعتها.[1346] واستند الاستبيان الذي استخدم في الدراسة الاستقصائية إلى الإطار القانوني الذي أتاحته اتفاقية بودابست بشأن الجرائم السيبرانية.

بيان بشأن محاربة الإرهاب (2002)

في عام 2002، أصدر قادة منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ بياناً بشأن مكافحة الإرهاب وتعزيز النمو من أجل سن قوانين شاملة تتعلق بالجريمة السيبرانية (APEC) وتنمية القدرات الوطنية على التحقيق في الجريمة السيبرانية.[1347] وأعلنوا التزامهم بالسعي 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 واتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

بحلول أكتوبر 2003. وتعهدوا أيضاً بتعيين وحدات وطنية معنية بالجريمة السيبرانية وجهات اتصال دولية للمساعدة في مجال التكنولوجيا الراقية وإنشاء هذه القدرات إن كانت لا تتوافر بالفعل، بحلول أكتوبر 2003 وإنشاء مؤسسات تتبادل التقييمات المتعلقة بالتهديدات وبأوجه الضعف (مثل أفرقة الاستجابة للطوارئ الحاسوبية)، بحلول أكتوبر 2003.

مؤتمر بشأن تشريعات الجريمة السيبرانية (2005)

نظم منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ[1348] مؤتمرات متنوعة[1349] ودعا إلى توثيق التعاون بين المسؤولين المعنيين بمكافحة الجريمة السيبرانية.[1350] وقد نظم المنتدى في 2005 مؤتمراً بشأن تشريعات الجريمة السيبرانية. وأما الأهداف الرئيسية للمؤتمر فهي الترويج لإنشاء أُطُر قانونية شاملة لمكافحة الجريمة السيبرانية وتعزيز الأمن السيبراني ومساعدة سلطات إنفاذ القانون التصدّي للقضايا المتعلقة بأحدث التطورات العلمية وللتحديات التي تطرحها أوجه التقدم في مجال التكنولوجيا والنهوض بالتعاون بين المحققين في الجرائم السيبرانية في كامل المنطقة.

فريق العمل المعني بالاتصالات والمعلومات

شارك فريق العمل المعني بالاتصالات والمعلومات التابع للمنتدى[1351] مشاركة نشيطة في نُهُج المنتدى الرامية إلى زيادة الأمن السيبراني.[1352] وفي عام 2002، اعتمد الفريق استراتيجية الأمن السيبراني لمنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ.[1353] وأبدى فريق العمل موقفه من تشريعات الجريمة السيبرانية بالإشارة إلى النهج الدولية المعمول بها في الأمم المتحدة ومجلس أوروبا.[1354] وطرحت تجارب صياغة تشريعات الجريمة السيبرانية للنقاش داخل فريق المهام المعني بالأمن الإلكتروني التابع لفريق العمل المعني بالاتصالات والمعلومات التابع لمنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ أثناء انعقاد مؤتمرين[1355] في تايلاند في عام 2003.[1356]

5.2.5 الكومنولث

يتولى الكومنولث معالجة قضايا عديدة ومن بينها الجريمة السيبرانية. وتركز الأنشطة على مواءمة التشريعات بشكل خاص. وتأثر هذا النهج الرامي إلى تحقيق التواؤم بين التشريعات داخل الكومنولث وإفساح المجال أمام التعاون الدولي بأشياء عديدة منها إدراك مفاده أنه بدون هذا النهج سيحتاج الأمر إلى إبرام ما لا يقل عن 1 272 معاهدة ثنائية في إطار الكومنولث لتغطية متطلبات التعاون الدولي في هذا الشأن.[1357]

وقرر 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.[1358] وقدم فريق الخبراء تقريره وتوصياته في مارس 2002.[1359] ثم قدم في وقت لاحق من عام 2002 مشروع القانون النموذجي الخاص بالحاسوب والجريمة المتعلقة بالحاسوب.[1360] وجاء القانون النموذجي متماشياً مع المعايير التي حددتها اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، عملاً بالتعليمات الواضحة التي تلقاها فريق الخبراء، وإدراكاً منه لكون الاتفاقية تشكل معياراً دولياً. بيد أنه توجد اختلافات ستناقش بمزيد من التفصيل في الفصل 6.

وفي اجتماع 2000، قرر وزراء العدل ونواب العموم في البلدان الصغيرة في الكومنولث، إنشاء فريق خبراء لوضع تشريع نموذجي بشأن الأدلة الرقمية. وقدم القانون النموذجي في عام 2002.[1361]

وبالإضافة إلى توفير التشريعات، نظم الكومنولث عقدة أنشطة تدريبية. وشاركت شبكة الكومنولث لتكنولوجيا المعلومات والتنمية (COMNET-IT) في تنظيم دورة تدريبية بشأن الجرائم السيبرانية في أبريل 2007.

وفي عام 2009، عُقد في مالطا البرنامج التدريبي القطري الثالث للكومنولث المعني بالإطار القانوني لتكنولوجيا المعلومات والاتصالات بدعم من صندوق الكومنولث للتعاون التقني (CFTC) ونظمت دورة تدريبية أخرى في عام 2011.

وفي عام 2011، قدم الكومنولث "مبادرة الكومنولث بشأن الجرائم السيبرانية". وتهدف المبادرة بالأساس إلى مساعدة بلدان الكومنولث على بناء قدراتها المؤسسية والبشرية والتقنية فيما يتعلق بوضع السياسات والتشريعات والتنظيم والتحقيق وإنفاذ القانون.[1362] وترمي المبادرة إلى تمكين جميع بلدان الكومنولث من التعاون الفعال في مجال مكافحة الجرائم السيبرانية على الصعيد العالمي.

6.2.5 الاتحاد الإفريقي

خلال المؤتمر الاستثنائي لوزراء الاتحاد الإفريقي المسؤولين عن الاتصالات وتكنولوجيا المعلومات الذي عُقد في جوهانسبورغ في عام 2009، تطرّق الوزراء إلى موضوعات متنوعة تتعلق بزيادة استخدام تكنولوجيا المعلومات والاتصالات في البلدان الإفريقية. وتقرر أن تضع مفوضية الاتحاد الإفريقي بالاشتراك مع لجنة الأمم المتحدة الاقتصادية ل إفريقيا إطاراً قانونياً للبلدان الإفريقية يعالج مسائل مثل المعاملات الإلكترونية والأمن السيبراني وحماية البيانات.[1363]

وفي عام 2011، قدم الاتحاد الإفريقي مشروع اتفاقية الاتحاد الإفريقي بشأن إرساء إطار قانوني موثوق للأمن السيبراني في إفريقيا.[1364] وتهدف الأطراف التي صاغت الاتفاقية إلى تعزيز التشريعات القائمة في الدول الأعضاء فيما يتعلق بتكنولوجيا المعلومات والاتصالات. وفيما يتصل بالولاية، التي لم تقتصر على الجريمة السيبرانية بل شملت أيضاً غيرها من قضايا مجتمع المعلومات مثل حماية البيانات والمعاملات الإلكترونية، فإن الاتفاقية أكثر شمولاً من أغلب النهج الإقليمية الأخرى.[1365] وتحتوي الاتفاقية على أربعة أجزاء. ويتعلق الجزء الأول بالتجارة الإلكترونية فهو يتناول جوانب مختلفة مثل المسؤولية التعاقدية للموردين الإلكترونيين للسلع والخدمات، والتزامات المعاهدة في شكل إلكتروني وأمن المعاملات الإلكترونية.[1366] ويتناول الجزء الثاني قضايا حماية البيانات.[1367] ويتعلق الجزء الثالث بمكافحة الجريمة السيبرانية. ويحتوي القسم الأول خمسة فصول.[1368] ويحتوي القسم على مجموعة من ستة تعاريف (الاتصالات الإلكترونية والبيانات المحوسبة والعنصرية وكراهية الأجانب في مجال تكنولوجيا المعلومات والاتصالات والقاصر والمواد الإباحية التي يستغل فيها الأطفال ونظام الحاسوب).[1369]

المادة III-1:

لأغراض هذه الاتفاقية:

1) يُقصد بالاتصال الإلكتروني أي إرسال إلى الجمهور أو قسم منه بوسائل إلكترونية أو مغنطيسية للإشارات أو العلامات أو النصوص المكتوبة أو الصور أو الأصوات أو الرسائل، أياً كانت طبيعتها؛

2) ويُقصد بالبيانات المحوسبة أي تمثيل للوقائع أو المعلومات أو المفاهيم بأي شكل من الأشكال يسمح بمعالجتها حاسوبياً؛

3) يُقصد بالعنصرية وكراهية الأجانب في مجال تكنولوجيا المعلومات والاتصالات أي موضوع مكتوب أو صورة أو أي تمثيل آخر للأفكار أو النظريات يدعو أو يشجع على الكراهية والتمييز أو العنف ضد شخص أو مجموعة من الأشخاص بسبب العرق أو اللون أو النسب أو الأصل القومي أو العرقي أو الدين، حيث تكون هذه بمثابة ذريعة سواء للعنصرية أو كراهية الأجانب أو كدافع لهما؛

4) يُقصد بالقاصر أي شخص يقلّ عمره عن ثماني عشرة سنة (18) طبقاً لاتفاقية الأمم المتحدة لحقوق الطفل؛

5) يُقصد بالمواد الإباحية التي يستغل فيها الأطفال أي بيانات، بغض النظر عن طبيعتها أو شكلها، تجسد بصرياً خضوع قاصر لفعل جنسي صريح، أو صوراً واقعية تجسّد خضوع قاصر لسلوك جنسي صريح؛

6) يُقصد بنظام الحاسوب أي جهاز، سواء كان قائماً بذاته أو غير ذلك، ومجموعة من الأجهزة الموصولة بينياً المستخدمة جزئياً أو كلياً للمعالجة المؤتمتة للبيانات بغرض تنفيذ برنامج.

وعلاوةً على ذلك، يتناول الجزء الثالث الحاجة إلى سياسة وطنية واستراتيجية مقترنة بها في مجال الأمن السيبراني.[1370] ويتطرّق الفصل الثاني إلى الجوانب العامة المتعلقة بالتدابير القانونية. حيث يتضمن المعايير المرتبطة بالسلطات الأساسية والمبادئ الديمقراطية وحماية البنية التحتية الأساسية للمعلومات والمواءمة وازدواج الجرائم والتعاون الدولي.[1371] ويتناول الفصل الثالث مسائل تتعلق بنظام الأمن السيبراني الوطني. حيث يتضمن ثقافة الأمن ودور الحكومة والشراكة بين القطاع الخاص والعام والتعليم والتدريب وإذكاء الوعي العام.[1372] ويخصص الفصل الرابع للهياكل الوطنية المعنية برصد الأمن السيبراني. ويتناول الفصل الخامس موضوع التعاون الدولي. ويتمثل الاختلاف الرئيسي بين اتفاقية الاتحاد وغيرها من الأُطر الإقليمية المماثلة مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في أن مشروع اتفاقية الاتحاد الإفريقي، في حال عدم وجود أي صك يتعلق بالتعاون الدولي، لا يمكن استخدامه لهذا الغرض. وقد عبّرت المادتان 21 و25 على وجه الخصوص عن هذا المفهوم المختلف.

المادة III-1-21: التعاون الدولي

يتعيّن على كل دولة من الدول الأعضاء اتخاذ التدابير التي تراها ضرورية لتعزيز تبادل المعلومات وتقاسم البيانات على نحو سريع وعاجل ومتبادل من قبل منظمات الدول الأعضاء والمنظمات المماثلة في الدول الأعضاء الأخرى المسؤولة عن تطبيق القانون في الإقليم على اساس ثنائي أو متعدد الأطراف.

المادة III-1-25: نموذج التعاون الدولي

يتعيّن على كل دولة عضو أن تتخذ التدابير والاستراتيجيات التي تراها ضرورية للمشاركة في التعاون الإقليمي والدولي في مجال الأمن السيبراني. وقد اعتمد عدد كبير من الهيئات الحكومية الدولية، بما فيها الأمم المتحدة والاتحاد الإفريقي والاتحاد الأوروبي ومجموعة الثمانية، وغيرها، القرارات الموجهة إلى تعزيز مشاركة الدول الأعضاء في هذا الإطار من العلاقات. ووضعت منظمات مثل الاتحاد الدولي للاتصالات ومجلس أوروبا ودول الكومنولث وغيرها، أطراً نموذجية للتعاون الدولي التي قد تعتمدها الدول الأعضاء للتوجيه.

ويتناول القسم الثاني من الجزء الثالث القانون الجنائي الموضوعي. ويتضمن الباب الأول تجريم النفاذ غير المشروع إلى نظام حاسوبي،[1373] والمكوث غير القانوني في نظام حاسوبي[1374] والتداخل غير القانوني على النظام[1375] وإدخال البيانات بصورة غير قانونية[1376] والاعتراض غير قانوني للبيانات[1377] والتداخل غير القانوني على البيانات.[1378] وتظهر الأحكام الكثير من أوجه التشابه مع أفضل الممارسات المستمدّة من مناطق أخرى، بما في ذلك المعايير المطبقة في إفريقيا. ومن الأمثلة على ذلك تجريم المكوث غير القانوني في نظام الحاسوب الذي أدرجه مشروع توجيه الجماعة الاقتصادية لدول غرب إفريقيا.[1379]

المادة III-3:

يتعيّن على كل دولة عضو من الاتحاد الإفريقي اتخاذ التدابير التشريعية اللازمة لتجريم البقاء أو محاولة البقاء عن طريق الاحتيال في جزء أو في كامل نظام الحاسوب.

مفهوم واحد جديد – ولكنه ليس حكماً قانونياً جنائياً ولكنه إجراء جانبي لم تُدرجه في هذا الصدد الأُطُر الإقليمية الأخرى وهو العمل على إلزام دوائر الأعمال التجارية على إخضاع منتجاتها لاختبار الكشف عن مواطن الضعف.

المادة III-7:

[...]

2) يتعيّن على الدول الأعضاء اعتماد قواعد لإجبار بائعي منتجات تكنولوجيا المعلومات والاتصالات على إخضاع لاختبارات مواطن الضعف والضمان على أن يتولى إجراء هذه الاختبارات خبر مستقلون، وعلى إطلاع الجمهور على أي شكل من مواطن الضعف يتم اكتشافه في المنتجات المعنية والتدابير الموصى بها لإيجاد حل لها.

ويشمل القسم 2 تجريم جوانب التزوير ذو الصلة بالحاسوب[1380] والاستخدام غير المشروع للبيانات[1381] والتدخل غير القانوني في النظام بهدف الحصول على منفعة[1382] وحماية البيانات من الانتهاكات[1383] والأجهزة غير القانونية[1384] والمشاركة في منظمة إجرامية.[1385]

المادة III-9:

يتعيّن على كل دولة عضو في الاتحاد الإفريقي اتخاذ التدابير التشريعية اللازمة لتجريم استخدام البيانات المجمّعة مع الإدراك التام للحالة.

ويتجاوز تجريم الاستخدام غير المشروع للبيانات الحاسوبية على وجه الخصوص، المعايير التي حددتها معظم الصكوك الإقليمية الأخرى.

ويتناول القسم 3 تجريم المحتوى غير القانوني. وأدرك مشروع اتفاقية الاتحاد الإفريقي تجريم إنتاج المواد الإباحية التي يستغل فيها الأطفال ونشرها[1386] والحصول على هذه المواد وجلبها[1387] وتملكها[1388] وتيسير نفاذ القصّر[1389] إلى هذه المواد الإباحية[1390] ونشر مواد تنطوي على العنصرية وكره الأجانب[1391] والهجمات العنصرية المرتكبة من خلال أنظمة حاسوبية[1392] وإنكار الإبادة الجماعية أو الجرائم ضد الإنسانية أو استحسانها.[1393]

ويحتوي القسم الأخير من الفصل 1 أحكاماً تتناول بطريقة أوسع التشريعات المتعلقة بالجريمة السيبرانية ومدى قبول الأدلة الإلكترونية ("مادة إلكترونية مكتوبية").

المادة III-23-1: قوانين مكافحة الجريمة السيبرانية

يتعيّن على كل دولة عضو اعتماد التدابير التشريعية التي تراها فعالة لتعريف الجرائم الجنائية المادية كأفعال تؤثر في سرية أنظمة تكنولوجيا المعلومات والاتصالات وما يتصل بها من شبكات البنية التحتية وسلامتها وتوفرها واستدامتها؛ فضلاً عن التدابير الإجرائية التي تراها فعالة لإيقاف الجناة وملاحقتهم قضائياً. ويتعيّن دعوة الدول الأعضاء إلى مراعاة، حيثما كان ضرورياً، الخيار اللغوي المعتمد في النماذج التشريعية الدولية بشأن الجرائم السيبرانية مثل الخيار اللغوي الذي اعتمده مجلس أوروبا ودول الكومنولث.

المادة III-23-2:

يتعيّن على كل دولة عضو بالاتحاد الإفريقي اتخاذ التدابير التشريعية اللازمة لكفالة قبول المواد الإلكترونية المكتوبة فيما يتعلق بالمسائل الإجرامية لتحديد الجرائم بموجب القانون الجنائي شريطة تقديم هذه المواد المكتوبة خلال المداولات وأن تطرح للنقاش أمام القاضي وأن يتسنّى تحديد هوية الشخص مصدر هذه المواد المكتوبة على النحو الواجب وأن تكون هذه المواد المذكورة مُعدّة ومحتفظاً بها في ظل ظروف يُرجّح بأنها تضمن سلامتها.

وفيما يتعلق بالمادة II-23-1، على وجه الخصوص، فإن قصد القائمين بالصياغة غير مفهوم تماماً حيث إن الجرائم الواردة في الأجزاء السابقة من الفصل 1 تعرّف الجرائم كجرائم ضد سلامة الأنظمة الحاسوبية وتيسُّرها. وبالتالي فإنه من غير المؤكد مطالبة المادة II-23-1 الدول بتجاوز الجرائم التي سبق لمشروع اتفاقية الاتحاد تحديدها بمزيد من التفصيل.

ويحتوي الفصل الثاني على أحكام ترمي إلى تحديث الأحكام التقليدية لضمان القدرة على التطبيق متى تعلّق الأمر بأنظمة الحاسوب والبيانات. ويلزم هذا الفصل الدول الأعضاء بتشديد العقوبة إذا ما ارتكبت الجرائم التقليدية باستخدام تكنولوجيا المعلومات والاتصالات[1394] وتجريم التعدّي على الممتلكات بجرائم مثل السرقة أو استغلال الثقة أو الابتزاز المتعلق بالبيانات الحاسوبية[1395] وتحديث الأحكام التي تتضمن وسائل النشر لضمان تغطية استخدام وسائل الاتصال الإلكتروني الرقمي[1396] وضمان أن الأحكام التي تحمي السرية لاعتبارات الأمن الوطني تنطبق فيما يتعلق بالبيانات الحاسوبية.[1397] وهذه الأحكام غير مُدرجة في الأُطر الإقليمية الأخرى. وفيما يتعلق بالمادة III-24، فإنه من غير المؤكد كيف أن مجرد استخدام نظام حاسوبي في مرحلة محددة من ارتكاب الجريمة التقليدية (يرسل الجُناة رسالة إلكترونية قبل اقتحام مصرف عوضاً عن إجراء مكالمة هاتفية) يؤدي إلى تشديد العقوبة.

المادة III-24:

يتعيّن على كل دولة عضو في الاتحاد الإفريقي اتخاذ التدابير التشريعية اللازمة لتنص على أن استخدام تكنولوجيا المعلومات والاتصالات لارتكاب الجرائم الواردة في القانون العرفي مثل السرقة والتحايل وامتلاك مسروقات واستغلال الثقة وابتزاز الأموال والإرهاب وغسيل الأموال وغيرها ظرف مشدّد.

وتتناول المادة III-28 والمادة III-35 موضوعا المسؤولية والعقوبات.

ويتناول القسم III القانون الإجرائي. وهو يلزِم الدول الأعضاء بتمكين الحفاظ على البيانات[1398] الحاسوبية والاستيلاء[1399] على البيانات الحاسوبية وعمليات الحفظ المعجّلة[1400] واعتراض اتصالات البيانات.[1401] وحتى يوليو 2014، لم تُعتمد الاتفاقية بعد.[1402]

7.2.5 الجامعة العربية ومجلس التعاون لدول الخليج[1403]

اتخذ بالفعل عدد من البلدان في المنطقة العربية تدابير وطنية واعتمد نهجاً لمكافحة الجريمة السيبرانية، أو هو بصدد صوغ تشريعات في هذا الشأن.[1404] ومن أمثلة هذه البلدان: باكستان،[1405] ومصر،[1406] والإمارات العربية المتحدة (UAE).[1407] وسعياً نحو مواءمة التشريعات في المنطقة، قدّمت الإمارات العربية المتحدة تشريعات نموذجية للجامعة العربية (القانون الموجه لمحاربة جرائم تكنولوجيا المعلومات)[1408] وفي عام 2003، اعتمد مجلسا وزراء الداخلية والعدل العرب هذا القانون[1409] وأوصى مجلس التعاون لدول الخليج (GCC)[1410] في مؤتمر عُقد في عام 2007 بأن تسعى بلدان المجلس إلى اتباع نهج مشترك يأخذ المعايير الدولية في الاعتبار.[1411]

8.2.5 منظمة الدول الأمريكية[1412]

تعكف منظمة الدول الأمريكية (OAS) بشكل نشط منذ عام 1999 على معالجة قضية الجريمة السيبرانية داخل المنطقة التي تُعنى بها. وقامت المنظمة، ضمن ما اضطلعت به من أنشطة في هذا الصدد، بعقد عدد من الاجتماعات في إطار ولاية عمل وزراء العدل أو الوزراء الآخرين أو النواب العاملين في الأمريكتين.[1413]

فريق الخبراء الحكومي الدولي المعني بالجريمة السيبرانية

ففي عام 1999، أوصى اجتماع وزراء العدل والوزراء والمدّعين العامين في الأمريكتين بإنشاء فريق خبراء حكومي دولي معني بالجريمة السيبرانية. وفوّض فريق الخبراء في القيام بوضع تشخيص كامل للنشاط الإجرامي الذي يستهدف الحواسيب

والمعلومات، أو الذي يستخدم الحواسيب كوسيلة لارتكاب الجريمة؛ ووضع تشخيص كامل للتشريعات والسياسات والممارسات الوطنية المتعلقة بهذا النشاط؛ وتعيين الكيانات الوطنية والدولية التي تملك الخبرة في هذا الصدد؛ وأخيراً تحديد آليات التعاون في إطار منظومة الدول الأمريكية لمكافحة الجريمة السيبرانية.

توصيات وزراء العدل

عقد وزراء العدل والوزراء والمدّعون العامون في الأمريكتين ثمانية اجتماعات حتى عام 2010[1414] وخلال الاجتماع الثالث الذي عُقد في عام 2000، بحث وزراء العدل أو المدّعون العامون في الأمريكتين موضوع الجريمة السيبرانية واتفقوا على عدد من التوصيات.[1415] وتشمل هذه التوصيات 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، أو يواصل دعم إعداد الاستراتيجية. وأوصى الاجتماع بأن تستعرض الدول الأعضاء 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 24/7 التي أنشأتها مجموعة الثمانية للمساعدة في التحقيقات المتعلقة بالجريمة السيبرانية. وطلب إلى الدول الأعضاء تقييم مدى استصواب تنفيذ المبادئ الواردة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والنظر في إمكانية الانضمام إلى تلك الاتفاقية. وبالإضافة إلى الولايات المتحدة وكندا اللتين وقّعتا على الاتفاقية بشأن الجريمة السيبرانية في عام 2001، دعا مجلس أوروبا في هذه الأثناء شيلي وكوستاريكا والجمهورية الدومينيكة والمكسيك إلى الانضمام إلى الاتفاقية. وأخيراً دعت التوصيات أن تستعرض الدول الأعضاء في منظمة الدول الأمريكية وأن تُحي، إذا كان ذلك ملائماً، هيكل وعمل الهيئات المحلية، أو الوكالات المعنية بإنفاذ القوانين كي تتكيّف مع الطبيعة المتحوّلة 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 أو المدّعين العامين في الأمريكتين لعام 2002، بأن يجري، في إطار أنشطة فريق العمل التابع للمنظمة المتعلقة بمتابعة توصيات وزراء العدل، دعوة فريق الخبراء الحكوميين المعني بالجريمة السيبرانية[1416] إلى الانعقاد مجدداً وتفويضه بمتابعة تنفيذ التوصيات التي أعدها ذلك الفريق والتي اعتمدها وزراء العدل في الأمريكتين في اجتماعهم الثالث والنظر في إعداد صكوك قانونية وتشريعات نموذجية ملائمة للدول الأمريكية بغرض تعزيز التعاون في نصف الكرة الغربي على مكافحة الجريمة السيبرانية والنظر في المعايير المتعلقة بالخصوصية وحماية المعلومات والجوانب الإجرائية ومنع الجريمة.

وكان من بين التوصيات المنبثقة عن الاجتماع السادس لوزراء العدل[1417] الدعوة إلى مواصلة تعزيز التعاون مع مجلس أوروبا، بحيث تنظر الدول الأعضاء في منظمة الدول الأمريكية في تطبيق المبادئ الواردة في الاتفاقية بشأن الجريمة السيبرانية[1418] والانضمام إليها، واعتماد التدابير القانونية والتدابير الأخرى المطلوبة لتنفيذها. وبالمثل، أوصى الاجتماع أن تتواصل الجهود من أجل تقوية آليات تبادل المعلومات والتعاون مع المنظمات والوكالات الدولية الأخرى في مجال الجريمة السيبرانية، مثل الأمم المتحدة والاتحاد الأوروبي ومنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ ومنظمة التعاون والتنمية في الميدان الاقتصادي ومجموعة الثمانية والكومنولث والإنتربول، كي تنتفع الدول الأعضاء في منظمة الدول الأمريكية من التقدّم المحرز في تلك المحافل. وطلب إلى الدول الأعضاء أيضاً أن تُنشئ وحدات متخصصة للتحقيق في الجريمة السيبرانية وأن تعين السلطات التي ستقوم بدور جهات الاتصال في هذا المجال وأن تعجّل بتبادل المعلومات والحصول على الأدلة وأن تقوم، علاوةً 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[1419] الذي أوصى فضلاً عن ذلك بأن 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. وبالمثل أوصى الاجتماع بأن يتواصل 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 المحرَز في تلك المحافل. وأخيراً طلب إلى أمانة لجنة الدول الأمريكية لمكافحة الإرهاب (CICTE) وأمانة لجنة الدول الأمريكية للاتصالات (CITEL) وفريق العمل المعني بالجريمة السيبرانية مواصلة 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).

وفي عام 2010، تناول اجتماع وزراء العدل أو المدعين العامين قضية الجريمة السيبرانية في اجتماعهم الثامن.[1420] وناقشوا بإيجاز أهمية مواصلة تعزيز بوابة البلدان الأمريكية المخصصة للتعاون في مجال الجريمة السيبرانية من خلال صفحة منظمة الدول الأمريكية على الإنترنت وتحديثها وتقوية قدرات الدول على وضع تدابير تشريعية وإجرائية تتعلق بالجريمة السيبرانية والأدلة الإلكترونية. وعلاوةً على ذلك، سلّطت التوصيات المنبثقة عن الاجتماع الضوء على الرغبة في تقوية الآليات التي تسمح بتبادل المعلومات والتعاون مع المنظمات والوكالات الدولية الأخرى في مجال الجريمة السيبرانية، ومجلس أوروبا والأمم المتحدة والاتحاد الأوروبي ومنتدى التعاون الاقتصادي لآسيا 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 الكيانات.

وخلال الاجتماع الذي عقد في 2012، تناول وزراء العدل مرة أخرى مختلف جوانب الجريمة السيبرانية.[1421] وأدرك المشاركون أهمية وحدات الجريمة السيبرانية المحددة.[1422] وبالإضافة إلى ذلك، دعوا الدول الأعضاء إلى النظر في النظام القانوني لديها، واعتماد التشريعات اللازمة فيما يتعلق بقانون الإجراءات والأدلة الإلكترونية والمحاكمات الجنائية.[1423] وتشمل التوصية أيضاً الدعوة إلى وضع استراتيجية للأمن السيبراني تتضمن تدابير لمكافحة الجريمة السيبرانية. ومن القضايا الأخرى التي طرحت تثقيف المواطنين والاعتراف بنتائج مؤتمر الأمم المتحدة لمنع الجريمة. وخلافاً لما كان الحال في السنوات الأولى، لا تدعو التوصية للتصديق على اتفاقية الجريمة السيبرانية بل تستخدم لغة أكثر ليونة وتدعو الدول الأعضاء إلى "الاعتراف بالاعتبار الذي أولته بعض الدول الأعضاء في منظمة الدول الأمريكية لتطبيق مبادئ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والانضمام إليها ... ".[1424]

واعتمد اجتماع عام 2014[1425] توصيات تتماشى إلى حد كبير مع توصيات الاجتماعات السابقة. وكان من أحد العناصر الجديدة الإعلان بأن وضع تشريع نموذجي قد أخذ في الاعتبار.[1426]

9.2.5 منطقة الكاريبي

في ديسمبر 2008، أطلق الاتحاد الدولي للاتصالات والاتحاد الأوروبي مشروع "تقوية المنافسة في منطقة الكاريبي من خلال مواءمة سياسات تكنولوجيا المعلومات والاتصالات والإجراءات التشريعية والتنظيمية" (HIPCAR) للنهوض بقطاع تكنولوجيا المعلومات والاتصالات في منطقة الكاريبي ويشكل المشروع جزءاً من برنامج "تكنولوجيا المعلومات والاتصالات في بلدان إفريقيا والكاريبي والهادئ" وصندوق التنمية الأوروبي التاسع. أما البلدان المستفيدة فهي 15 بلداً في منطقة الكاريبي.[1427] ويهدف المشروع إلى مساعدة منتدى بلدان منطقة الكاريبي[1428] على مواءمة سياساتها وأُطُرها القانونية في مجال تكنولوجيا المعلومات والاتصالات.[1429]

وفي إطار هذا المشروع، حددت تسعة مجالات عمل[1430] وضعت فيها سياسات نموذجية ونصوص تشريعية نموذجية لتسهيل تطوير التشريعات في المنطقة ومواءمتها. وكانت الجريمة السيبرانية واحدة من مجالات العمل التسعة. ووضع النص التشريعي النموذجي على ثلاث مراحل. ففي المرحلة الأولى، جمعت التشريعات القائمة في البلدان المستفيدة واستعرضت. وفي موازاة ذلك، حددت أفضل الممارسات الإقليمية والدولية. وأُعطيت الأولوية للمعايير التي يمكن تطبيقها مباشرة على الأقل في بعض البلدان المستفيدة (مثل القانون النموذجي للكومنولث من عام 2002). ومع ذلك، شمل الاستعراض أيضاً أفضل الممارسات من المناطق الأخرى، مثل الاتحاد الأوروبي وإفريقيا. واحتوى تقرير التقييم[1431] لمحة عامة عن التشريعات القائمة، فضلاً عن تحليل مقارن للقوانين قارن بين التشريعات القائمة وأفضل الممارسات الإقليمية والدولية. وسعياً نحو إعداد تحليل للثغرات، حدد تقرير التقييم أيضاً الاحتياجات الخاصة في المنطقة (مثل التشريعات المتعلقة بالرسائل الاقتحامية) التي لا تعالج بالضرورة بواسطة أفضل

الممارسات الدولية. وفي إطار ورشة عمل نظمت في عام 2010، نوقش تقرير التقييم مع أصحاب المصلحة من البلدان المستفيدة.[1432] على أساس تقرير التقييم وتحليل الثغرات، وضعت الجهات المعنية مبادئ توجيهية نموذجية بشأن السياسات.

وفي المرحلة الثانية، وضع نص تشريعي نموذجي أخذ في الاعتبار المبادئ التوجيهية بشأن السياسات. وفي ورشة عمل ثانية، ناقش خبراء في السياسة العامة وواضعو القوانين وغيرهم من أصحاب المصلحة من البلدان المستفيدة، مشروع النص التشريعي النموذجي الذي أُعِدَّ للاجتماع وعدلوه واعتمدوه. وينطوي النص التشريعي النموذجي على ثلاثة أهداف رئيسية وهي: أنه يوفر عيّنة لغوية محددة تتماشى مع افضل الممارسات الدولية وتعبّر عن المتطلبات الخاصة للمنطقة، وأن يوضع النص بحيث يُراعي ممارسات صياغة القوانين في المنطقة، وذلك لضمان سلاسة التنفيذ. ويحتوي النص التشريعي النموذجي على مجموعة معقدة من التعاريف وأحكام القانون الجنائي الموضوعي، بما في ذلك الأحكام التي تتناول قضايا مثل الرسائل الاقتحامية التي لها أولوية قصوى بالنسبة إلى المنطقة ولكنها ليست بالضرورة واردة في الأُطُر الإقليمية مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

15.(1) أي شخص، يقوم عمداً، وبدون سند أو مُبرِّر قانوني بالآتي:

أ) يبدأ عمداً في إرسال العديد من رسائل البريد الإلكتروني من نظام حاسوبي أو بواسطته؛ أو

ب) يستخدم نظاماً حاسوبياً محمياً لترحيل أو إعادة إرسال العديد من رسائل البريد الإلكتروني بقصد خداع أو تضليل المستخدمين، أو أي مورّد خدمة بريد إلكتروني أو إنترنت، فيما يتعلق بمصدر هذه الرسائل؛ أو

ج) يزيف مادياً معلومات رأسية في العديد من رسائل البريد الإلكتروني ويبدأ عمداً في إرسال هذه الرسائل؛

يرتكب جريمة يعاقب عليها القانون، في حالة إدانته، بالحبس لمدة لا تزيد على [فترة] أو بغرامة لا تزيد على[المبلغ]، أو الاثنين.

(2) ويجوز للدولة تقييد التجريم فيما يتعلق بإرسال رسائل البريد الإلكتروني المتعددة ضمن علاقات العملاء أو دوائر الأعمال التجارية. ويجوز للبلد أن يقرر عدم تجريم السلوك في المادة 15 (1) (أ) شريطة توفير سبل علاج فعالة أخرى.

وعلاوةً على ذلك، يحتوي النص على أحكام قانون الإجراءات (بما في ذلك أدوات التحقيق المتقدمة مثل استخدام أدوات الأدلة الجنائية عن بُعد) والأحكام المتعلقة بمسؤولية مورّدي خدمة الإنترنت (ISP).

10.2.5 منطقة المحيط الهادئ

بالتوازي مع المشروع الممول من الاتحاد الدولي للاتصالات والاتحاد الأوروبي في منطقة البحر الكاريبي، أطلقت نفس المنظمتين مشروعاً في منطقة المحيط الهادئ (ICB4PAC)[1433] ويهدف المشروع – بناءً على طلب من البلدان الجزري في المحيط الهادئ – إلى توفير بناء القدرات المتصلة بسياسات تكنولوجيا المعلومات والاتصالات ولوائحها. وفي هذا الصدد، يركز المشروع على بناء القدرات البشرية والمؤسسية في مجال تكنولوجيا المعلومات والاتصالات من خلال التدريب والتعليم وتدابير تقاسم المعرفة. والبلدان المستفيدة هي 15 بلداً من البلدان الجزرية في المحيط الهادئ.[1434] وفي مارس 2011، أنظمة في فانواتو ورشة عمل تتناول تشريعات الجريمة السيبرانية الحالية في منطقة المحيط الهادئ.[1435] وخلال ورشة العمل عرض تحليل قانوني مقارن شامل قدم لمحة عامة عن التشريعات القائمة في المنطقة، فضلاً عن مقارنة أفضل الممارسات المستمدة من مناطق أخرى.[1436] وكمتابعة لهذه الورشة نظم مؤتمر يتناول تقنيات وضع السياسات والتشريعات المتعلقة بالجريمة السيبرانية في أغسطس 2011 في ساموا. وخلال المؤتمر، عرضت أفضل الممارسات من المناطق الأخرى وأُنشئت الهياكل اللازمة لوضع سياسات وتشريعات منسقة. وتناولت القانون الجنائي الموضوعي والقانون الإجرائي والتعاون الدولي ومسؤولية مورد خدمة إنترنت (ISP) والأدلة الإلكترونية وتدابير منع الجريمة.[1437]

وفي أبريل 2011، نظمت الأمانة العامة لمجموعة بلدان المحيط الهادئ[1438] مؤتمراً يتعلق بمكافحة الجريمة السيبرانية في منطقة المحيط الهادئ. وشارك مجلس أوروبا في تنظيم الحدث. ونوقش خلال المؤتمر جوانب متعلق بالقانون الجنائي الموضوعي والقانون الإجرائي والتعاون الدولي.[1439]

11.2.5 الجماعة الإنمائية للجنوب الإفريقي (SADC)

اعتمدت الجماعة الإنمائية للجنوب الإفريقي (SADC) تشريعات نموذجية تتبع نهجاً مماثلاً لنهج الاتحاد الإفريقي. وهي تتناول قضايا حماية البيانات[1440]، والتجارة الإلكترونية[1441] والجريمة السيبرانية.[1442]

3.5 النُّهُج العلمية والمستقلة

1.3.5 مشروع اتفاقية ستانفورد الدولية

من الأمثلة المعروفة للنهج العلمي في وضع إطار قانوني للتصدي للجريمة السيبرانية على المستوى العالمي مشروع اتفاقية ستانفورد الدولية ("مشروع ستانفورد").[1443] وقد أُعد مشروع ستانفورد في إطار متابعة مؤتمر استضافته جامعة ستانفورد بالولايات المتحدة في عام 1999[1444] وتُظهر مقارنة المشروع باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية،[1445] التي صِيغت 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 مجلس أوروبا بشأن الجريمة السيبرانية يمكن أن تنطبق على الجرائم التقليدية أيضاً.[1446]

2.3.5 البروتوكول العالمي بشأن الأمن السيبراني والجريمة السيبرانية

خلال منتدى إدارة الإنترنت في مصر في عام 2009، قدم كل من السيد شولبارغ والسيدة غرناؤوطي–هيلي اقتراحاً حول بروتوكول عالمي بشأن الأمن السيبراني والجريمة السيبرانية.[1447] وتتصل المادة 1-5 بالجريمة السيبرانية وتوصي بتنفيذ أحكام القانون الجنائي الموضوعي وأحكام قانون الإجراءات والتدابير المضادة لإساءة استخدام الإرهابيين للإنترنت وتدابير للتعاون الدولي وتبادل المعلومات وتدابير بشأن الخصوصية وحقوق الإنسان.[1448] ويستند التشريع النموذجي الوارد في التذييل لهذا البروتوكول إلى حد كبير (المادة 1-25) إلى صياغة الأحكام التي توفرها اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

وفي يونيو 2014، قدمت Scholberg الطبعة التاسعة من مشروع معاهدة الأمم المتحدة بشأن إنشاء محكمة جنائية أو هيئة قضائية دولية للفضاء السيبراني.[1449] والنهج العلمي، الذي لا يقوم على ولاية رسمية للأمم المتحدة، يؤكد التحديات التي تواجه الولاية القضائية في الفضاء السيبراني ويضع مفهوم محكمة دولية ذات ولاية قضائية محدودة على غرار محكمة العدل الدولية الدائمة.

4.5 العلاقة بين النُّهُج التشريعية الإقليمية والدولية المختلفة

يدعو نجاح معايير شتى تأخذ بها البروتوكولات التقنية إلى التساؤل عن كيفية تجنّب الصراعات بين النهج الدولية المختلفة.[1450] وتشكل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والقانون النموذجي لكومنولث الدول المستقلة بشأن الجريمة السيبرانية الأُطُر التي تتبع أكثر النهج شمولاً حيث إنها تشمل القانون الجنائي الموضوعي وقانون الإجراءات والتعاون الدولي. ولكن لم يخضع أي صك حتى الآن للتعديل لمعالجة التطورات التي حدثت في السنوات الأخيرة. وعلاوةً على ذلك، فإن نطاق الصكين محدود. وقد سلّطت المداولات التي جرت خلال مؤتمر الأمم المتحدة حول الجريمة الضوء على اهتمام البلدان بالصكوك الدولية.[1451] ويثير ذلك تساؤلات تتصل بالعلاقة بين النهج الإقليمية والإجراءات الدولية المحتملة. وتوجد ثلاثة سيناريوهات محتملة.

فإذا حدد نهج قانوني جديد معايير لا تتفق مع النهج المتسقة الراهنة على المستويين الإقليمي والوطني، فقد يكون ذلك، على الأقل في البداية، أثر سلبي على عملية تحقيق التواؤم الضرورية. وبالتالي فإنه من المرجح أن يحلل أي نهج جديد المعايير القائمة

بدقة لضمان الاتساق. ومن الأمثلة على ذلك تجريم النفاذ غير القانوني الذي يعرّف بطريقة مشابهة من قبل القسم 5 من القانون النموذجي للكومنولث بشأن الجريمة السيبرانية والمادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

وزيادة على ذلك، يمكن للنهج الجديد تجنب إدراج الأحكام التي أدت إلى صعوبات في التطبيق أو حتى منعت بعض البلدان من الانضمام إلى صك ما. ومن الأمثلة على ذلك الحكم الذي كان موضع خلاف في المادة 32ب من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. فقد انتقد الوفد الروسي هذا الحكم إبان الاجتماع الذي عقدته لجنة الجريمة السيبرانية في عام 2007.[1452]

وأخيراً بإمكان نهج دولي جديد، علاوةً على تضمّنه معايير أساسية تتشابه في مختلف النهج القانونية، التركيز على تحليل الثغرات لتحديد المجالات التي لم تعالج بالقدر الكافي وبالتالي تجريم أعمال معينة تتعلق بالجريمة السيبرانية وتحديد أدوات إجرائية لم تتعرض لها الصكوك القائمة بعد. فمنذ عام 2001، استجد عدد من التطورات الهامة. فحين صيغت اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لم تكن جرائم "التصيّد الاحتيالي"،[1453] و"انتحال الهوية"[1454] والجرائم المتعلقة بالألعاب المتاحة على الخط والشبكات الاجتماعية تتسم بنفس القدر من الأهمية الذي اكتسبته منذ ذلك الحين. وبمقدور نهج دولي جديد أن يواصل عملية تحقيق التواؤم بإدراج مزيد من الجرائم ذات البعد الدولي.[1455]

5.5 العلاقة بين النُّهُج التشريعية الوطنية والدولية

تُعدّ الجريمة السيبرانية بحق، كما سَلَفَت الإشارة، جريمة عبر وطنية.[1456] ولما كان الجناة يستطيعون، بوجه عام، أن يستهدفوا مستخدمين موجودين في أي بلد في العالم، فإن التعاون الدولي لوكالات إنفاذ القانون يُعد شرطاً جوهرياً للتحقيقات الدولية في الجريمة السيبرانية.[1457] فالتحقيقات تقتضي التعاون وتعتمد على تحقيق التواؤم بين القوانين. وإعمالاً للمبدأ المشترك المتعلق بالإجرام المزدوج،[1458] يتطلب التعاون الفعال، بادئ ذي بدء، تحقيق التواؤم بين الأحكام الموضوعية للقانون الجنائي للحيلولة دون توافر ملاذات آمنة.[1459] 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.[1460] ولذا، فإن أهمية تحقيق التواؤم، تثير الحاجة إلى المشاركة في عملية تحقيق التواؤم هذه على الصعيد العالمي التي تشكل على الأقل اتجاهاً، إن لم تشكل 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 مازالت لم تستكمل إلى حد بعيد.[1461] ومن أسباب اضطلاع النهج الوطنية بدور هام في مكافحة الجريمة السيبرانية أن تأثير الجرائم ليس واحداً في كل مكان. ومن الأمثلة على ذلك، النهج المتّبع في مكافحة الرسائل الاقتحامية.[1462] فهذه الرسائل تؤثر بوجه خاص على البلدان النامية، وقد حُلِّلت هذه المسألة في تقرير صادر عن منظمة التعاون والتنمية في الميدان الاقتصادي.[1463] فلما كانت الموارد في البلدان النامية أكثر ندرة وأعلى تكلفة، فإن الرسائل الاقتحامية تُعد مشكلة أخطر في هذه البلدان عنها في البلدان الغربية.[1464] 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.[1465] واتباع معايير واحدة شرط جوهري لتشغيل الشبكات. غير أن المعايير القانونية مازالت تتباين، على عكس المعايير التقنية.[1466] ويجب التساؤل عن مدى فعالية النهج الوطنية في ضوء البعد الدولي للجريمة السيبرانية.[1467] وهذا سؤال له أهميته لجميع النهج الوطنية والإقليمية التي تطبّق 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 تتجنّب ما يُصادف لدى إجراء التحقيقات الدولية من مشكلات وصعوبات.[1468]

وثمة سببان رئيسيان لتزايد عدد النهج الإقليمية والوطنية. والسبب الأول هو السرعة التشريعية. فليس بمقدور الكومنولث ولا مجلس أوروبا إجبار أي من الدول الأعضاء فيهما باستخدام صكوكهما. ومجلس أوروبا على وجه الخصوص، ليس لديه صك لتكليف أي من موقعي الاتفاقية بشأن الجريمة السيبرانية للتصديق عليها. ولذا تعتبر عملية تحقيق التواؤم في كثير من الأحيان عملية بطيئة بالقياس إلى النهج التشريعية الوطنية والإقليمية.[1469] أما الاتحاد الأوروبي فيملك، خلافاً لمجلس أوروبا، وسائل لإلزام الدول الأعضاء بتنفيذ المقررات والتوجيهات الإطارية. وهذا هو السبب الذي يوضح لماذا عمد عدد من بلدان الاتحاد الأوروبي التي وقّعت 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.[1470] وعلى الرغم من أن تحقيق التواؤم الدولي بين أحكام القانون الجنائي المتعلقة بالجرائم ضد الرموز الدينية لن يكون ممكناً على الارجح، فإن اتباع نهج وطني يمكنه أن يضمن في هذا الصدد إمكانية الحفاظ على المعايير القانونية المطبّقة 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.[1471] فإذا ما أتى الجناة بأفعالهم في بلد لا يجرم سلوكاً معيناً، فإن التحقيقات الدولية، فضلاً عن طلبات تسليم الجناة، ستُمنى بالفشل في كثيرٍ من الأحيان. ولذا، فإن من الأهداف الرئيسية للنهج القانونية الدولية الحيلولة دون إيجاد تلك الملاذات الآمنة عن طريق وضع وتطبيق معايير عالمية.[1472] وبناء على ذلك، تتطلّب النهج الوطنية بوجه عام تدابير جانبية إضافية كي تصبح مؤثرة.[1473] 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 مقدّم الخدمات الذي يعمل من الخارج.

تجريم الخدمات المستخدمة في ارتكاب الجريمة

يتمثل 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.[1474]

ومما يتعلق عن كثب بهذا التدبير فرض التزامات بترشيح محتوى معين متاح على الإنترنت.[1475] وقد نوقش هذا النهج في إطار القرار الشهير المتعلق بياهو Yahoo،[1476] وهو يناقش في الوقت الحاضر في إسرائيل، حيث قد يُضطر مقدمو خدمة النفاذ إلى تقييد النفاذ إلى مواقع الويب التي تضمن 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 (OpenNetInitiative)[1477] أن هذا النوع من الرقابة يمارس من جانب ما يزيد على عشرين بلداً.[1478]

1047 This includes regional approaches.

1048 The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, United Kingdom, United States and the Russian Federation. The presidency of the group, which represents more than 60 per cent of the world economy (source: http://undp.org), rotates every year.

1049 The idea of the creation of five subgroups – among them, one on high-tech crimes – was to improve implementation of the 40 recommendations adopted by G8 Heads of State in 1996.

1050 The establishment of the subgroup (also described as the subgroup to the "Lyon Group") continued the efforts of the G8 (at that time still G7) in the fight against organized crime, which started with the launch of the Senior Experts Group on Organized Crimes (the "Lyon Group") in 1995. At the Halifax summit in 1995, the G8 stated: "We recognize that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from drug trafficking and other serious crimes. To implement our commitments in the fight against transnational organized crime, we have established a group of senior experts with a temporary mandate to look at existing arrangements for cooperation both bilateral and multilateral, to identify significant gaps and options for improved coordination and to propose practical action to fill such gaps". See: Chairman's Statement, Halifax G7 Summit, June 17 1995. For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1051 Regarding the G8 activities in the fight against cybercrime, see also: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1052 "Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October 1999.

1053 14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

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

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

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries.

Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

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

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

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

1054 The idea of a 24/7 network has been picked up by a number of international approaches in the fight against cybercrime. One example is Article 35 of the Convention on Cybercrime:

(1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) the preservation of data pursuant to Articles 29 and 30;

c) the collection of evidence, the provision of legal information, and locating of suspects. […]

1055 *Jean-Pierre Chevenement*, the French Minister of the Interior, stated: "Now that the G8 has provided the impetus, it's vital that we formalize the new legal rules and procedures for cooperation in a legal instrument applying world-wide. For France, the negotiations under way in the Council of Europe on a Convention on Cyber-Crime are of fundamental importance for several reasons. The draft currently under discussion defines the offences which all States would have to recognize. It goes on to propose ways in which they could cooperate, taking up, for example, the idea of national contact points. It also proposes extradition procedures. In short, this agreement is an essential instrument, which France wants to see concluded within a reasonable period of time. The important thing about these negotiations is that the countries involved include some major countries outside the Council of Europe and that, once signed, this convention will be opened for signature by all States wishing to accede to it. The idea is in fact to get a convention which applies world-wide so that there can be no more "digital havens" or "Internet havens" in which anyone wanting to engage in shady activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must never lose sight of the fact that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate."

1056 G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

1057 The experts expressed their concerns regarding implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible"; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001.

1058 G8 Justice and Home Affairs Communiqué, Washington DC, 11 May 2004.

1059 G8 Justice and Home Affairs Communiqué Washington DC, 11 May 2004:10. "Continuing to Strengthen Domestic Laws: To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."

1060 The participants expressed their intention to strengthen the instruments in the fight against cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors". See: www.g7.utoronto.ca/justice/justice2006.htm.

1061 Regarding the topic of cyberterrorism, see above: § 2.9.1. In addition, see: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis,* Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeldt*, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

1062 The summit declaration calls for measures in the fight against cyberterrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists". For more information, see: http://en.g8russia.ru/docs/17.html.

1063 For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1064 Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 6, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

1065 Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 7, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

1066 G8 Summit 2010 Muskoka Declaration, 2010, available at: www.g7.utoronto.ca/summit/2010muskoka/communique.html.

1067 See press release from 30.5.2011, available at: www.eg8forum.com/en/documents/news/Final_press_release_May_30th.pdf.

1068 See G8 Declaration, Renewed Commitment for Freedom and Democracy, available at: www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html.

1069 The United Nations (UN) is an international organization founded in 1945. It had 192 Member States in 2010.

1070 A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.

1071 A/RES/45/121, adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.

1072 UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at www.uncjin.org/Documents/EighthCongress.html.

1073 See the preface to the Optional Protocol.

1074 See Art. 2.

1075 See especially the background paper: Crimes related to computer networks, A/CONF.187/10.

1076 Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.

1077 Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 174, available at: www.uncjin.org/Documents/congr10/15e.pdf.

1078 "The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks".

1079 A/RES/55/63. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

1080 A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

1081 A/RES/57/239, on Creation of a global culture of cybersecurity; A/RES/58/199, on Creation of a global culture of cybersecurity and the protection of critical information infrastructure.

1082 Measures to Combat Computer-related Crime, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, A/CONF.203/14.

1083 Committee II Report, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19.

1084 Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

1085 30(d): "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

1086 Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

1087 See in this context especially the background paper prepared by the secretariat.

1088 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1089 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1090 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

1091 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

1092 *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

1093 Regarding the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

1094 Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

1095 Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

1096 Resolutions 55/63 and 56/121.

1097 Resolutions 57/239 and 58/199.

1098 Draft topics for consideration in a comprehensive study on the impact o fand response to cybercrime, 2010, UNODC, UNODC/CCPCJ/EG.4/2011/2.

1099 Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive studay of the problem of cybercrime held in Vienna from 17 to 21 January 2011, UNODC/CCPCJ/EG.4/2011/3.

1100 www.unodc.org/cybercrime-study/

1101 UNODC Press Release (26.01.2012) available at: www.unodc.org/unodc/en/frontpage/2012/January/unodc-chief-announces-a-comprehensive-study-on-cybercrime.html

1102 United Nations Commission on Crime Prevention and Criminal Justice.

1103 www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

1104 Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, page X.

1105 Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, S. XIX.

1106 UNODC/CCPCJ/EG.4/2013/3.

1107 Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

1108 Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

1109 Commission on Crime Prevention and Criminal Justice, Report on the twenty-thrid session (13 December 2013 and 12 to 16 May 2014), Economic and Social Council, Official Records,2014, Supplement No. 10

1110 Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

1111 Development in the Field of Information and Telecommunications in the Context of International Security, 2013, available at: www.un.org/disarmament/topics/informationsecurity/

1112 See: Development in the Field of Information and Telecommunications in the Context of International Security, 2013, page 1.

1113 The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf.

1114 Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

1115 The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council.

1116 CCPCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process in the development of the resolution and for an overview of different existing legal instruments, see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, see: www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

1117 The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

1118 ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

1119 For more information on the development process and the work of the intergovernmental expert group, see: Results of the second meeting of the Intergovernmental Expert Group to Prepare a study on Fraud and the Criminal Misuse and Falsification of Identity, Commission on Crime Prevention and Criminal Justice, 16th session, 2007, E/CN.15/2007/8, page 2.

1120 ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

1121 Regarding Internet-related ID-theft, see above: § 2.8.3, and below: § 6.2.16.

1122 ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.

1123 ECOSOC Resolution 2004/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

1124 Reports related to the activities of the working group are published. See: First meeting of the Core Group of Experts on Identity-Related Crime, Courmayeur Mont Blanc, Italy, 29-30 November 2007, available at: www.unodc.org/documents/organized-crime/Courmayeur_report.pdf (last visited: October 2008); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, available at: www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf (last visited: October 2008).

1125 See for example: Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, 2009, E/CN.15/2009/CRP.13.

1126 ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

1127 For further information see: www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html.

1128 The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. For more information, see: www.itu.int.

1129 WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

1130 WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

1131 For more information on Action Line C5, see: 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: www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, available at: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

1132 For more information, see www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

1133 www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

1134 The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building, international cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

1135 See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

1136 www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; See: *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2009, Issue 7, page 533.

1137 See, in this context: *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1, page 7 *et seq.*

1138 Global Strategic Report, Chapter 1.6.

1139 Global Strategic Report, Chapter 1.7.

1140 Global Strategic Report, Chapter 1.10.

1141 Global Strategic Report, Chapter 1.11.

1142 23-25 November 2009 (Santo Domingo, Dominican Republic): www.itu.int/ITU-D/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa; 15-18 July 2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information

Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP); 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP).

1143 Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/

1144 For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

1145 Information about the project are available at: www.itu.int/ITU-D/treg/projects/itu-ec/index.html

1146 The adoption took place during the 3rd Ordinary General Assembly of the West African Telecommunications Regulators Assembly.

1147 www.itu.int/ITU-D/treg/projects/itu-ec/ECOWAS_MINISTERS_ADOPTS_GUIDELINES_FOR_TELECOMMUNICATION_MARKET_AT_ABUJA.pdf

1148 http://news.ecowas.int/en/presseshow.php?nb=2&lang=en&annee=2007

1149 Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cap-Verde, Chad, Congo, Cote d'Ivoire, Eritrea, Gabon, Gambia, Ghana, Guinea, Guinea Equatorial, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Uganda, Central African Republic, Democratic Republic of Congo, Rwanda, Sao Tome-e-Principe, Senegal, Seychelles, Sierra Leone, South Africa, Swaziland, Tanzania, Togo, Zambia and Zimbabwe.

1150 ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 5.

1151 The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

1152 CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

1153 Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

1154 Detailed information about requested support, activities and documents are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

1155 For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html

1156 Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

1157 The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

1158 Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

1159 The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD and UN. Source: *Nilsson* in *Sieber*, Information Technology Crime, page 577.

1160 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1161 *Nilsson* in Sieber, Information Technology Crime, page 576.

1162 Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

1163 Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

1164 The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.

1165 Decision CDPC/103/211196. CDPC explained its decision by pointing out the international dimension of computer crimes: "By connecting to communication and information services, users create a kind of common space, called "cyber-space", which is used for legitimate purposes, but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."

1166 Explanatory Report of the Convention on Cybercrime (185), No. 10.

1167 The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

1168 For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

1169 Albania, 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, Turkey, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

1170 Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Malta, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland. The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, United States.

1171 The need for a ratification is laid down in Article 36 of the Convention on Cybercrime:

Article 36 – Signature and entry into force

1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2)This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

1172 Australia, Dominican Republic, Mauritius and Philippines.

1173 Argentina, Australia, Chile, Colombia, Costa Rica, Dominican Republic, Israel, Mauritius, Mecixo, Panama, Philippines, Senegal.

1174 Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico and Philippines.

1175 Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention on Cybercrime shall be distributed to all Interpol member countries in the four official

languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf; APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 19, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

1176 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

1177 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention on Cybercrime."

1178 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1179 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1180 See Art. 3 of the Fourth Draft Convention, PC-CY (98) Draft No. 4, 17.04.1998.

1181 Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, South Africa, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine.

1182 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Finland, France, Germany, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine.

1183 Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp. The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf.

1184 For more information on the achievements and shortcomings see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

1185 Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

1186 Draft Electronic Crime Act 2006.

1187 Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

1188 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

1189 Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

1190 Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.1191 Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, page 18.

1192 Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

1193 Albania, Croatia,

1194 Estonia, Hungary.

1195 Lithuania, Romania, Slovenia, The former Yugoslav Republic of Macedonia.

1196 Bulgaria, Cyprus, Denmark.

1197 Armenia, Bosnia and Herzegovina, France, Netherlands, Norway, Ukraine, United States.

1198 Finland, Iceland, Latvia.

1199 Italy, Slovakia.

1200 Germany, Moldova, Serbia.

1201 Azerbaijan, Montenegro, Portugal, Spain.

1202 United Kingdom, Switzerland.

1203 Austria, Belgium, Georgia, Malta, Australia and Japan.

1204 Czech Republic, Dominican Republic and Mauritius.

1205 See Sec. 202a of the German Penal Code.

1206 Country profiles can be downloaded at www.coe.int/cybercrime.

1207 For details on the requirements, see: *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025, available at: www.fas.org/sgp/crs/misc/97-1025.pdf.

1208 *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

1209 See in this context, for example: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4,

1210 See Art. 44 Convention on Cybercrime.

1211 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1212 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1213 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

1214 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime

Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

1215 *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

1216 Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1217 See *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009, page 127-150.

1218 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

1219 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.8.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

1220 Criticism about the lack of coverage of such topics in the existing instruments: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07, page 7.

1221 See: Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, COM(2010) 517, page 6.

1222 *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

1223 See Art. 44 Convention on Cybercrime.

1224 See Art. 37 Convention on Cybercrime.

1225 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1226 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1227 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

1228 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

1229 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

1230 See: Art. 41 Salvador Declaration on Comprehensive Strategies for Global Challenges, 2010. Available at: www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

1231 See ITU Resolution 130 (Rev. Guadalajara, 2010).

1232 San Marino did not even sign the Convention. Andorra, Monaco and Lichtenstein signed but never ratified the Convention.

1233 See Explanatory Report to the Convention on Cybercrime, No. 298.

1234 *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

1235 The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

1236 ICB4PAC Workshop on Concepts and Techniques of Developing CyberCrime Policy and Legislation, Apia, Samoa 22-25 August 2011.

1237 Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, No. 47.

1238 Model Law on Computer and Computer Related Crime, LMM(02)17. For more information about the Model Law

1239 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

1240 For further information and references on electronic evidence see blow: § 6.5.

1241 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

1242 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1243 Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, Moldova,Monaco, Montegegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Sweden, The former Yugoslav Republic of Macedonia, Turkey, Ukraine and United Kingdom.

1244 Albania, Andorra, Austria, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Greece, Ireland, Italy, Latvia, Luxemburg, Malta, Moldova, Montegegro, Netherlands, Portugal, Romania, Russia, San Marino, Serbia, Slovenia, Spain, Sweden, Sweden, The former Yugoslav Republic of Macedonia and Turkey.

1245 For more details, see: *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

1246 Cybercrime Convention Committee (T-CY).

1247 Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3.

1248 Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

1249 Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

1250 EDRI, Transborder Data Access: Strong Criticsm on planst o extend CoE Cybercrime Treaty, 5.6.2013, available at: www.edri.org/edrigram/number11.11/transborder-data-access-cybercrime-treaty

1251 Report of the Transborder Group for 2013, Cybercrime Convention Committee, T-CY (2013) 30.

1252 1: transborder access with consent but without the limitation to data stored "in another Party"; 2: transborder access without consent but with lawfully obtained credentials; 3: transborder access without consent in good faith or in exigent or other circumstances; 4: extending a search from the original computer to connected systems without the limitation "in its territory"; 5: the power of disposal as connecting legal factor.

1253 T-CY Guidance Note #3 Transborder Access to Data (Article 32), Cybercrime Convention Committee, T-CY (2013) 7E.

1254 The European Union is a supranational and intergovernmental union with, as at today, 27 Member States from the European continent.

1255 One example is the EU funded HIPCAR project on Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures. For more information, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html

1256 *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007, page 69 *et seq.*; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007, page 15 *et seq.*; *Ambos*, Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections, Maastricht Journal of European and Comparative Law, 2005, 173 *et seq.*

1257 See: *Satzger*, International and European Criminal Law, 2005, page 84 for further reference.

1258 itle VI, Treaty on European Union.

1259 Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

1260 Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03. See in this context: *Gercke.*

1261 Communication from the Commission to the European Parliament and the Council on the implications of the Court's judgement of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

1262 Decision of the Court of Justice of the European Communities, 23.10.2007, Case C-440/05; See in this context: *Eisele*, Anmerkung zum Urteil des EuGH C 440/05, JZ 2008, page 251 *et seq.*; *Fromm*, Anmerkung zum Urteil des EuGH C 440/05, ZIS 2008, page 168 *et seq.*

1263 ABl. 2007 C 306, 1.

1264 Regarding the impact of the reform on the harmonization of criminal law, see: *Peers*, EU criminal law and the Treaty of Lisbon, European law review 2008, page 507 *et seq.*; *Zeder*, EU-minimum rules in substantive penal law: What will be new with the Lisbon Treaty?, ERA Forum 2008, page 209 *et seq.*

1265 Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009.

1266 Regarding the Hague Programme, see: *Braum*, Das Haager-Programm der Europaeischen Union: falsche und richtige Schwerpunkte europaeischer Strafrechtsentwicklung in *Joerden/Szwarc*, Europaeisierung des Strafrechts in Deutschland und Polen, 2007, page 11 *et seq.*

1267 See: Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009, No. 3.3.1.

1268 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

1269 See: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487, page 24.

1270 Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

1271 Communication of 8 December 1999 on a Commission initiative for The Lisbon Special European Council, 23 and 24 March 2000 – *e*Europe – An information society for all – COM 1999, 687. See in this regard also: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

1272 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26.1.2001, COM(2000) 890.

1273 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

1274 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

1275 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 31.

1276 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 32.

1277 Network and Information Security – A European Policy approach – adopted 6 June 2001.

1278 For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

1279 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1280 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

1281 See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

1282 See Directive 2000/31/EC, recital 1 *et seq.*

1283 For more details, see below: § 6.

1284 *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 *et seq*

1285 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

1286 Decision No. 276/1999/EC of the **European** Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

1287 Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA).

1288 See Art. 4 of the Framework Decision.

1289 This instrument was in the meantime substituted by the 2012 Directive (see below).

1290 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

1291 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1292 See the explanation of the Framework Decision in the Proposal For A Council Framework Decision on combating serious attacks against information systems, No. 1.6.

1293 Council Framework Decision 2005/222/JHA of 24.02.2005 on attacks against information systems, recital 5.

1294 Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

1295 See below.

1296 *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, page 286.

1297 European Court of Justice, Case C-275/06.

1298 See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

1299 In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

1300 Data Retention Directive, recital 6.

1301 Data Retention Directive, recital 6.

1302 Case C-301/06.

1303 Judgement in Joined Cases C-293/12 and C-594/12.

1304 Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

1305 "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

1306 "Training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

1307 Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2010) 94.

1308 Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

1309 See: Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, page 2.

1310 ETS 201. For more information see: § 5.2.1

1311 See Art. 5, No. 3, of the Draft Directive.

1312 Regarding the challenges related to the use of encryption technology, see above: § 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

1313 See Explanatory Report to the Convention on the Protection of Children, No. 140.

1314 The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180.

1315 Regarding the underlying technology, see: *Austerberrry*, The Technology of Video & Audio Streaming, 2004, page 130 *et seq.*; *Wu/Hou/Zhu/Zhang/Peha*, Streaming Video over the Internet: Approaches and Directions, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 3, 2001, page 282 *et seq.*; *Garfia/Pau/Rico/Gerla*, P2P Streaming Systems: A Survey and Experiments, 2008.

1316 Regarding filter obligations/approaches, see*: Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide.

1317 See *Gercke*, The Role of Internet Service Providers in the Fight against Child Pornography, Computer Law Review International, 2009, page 69 *et seq.*

1318 *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

1319 *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

1320 *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55.

1321 *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

1322 *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009, page 131 *et seq.*; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page ix.

1323 Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

1324 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Deciion 2005/222/JHA.

1325 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1326 Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, page 3.

1327 1999/364/JHA: Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the draft Convention on Cyber Crime held in the Council of Europe.

1328 See Art. 1 of the Common Position.

1329 See in this context: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

1330 See *Gercke*, The Slow Awake of a Global Approach against Cybercrime, Computer Law Review International, page 145.

1331 The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is based in Paris. For more information, see: www.oecd.org.

1332 *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1333 OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

1334 In 1992, the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information Systems. The 24 OECD member countries adopted the guidelines later.

1335 Adopted by the OECD Council at its 1037th session on 25 July 2002. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

1336 Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1337 See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1338 The report is available at: www.legislationline.org/upload/lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

1339 Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

1340 Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, page 5, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

1341 Computer Viruses and other malicious software: A threat to the internet economy, OECD, 2009.

1342 The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties. It has 21 members.

1343 "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

1344 The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

1345 Australia, Brunei Darussalam, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Philippines, Singapore, Chinese Taipei, Thailand and United States.

1346 See: Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

1347 APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, on 26 October 2002. Regarding national legislation on cybercrime in the Asian-Pacific region, see: *Urbas*, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf. See also in this regard: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

1348 APEC TEL-OECD Malware Workshop (2007); APEC TEL and ASEAN Workshop on Network Security (2007); Workshop on Cyber Security and Critical Information Infrastructure Protection (CIIP); APEC Symposium on Spam and Related Threats (2007); APEC Best Practices In International Investigations Training Sessions (2004); Conference on cybercrime for the APEC region (2005); Conference on cybercrime for the APEC region (2004); Conference on cybercrime for the APEC region (2003); Cybercrime legislation training workshops (several, 2003); Judge and Prosecutor Capacity Building Project.

1349 "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

1350 Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar, APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

1351 "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws."

1352 The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

1353 For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/som/mtg/2002/word.Par.0204.File.v1.1

1354 See: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

1355 Cybercrime Legislation & Enforcement Capacity Building Workshop, and Electronic Commerce Steering Group Meeting.

1356 2003/SOMIII/ECSG/O21.

1357 *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.

1358 See: Model Law on Computer and Computer Related Crime, LMM(02)17, Background information.

1359 See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

1360 Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1361 Draft Model Law on Electronic Evidence, LMM(02)12.

1362 For more information see: www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf.

1363 For more information see: African Union, Oliver Tambo Declaration, Johannesburg 2009, available at: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf.

1364 The Draft Convention is available for download at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

1365 See Part 1, Sec. II, Ch. II.

1366 See Part 1, Sec. IV.

1367 See Part 1, Sec. V.

1368 See Part 2.

1369 Art. III-1.

1370 Part 3, Chaptr 1, Art. 1 and Art. 2.

1371 Art. III-1-1 to Art. III-1-7

1372 Art. III-1-8 to Art. III-1-12.

1373 Art. III-2.

1374 Art. III-3.

1375 Art. III-4.

1376 Art. III-5.

1377 Art. III-6.

1378 Art. III-7 1).

1379 For more information see below: § 6.2.2.

1380 Art. III-8.

1381 Art. III-9.

1382 Art. III-10.

1383 Art. III-11.

1384 Art. III-12.

1385 Art. III-13.

1386 Art. III-14.

1387 Art. III-15.

1388 Art. III-16.

1389 Art. III-17.

1390 Art. III-19.

1391 Art. III-20.

1392 Art. III-21.

1393 Art. III-22.

1394 Art. III-24.

1395 Art. III-25.

1396 Art. III-26.

1397 Art. III-27.

1398 Art. III-36.

1399 Art. III-37.

1400 Art. III-39.

1401 Art. III-41.

1402 Regarding reasons for this delay see for example: Gareth van Zyl, Adoption of flawed AU cybersecurity convention postponed, IT Web Africa, 21.01.2014, available at: www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed .

1403 The League of Arab States is a regional organization, with currently 22 members.

1404 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1405 Draft Electronic Crime Act 2006.

1406 Draft Law on Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

1407 Law No. 2 of 2006, enacted in February 2006.

1408 Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

1409 Decision of the Arab Justice Ministers Council, 19th session, 495-D19-8/10/2003.

1410 Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE.

1411 Non-official translation of the recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18 June 2007, Abu Dhabi:

1) Calling for the adoption of a treaty by the Gulf Cooperation Council (GCC) countries, inspired by the Council of Europe Cybercrime convention, to be expanded later to all Arab countries.

2) Calling all GCC countries to adopt laws combating cybercrime inspired by the model of the UAE cybercrime Law.

3) Calling for the adoption of laws in relation to procedural matters such as seizure, inspection and other investigation procedures for such special type of crimes.

5) Providing trainings to inspection and law enforcement officials on dealing with such crimes.

6) Providing sufficient number of experts highly qualified in new technologies and cybercrime particularly in regard to proof and collecting evidence.

7) Recourse to the Council of Europe's expertise in regard to combating cybercrime particularly in regard to studies and other services which would contribute in the elaboration and development of local countries legislation in GCC countries.

8) Harmonization of the legislations in Arab and particularly GCC countries in regard to basic principles in combating this type of crimes on both procedural and substantive level.

9) Increasing cooperation between public and private sectors in the intent of raising awareness and exchange of information in the cybercrime combating field.

1412 The Organization of American States is an international organization with 34 active Member States. For more information, see: www.oas.org/documents/eng/memberstates.asp.

1413 For more information, see: www.oas.org/juridico/english/cyber.htm, and the Final report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations, at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1414 The conclusions and recommendation of the meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas on Cyber Crime are available at: www.oas.org/juridico/english/cyber_meet.htm.

1415 The full list of recommendations from the 2000 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber. The full list of recommendations from the 2003 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1416 The OAS General Secretariat, through the Office of Legal Cooperation of the Department of International Legal Affairs, serves as the technical secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: www.oas.org/dil/department_office_legal_cooperation.htm.

1417 In addition, the Working Group of Governmental Experts on cybercrime recommended that training be provided in the management of electronic evidence and that a training programme be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G8 to help conduct cybercrime investigations. Pursuant to such recommendation, three OAS regional technical workshops were held during 2006 and 2007, the first being offered by Brazil and the United States, and the second and third by the United States. The list of technical workshops is available at: www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

1418 In the meantime, OAS has established joint collaboration with the Council of Europe and attended and participated in the 2007 Octopus Interface Conference on Cooperation against cybercrime. See: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

1419 Conclusions and Recommendations of REMJA-VII, 2008, are available at: www.oas.org/juridico/english/cybVII_CR.pdf.

1420 Conclusions and Recommendations of REMJA-VIII, 2010, are available at: www.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf.

1421 The seventh meeting of the working group on Cybercrime took place from 6-7 February 2012.

1422 Recommendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VII/doc.6/12rev.1.

1423 Recommendation of the Working Group: OEA/Ser.K/ XXXIV, CIBER-VII/doc.6/12rev.1.

1424 Recommendation of the Working Group: OEA/Ser.K/ XXXIV, CIBER-VII/doc.6/12rev.1. The eighth meeting oft he Working Group on Cyber-Crime took place from 27-28 February 2014.

1425 The eighth meeting oft he Working Group on Cyber-Crime took place from 27-28 February 2014.

1426 Recommendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VIII/doc.4/14rev.1.

1427 For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1428 The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

1429 CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

1430 Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

1431 The assessment report is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1432 The workshop was held in Saint Lucia on 8-12 March 2010. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1433 For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

1434 Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

1435 More information about the event are available at: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/port_vila/port_vila.html.

1436 The assessment report will be made available through the project website.

1437 www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/samoa/samoa.html.

1438 More information about the event are available at: www.spc.int/en/component/content/article/704-responding-to-cybercrime-threats-in-the-pacific.html.

1439 An overview about the output of the conference is available at: and www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_tonga_apr_11/AGREED_Cybercrime_Workshop_Outcomes.pdf.

1440 The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

1441 The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

1442 The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_cybercrime.pdf

1443 *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

1444 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf ; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. ABA International Guide to Combating Cybercrime, 2002, page 78.

1445 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq*.

1446 Regarding the application of Art. 23 *et seq.* with regard to traditional crimes, see: Explanatory Report to the Convention on Cybercrime, No. 243.

1447 *Schjolberg*, A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, twelfth UN Crime Congress, 2010, A/CONF.213, page 3, available at: www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

1448 *Schjolberg/Ghernaouti-Helie*, A Global Protocol on Cybersecurity and Cybercrime, 2009, available at: www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

1449 Available online: www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf

1450 For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

1451 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations, No. 41 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations, No. 47 (page 10); "The Meeting recommended that the development of an international convention

on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations, No. 29 (page 7); "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations, No. 40 (page 10).

1452 Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/6_cybercrime/t%2Dcy/FINAL%20T-CY%20_2007_%2003%20-%20e%20-%20Report%20of%20the%20meeting1.pdf.

1453 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions, see *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon of phishing, see *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

1454 For an overview of the different legal approaches, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm. Regarding the economic impact, see for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

1455 There are two aspects that need to be taken into consideration in this context: To avoid redundancy, a new approach should focus on offences that are not intended to be covered within further amendments of the Convention on Cybercrime. The second aspect is related to the difficulties in finding a common position all countries can agree on. Based on the experiences with the negotiations of the Convention on cybercrime, it is likely that negotiations of criminalization that go beyond the standards of the Convention will run into difficulties.

1456 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1457 Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cybercrime, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 35 *et seq*., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 1 *et seq*., available at: http://media.hoover.org/documents/0817999825_1.pdf.

1458 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties which the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and surrender procedures between Member States (2002/584/JHA).

1459 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1460 See Convention on Cybercrime, Articles 23-35.

1461 See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq.*

1462 See above: § 2.6.7.

1463 See Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1464 See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1465 Regarding the network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1466 See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper, No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

1467 Regarding the international dimension, see above: § 3.2.6.

1468 With regard to the Convention on Cybercrime, see: Explanatory Report to the Convention on Cybercrime, No. 33.

1469 Regarding concerns related to the speed of the ratification process, see *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 144.

1470 See below: § 6.2.10.

1471 See above: §§ 3.2.6 and 3.2.7.

1472 The issue has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 stipulates: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 Ten-Point Action Plan highlights: "There must be no safe havens for those who abuse information technologies".

1473 For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*

1474 For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm. For more information, see below: § 6.2.11.

1475 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches, see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf; *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

1476 See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *www.juriscom.net/en/uni/doc/yahoo/poullet.htm*; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

1477 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

1478 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

6 الاستجابة القانونية

يقدِّم الفصل التالي عرضاً عاماً للاستجابة القانونية لظاهرة الجريمة السيبرانية من خلال توضيح النُهج القانونية لتجريم بعض الأفعال.[1479] وستُعرض النُهج الدولية كلما أمكن. أما في تلك الحالات التي لا توجد فيها نُهج دولية فسوف تُعرض أمثلة للنُهج الوطنية أو الإقليمية.

1.6 التعاريف

Bibliography (selected): *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.; *Macagno*, Definitions in Law, Bulletin Suisse de Linguistique Appliquée, Vol. 2, 2010, page 199 et seq, available at: http://ssrn.com/abstract=1742946.

1.1.6 وظيفة التعاريف

تعتبر التعاريف عنصراً مشتركاً بين أطر قانونية وطنية وإقليمية مختلفة. ومع ذلك، من المهم التمييز بين وظائف مختلفة تضطلع بها هذه التعاريف. ففي مجال القانون، يمكن بوجه عام تقسيم التعاريف إلى فئتين: التعاريف الوصفية والتعاريف القانونية.[1480] وتستعمل التعاريف الوصفية لشرح معنى الكلمات الغامضة بينما تهدف التعاريف القانونية إلى أن تضفي على الكلمات الخاضعة لمجال القانون تعريفاً محدداً.[1481] ولا تميز النظرة العامة التالية بين هذين الصنفين من التعاريف.

ولا تتبع الأُطُر القانونية الإقليمية والقوانين النموذجية مفاهيم مختلفة فقط فيما يتعلق بصنف التعاريف بل أيضاً عندما يتعلق الأمر بالجوانب الكمية. وتتضمن الاتفاقية المعنية بالجريمة السيبرانية خمسة تعاريف فقط[1482]، بينما يتضمن النص التشريعي النموذجي لتنسيق السياسات والقوانين والإجراءات التنظيمية الخاصة بتكنولوجيا المعلومات والاتصالات HIPCAR بشأن الجريمة السيبرانية عشرين تعريفاً.

2.1.6 مقدم خدمة النفاذ

يقوم مقدمو خدمة النفاذ بدور مهم إذ إنهم يتيحون توصيل المستخدمين بالإنترنت. ويستعمل مصطلح مقدم خدمة النفاذ في قانون الجريمة السيبرانية فيما يخص تنظيم المسؤولية والمشاركة[1483] في التحقيقات على حد سواء – لا سيما الاعتراض القانوني للاتصالات.[1484] ويرد تعريف للمصطلح في النص التشريعي النموذجي لتنسيق السياسات والقوانين والإجراءات التنظيمية الخاصة بتكنولوجيا المعلومات والاتصالات HIPCAR بشأن الجريمة السيبرانية.

> ***تعاريف***
>
> ***3*** *1) يعني مقدم خدمة النفاذ أي شخص طبيعي أو اعتباري يقدم خدمة إرسال البيانات الإلكترونية من خلال إرسال معلومات مقدمة من طرف أو إلى مستعمل الخدمة ضمن شبكة للاتصالات أو توفير النفاذ إلى شبكة للاتصالات.*
>
> *[...]*

وتكتسي عبارة تقديم الخدمة معنىً واسعاً حيث إنها تشمل مقدمي الخدمات التجاريين فضلاً عن الشركات التي تقدم خدمة النفاذ فقط للموظفين ومشغلي الشبكات الخاصة. وفي حين يتميز هذا النهج بأنه مفيد عندما يتعلق الأمر بتطبيق لوائح المسؤولية على نطاق واسع، فإنه قد يؤدي إلى تحديات إذا طبق التعريف أيضاً ضمن القانون الإجرائي (وهو أمر لم يهدف إليه صائغو النص التشريعي النموذجي HIPCAR).

3.1.6 مقدم خدمة التخزين المؤقت

يتيح مقدمو خدمة التخزين المؤقت خدمة كبيرة لزيادة سرعة النفاذ للمحتويات الشعبية. وبالنظر إلى الحاجة إلى تنظيم مسؤولية[1485] مقدمي خدمة التخزين المؤقت، قرر صاغة النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية إدراج تعريف لهذا المصطلح.

> ***تعاريف***
>
> *3 [...]*
>
> *2) يعني مقدم خدمة التخزين المؤقت أي شخص طبيعي أو اعتباري يقدم خدمة الإرسال البيانات الإلكترونية من خلال التخزين الآلي والوسيطي والمؤقت للمعلومات والتي تجري بغية غرض وحيد وهو جعل الإرسال في الاتجاه الرئيسي للمعلومات إلى المستخدمين الآخرين بناء على طلبهم أكثر فعالية؛*
>
> *[...]*

وعلى غرار تعريفهم لمقدم خدمة النفاذ، لم يحصر صائغو النص تطبيق الحكم على العمليات التجارية. ونتيجة لذلك، يشمل الحكم أيضاً الشركات ومشغلي القطاع الخاص للشبكة.

4.1.6 الطفل

يعتبر مصطلح الطفل مهماً خاصة فيما يتعلق بتجريم استغلال الأطفال في المواد الإباحية.[1486] ويستعمل أيضاً في سياق الأحكام التي تجرّم إتاحة بعض المحتويات للقاصرين (على سبيل المثال المواد الإباحية الخاصة بالبالغين).[1487] وأحد أكثر التعاريف استعمالاً متاح في اتفاقية الأمم المتحدة المعنية بحقوق الطفل منذ عام 1989.

> *ولأغراض هذه الاتفاقية، يعني مصطلح طفل كل إنسان لم يتجاوز الثامنة عشرة، ما لم يبلغ سن الرشد قبل ذلك بموجب القانون المنطبق عليه.*

وتتضمن عدة أُطر قانونية وقوانين نموذجية خاصة بالجريمة السيبرانية مثل التوجيه الصادر عن الاتحاد الأوروبي بشأن مكافحة استغلال الأطفال في المواد الإباحية لعام 2011[1488] واتفاقية مجلس أوروبا بشأن حماية الطفل لعام 2007[1489] والنص التشريعي النموذجي HIPCAR لعام 2009[1490] بشأن الجريمة السيبرانية على تعاريف مماثلة. ولا تعرف اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية الطفل ولكن تعرف فقط استغلال الأطفال في المواد الإباحية.

5.1.6 استغلال الأطفال في المواد الإباحية

تُعدّ المواد الإباحية المستغلة للطفل إحدى الجرائم القلائل المتعلقة بفئة المحتويات غير القانونية التي اتفقت معظم البلدان على تجريمها.[1491] وحيث إن التمييز بين الأشكال القانونية للمواد المرتبطة بالجنس والمواد الإباحية المستغلّة للطفل يمكن أن يكون صعباً، تقدم بعض الأطر القانونية تعريفاً للمواد الإباحية المستغلة للطفل.

ومن بين التحديات الرئيسية التي تواجه واضعي القوانين في هذا الصدد تجنب أوجه التضارب بين الشرائح العمرية المختلفة من أجل تفادي إمكانية التجريم غير المقصود في الحالات التي يختلف فيها سن الزواج أو القبول الجنسي والحد الأدنى للسن ضمن تعريف المواد الإباحية المستغلة للطفل.[1492] وإذا عرفت المواد الإباحية المستغلة للطفل، على سبيل المثال، بأنها تصوير للأفعال الجنسية لشخص تحت سن 18 وفي الوقت نفسه كان سن القبول الجنسي وسن الزواج هو 16 سنة، فبإمكان شاب

وشابة عمرهما 17 سنة الزواج أو ممارسة العلاقة الجنسية قانونياً غير أنهما سيرتكبان جريمة خطيرة (إنتاج المواد الإباحية المستغلة للأطفال) إذا قاما بتصوير صورة أو فيلم لهذا الفعل.[1493]

وطرحت المادة 2 ج) من البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية تعريفاً لهذا المفهوم.

> ***المادة 2***
>
> *لغرض هذا البروتوكول:*
>
> *[...]*
>
> *ج) يُقصد باستغلال الأطفال في المواد الإباحية تمثيل لأي طفل، بأي وسيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي يمثل للأعضاء الجنسية للطفل لأغراض جنسية تحديداً.*

ولا يشمل التعريف المتاح في البروتوكول الاختياري بوضوح أشكال استغلال الأطفال في المواد الإباحية التصويرية مثل الصور الحقيقية. ولضمان إدراج مثل هذه المواد أيضاً قامت بعض الأطر القانونية مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية بتعديل تعريف مصطلح استغلال الأطفال في المواد الإباحية.

> ***المادة 9 – الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية***
>
> *[...]*
>
> *2) لأغراض الفقرة 1 أعلاه، يشمل مصطلح " استغلال الأطفال في المواد الإباحية" المواد الإباحية التي تصور بصورة مرئية:*
>
> *أ) قاصراً يمارس سلوكاً جنسياً صريحاً؛*
>
> *ب) شخصاً يبدو أنه قاصر يمارس سلوكاً جنسياً صريحاً؛*
>
> *ج) صور حقيقية تصور قاصراً يمارس سلوكاً جنسياً واضحاً.*
>
> *3) لأغراض الفقرة 2 أعلاه، يشمل مصطلح "قاصر" جميع الأشخاص تحت سن 18. ويجوز، رغم ذلك، أن يفرض طرف ما حداً أدنى للسن لا يقل عن 16 سنة.*
>
> *[...]*

تقدم المادة 9، الفقرة 2، ثلاثة أقسام فرعية بشأن المواد التي تصور استغلال الأطفال في المواد الإباحية: قاصر يمارس سلوكاً جنسياً صريحاً وشخص يبدو أنه قاصر يمارس سلوكاً جنسياً صريحاً وصور حقيقية تصور قاصراً يمارس سلوكاً جنسياً صريحاً.

وفي حين توسع الاتفاقية بشأن الجريمة السيبرانية نطاق التعريف الوارد في البروتوكول الاختياري الملحق باتفاقية الأمم المتحدة من جهة، فمن جهة أخرى تقلص فرص التطبيق على جانبين مهمين.

ورغم تشديد واضعي الاتفاقية بشأن الجريمة السيبرانية على أهمية اعتماد معيار دولي موحد فيما يخص السن،[1494] تسمح الاتفاقية بشأن الجريمة السيبرانية مع ذلك للأطراف فرض حدٍّ أدنى للسن مختلف لا يقل عن 16 سنة.

ويتمثل الاختلاف الرئيسي الثاني للتعريف الذي يقدمه البروتوكول الاختياري في كون التعريف الوارد في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية يركز على التصوير البصري. ذلك أن استغلال الأطفال في المواد الإباحية لا يوزع فقط بواسطة الصور والأفلام ولكن أيضاً بواسطة الملفات الصوتية.[1495] ونظراً إلى أن الحكم الوارد في المادة 9 يشير إلى "المواد التي تصور بشكل مرئي" الطفل، فإنه لا يشمل الملفات الصوتية.

ونتيجة لذلك، تعتمد النُهج الأحدث عهداً مثل النص التشريعي HIPCAR بشأن الجريمة السيبرانية[1496] المفهوم الوارد في البروتوكول الاختياري الملحق باتفاقية الأمم المتحدة[1497] بدلاً من مفهوم اتفاقية مجلس أوروبا وتتفادى مصطلح "مرئي".

تعاريف

3

[...] 4) يقصد بمصطلح " استغلال الأطفال في المواد الإباحية" المواد الإباحية التي تصور أو تقدم أو تمثل:

أ) قاصراً يمارس سلوكاً جنسياً صريحاً؛

ب) شخصاً يبدو أنه قاصر يمارس سلوكاً جنسياً صريحاً؛

ج) صور حقيقية تصور قاصراً يمارس سلوكاً جنسياً صريحاً؛

ويشمل هذا على سبيل المثال لا الحصر، أي مواد سمعية أو مرئية أو نصوص إباحية.

ويمكن أن يقيد بلد معين التجريم بعدم تنفيذ ب) وج).

وترد تعاريف استغلال الأطفال في المواد الإباحية أيضاً في الأمر التوجيهي للاتحاد الأوروبي بشأن مكافحة استغلال الأطفال في المواد الإباحية لعام 2011[1498] وفي اتفاقية مجلس أوروبا بشأن حماية الأطفال لعام 2007.[1499]

6.1.6 البيانات الحاسوبية

يؤدي تزايد استخدام تكنولوجيا الحاسوب فضلاً عن الاتجاه إلى رقمنة البيانات إلى تزايد أهمية البيانات الحاسوبية. ونتيجة لذلك أصبحت البيانات الحاسوبية في كثير من الأحيان هدفاً للهجمات التي تتراوح من تداخل البيانات إلى التجسس على البيانات.[1500] وتتضمن أطر إقليمية مختلفة تعاريف للبيانات الحاسوبية.[1501] وأحد هذه الأمثلة يرد في الفصلي 3 من القانون النموذجي لدول الكومنولث بشأن الحاسوب والجرائم المتعلقة بالحاسوب.

تعاريف

3 *في هذا القانون، ما لم يُنص على خلاف ذلك*

يقصد "بالبيانات الحاسوبية" أي تمثيل لوقائع أو معلومات أو مفاهيم في صورة ملائمة لمعالجتها في نظام الحاسوب، بما في ذلك وضع برنامج مناسب يمكّن نظام الحاسوب من أداء وظيفته؛

[...]

وترد تعاريف مماثلة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لعام 2001[1502] والقرار الإطاري للاتحاد الأوروبي بشأن الهجمات على نظم المعلومات لعام 2005[1503] ومشروع الأمر التوجيهي الصادر عن الجماعة الاقتصادية لدول غرب إفريقيا لمكافحة الجريمة السيبرانية لعام 2008[1504] والنص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية.[1505]

7.1.6 جهاز تخزين البيانات الحاسوبية

تقوم أجهزة التخزين بدور مهم فيما يتعلق بالجريمة السيبرانية – فيما يخص تداخل البيانات وكذلك فيما يتعلق بوضع اليد على الأدلة. وهناك مثال للإطار الإقليمي يتضمن تعريفاً وهو الفصل 3 من القانون النموذجي لدول الكومنولث بشأن الحاسوب والجرائم الحاسوبية.

> **تعاريف**
>
> **3**
>
> *[...]*
>
> *يقصد بمصطلح "وسط تخزين البيانات الحاسوبية" أي أداة أو مادة (على سبيل المثال، قرص) يمكن بواسطتها استخراج نسخة بمساعدة أو دون مساعدة أي أداة أو جهاز آخر؛*
>
> *[...]*

ويرد تعريف مماثل في النص التشريعي النموذجي لبلدان الكاريبي HIPCAR.[1506]

8.1.6 نظام الحاسوب

يستعمل مصطلح نظام الحاسوب في قوانين الجريمة السيبرانية فيما يتعلق بالقانون الجنائي الموضوعي وكذلك القانون الإجرائي. ويمكن أن تكون أنظمة الحاسوب هدفاً للهجمات ويمكن أن تستعمل كأداة لارتكاب جريمة وفي نهاية المطاف يمكن وضع اليد عليها باعتبارها دليلاً قانونياً. ونتيجة لذلك، تتضمن معظم الأُطر والقوانين النموذجية الإقليمية المطبّقة هذا التعريف. ويرد أحد تلك الأمثلة في الفصل 3 من القانون النموذجي لدول الكومنولث بشأن الحاسوب والجرائم المتعلقة بالحاسوب:

> **تعاريف**
>
> **3**
>
> *[...]*
>
> *يُقصد "بنظام الحاسوب" جهاز أو مجموعة من الأجهزة الموصولة بينياً أو أي أجهزة ذات صلة بما في ذلك الإنترنت والتي تقوم واحدة منها أو أكثر، حسب البرنامج، بالمعالجة الآلية للبيانات أو أي وظيفة أخرى؛*
>
> *[...]*

ويتمثل أحد الجوانب غير المألوفة في أن التعريف يشير إلى "الإنترنت". وتُعرّف الإنترنت على نطاق واسع باعتبارها نظاماً من الشبكات الموصولة.[1507] ومن منظور تقني لا تعتبر الإنترنت في حد ذاتها نظام حاسوب وإنما هي شبكة وبالتالي لا ينبغي أن تُدرج في التعريف الخاص بأنظمة الحاسوب وإنما ينبغي أن تُدرج في تعريف شبكات الحاسوب. ورغم ذلك، حذا العديد من واضعي الأُطر القانونية حذو القانون النموذجي للكومنولث أدرجوا الإنترنت في تعريف نظام الحاسوب.

وترد كذلك تعاريف في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لعام 2001[1508] والمقرر الإطاري للاتحاد الأوروبي بشأن الهجمات على أنظمة المعلومات لعام 2005[1509] ومشروع التوجيه التوجيهي الصادر عن الجماعة الاقتصادية لدول غرب إفريقيا لمكافحة الجريمة السيبرانية لعام 2008[1510] والنص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية.[1511]

9.1.6 البُنى التحتية الحرجة

نتيجة لتزايد استخدام تكنولوجيات الحاسوب أو الشبكة في تشغيل البُنى التحتية الحرجة، فقد أصبحت هذه البُنى التحتية هدفاً محتملاً للهجمات.[1512] ومع مراعاة التأثير المحتمل لهذه الهجمات، تشتمل بعض أحدث هذه الأطر على تجريم خاص أو عقوبة مشددة على بعض الهجمات على البُنى التحتية الحرجة وبالتالي يجب كذلك وضع تعريف في هذا الصدد. وأحد هذه الأمثلة هو النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية.

تعاريف

3

[...]

8) يُقصد بالبُنى التحتية الحرجة أنظمة الحاسوب والأجهزة والشبكات وبرامج الحاسوب وبيانات الحاسوب التي لها أهمية بالغة بالنسبة للبلاد بحيث إن إعاقة أو تخريب أو التشويش على هذه الأنظمة والممتلكات قد يترتب عنها آثار ضارة على الأمن والأمن القومي والاقتصادي والصحة العامة والسلامة الوطنية أو أي مزيج من هذه الأمور؛

[...]

10.1.6 التجفير

يمكن أن يعرقل استخدام المجرمين لتكنولوجيا التجفير كثيراً الوصول إلى الأدلة المهمة.[1513] ونتيجة لذلك، نفذت عدة بلدان التشريع الذي يتناول استخدام تكنولوجيا التجفير وأدوات التحقيق المتعلقة بإنفاذ القانون.[1514] ورغم ذلك، من بين مختلف الأطر الإقليمية التي تتطرق للجريمة السيبرانية، نجد أن مشروع اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني[1515] وحده هو الذي يقدم تعريفاً للتجفير في المادة I-1.

8) يُقصد بالتجفير العلم الذي يُعنى بحماية وتأمين المعلومات خاصة بهدف ضمان السرية والاستيقان والسلامة وعدم الإنكار؛

11.1.6 الجهاز

يستعمل مصطلح جهاز بوجه خاص بشأن تجريم "الأجهزة غير القانونية".[1516] وفيما يتعلق بالخطر المحتمل لإمكانية انتشار هذه الأجهزة على نطاق واسع واستخدامها لارتكاب جرائم، قرر واضعو العديد من الأُطر الإقليمية إدراج حكم يجرّم بعض الأنشطة المتعلقة بالأجهزة غير القانونية. وخلافاً لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والقانون النموذجي لدول الكومنولث، اللذين يستعملان معاً مصطلح جهاز، يتضمن النموذج التشريعي HIPCAR تعريفاً للمصطلح في المادة 3.

تعاريف

3

[...]

9) يشمل الجهاز على سبيل المثال لا الحصر، على

أ) مكونات أنظمة الحاسوب مثل البطاقات البيانية و الذاكرة والرقاقات؛

ب) مكونات التخزين مثل محركات الأقراص الصلبة وبطاقات الذاكرة والأقراص المدمجة والأشرطة؛

ج) أجهزة الإدخال مثل لوحات المفاتيح والفأرة ولوحة المسار والماسح والكاميرات الرقمية؛

د) أجهزة المخرجات مثل الطابعة والشاشات؛

[...]

وهذا بالفعل تعريف وصفي نموذجي ذلك أن الحكم يشير بوضوح إلى أن تعريف الجهاز لا يجب أن يقتصر على المكونات المدرجة ("على سبيل المثال لا الحصر"). وبالإشارة إلى الحكم الضمني[1517] الذي يجرّم الأجهزة غير القانونية يشمل المصطلح أيضاً برامج الحاسوب.

12.1.6 العرقلة

يعتبر تشغيل أنظمة الحاسوب أمراً أساسياً في مجتمعات المعلومات والاقتصادات التي تتضمن التجارة الإلكترونية. ويمكن للهجمات ضد نظام الحاسوب التي تعرقله بشدة عن تنفيذ العمليات أن تؤثر بشدة على المجتمع والاقتصاد. ونتيجة لذلك، تجرم عدة أطر إقليمية عرقلة نظام الحاسوب عن أداء عمله.[1518] ويتضمن النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية تعريفاً خاصاً لمصطلح العرقلة في سياق الجريمة السيبرانية في المادة 3.

تعاريف

3

[...]

10) يشمل مصطلح عرقلة فيما يتعلق بنظام الحاسوب على سبيل المثال لا الحصر ما يلي:

أ) قطع تزويد نظام الحاسوب بالكهرباء؛ و

ب) التسبّب في تداخل كهرومغناطيسي على نظام الحاسوب؛ و

ج) إفساد نظام الحاسوب بأي وسيلة من الوسائل؛ و

د) إدخال بيانات في الحاسوب أو إرسالها أو تعطيلها أو حذفها أو إتلافها أو تحويرها أو شطبها؛

[...]

ويؤكد التعريف على أن التلاعب بنظام الحاسوب يشمل التدخل المادي (مثل قطع مصدر الكهرباء) وكذلك التلاعب بالبيانات (مثل إدخال بيانات في الحاسوب).

13.1.6 مقدم خدمة الاستضافة

يضطلع مقدمو خدمات الاستضافة بدور بالغ الأهمية فيما يتعلق بمكافحة الجريمة السيبرانية لأن خدماتهم تستخدم، على سبيل المثال، لتخزين المحتويات غير القانونية. وبالتالي، تتناول أطر إقليمية مختلفة القضايا المتعلقة بمسؤولية مقدم خدمة الإنترنت.[1519] ومع ذلك، لا تقدم الأطر الإقليمية الرئيسية تعريفاً لمقدم خدمة الاستضافة. غير أن هذا التعريف يرد في النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية.

تعاريف

3

[...]

11) يُقصد بمقدم خدمة الاستضافة أي شخص طبيعي أو اعتباري يقدم خدمة إرسال البيانات الإلكترونية بواسطة تخزين المعلومات التي يقدمها مستعمل الخدمة؛

[...]

ولا يحصر التعريف تطبيق الحكم على المقدم التجاري للخدمة ولكن يشمل أيضاً المشغل الخاص. ونتيجة لذلك، يمكن أن تشمل لوائح المسؤولية ذات الصلة أيضاً مشغل موقع إلكتروني خاص يُمكن آخرين من تخزين معلومات في الموقع الإلكتروني.

14.1.6 وصلة الإحالة الإلكترونية

على الرغم من أن مقدمي خدمة الاستضافة وخدمة النفاذ وخدمة التخزين المؤقت ينضوون ضمن الفئات العمرية لمقدم خدمة الإنترنت (ISP)، تقدم عدة أطر قانونية لوائح محددة لخدمات أخرى مثل محركات البحث[1520] ووصلات الإحالة الإلكترونية. وفي هذا الصدد، يقدم النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية تعريفاً لوصلات الإحالة الإلكترونية.

> **تعاريف**
>
> *3*
>
> *[...]*
>
> *(12) يُقصد بوصلة الإحالة الإلكترونية ميزة أو خاصية لعنصر مثل رمز أو كلمة أو عبارة أو جملة أو صورة تحتوي على معلومات بخصوص مصدر آخر وتشير وتتسبب في عرض وثيقة أخرى عند تنفيذها.*
>
> *[...]*

ويعتبر التعريف واسع النطاق ويشمل أصنافاً مختلفة من وصلات الإحالة الإلكترونية مثل الوصلات العميقة.

15.1.6 اعتراض الاتصالات

يُستعمل مصطلح الاعتراض كثيراً في القانون الجنائي الموضوعي فيما يخص تجريم الاعتراض غير القانوني[1521] وكذلك في القانون الجنائي الإجرائي فيما يتعلق بالاعتراض القانوني للاتصالات. وفي حين تتضمن الأطر الإقليمية مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والقانون النموذجي للكومنولث أحكاماً تتعلق بالاعتراض غير القانوني فضلاً عن الاعتراض القانوني للاتصالات، إلا أن هذه الأُطر لا تقدم تعريفاً للاعتراض. بيد أن هذا الحكم ويرد في النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية.

> **تعاريف**
>
> ***3***
>
> *[...]*
>
> *(13) يشمل اعتراض الاتصالات على سبيل المثال لا الحصر الحصول على أي شكل من اتصالات البيانات الحاسوبية ومعاينتها والاستيلاء عليها سواء بالوسائل السلكية أو اللاسلكية أو الإلكترونية أو البصرية أو المغنطيسية أو الشفوية أو أي وسائل أخرى أثناء إرسال البيانات بواسطة استخدام أي جهاز تقني؛*
>
> *[...]*

16.1.6 التداخل

التداخل مصطلح معياري يستخدم في عدة أحكام متعلقة بالجريمة السيبرانية. ومن بين الأمثلة التداخل على البيانات وكذلك التداخل على النظام.[1522] ورغم ذلك، يستخدم المصطلح في عدة صكوك إقليمية فقط في العناوين الرئيسية لبعض الأحكام،[1523] غير أنه لا يصف التصرف الذي جرى تجريمه في حد ذاته. وبالتالي لا تعرف معظم الأطر الإقليمية والقوانين النموذجية أيضاً هذا المصطلح.

17.1.6 الرسائل الإلكترونية المتعددة

يُعدُّ عدد كبير من الرسائل الإلكترونية المرسلة بمثابة رسائل اقتحامية. ونتيجة لذلك قام عدد من البلدان وكذلك أحدث القوانين النموذجية بإدراج أحكام تجرّم الأفعال المتعلقة بتوزيع الرسائل الاقتحامية.[1524] وأحد المصطلحات الرئيسية المستعملة في هذا الحكم هو مصطلح الرسائل الإلكترونية المتعددة. ويتضمن النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية تعريفاً لهذا المصطلح.

تعاريف

3

[...]

14) يُقصد بالرسائل الإلكترونية المتعددة رسالة بريدية بما في ذلك البريد الإلكتروني والرسائل اللحظية المرسلة لأكثر من ألف من المستقبلين؛

[...]

18.1.6 برمجيات تحديد الأدلة الجنائية عن بُعد

تتضمن بعض أحدث الأطر القانونية وأكثرها تقدماً أحكاماً إجرائية تأذن في بعض الحالات لوكالات إنفاذ القانون بتطبيق أدوات تحديد الأدلة الجنائية المتقدمة – مثل أداة تسجيل بيانات النقر على المفاتيح.[1525] ويتضمن النص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية تعريفاً لمصطلح برمجيات تحديد الأدلة الجنائية عن بُعد.

تعاريف

3

[...]

15) يُقصد ببرمجيات تحديد الأدلة الجنائية عن بُعد برمجية للتحقيق تثبّت على نظام الحاسوب وتستخدم للقيام بمهام تشمل على سبيل المثال لا الحصر تسجيل بيانات النقر على لوحة المفاتيح أو إرسال عنوان بروتوكول الإنترنت؛

[...]

وفي إطار مناقشة عن استخدام معايير HIPCAR والتي وُضعت من أجل بلدان الكاريبي، في المحيط الهادئ، تمت الإشارة إلى أنه بغية تغطية المجموعة الكاملة لحلول تحديد الأدلة الجنائية، يعتبر مصطلح أداة (الذي يشمل أيضاً الحلول المرتبطة بالعتاد والحاسوب) أكثر ملائمة مقارنة ببرمجية.

19.1.6 المصادرة

تظل المصادرة إحدى أهم أدوات التحقيق المستعملة لجمع الأدلة ليس فقط فيما يتعلق بالجرائم التقليدية بل أيضاً فيما يتعلق بالجريمة السيبرانية.[1526] ويحتوي القانون النموذجي للكومنولث الخاص بالحاسوب والجريمة المتعلقة بالحاسوب على تعريف لمصطلح المصادرة، يرد في المادة 11 القسم III.

تعاريف بخصوص هذا الجزء

[...]

11 في هذا الجزء:

[...]

تشمل "المصادرة"

أ) عمل نسخ من البيانات الحاسوبية والاحتفاظ بها، بما في ذلك من خلال استخدام المعدات الموجودة في الموقع؛

ب) وجعل هذه البيانات الحاسوبية غير قابلة للوصول إليها أو إزالتها من نظام الحاسوب الذي تم الدخول إليه؛

ج) وأخذ نسخة مطبوعة من ناتج بيانات الحاسوب.

وأُجري تعديل إضافي على هذا التعريف الذي يحتوي على ثلاثة أقسام فرعية في إطار تطوير النص التشريعي النموذجي لبلدان الكاريبي (HIPCAR) بشأن الجريمة السيبرانية. وأدرج تعريف في الفصل 3 (16).

تعاريف

3

[...]

(16) تشمل "المصادرة" :

أ) تفعيل أي نظام حاسوبي في الموقع وأي وسيط لتخزين بيانات الحاسوب؛

ب) أو عمل نسخ من البيانات الحاسوبية والاحتفاظ بها، بما في ذلك استخدام المعدات الموجودة في الموقع؛

ج) أو الحفاظ على سلامة البيانات الحاسوبية المخزنة ذات الصلة؛

د) أو جعل هذه البيانات الحاسوبية غير قابلة للوصول إليها أو إزالتها من نظام الحاسوب الذي تم الدخول إليه؛

هـ) أو أخذ نسخة مطبوعة من ناتج بيانات الحاسوب؛

و) أو مصادرة نظام الحاسوب أو التحكم فيه أو جزء منه أو وسيط تخزين بيانات الحاسوب؛

[...]

وتنتهج اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية نهجاً مختلفاً وتدرج مختلف عناصر المصادرة في الحكم ذاته.[1527]

20.1.6 مقدم الخدمة

يعتبر مقدم الخدمة فئة تستعمل لوصف مختلف أصناف مقدمي خدمة الإنترنت. وكما أشير إلى ذلك سلفاً تحتوي أطر إقليمية مختلفة على أحكام تتناول مقدم الخدمة (مثل الأحكام المتعلقة بمسؤولية مختلف أشكال مقدمي الخدمات أو الأحكام الإجرائية التي تستوجب دعم مقدم الخدمة لأنشطة إنفاذ القانون). غير أنها جميعاً لا تميز بين مختلف أشكال مقدمي الخدمات. ونتيجة لذلك، تدرج تلك الأطر الإقليمية، على نحو خاص، التي لا تميز شكل مقدم الخدمة تعريفاً لمصطلح مقدم الخدمة. ومن أمثلة ذلك، تعريف اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

المادة 1 – تعاريف

[...]

ج) *يقصد بمصطلح "مقدم الخدمة"*

'1' كل كيان عام أو خاص يتيح لمستخدمي خدماته القدرة على الاتصال بواسطة نظام حاسوب،

'2' كل كيان آخر يقوم بمعالجة البيانات الحاسوبية أو تخزينها بالنيابة عن خدمة الاتصالات هذه أو مستخدميها؛

[...]

كما يحتوي كل من القانون النموذجي للكومنولث الخاص بالحاسوب والجريمة المتعلقة بالحاسوب لعام 2002[1528] والنص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية لعام 2009[1529] على تعاريف مماثلة.

21.1.6 بيانات الحركة

تعتبر بيانات الحركة فئة من البيانات التي قامت بعض الأطر القانونية الإقليمية والقوانين النموذجية بتقديم أدوات تحقيق بشأنها. ونتيجة لذلك، غالباً ما تقدم هذه الأُطر القانونية هي الأخرى تعريفاً بشأنها.[1530] وهناك مثال وارد في الفصل 3 مقتبس من القانون النموذجي للكومنولث الخاص بالحاسوب والجريمة المتعلقة بالحاسوب لعام 2002.

تعاريف

3

[...]

يقصد "ببيانات الحركة" بيانات الحاسوب:

أ) المتعلقة باتصال عن طريق نظام الحاسوب؛

ب) والتي تنشأ عن نظام حاسوب تشكل جزءاً في سلسلة الاتصالات؛

ج) والتي توضح مصدر الاتصال ومقصده والمسير الذي تسلكه ووقت وتاريخ وحجم ومدة ونوع الخدمات المسجلة.

وهناك تعاريف مشابهة في كل من اتفاقية مجلس أوروبا[1531] بشأن الجريمة السيبرانية والنص التشريعي النموذجي HIPCAR بشأن الجريمة السيبرانية لعام 2009.[1532]

2.6 القانون الجنائي الموضوعي

Bibliography (selected): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002; *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke/Tropina*, from

Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, Cybercrime Training for Judges, 2009; *Gercke*, How Terrorist Use the Internet in Pieth/Thelesklaf/Ivory, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf; Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.*, available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf; *Lavalle*, A Politicized and Poorly Conceived Notion Crying Out for Clarification: The Alleged Need for Universally Agreed Definition of Terrorism, Zeitschrift fuer auslaendisches oeffentliches Recht und Voelkerrecht, 2006, page 89 *et seq.*; *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999; *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11; *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact and Prevention, Youth & Society, Vol. 34, 2003; *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; *Parsonage*, Web Browser Session Restore Forensics, A valuable record of a user's internet activity for computer forensic examinations, 2010, available at: http://computerforensics.parsonage.co.uk/downloads/WebBrowserSessionRestoreForensics.pdf; Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement Act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII; *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, 2001; *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP/e-RIAPL, 2008, C-07; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33; *Walden*, Computer Crimes and Digital Investigations, 2006; *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2; *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available

at: www.cops.usdoj.gov/mime/open.pdf?Item=1729; *Wolak/ Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

1.2.6 النفاذ غير القانوني (القرصنة)

منذ تطوير شبكات الحاسوب بحكم قدرتها على توصيل الحواسيب وإتاحة النفاذ إلى الأنظمة الحاسوبية الأخرى أمام المستعملين، ظل القراصنة يستعملون الحواسيب لأغراض إجرامية.[1533] وتتباين حوافز القراصنة تبايناً كبيراً.[1534] وليس من الضروري أن يتواجد القراصنة في مسرح الجريمة؛[1535] إذ إنهم يحتاجون فقط إلى الالتفاف على الحماية التي تؤمن الشبكة.[1536] 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.[1537]

والنفاذ غير القانوني إلى أنظمة الحواسيب يعوق مشغلي الحواسيب عن إدارة وتشغيل ومراقبة أنظمتهم بدون إزعاج أو موانع.[1538] وهدف الحماية هو الحفاظ على سلامة الأنظمة الحاسوبية.[1539] ومن الأهمية الحاسمة التمييز بين النفاذ غير القانوني وما يعقبه من جرائم (مثل التجسُّس على البيانات[1540])، 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 وسريّة البيانات).[1541]

والسؤال هو ما إن كان ينبغي تجريم فعل النفاذ غير القانوني بالإضافة إلى الجرائم اللاحقة؟[1542] 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.[1543] وتجرِّم بعض البلدان مجرَّد النفاذ في حين تقصر بلدان أخرى التجريم على الجرائم التي يكون فيها النظام الحاسوبي المخترق خاضعاً لحماية تدابير أمنية، أو عندما يكون لدى الجاني نية إحداث ضرر، أو في حالات الحصول على بيانات أو تعديلها أو إفسادها.[1544] ولا تجرِّم بلدان أخرى النفاذ بحد ذاته ولكنها تجرِّم الجرائم اللاحقة.[1545] ويشير معارضو 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.[1546]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تشمل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية حكماً بشأن النفاذ غير القانوني يحمي سلامة الأنظمة الحاسوبية بتجريم النفاذ غير المأذون به إلى النظام. ومع ملاحظة النُهج غير المتسقة على الصعيد الوطني،[1547] تعرض الاتفاقية بشأن الجريمة السيبرانية 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.[1548] ويرمي الحكم إلى حماية سلامة الأنظمة الحاسوبية.

الحكم

> ***المادة 2 – النفاذ غير المشروع:***
>
> *تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما أُرتكب عمداً، وبغير حق: النفاذ إلى كامل أو على جزء من منظومة الحاسوب. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات حاسوب أو بقصد آخر غير أمين، أو فيما يتعلق بمنظومة حاسوب متصلة بمنظومة حاسوب أخرى.*

الأفعال المشمولة

لا يحدِّد مصطلح "النفاذ" وسيلة معيَّنة للاتصال، ولكنه مصطلح مفتوح الحدود ويمكن أن تدخل عليه تطورات تقنية أخرى.[1549] ويشمل جميع وسائل النفاذ إلى منظومة حاسوبية أخرى، بما في ذلك هجمات الإنترنت[1550]، 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 السر).[1551] وهذا النهج الواسع يعني أن النفاذ غير المشروع لا يشمل فقط التطورات التقنية المقبلة ولكنه يشمل أيضاً البيانات السرية التي ينفذ إليها المطَّلعون والعاملون.[1552] والجملة الثانية من المادة 2 تتيح إمكانية اقتصار تجريم النفاذ غير القانوني على النفاذ عبر شبكة.[1553]

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.[1554]

العنصر الذهني

كما حدث في حالة جميع الجرائم الأخرى المعرَّفة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تقتضي المادة 2 أن يرتكب الجاني جريمته عمداً.[1555] ولا تتضمن الاتفاقية المتعلقة بالجريمة السيبرانية تعريفاً لمصطلح "عمداً". وفي التقرير التفسيري يشير واضعو الاتفاقية إلى أن التعبير "عمداً" ينبغي أن يُعرّف على صعيد وطني.[1556]

بغير حق

لا يمكن ملاحقة النفاذ إلى الحاسوب بموجب المادة 2 من الاتفاقية بشأن الجريمة السيبرانية إلا إذا حدث "بغير حق".[1557] 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".[1558] وبالإضافة إلى موضوع النفاذ بحرية، نوقشت أيضاً شرعية إجراء اختبار الأمن.[1559] وكان مديرو الشبكات وشركات الأمن التي تختبر حماية النُظم الحاسوبية من أجل تعيين الفجوات المحتملة في تدابير الأمن يشعرون بالتوجس من خطر التجريم بموجب النفاذ غير القانوني.[1560] ورغم أن هؤلاء المهنيين يعملون عموماً بإذن من المالك وبالتالي يعملون بصورة قانونية، فإن واضعي نص الاتفاقية بشأن الجريمة السيبرانية أكدوا على أن "اختبار أو حماية أمن النظام الحاسوبي بإذن من جانب المالك أو المشغِّل، [...] يجري بحق".[1561]

ولكن قيام ضحية الجريمة بتسليم كلمة سر 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 سر أو شفرة النفاذ بواسطة اقتراب احتيالي اجتماعي ناجح[1562] فسيكون من الضروري التحقق مما إذا كان الإذن الذي أعطاه الضحية يشمل فعلاً التصرُّف الذي قام به الجاني.[1563] ولكن الأمر لا يكون على هذا النحو عموماً ولذلك يكون الجاني قد تصرف بغير حق.

التقييدات والتحفظات

تتيح الاتفاقية بشأن الجريمة السيبرانية كبديل لهذا النهج العريض إمكانية تقييد التجريم بعناصر إضافية يرد ذكرها في الجملة الثانية.[1564] وتنص المادة 42 من الاتفاقية بشأن الجريمة السيبرانية على الإجراءات التي يمكن بها استخدام هذا التحفُّظ.[1565] والتحفظات المحتملة تتصل بالتدابير الأمنية،[1566] أو قصد الحصول على بيانات الحاسوب،[1567] أو القصد الآخر غير الأمين الذي يبرِّر الجُرم الجنائي، أو اقتضاء ارتكاب الجريمة ضد نظام حاسوبي من خلال شبكة.[1568] ويمكن الاطلاع على نهج مشابه في القرار الصادر عن الاتحاد الأوروبي[1569] باسم القرار الإطاري بشأن الهجمات ضد أنظمة المعلومات.[1570]

قانون الكومنولث النموذجي بشأن الجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في المادة 5 من قانون الكومنولث النموذجي لعام 2002.[1571] وكما هو الحال في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، يحمي الحكم سلامة أنظمة الحاسوب.

النفاذ غير المشروع 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.

تتّبع المادة 5 نهجاً شبيهاً بالمادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. والاختلاف الرئيسي عن الاتفاقية المتعلقة بالجريمة السيبرانية هو أن المادة 5 من قانون الكومنولث النموذجي لا تتضمن خيارات لإبداء تحفظات.

توجيه الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات

تتضمن المادة 3 من توجيه الاتحاد الأوروبي لعام 2013 بشأن الهجمات ضد نظم المعلومات[1572] حكماً يجرّم النفاذ غير المشروع إلى نظم المعلومات.

المادة 3 – النفاذ غير المشروع إلى نظم المعلومات

تتخذ الدول الأعضاء التدابير اللازمة لضمان أن النفاذ بدون حق في نظام معلومات بكامله أو في أي جزء منه، عندما يرتكب عمداً، يعاقب عليه كجريمة جنائية، وعندما يرتكب بانتهاك التدابير الأمنية، في الحالات التي لا تكون بسيطة على الأقل.

وقد صيغ الحكم وفقاً للمعايير التي حددتها اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[1573] والاختلاف الرئيسي الأول عن الاتفاقية بشأن الجريمة السيبرانية هو أن الدول الأعضاء يمكنها أن تقتصر على تجريم الحالات التي ليست بسيطة. وفي هذا السياق، يشير القرار الإطاري صراحة إلى أن الحالات البسيطة ينبغي ألا تكون مشمولة بالصك.[1574] والاختلاف الرئيسي الثاني هو أن المادة 3 تقيد مدى الانطباق على الحالات التي يكون فيها التدبير الأمني قائم ويتم انتهاكه. وفي اتفاقية الجريمة السيبرانية فإن هذا التقييد خياري فقط.

مشروع اتفاقية ستانفورد الدولية

يعترف المشروع غير الرسمي[1575] لاتفاقية ستانفورد الدولية 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 أُرتكبت إذا قام أي شخص بصورة غير مشروعة وعمداً بممارسة 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؛

[...]

الأفعال المشمولة

يظهر في مشروع الحكم عدد من نقاط التشابه مع المادة 2 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. فالاثنان 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"[1576] المستعمل في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية ويهدف صراحة إلى إدخال مفهوم الدفاع عن النفس.[1577] والاختلاف الآخر عن النهج الإقليمية مثل الاتفاقية بشأن الجريمة السيبرانية 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 حاسوب" المنصوص عليه في الفقرة أ) من المادة 1 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[1578] ورغم أن مشروع الاتفاقية يشير إلى أفعال تتصل بتبادل البيانات، وبالتالي لا يركِّز أساساً على الأنظمة الحاسوبية القائمة على الشبكات، فإن كلا التعريفين يشملان الحواسيب المتصلة توصيلاً بينياً إلى جانب الأجهزة القائمة بذاتها.[1579]

2.2.6 *البقاء غير المشروع*

يمكن انتهاك سلامة أنظمة الحاسوب ليس فقط من خلال الدخول بصورة غير مشروعة إلى نظام حاسوبي، وإنما أيضاً بمواصلة استخدام النظام الحاسوبي بعد انتهاء صلاحية الإذن. ونظراً لأنه لم يتم النفاذ إلى النظام الحاسوبي بصورة غير مشروعة في مثل هذه الحالات، فإن تطبيق أحكام تجريم النفاذ غير المشروع إلى شبكات الحاسوب يمكن أن تكتنفها صعوبات.

مجلس أوروبا

إن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية تجرّم النفاذ غير المشروع إلى نظام حاسوبي ولكنها لا تجرّم البقاء غير المشروع في نظام حاسوبي. ومع ذلك، نوقش البقاء غير المشروع أثناء التفاوض بشأن الاتفاقية. وفي 1998، عندما تم الانتهاء من الصيغة الرابعة لمشروع الاتفاقية بشأن الجريمة السيبرانية، كانت ما زالت تتضمن هذا العنصر.

> ***المادة 2 – الجرائم ضد سرية بيانات وأنظمة الحاسوب وسلامتها وتوفرها***
>
> *يتعين على كل طرف اعتماد هذه التشريعات وغيرها من التدابير التي قد تكون ضرورية لوضع السلوك التالي في قانونها الداخلي كجرائم جنائية [عندما ترتكب عمداً]:*
>
> *[...]*
>
> *1 مكرراً: الفشل المتعمد في الخروج من نظام حاسوبي، يكون شخص قد قام دون قصد بالنفاذ إليه بالكامل أو إلى جزء منه بدون حق، حالما يدرك هذه الحالة [التي لا مبرر لها].*

غير أن الصيغة النهائية للاتفاقية بشأن الجريمة السيبرانية التي فُتح باب التوقيع عليها في 2001 لم تعد تتضمن حكماً من هذا القبيل.

مثال

يشمل النص التشريعي للجريمة السيبرانية لبعض النهج الحديثة مثل تنسيق سياسات تكنولوجيا المعلومات والاتصالات والإجراءات التشريعية والتنظيمية 1593 [1580] أحكاماً محددة لمعالجة هذه المسألة.[1581] وتجرّم المادة 5 البقاء غير المشروع في نظام حاسوبي. وعلى غرار تجريم النفاذ غير المشروع، فإن المصلحة القانونية المحمية هي سلامة أنظمة الحاسوب.

البقاء غير المشروع

5.(1) *أي شخص يقوم عمداً وبدون عذر أو مبرِّر مشروع أو تجاوزاً لعذر أو مبرر مشروع، بالبقاء في نظام حاسوبي بأكمله أو في جزء منه يرتكب جريمة يعاقب عليها في حالة الإدانة بالحبس لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.*

(2) يمكن أن يقرر بلد عدم تجريم البقاء غير المشروع شريطة توفر سبل انتصاف فعالة أخرى. وبدلاً من ذلك قد يتطلب بلد أن تكون الجريمة قد ارتكبت عن طريق خرق التدابير الأمنية أو بِنية الحصول على بيانات الحاسوب أو غيرها من النوايا غير الشريفة.

يبين الحكم الذي لا يرد في شكل مماثل في أيّ من النهج الإقليمية، أن سلامة نظام حاسوبي يمكن أن تُنتهك ليس فقط بالدخول إلى نظام حاسوبي بدون حق، بل ومن خلال البقاء في هذا النظام بعد انتهاء صلاحية الإذن كذلك. ويتطلب البقاء أن يستمر الجاني في النفاذ إلى النظام الحاسوبي. ويمكن أن تطرأ هذه الحالة، على سبيل المثال، إذا ظل الجاني موصلاً بالنظام واستمر في تشغيله. وكونه يتمتع بإمكانية نظرية للدخول إلى النظام الحاسوبي ليس كافياً. وتتطلب المادة 54 أن يرتكب الجاني الجرائم عن قصد. كما أن الأفعال المتهورة غير مشمولة بذلك. وبالإضافة إلى ذلك، لا تجرّم المادة 54 سوى الأفعال التي تُرتكب "بدون عذر أو مبرر مشروع".

3.2.6 الحيازة غير المشروعة لبيانات الحاسوب

تتضمن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية وكذلك قانون الكومنولث النموذجي ومشروع اتفاقية ستانفورد الدولية حلولاً قانونية للاعتراض غير المشروع فقط.[1582] ومن المشكوك فيه أن المادة 3 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية تنطبق على حالات أخرى خلاف الحالات التي تنطوي على ارتكاب جرائم من خلال اعتراض عمليات نقل البيانات. وكما يلاحظ أدناه،[1583] نوقشت باهتمام كبير مسألة ما إن كان النفاذ غير القانوني إلى المعلومات المخزونة على قرص صلب تدخل في عداد المسائل التي تشملها الاتفاقية بشأن الجريمة السيبرانية.[1584] ونظراً لأن عملية النقل عملية مطلوبة، فمن المرجَّح أن المادة 3 من الاتفاقية المتعلقة بالجريمة السيبرانية لا تغطي أشكال التجسُّس على البيانات خلاف اعتراض عمليات النقل.[1585] وهذا أمر مثير للاهتمام علماً أن المشروع التاسع للاتفاقية بشأن الجريمة السيبرانية يشير إلى أهمية تجريم التجسس على البيانات.

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.[1586]

ونظراً لتخزين الكثير من البيانات الحيوية الآن 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.[1587] واليوم يستطيع مستعملو الحاسوب استعمال مختلف أجهزة العتاد وأدوات البرمجيات لحماية المعلومات السرية. فهم يستطيعون إقامة حواجز نيران للحماية وأنظمة مراقبة النفاذ أو تجفير المعلومات المخزونة ويستطيعون بذلك تقليل خطر التجسُّس على البيانات.[1588] 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.[1589] 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.

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.

قانون الولايات المتحدة

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 500 000 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 10 000 000 دولار.

تم إدخال هذا البند 1831[1590] بواسطة قانون التجسس الاقتصادي لعام 1996. وحتى 1996، كان يتم تجريم التجسس الاقتصادي فقط بموجب قوانين الدولة غير المتناسقة إلى حد ما.[1591] ويجرّم قانون التجسس الاقتصادي نوعين أنواع اختلاس الأسرار التجارية الواردة في العنوان 18 – سرقة الأسرار التجارية لصالح حكومة أجنبية أو هيئة أو عميل، وسرقة الأسرار التجارية لتحقيق مزايا اقتصادية، سواء أكانت لصالح حكومة أجنبية أو هيئة أو عميل.[1592] وعلى الرغم من أن الحكم يركز على حماية المحتوى (الأسرار التجارية) ولا يتطلب نسقاً محدداً (بيانات الحاسوب)، فهو لا يتصل بالجريمة التقليدية فقط ولكن بالجرائم المتصلة بالحاسوب أيضاً.[1593] وبصفة عامة، ينطبق العنوان 18 من مدونة الولايات المتحدة، البند 1030 (أ)(2) في مثل هذه الحالات أيضاً. وفيما يتعلق بالقضايا المتصلة بالحاسوب، تكون الأعمال مشمولة بالبند 1831(أ) (2)-(5).[1594]

النص التشريعي للجريمة السيبرانية لسياسات تكنولوجيا المعلومات والاتصالات والإجراءات التشريعية والتنظيمية

وهناك مثال آخر في المادة 8[1595] من النص التشريعي للجريمة السيبرانية لسياسات تكنولوجيا المعلومات والاتصالات والإجراءات التشريعية والتنظيمية.[1596]

التجسس على البيانات

8 (1) *أي شخص يبادر عمداً وبدون عذر أو مبرِّر مشروع أو تجاوزاً لعذر أو مبرر مشروع، بالحصول لنفسه أو لشخص آخر على بيانات حاسوبية غير مقصودة له وتتمتع بحماية خاصة ضد النفاذ غير المصرح به، يرتكب جريمة يعاقب عليها في حالة الإدانة بالحبس لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.*

(2) *يجوز لبلد قصر التجريم على فئات معينة من البيانات الحاسوبية.*

يحمي البند 8 سرية البيانات الحاسوبية المخزنة والمحمية. وتتطلب الحماية الخاصة أن ينفذ مستضيف المعلومات تدابير الحماية التي تزيد بشكل كبير من صعوبة النفاذ إلى البيانات دون الحصول على إذن. ومن أمثلة ذلك التجفير والحماية بكلمة سر. وتشير الملاحظات التوضيحية للنص التشريعي إلى أنه من الضروري أن تتجاوز تدابير الحماية تدابير الحماية المعيارية التي تنطبق على البيانات وعلى غيرها من الممتلكات، مثلاً فرض قيود على النفاذ إلى بعض الأجزاء من المباني الحكومية.[1597]

القانون الجزائي الألماني

يمكن العثور على نهج مماثل في المادة 202أ من القانون الجزائي الألماني في النسخة السارية حتى 2007.[1598]

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.*

وهذا الحكم لا يغطي فقط الأسرار الاقتصادية ولكنه يغطي البيانات المخزونة في الحاسوب عموماً.[1599] 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.[1600] وهكذا، فإن حماية البيانات المخزونة في الحواسيب بموجب القانون الجزائي الألماني تقتصر على حالة الأشخاص أو الشركات التجارية التي تتخذ تدابير لتجنُّب وقوعها ضحية لهذه الجرائم.[1601]

أهمية هذه الأحكام

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.[1602] وفيما يتعلق بمسألة تغطية هذا التصريح للنفاذ إلى النظام الحاسوبي، فإنه ليس من الممكن عموماً تغطية هذه الحالات بالأحكام التي تجرِّم النفاذ غير القانوني.

بغير حق

يتطلب تطبيق الأحكام المتصلة بالتجسُّس على البيانات عموماً أن تكون البيانات التي يتم الحصول عليها بدون موافقة الضحية. ونجاح هجمات التصيُّد الاحتيالي[1603] يثبت بوضوح نجاح الرسائل الاقتحامية استناداً إلى التلاعب بالمستعملين.[1604] ولا يمكن، استناداً إلى الأحكام المذكورة أعلاه، ملاحقة الجناة الذين ينجحون في التلاعب بالمستعملين للإفصاح عن المعلومات السرية، وذلك نظراً لموافقة الضحية.

4.2.6 الاعتراض غير القانوني

يقترن استعمال تكنولوجيا المعلومات والاتصالات بعدة مخاطر تتصل بأمن نقل المعلومات.[1605] 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.[1606] 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؛
- زيادة أهمية المعلومات الشخصية للجناة.

وتتيح تكنولوجيات الشبكات الجديدة (مثل "شبكة المنطقة المحلية اللاسلكية") عدة مزايا للنفاذ إلى الإنترنت.[1607] 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.[1608] وفي معظم الحالات ينشأ الافتقار إلى الحماية عن الافتقار إلى المعرفة بطريقة تشكيل تدابير الحماية.[1609]

وفي الماضي، كان الجناة يركزون أساساً على الشبكات التجارية لاعتراضها بصورة غير قانونية.[1610] إذ إن اعتراض مراسلات الشركات يولِّد على الأرجح معلومات ذات فائدة أكبر من اعتراض البيانات المنقولة داخل الشبكات الخاصة. ويشير ارتفاع عدد حالات انتحال هوية البيانات الشخصية الخاصة إلى أن نقطة تركيز الجناة ربما تكون قد تغيَّرت.[1611] فقد أصبحت البيانات الخاصة، مثل أرقام بطاقات الائتمان وأرقام الضمان الاجتماعي[1612]، وكلمات المرور ومعلومات الحسابات المصرفية ذات أهمية كبيرة للجناة.[1613]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تشمل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية 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.[1614]

الحكم

> ***المادة 3 – الاعتراض غير المشروع***
>
> *تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتُكب عمداً، وبغير حق: الاعتراض باستخدام وسائل فنية، لعمليات إرسال غير عمومية لبيانات حاسوبية إلى أو من أو خلال نظام حاسوبي، بما في ذلك ما ينبعث من نظام حاسوبي من موجات كهرمغنطيسية تحمل هذه البيانات. يجوز لطرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات حاسوبية أو بقصد آخر غير أمين، أو فيما يتعلق بنظام حاسوبي متصل بنظام حاسوبي آخر.*

الأفعال المشمولة

يقتصر انطباق المادة 3 على اعتراض الإرسالات الذي يتحقق بتدابير تقنية.[1615] والاعتراضات التي تتصل بالبيانات الإلكترونية يمكن تعريفها بأنها فعل بقصد الحصول على بيانات أثناء عملية النقل.[1616]

وكما جاء أعلاه، يثور الجدل عند مناقشة مسألة تغطية النفاذ غير القانوني إلى المعلومات المخزونة على قرص صلب بموجب هذا الحكم.[1617] وعموماً ينطبق الحكم فقط على اعتراض الإرسالات – وعدم اعتبار النفاذ إلى المعلومات المخزونة اعتراضاً لعملية الإرسال.[1618] ومناقشة تطبيق الحكم حتى في الحالات التي ينفذ فيها الجاني مادياً إلى نظام حاسوبي قائم بذاته هي مناقشة تنشأ في جانب منها لأن الاتفاقية لا تتضمن حكماً يتصل بالتجسُّس على البيانات[1619] 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.[1620] 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. وتتصل النقطة الثانية بتجريم الحيازة غير المشروعة لبيانات الحاسوب.

ويشير الدليل إلى أن الاعتراض يمكن ارتكابه إما بصورة غير مباشرة من خلال استعمال أجهزة التنصُّت أو "من خلال النفاذ إلى المنظومة الحاسوبية واستعمالها".[1621] وإذا تمكَّن الجناة من النفاذ إلى منظومة حاسوبية واستعمالها لإصدار نُسخ غير مأذون بها من البيانات المخزونة على محرِّك قرص خارجي، بحيث 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.[1622]

ويغطي مصطلح "الإرسال" جميع عمليات إرسال البيانات، سواء كان ذلك بالهاتف أو الفاكس أو البريد الإلكتروني أو نقل الملفات.[1623] وتنطبق الجريمة المحدَّدة بموجب المادة 3 على الإرسالات غير العمومية فقط.[1624] ويكون الإرسال "غير عمومي" إذا كانت عملية الإرسال سرية.[1625] 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".

العنصر الذهني

كما حدث في حالة جميع الجرائم الأخرى المعرَّفة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تقتضي المادة 3 أن يرتكب الجاني جريمته عمداً.[1626] ولا تتضمن الاتفاقية بشأن الجريمة السيبرانية تعريفاً لمصطلح "عمداً". وفي التقرير التفسيري يشير واضعو الاتفاقية إلى أن التعبير "عمداً" ينبغي أن يُعرف على صعيد وطني.[1627]

بغير حق

لا يمكن ملاحقة اعتراض الاتصال بموجب المادة 3 من الاتفاقية بشأن الجريمة السيبرانية إلا إذا وقع هذا الاعتراض "بغير حق".[1628] ويقدِّم واضعو الاتفاقية بشأن الجريمة السيبرانية مجموعة من الأمثلة لعمليات الاعتراض التي لا تجري بغير حق. ويشمل ذلك التصرُّف بناءً على تعليمات أو إذن من جانب المشاركين في عملية الإرسال،[1629] والاختبار المأذون أو أنشطة الحماية المأذونة التي يوافق عليها المشاركون،[1630] والاعتراض القانوني استناداً إلى أحكام القانون الجنائي أو لصالح الأمن القومي.[1631]

وأثيرت قضية أخرى في إطار المفاوضات بشأن الاتفاقية المتعلقة بالجريمة السيبرانية وهي مسألة ما إذا كان استعمال ملفات الارتباط "الكوكيز" تؤدي إلى جزاءات جنائية بموجب المادة 3.[1632] وأشار واضعو الاتفاقية إلى أن الممارسات التجارية الشائعة (مثل ملفات الكوكيز) لا تعتبر عمليات اعتراض بغير حق.[1633]

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.

توجيه الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات

يتضمن توجيه الاتحاد الأوروبي 2013 بشأن الهجمات ضد نظم المعلومات[1634] في المادة 6 حكماً يجرّم الاعتراض غير القانوني.

> ***المادة 6 – الاعتراض غير القانوني***
>
> *تتخذ الدول الأعضاء التدابير اللازمة لضمان أن اعتراض الإرسالات غير العامة من البيانات الحاسوبية، بوسائل تقنية، من نظام معلومات أو إليه أو داخله، بما في ذلك عمليات البث الكهرمغنطيسية من نظام معلومات يحمل هذه البيانات الحاسوبية، عمداً وبغير حق، يعاقب كجريمة جنائية، على الأقل في الحالات التي لا تكون بسيطة.*

الحكم كما صيغ وفقاً للمعايير المحددة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[1635] والفرق الرئيسي هو إمكانية تقييد التجريم في الحالات البسيطة.

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مماثل في المادة 8 من قانون الكومنولث النموذجي لعام 2002.[1636]

> ***الاعتراض غير القانوني للبيانات وما شابهها***
>
> ***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 لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.*

تتبع المادة 8 نهجاً شبيهاً بالمادة 3 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. وعلى غرار الاتفاقية المتعلقة بالجريمة السيبرانية، يحمي الحكم البيانات أثناء عمليات الإرسال غير العامة.

مشروع اتفاقية ستانفورد الدولية

لا يجرِّم مشروع اتفاقية ستانفورد الدولية غير الرسمي[1637] لعام 1999 صراحة اعتراض البيانات الحاسوبية.

5.2.6 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.[1638] ويمكن أن تؤدي الهجمات أو الحصول على هذه

المعلومات إلى خسائر مالية.[1639] وإلى جانب حذف هذه المعلومات، فإن تغييرها يمكن أيضاً أن ينطوي على عواقب جسيمة.[1640] ولم تحقّق 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.[1641]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تتضمن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في المادة 4 حكماً يحمي سلامة البيانات من التداخل غير المأذون.[1642] 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.[1643]

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 أُرتكبت عمداً، وبغير حق: إتلاف، أو محو، أو إفساد، أو تعديل، أو تدمير بيانات موجودة على حاسوب.*
>
> *(2) يجوز لطرف أن يحتفظ بحقه في أن يستلزم أن تتسبَّب الأفعال الموضَّحة بالفقرة 1 في ضرر جسيم.*

الأفعال المشمولة

تجرم المادة 4 أفعال مختلفة. يعني مصطلحا "إتلاف" و"إفساد" أي فعل يتصل بالتعديل السلبي لسلامة المحتوى المعلوماتي في البيانات والبرامج.[1644] ومصطلح "محو" يغطي أي أفعال يتم بموجبها إزالة المعلومات من وسيط التخزين ويعتبر مشابهاً لتدمير الأشياء الملموسة. ولدى وضع التعريف لم يفرّق واضعو الاتفاقية بشأن الجريمة السيبرانية بين الطرق المختلفة التي يمكن بها حذف البيانات.[1645] وإلقاء أي ملف في سلة المهملات الافتراضية لا يزيل الملف من القرص الصلب.[1646] وحتى "تفريغ" سلة المهملات لا يزيل الملف بالضرورة.[1647] ولذلك، فليس من المؤكد إذا كانت القدرة على استعادة ملف محذوف توقف تطبيق الحكم.[1648] ويشير "تدمير" البيانات الحاسوبية إلى عمل يؤثر على توفر البيانات للشخص الذي يملك النفاذ إلى الوسيط، حيث يتم تخزين المعلومات بطريقة سلبية.[1649] ونوقش تطبيق هذا الحكم بصورة خاصة في صدد منع الخدمة[1650] بسبب الهجمات.[1651] وأثناء هذا الهجوم لا تعود المعلومات المتوفِّرة على المنظومة الحاسوبية المستهدفة متوفِّرة للمستعمل المحتمل أو لصاحب المنظومة الحاسوبية.[1652] ويغطي مصطلح "تعديل" تغيير البيانات القائمة بدون أن يؤدي ذلك بالضرورة إلى تقليل إمكانية الاستفادة من البيانات.[1653] وهذا الفعل يغطي بوجه خاص تركيب برمجيات ضارة مثل برمجيات التجسُّس أو الفيروسات أو برامج الإعلانات في حاسوب الضحية.[1654]

العنصر الذهني

كما يحدث في حالة جميع الجرائم الأخرى المعرَّفة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تقتضي المادة 4 أن يرتكب الجاني جريمته عمداً.[1655] ولا تتضمن الاتفاقية المتعلقة بالجريمة السيبرانية تعريفاً لمصطلح "عمداً". وفي التقرير التفسيري يشير واضعو الصياغة إلى أن التعبير "عمداً" ينبغي أن يُعرّف على صعيد وطني.[1656]

بغير حق

يجب أن يكون ارتكاب الأفعال "بغير حق"[1657] على نحو مشابه للأحكام التي نوقشت أعلاه. وقد نوقش الحق في تغيير البيانات، وخاصة في سياق "أنظمة إعادة إرسال الرسائل".[1658] وتستعمل أنظمة إعادة إرسال الرسائل لتعديل بعض البيانات

بغرض تسهيل الاتصالات مجهولة الهوية.[1659] ويذكر التقرير التفسيري أن هذه الأفعال تعتبر من ناحية المبدأ حماية مشروعة للخصوصية ولهذا يمكن اعتبار أنها تجري بأذن.[1660]

التقييدات والتحفظات

تتيح المادة 4 خيار تقييد التجريم من خلال الاقتصار على الحالات التي ينشأ عنها ضرر جسيم، وهو نهج يشبه النهج المتّبع في القرار الإطاري للاتحاد الأوروبي بشأن الهجمات ضد أنظمة المعلومات[1661]، وهو ما يمكِّن الدول الأعضاء من الاقتصار في تطبيق حكم القانون الجنائي الموضوعي على "الحالات غير البسيطة".[1662]

توجيه الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات

يتضمن توجيه الاتحاد الأوروبي لعام 2013 بشأن الهجمات ضد نظم المعلومات[1663] في المادة 5 حكماً يجرّم التدخل غير القانوني في البيانات.

> ***المادة 5 – التدخل في البيانات***
>
> *تتخذ الدول الأعضاء التدابير اللازمة لضمان أن حذف البيانات من نظام معلومات أو إتلافها أو تشويهها أو تغييرها أو إزالتها، أو جعل هذه البيانات غير قابلة للنفاذ، عمداً وبغير حق، يعاقب كجريمة جنائية، على الأقل في الحالات التي لا تكون بسيطة.*

الحكم كما صيغ وفقاً للمعايير المحددة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[1664] والفرق الرئيسي هو إمكانية تقييد التجريم في الحالات البسيطة.

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج يتسق مع المادة 4 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في المادة 8 من قانون الكومنولث النموذجي لعام 2002.[1665]

الحكم

> ***التداخل الضار في البيانات***
>
> ***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؛*
>
> *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؛*
>
> *هـ) أو حرمان أي شخص يحق له النفاذ إلى البيانات من النفاذ إليها؛*
>
> *فإنه يرتكب جريمة يعاقب عليها بعد الإدانة بالحبس لمدة 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.*

والاختلاف الرئيسي الأول بين المادة 6 والحكم المقابل في الاتفاقية المتعلقة بالجريمة السيبرانية هو أن هذا الحكم الوارد في قانون الكومنولث النموذجي[1666] يجرم الأفعال المتهورة والأفعال المتعمدة أيضاً. وخلافاً للمادة 6، فإن ثلاثة أحكام أخرى من القانون النموذجي، مثل الاتفاقية المتعلقة بالجريمة السيبرانية، تقصر التجريم على الأفعال المتعمدة. وتغطية الاستهتار توسّع

النهج إلى حد كبير، علماً أن حتى محو الملفات غير المقصود من نظام حاسوبي أو إتلاف جهاز تخزين من شأنه أن يؤدي إلى فرض عقوبات جنائية.

والاختلاف الثاني هو أن الأحكام المشمولة بالمادة 6 تختلف بشكل طفيف عن الحكم المقابل في الاتفاقية المتعلقة بالجريمة السيبرانية. وأخيراً، يتضمن الحكم توضيحاً في الجزء الفرعي 2 يشير إلى أن الآثار المؤقتة مشمولة أيضاً وليس الأثر الدائم فقط.

مشروع اتفاقية ستانفورد الدولية

يتضمن مشروع اتفاقية ستانفورد الدولية غير الرسمي[1667] 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية وقانون الكومنولث النموذجي من جهة والنهج المتبع في مشروع ستانفورد من جهة أخرى هو أن مشروع ستانفورد 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية وقانون الكومنولث النموذجي نهجاً أكثر اتساعاً بحمايتهما سلامة البيانات الحاسوبية دون الاشتراط الإلزامي بإحداث آثار أخرى.

6.2.6 التداخل في النظام

يعتمد الأشخاص أو مؤسسات الأعمال التي تعرض خدمات تستند إلى تكنولوجيا المعلومات والاتصالات على سير عمل أنظمتهم الحاسوبية.[1668] وعدم توفُّر صفحات شبكة الويب التي تقع ضحية لهجمات منع الخدمة (DOS)[1669] تثبت مدى خطورة تهديد هذه الهجمات.[1670] وهجمات من هذا القبيل يمكن أن تسبِّب خسائر مالية خطيرة وتؤثر حتى على الأنظمة القوية.[1671] 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.[1672]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

لحماية نفاذ المشغلين والمستعملين إلى تكنولوجيا المعلومات والاتصالات تدخل الاتفاقية المتعلقة بالجريمة السيبرانية حكماً في المادة 5 يجرِّم الإعاقة المتعمَّدة للاستعمال القانوني للأنظمة الحاسوبية.[1673]

الحكم

> ***المادة 5 – التدخل في النظام***
>
> *تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما أُرتُكِب عمداً، وبغير حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال أو إرسال، أو إتلاف، أو محو، أو تغيير، أو تبديل، أو تدمير بيانات حاسوبية.*

الأفعال المشمولة

يتطلب تطبيق الحكم إعاقة تشغيل النظام الحاسوبي.[1674] وتعني "الإعاقة" أي فعل يتداخل في التشغيل الصحيح للنظام الحاسوبي.[1675] ويقتصر تطبيق الحكم على الحالات التي تحدث فيها الإعاقة بأحد الأفعال المذكورة. وبالإضافة إلى ذلك، يتطلب الحكم أن تكون الإعاقة "خطيرة". وتقع على الأطراف مسؤولية تحديد المعايير التي يتعيَّن الوفاء بها من أجل اعتبار الإعاقة خطيرة.[1676] ويمكن أن تشمل التقييدات المحتملة بموجب القانون الوطني قدراً أدنى من الضرر، وكذلك اقتصار التجريم على الهجمات ضد الأنظمة الحاسوبية الهامة.[1677]

وقائمة الأفعال التي تؤثر على تشغيل النظام الحاسوبي بطريقة سلبية قائمة جامعة.[1678]

ولا تعرِّف الاتفاقية بشأن الجريمة السيبرانية 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.[1679]

ومصطلح "إتلاف" و"تغيير" يتداخلان ويعرفهما واضعو الاتفاقية المتعلقة بالجريمة السيبرانية في التقرير التفسيري بشأن المادة 4 باعتبارهما تبديل سلبي في سلامة المحتوى المعلوماتي للبيانات والبرامج.[1680]

وعرَّف واضعو الاتفاقية أيضاً مصطلح "محو" ويغطي التقرير التفسيري بشأن المادة 4 الأفعال التي يتم بها إزالة المعلومات من وسيط التخزين.[1681]

ومصطلح "تبديل" يغطي تعديل البيانات القائمة بدون أن يقلِّل ذلك بالضرورة من إمكانية استخدام البيانات.[1682]

ويشير "تدمير" البيانات الحاسوبية إلى فعل يؤثر على توفُّر البيانات للشخص الذي يملك النفاذ إلى الوسيط الذي يتم فيه تخزين المعلومات بطريقة سلبية.[1683]

تطبيق الحكم بصدد الرسائل الاقتحامية

نوقشت إمكانية معالجة مشكلة رسائل البريد الإلكتروني الاقتحامية[1684] تحت المادة 5، نظراً لأن الرسائل الاقتحامية يمكن أن تشكِّل حمولة زائدة على الأنظمة الحاسوبية.[1685] 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".[1686] ولاحظ واضعو الاتفاقية أيضاً أن الأطراف قد تعتنق نهجاً مختلفاً في التعامل مع الإعاقة بموجب تشريعاتها الوطنية،[1687] مثل اعتبار أفعال التداخل جرائم إدارية أو خاضعة للجزاءات.[1688]

العنصر الذهني

كما يحدث في حالة جميع الجرائم الأخرى المعرَّفة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تقتضي المادة 5 أن يرتكب الجاني جريمته عمداً.[1689] ويشمل ذلك قصد القيام بأحد الأفعال المذكورة وكذلك قصد إحداث إعاقة خطيرة لعمل النظام الحاسوبي.

ولا تتضمن الاتفاقية بشأن الجريمة السيبرانية تعريفاً لمصطلح "عمداً". وفي التقرير التفسيري يشير واضعو الاتفاقية إلى أن التعبير "عمداً" ينبغي أن يُعرف على صعيد وطني.[1690]

بغير حق

يتعيَّن اقتراف الفعل "بغير حق".[1691] وكما ذكرنا أعلاه شعر مديرو الشبكات وشركات الأمن التي تختبر حماية الأنظمة الحاسوبية بالخوف من إمكانية تجريم عملهم.[1692] 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.[1693]

التقييدات والتحفظات

بعكس المادة 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 لضبط التجريم أثناء عملية التنفيذ. ويمكن الاطلاع على نهج مماثل في القرار الإطاري[1694] للاتحاد الأوروبي بشأن الهجمات ضد الأنظمة الحاسوبية.[1695]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج يتسق مع المادة 5 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في المادة 7 من قانون الكومنولث النموذجي لعام 2002.[1696]

الحكم

التداخل الضار في نظام حاسوبي

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

أ) بإعاقة سير عمل نظام حاسوبي أو التداخل فيه؛

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

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

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 الحكم المقابل في اتفاقية المجلس الأوروبي هو أن المادة 7 من قانون الكومنولث النموذجي تنص على تجريم الأفعال التي تجري باستهتار. وحتى قطع التيار الكهربائي دون قصد أثناء أعمال البناء يمكن أن يؤدي إلى فرض عقوبات جنائية. ويتجاوز القانون النموذجي باعتناقه هذا النهج الاشتراطات الواردة في الاتفاقية المتعلقة بالجريمة السيبرانية. وهناك

اختلاف آخر وهو أن تعريف "الإعاقة" في المادة 7 من قانون الكومنولث النموذجي يتضمن قائمة بالأفعال مقارنة بالمادة 5 من اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية.

توجيه الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات

يتضمن توجيه الاتحاد الأوروبي لعام 2013 بشأن الهجمات ضد نظم المعلومات[1697] في المادة 4 حكماً يجرّم التدخل غير القانوني في النظم.

> ***المادة 4 – التدخل غير القانوني في النظم***
>
> *تتخذ الدول الأعضاء التدابير اللازمة لضمان أن عرقلة عمل نظام معلومات بشكل جدي أو توقيفه عن العمل من خلال إدخال بيانات حاسوبية أو بإرسال هذه البيانات أو إتلافها أو حذفها أو تشويهها أو تغييرها أو إزالتها، أو جعل هذه البيانات غير قابلة للنفاذ، عمداً وبغير حق، يعاقب كجريمة جنائية، على الأقل في الحالات التي لا تكون بسيطة.*

الحكم كما صيغ وفقاً للمعايير المحددة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. والفرق الرئيسي هو إمكانية تقييد التجريم في الحالات البسيطة. ويقوم هذا النهج على اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. والاختلاف الرئيسي الأول هو أن المادة 4 تجرّم أيضاً إعاقة تشغيل نظام المعلومات من خلال جعل بيانات الحاسوب غير قابلة للنفاذ بالإضافة إلى الأفعال التي تغطيها الاتفاقية المتعلقة بالجريمة السيبرانية (إدخال وإرسال وإلحاق الضرر ومحو وإتلاف وتغيير وإلغاء). وتصبح البيانات غير قابلة للنفاذ إذا قام الجاني بمنع شخص من الوصول إليها عن طريق ارتكاب الفعل. ولكن، على الرغم من قائمة الأفعال الأكثر تعقيداً في المادة 4، ليس هناك اختلاف عن المادة المقابلة في اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية بحيث أن عملية جعل البيانات غير قابلة للنفاذ مشمولة بفعل محو بيانات الحاسوب. ويبين تفسير مشروع النسخة التاسعة عشرة من الاتفاقية بشأن الجريمة السيبرانية أن فريق الخبراء الذي وضع الاتفاقية بشأن الجريمة السيبرانية اتفق على أن التعبير إلغاء يحمل معنيين: حذف البيانات بحيث لم تعد موجودة فعلياً وجعل البيانات غير قابلة للنفاذ.[1698]

مشروع اتفاقية ستانفورد الدولية

يتضمن مشروع اتفاقية ستانفورد الدولية غير الرسمي[1699] لعام 1999 حكماً يجرّم 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية وقانون الكومنولث النموذجي والنهج المتّبع في مشروع ستانفورد هو أن مشروع ستانفورد يغطي أي تلاعب في الأنظمة الحاسوبية، في حين أن اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية وقانون الكومنولث النموذجي يقصران التشغيل على إعاقة تشغيل النظام الحاسوبي.

7.2.6 المواد المثيرة جنسياً أو المواد الإباحية

يتباين تجريم المحتوى غير القانوني والمحتوى الصريح جنسياً كما تتباين خطورة هذا التجريم من بلد لآخر.[1700] وكانت الأطراف التي تفاوضت على اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية قد ركَّزت على تنسيق القوانين المتعلقة باستخدام الأطفال في المواد الإباحية واستبعدت التجريم الواسع للمواد المثيرة جنسياً والمواد الإباحية. وعالجت بعض البلدان هذه المشكلة بتطبيق أحكام تجرِّم تبادل المواد الإباحية 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.[1701]

أمثلة

يرد أحد أمثلة تجريم تبادل المواد الإباحية في المادة 184 من القانون الجزائي الألماني.

المادة 184 – نشر الكتابات الإباحية

(1) أي شخص، فيما يتعلق بالكتابات الإباحية (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 الإباحية لا ينبغي تجريمها إذا لم يمس الموضوع أشخاصاً قاصرين.[1702] واستناداً إلى ذلك يهدف القانون إلى حماية تنمية القُصَّر دون إزعاج.[1703] وتجري مناقشة حامية لمسألة ما إن كان النفاذ إلى المواد الفاضحة يؤثر سلباً على تنمية القُصَّر.[1704] ولا تجرِّم المادة 184 تبادل الكتابات الإباحية بين الكبار. ومصطلح "الكتابات" لا يغطي فقط الكتابات التقليدية ولكنه يغطي أيضاً التخزين الرقمي.[1705] وبالمثل، فإن "تسهيل الاطلاع عليها" لا ينطبق فقط على الأفعال خارج الإنترنت ولكنه يغطي أيضاً الحالات التي يوفِّر فيها الجناة المحتوى الإباحي في مواقع شبكة الويب.[1706]

والمادة 4.ج.1 من مشروع القانون التشريعي رقم 3777 لعام 2007[1707] في الفلبين تقدِّم مثالاً لنهج يتجاوز هذه القاعدة ويجرِّم أي محتوى جنسي.

> ***المادة 4.ج.1:*** *الجرائم المتصلة بالجنس في الفضاء 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 ' 1 ':*** *الجنس السيبراني أو الجنس الافتراضي – ويشير إلى أي شكل من أشكال النشاط الجنسي أو الإثارة الجنسية بمساعدة الحواسيب أو شبكات الاتصال*

ويعتنق هذا الحكم نهجاً عريضاً جداً، نظراً لأنه يجرِّم أي نوع من الإعلانات الجنسية أو تسهيل النشاط الجنسي عبر الإنترنت. وبسبب مبدأ ازدواج الجُرم[1708] تسير التحقيقات الدولية في صدد هذه النُهج الواسعة بصعوبة.[1709]

8.2.6 استغلال الأطفال في المواد الإباحية

تتجه الإنترنت إلى أن تكون الأداة الرئيسية لتجارة وتبادل المواد التي تحتوي على صور فاضحة للأطفال.[1710] والأسباب الرئيسية لهذا التطوُّر هي سرعة وكفاءة الإنترنت في نقل الملفات وانخفاض تكاليف الإنتاج والتوزيع والاعتقاد باختفاء الهوية.[1711] ويستطيع ملايين المستعملين في كل أنحاء العالم[1712] النفاذ إلى الصور المنشورة في صفحات الويب وتفريغها. ومن أهم أسباب "نجاح" صفحات الويب التي تعرض المواد الإباحية أو حتى المواد الإباحية التي يستغل فيها 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[1713] ما لم يلجأ المستعمل إلى أساليب الاتصال مجهول الهوية. ومعظم مستعملي الإنترنت لا يدركون الأثر الإلكتروني الذي يتركونه أثناء التصفُّح.[1714]

يُقصد بالأحكام التي تجرم المواد الإباحية بشكل عام حماية المصالح القانونية المختلفة. ويسعى تجريم إنتاج المواد الإباحية إلى حماية الأطفال من الوقوع ضحية للاعتداء الجنسي.[1715] وفيما يتعلق بحظر الأفعال المتصلة بتبادل المواد الإباحية التي يستغل فيها الأطفال (عرض، توزيع) فضلاً عن حيازتها، فإن التجريم يُراد به تدمير السوق نظراً لأن الطلب المستمر على المواد الجديدة يمكن أن يحفز المجرمين على مواصلة الاعتداء على الأطفال.[1716] وإضافة إلى ذلك، يسعى حظر التبادل إلى جعل من الصعب أكثر على الناس الحصول على هذه المواد وبذلك منع تأثير مثير على الاستغلال الجنسي للأطفال. وأخيراً، يُقصد بالتجريم منع المجرمين من استخدام المواد الإباحية التي يستغل فيها الأطفال لإغراء الأطفال بالمشاركة في جماع جنسي.[1717]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

لتحسين وتنسيق حماية الأطفال من الاستغلال الجنسي،[1718] تشمل الاتفاقية مادة تعالج الصور الإباحية للأطفال.

الحكم

المادة 9 – الجرائم المتعلقة بالصور الإباحية 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 الإباحية بغرض توزيعها عبر نظام حاسوبي؛

ب) عرض أو توفير صور الأطفال الفاضحة عبر نظام حاسوبي؛

ج) توزيع أو بث صور أطفال فاضحة عبر نظام حاسوبي؛

د) الحصول على صور الأطفال الفاضحة عبر نظام حاسوبي لصالح الشخص ذاته أو لصالح الغير؛

هـ) حيازة صور الأطفال الفاضحة داخل نظام حاسوبي أو بوسيط تخزين بيانات حاسوبية؛

(2) لغرض الفقرة 1 أعلاه، 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.

(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(هـ) 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.[1719] ولهذا، فإن الاتفاقية بشأن الجريمة السيبرانية لم تقف عند حد سد الثغرات في القوانين الجنائية الوطنية[1720] - بل تسعى أيضاً إلى تنسيق مختلف اللوائح.[1721]

الأفعال المشمولة

يصف "الإنتاج" أي عملية لاستحداث مواد إباحية يستغل فيها الأطفال. وهناك مناقشة جارية بشأن تفسير هذا المصطلح. وفي المملكة المتحدة، يعتبر تنزيل صور إباحية يستغل فيها الطفل كإنتاج ("صنع") مواد إباحية يستغل فيها الأطفال.[1722] ويشير التمييز بين "حيازة" و"إنتاج" في المادة 9 من اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية أن واضع الاتفاقية لم يعتبر مجرد تنزيل مواد إباحية يستغل فيها الأطفال إنتاجاً. ومع ذلك يجب زيادة التفريق بين هذين التعبيرين حتى على أساس التمييز الوارد في الاتفاقية بشأن الجريمة السيبرانية. وإن التقاط الجاني لصور طفل يتعرض لاعتداء جنسي هو بمثابة إنتاج مواد إباحية يستغل فيها الأطفال؛ ولكن من غير المؤكد ما إذا كان الشخص الذي يستخدم صوراً إباحية في شكل رسوم متحركة يعتبر أيضاً أنه ينتج مواداً إباحية يستغل فيها الأطفال. وعلى الرغم من أنه منتج الرسوم المتحركة بالتأكيد، ليس من المؤكد ما إذا كان المصطلح "إنتاج" في اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية قابلاً للتطبيق فقط إذا كان في شكل وثائق بشأن الاعتداء الفعلي على الطفل. ونظراً لأن الاتفاقية بشأن الجريمة السيبرانية تقصد تجريم إنتاج المواد الإباحية الوهمية التي يستغل فيها الأطفال – التي لا تقتضي الاعتداء الفعلي للطفل – فإن ذلك يشكل حجّة تؤيد تفسيراً واسعاً للمصطلح "إنتاج".[1723]

ومن ناحية أخرى، يشير التقرير التفسيري للاتفاقية بشأن الجريمة السيبرانية إلى أن تجريم الإنتاج مطلوب لمكافحة الخطر "في المصدر". وعلى الرغم من أن اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية لا تحدد نية واضعي الاتفاقية، يقدم التقرير التفسيري لاتفاقية المجلس الأوروبي بشأن حماية الأطفال[1724] تفسيراً أكثر تحديداً للعوامل التي تدفع واضعو الاتفاقية إلى وضع حكم مماثل.[1725] وأبرز واضعو الاتفاقية بشأن حماية الأطفال أن تجريم إنتاج المواد الإباحية التي يستغل فيها الأطفال "ضروري لمكافحة أعمال الاعتداء والاستغلال الجنسي في مصدرها". ويمكن اعتبار ذلك حجة تؤيد اتباع نهج أضيق.

من الضروري أن يجري إنتاج المواد الإباحية التي يستغل فيها الأطفال للتوزيع من خلال نظام حاسوبي. وإذا كان الجاني ينتج هذه المواد لاستخدامه الخاص، أو يعتزم توزيعه في شكل غير إلكتروني، لا تنطبق المادة 9 من اتفاقية مجلس الأوروبي بشأن الجريمة السيبرانية. ونوقشت مشكلة أخرى في سياق الإنتاج ألا وهي تغطية التصوير الذاتي.[1726] وإذا قام الجاني، عن بُعد، بإقناع طفل بالتقاط صور فاضحة لنفسه، يمكن أن يؤدي ذلك إلى تجريم الضحية (الطفل) وليس المجرم تبعاً للتشريعات الوطنية.

ويغطي التعبير "عرض" التماس الآخرين للحصول على مواد إباحية يستغل فيها الأطفال. وليس من الضروري أن تتاح هذه المواد على أساس تجاري، ولكنها تعني ضمناً أن الجاني الذي يعرض هذه المواد قادر على توفيرها.[1727] ويشير التعبير "إتاحة" إلى فعل يمكّن المستخدمين الآخرين من الحصول على المواد الإباحية التي يستغل فيها الأطفال. ويمكن أن يرتكب الفعل من خلال إتاحة المواد الإباحية التي يستغل فيها الأطفال على مواقع إلكترونية أو التوصيل بنظام تقاسم الملفات وتمكين الآخرين من الوصول إلى هذه المواد بواسطة قدرات أو مجلدات تخزين غير مسدودة.

ويغطي التعبير "توزيع" أعمالاً نشطة تتمثل في إعادة توجيه المواد الإباحية لأشخاص آخرين. ويغطي التعبير "إرسال" جميع عمليات الاتصال عن طريق الإشارات المرسلة. ويغطي التعبير "حيازة" من أجل الشخص ذاته أو شخص آخر أي عمل بقصد الحصول الفعال على مواد إباحية.

وأخيراً تجرّم المادة 9 "حيازة" المواد الإباحية التي يستغل فيها الأطفال. ويختلف تجريم الحيازة أيضاً بين الأنظمة القانونية الوطنية.[1728] ويمكن أن يؤدي الطلب على هذه المواد إلى استمرار إنتاجها.[1729] ويمكن أن تشجع حيازة هذه المواد على الاعتداء الجنسي للأطفال، ولذا يشير واضعو الاتفاقية إلى أن أحد السبل الفعالة للحد من إنتاج المواد الإباحية التي يستغل فيها الأطفال هو جعل حيازة هذه المواد غير مشروعة.[1730] ومع ذلك، تمكّن الاتفاقيات الأطراف الفاعلة في الفقرة 4، من استبعاد تجريم مجرد حيازة هذه المواد بقصر المسؤولية الجنائية على إنتاج المواد الإباحية التي يستغل فيها الأطفال وعرضها وتوزيعها فقط.[1731] وتنطوي الحيازة على التحكم الذي يمارسه شخص عمداً على استغلال الأطفال في المواد الإباحية. ويتطلب ذلك أن يتمتع الجاني بالتحكم، الذي لا يقتصر على الحالة المتعلقة بأجهزة التخزين المحلي بل وأجهزة التخزين عن بُعد التي يمكن أن ينفذ إليها ويتحكم فيها. وعلاوة على ذلك، تتطلب الحيازة عموماً عنصراً ذهنياً كما ورد في التعريف أعلاه.

استغلال الأطفال في المواد الإباحية

تقدم الفقرة 2 من المادة 9 ثلاث فقرات فرعية بشأن مواد تصور استغلال الأطفال في مواد إباحية بشكل مرئي: مشاركة قاصر في سلوك جنسي صريح، ومشاركة شخص يبدو أنه قاصر في سلوك جنسي صريح، وصور واقعية تمثل قاصراً يشارك في سلوك جنسي صريح. ونظراً لأن التصوير المرئي مطلوب فإن الملفات الصوتية مستبعدة.

على الرغم من أن واضعي الاتفاقيات يسعون إلى تحسين حماية الأطفال من الاستغلال الجنسي، فإن المصالح القانونية التي تغطيها الفقرة 2 أوسع نطاقاً. وتركز الفقرة 2 (أ) مباشرة على الحماية ضد إساءة معاملة الأطفال. وتشمل الفقرتان 2(ب) و2(ج) صوراً أنتجت دون انتهاك حقوق الطفل مثل الصور التي أنتجت باستخدام برمجية النمذجة ثلاثية الأبعاد.[1732] والسبب في تجريم المواد الإباحية الوهمية التي يستغل فيها الأطفال هو أن هذه الصور، دون أن تؤدي بالضرورة إلى إلحاق الضرر "بطفل حقيقي"، يمكن استعمالها لإغراء الأطفال بالمشاركة في مثل هذه الأعمال.[1733]

وأحد التحديات الرئيسية المتعلقة بالتعريف هو أنه يركز على التصوير المرئي. واستغلال الأطفال في مواد إباحية لا يُوزع بالضرورة في شكل صور أو أفلام، وإنما في شكل ملفات صوتية أيضاً.[1734] ونظراً لأن الحكم الوارد في المادة 9 يشير إلى "المواد التي تشمل التصوير المرئي" للطفل، فإن هذا الحكم لا يشمل الملفات الصوتية. ونتيجة لذلك، تعتمد نهج أكثر حداثة مثل النص التشريعي[1735] للجريمة السيبرانية لسياسات تكنولوجيا المعلومات والاتصالات والإجراءات التشريعية والتنظيمية نهجاً مختلفاً وتتفادى المصطلح "مرئياً".[1736]

تعاريف

3

[...]

(4) تشير المواد الإباحية التي يستغل فيها الأطفال إلى المواد الإباحية التي تصور أو تقدم أو تمثل:

أ) طفلاً يشارك في سلوك جنسي صريح؛

ب) شخصاً يبدو أنه طفل يشارك في سلوك جنسي صريح؛ أو

ج) صوراً تمثل طفلاً يشار في سلوك جنسي صريح؛ ويشمل ذلك أي مواد إباحية سمعية أو مرئية أو نصية ولكن دون الاقتصار عليها.

وقد يقيد بلد التجريم بعدم تنفيذ البندين ب) و ج).

ويمكن العثور على تعريف أوسع آخر في الفقرة ج) من المادة 2 من البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلالهم في البغاء وفي المواد الإباحية.

المادة 2

لأغراض هذا البروتوكول:

[...]

ج) تشير المواد الإباحية التي يستغل فيها الأطفال إلى كل تمثيل للطفل، بأي وسيلة كانت، وهو يشارك في ممارسة جنسية صريحة سواء كانت بصورة حقيقية أو عن طريق المحاكاة أو كل تصوير للأعضاء الجنسية للطفل لأغراض الاستغلال الجنسي أساساً.

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[1737] بأنه أي شخص يقل عمره عن 18 سنة. وتعرِّف بلدان أخرى القاصر بأنه شخص يقل عمره عن 14 سنة.[1738] ويوجد نهج مشابه في القرار الإطاري لمجلس الاتحاد الأوروبي لعام 2003 بشأن مكافحة الاستغلال الجنسي للأطفال والمواد الإباحية للأطفال[1739] واتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي.[1740] وتشدِّد الاتفاقية على أهمية وجود معيار دولي واحد يتعلَّق بالسن وتعرِّف الاتفاقية بشأن الجريمة السيبرانية المصطلح وفقاً لاتفاقية الأمم المتحدة.[1741] ومع ذلك، تسمح الاتفاقية باقتضاء حد عمري مختلف لا يقل عن 16 سنة، وذلك اعترافاً منها بالاختلافات الكبيرة في القوانين الوطنية القائمة. وإحدى المشاكل التي تجري مناقشتها بصورة متزايدة هو التجريم الذي يحتمل أن يكون غير مقصود في الحالات التي يختلف فيها تعريف سن الموافقة على ممارسة الجنس والحد العمري.[1742] فعلى سبيل المثال يُعرّف استغلال الأطفال في المواد الإباحية كتصوير مرئي للأفعال الجنسية لشخص دون سن 18 عاماً وفي الوقت نفسه فإن سَن الرضا الجنسي هو 16 عاماً،

فمن الناحية القانونية، يمكن لشخصين يبلغان من العمر 17 عاماً أن يمارسان علاقة جنسية ولكنهما سوف يرتكبان جريمة خطيرة (إنتاج مواد إباحية يستغل فيها الأطفال) إذا قاموا بالتقاط صور أو أفلام تشمل هذا الفعل.[1743]

العنصر الذهني

كما حدث في حالة جميع الجرائم المعرَّفة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تقتضي المادة 9 أن يرتكب الجاني جريمته عمداً.[1744] وفي التقرير التفسيري يشير واضعو الاتفاقية صراحة إلى أن التفاعل مع المواد الفاضحة للأطفال بدون أي قصد ليس مشمولاً في الاتفاقية بشأن الجريمة السيبرانية. 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 بشأن الجريمة السيبرانية إلا إذا نُفذت هذه الأفعال "بغير حق".[1745] ولم يُدرج واضعو الاتفاقية بشأن الجريمة السيبرانية أي نص آخر يوضِّح الحالات التي يتصرف فيها المستعمل بموجب إذن. وعموماً يجري الفعل "بغير حق" إلا إذا كان تصرفاً من جانب وكالات إنفاذ القوانين في إطار أحد التحقيقات.

اتفاقية مجلس أوروبا بشأن حماية الأطفال

يرد نهج آخر لتجريم الأفعال المتصلة بالمواد الفاضحة للأطفال في المادة 20 من اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي.[1746]

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؛

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) وهـ) 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية ولذلك يتشابه إلى درجة كبيرة مع ذلك الحكم.[1747] والاختلاف الرئيسي هو أن الاتفاقية المتعلقة بالجريمة السيبرانية تركِّز على تجريم الأفعال المتصلة بخدمات المعلومات والاتصالات ("إنتاج صور الأطفال الفاضحة بغرض توزيعها عبر النظام الحاسوبي") 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 السيبرانية. فهي تجرِّم فعل الحصول على النفاذ إلى صور الأطفال الفاضحة عبر الحاسوب استناداً إلى الفقرة 1 و) من المادة 20 في اتفاقية حماية الطفل. ويشمل فعل الحصول أي فعل للشروع في عملية عرض معلومات متاحة من خلال تكنولوجيا المعلومات والاتصالات. وهذا هو الحال، على سبيل المثال، إذا أدخل الجاني اسم الميدان لموقع ويب معروف خاص بالمواد الإباحية التي يستغل فيها الأطفال وبدأ عملية تلقي المعلومات من الصفحة الأولى مما ينطوي على عملية تنزيل آلي ضروري. ويمكِّن ذلك وكالات إنفاذ القانون من ملاحقة الجناة في حالة تمكنها من إثبات أن الجاني فتح مواقع في شبكة الويب تتضمن 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 التجفير لحماية الملفات التي يتم تنزيلها على وسيط التخزين لديه.[1748] ويشير التقرير التفسيري لاتفاقية حماية الطفل إلى أن ذلك الحكم ينبغي أن ينطبق أيضاً في الحالات التي يقوم فيها الجاني فقط بمشاهدة صور الأطفال الفاضحة على الخط دون تنزيلها.[1749] وعموماً، فإن فتح موقع في شبكة الويب يبدأ عملية التنزيل تلقائياً – ويكون ذلك في كثير من الأحيان بدون معرفة المستعمل.[1750] ولذلك، فإن الحالة المذكورة في التقرير التفسيري لا تتصل إلا بالحالات التي لا يحدث فيها تنزيل في الخلفية. ولكنه ينطبق أيضاً في الحالات التي يمكن مشاهدة المواد الإباحية التي يستغل فيها الأطفال بدون تنزيل هذه المواد. ويمكن أن يحدث ذلك إذا كان الموقع الإلكتروني يتيح تدفق التسجيلات الفيديوية ولا يقوم بتخزين المعلومات المتلقاة ولكنه يستبعدها بعد الإرسال مباشرة (مثلاً إذا كان الجاني يستخدم التدفق الفيديوي) وذلك نظراً للتشكيلة التقنية لعملية التدفق.

قانون الكومنولث النموذجي بشأن الجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج يتماشى مع المادة 9 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في المادة 10 من قانون الكومنولث النموذجي لعام 2002.[1751]

استغلال الأطفال في المواد الإباحية

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.[1752]

(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.[1753]

(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 تمثّل 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية هي أن قانون الكومنولث النموذجي لا يقدِّم تعريفاً محدَّداً لمصطلح القاصر ويترك ذلك للدول الأعضاء لتحديد الحد العمري. وعلى غرار اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، لا ينص قانون الكومنولث النموذجي على تجريم الحصول على النفاذ إلى المواد الإباحية من خلال تكنولوجيا المعلومات.

البروتوكول الاختياري لاتفاقية الأمم المتحدة بشأن حقوق الطفل

يمكن العثور على نهج محايد تكنولوجياً في المادة 3 من البروتوكول الاختياري المتعلق ببيع الأطفال واستغلالهم في البغاء وفي المواد الإباحية.

المادة 3

1 كل دولة طرف ملزمة بكفالة أن يغطي قانونها الجنائي أو الجزائي تغطية كاملة وكحد أدنى الأفعال والأنشطة التالية، سواء ارتكبت تلك الجرائم داخل البلد أو عبر الحدود، وسواء على أساس فردي أو منظم:

[...]

ج) إنتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالطفل للأغراض المذكورة أعلاه على النحو المبين في المادة 2.

[...]

وعلى الرغم من أن البروتوكول الاختياري يشير صراحة إلى دور شبكة الإنترنت في توزيع هذه المواد،[1754] فإنه يجرم الأفعال المتصلة بالمواد الإباحية المتعلقة بالطفل بطريقة محايدة تكنولوجيا. وتُعرف المواد الإباحية المتعلقة بالطفل أنها أي تمثيل للطفل بأي وسيلة كانت وهو يشارك في ممارسة حقيقية أو عن طريق المحاكاة في أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل لأغراض الاستغلال الجنسي أساساً.[1755] والأعمال المشمولة بهذا البروتوكول قابلة للمقارنة بالأعمال المشمولة في الاتفاقية بشأن الجريمة السيبرانية، باستثناء أن الحكم الوارد في المادة 3 صيغ لكي يكون محايداً من الناحية التكنولوجية.

مشروع اتفاقية ستانفورد الدولية

لا يتضمن مشروع اتفاقية ستانفورد الدولية غير الرسمي[1756] لعام 1999 ("مشروع ستانفورد") نصاً يجرِّم تبادل صور الأطفال الفاضحة عبر المنظومات الحاسوبية. وأشار واضعو مشروع ستانفورد إلى أنه ليس من المطلوب عموماً معاملة أي نوع من الحديث أو النشر باعتباره إجرامياً بموجب مشروع ستانفورد.[1757] وأقرّ واضعو مشروع ستانفور بمختلف النُهج الوطنية فتركوا للدول حرية تقرير هذا الجانب من التجريم.[1758]

9.2.6 إغواء الأطفال

توفر الإنترنت إمكانية التواصل مع الآخرين دون الإفصاح عن السن أو نوع الجنس.[1759] ويمكن لمرتكبي الجرائم إساءة استخدام هذه القدرة لإغواء الأطفال. وكثيراً ما تُدعى هذه الظاهرة "الاستمالة".[1760] وتتضمن بعض الأطر القانونية الإقليمية أحكاماً تجرّم هذا الاتصال.

اتفاقية مجلس أوروبا بشأن حماية الأطفال

وأحد الأمثلة هي المادة 23 من اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والإيذاء الجنسي.[1761]

> ***المادة 23 – إغواء الأطفال لأغراض جنسية***
>
> *يتخذ كل طرف التدابير التشريعية أو غيرها من التدابير لتجريم اقتراح متعمد، من خلال تكنولوجيات المعلومات والاتصالات، من شخص بالغ للاجتماع مع طفل لم يبلغ السن المحددة تطبيقاً للفقرة 2 من المادة 18 لغرض ارتكاب أي من الأفعال المجرمة وفقاً للفقرة 1.أ من المادة 18، أو الفقرة 1.أ من المادة 20 ضده، حيث أعقبت هذا الاقتراح أفعال مادية تؤدي إلى مثل هذا الاجتماع.*

إن إغواء طفل لأغراض استغلال الطفل جنسياً عموماً غير مشمول بأحكام تجرّم الاعتداء الجنسي على الأطفال، نظراً لأن الإغواء يعتبر عملاً تحضيرياً. ونظراً لازدياد النقاش حول الاستمالة عبر الإنترنت، قرر واضعو الاتفاقية إدراج المادة 23 لتجريم الأعمال التحضيرية فعلاً.[1762] ولتجنب الإفراط في التجريم، أكد واضعو الاتفاقية أنه ينبغي ألاّ يعتبر التحادث الجنسي البسيط مع الطفل كافياً لارتكاب فعل الإغواء على الرغم من أن هذا الأمر يمكن أن يكون جزءاً من التحضير للاعتداء الجنسي.[1763]

هناك مشكلتان رئيسيتان تتصلان بهذا النهج. أولاً، يغطي الحكم فقط الإغواء من خلال تكنولوجيا المعلومات والاتصالات. وإن أشكالاً أخرى للإغواء غير مشمولة بالحكم. وأعرب واضعو الاتفاقية عن رأي مفاده أن التركيز على هذه التكنولوجيات له ما يبرره لأنه من الصعب رصدها. ومع ذلك، لم تقدم بيانات موثوقة علمياً لإثبات أن إغواء الأطفال هي مجرد مشكلة على الخط.[1764] وبالإضافة إلى ذلك، هناك أسباب جيدة ليس فقط لتفادي الحالات التي يكون فيها شيء معين غير قانوني عندما يرتكب خارج الخط وقانونياً عندما يرتكب على الخط، ولكن على العكس من ذلك، لضمان عدم تجريم السلوك على الخط عندما يكون قانونياً خارج الخط. ويشير الإعلان المشترك لعام 2001 بشأن التحديات التي تواجه حرية التعبير في القرن الجديد، على سبيل المثال، إلى أن الدول ينبغي ألاّ تعتمد قواعد منفصلة تحد من مضمون الإنترنت.[1765]

وهناك مشكلة أخرى بالنسبة لتجريم هذا العمل التحضيري تتمثل في أن ذلك قد يؤدي إلى صراعات في نظام القانون الجنائي، علماً أن حتى التحضير لأعمال أكثر خطورة غير مشمول بالتجريم. وإذا كان من المقرر تجريم التحضير للاعتداء الجنسي على الطفل بينما لم يُقرر تجريم التحضير لقتل طفل فإن ذلك سوف يشكل تحدياً لنظام قيمة البلد. ولذلك، ينبغي صياغة أي نهج من هذا القبيل في إطار مناقشة شاملة لمزايا ومخاطر تجريم الأعمال التحضيرية.

10.2.6 الخطاب المحرض على الكراهية، العنصرية

تختلف درجة تجريم الخطاب المحرض على الكراهية اختلافاً كبيراً،[1766] وخاصة في البلدان التي تمارس حماية دستورية قوية لحرية التعبير، إذ لا يُجرّم خطاب الكراهية[1767] في كثير من الأحيان. ويمكن أن يمارس الحظر في إفريقيا وأوروبا بوجه خاص.[1768]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (بروتوكول إضافي)

يؤدي مجلس أوروبا دوراً فعالاً في الكفاح ضد العنصرية، وبعد مؤتمر فيينا في 1993 اعتمد مجلس أوروبا إعلاناً وخطة عمل لمكافحة العنصرية وكراهية الأجانب ومعاداة السامية والتعصب[1769]. وفي 1995، اعتمد مجلس أوروبا توصيات بشأن بمكافحة العنصرية.[1770] وأثناء التفاوض على اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، نوقشت مسألة تجريم الخطاب المحرض على الكراهية والعنصرية على الخط. ونظراً لأن الأطراف المتفاوضة على الاتفاقية[1771] بشأن الجريمة السيبرانية لم تتمكن من الاتفاق بشأن موقف مشترك بشأن تجريم الخطاب المحرض على الكراهية والمواد المعادية للأجانب، أُدمجت الأحكام المتعلقة بهذه الجرائم في بروتوكول منفصل أول للاتفاقية.[1772] وتتمثل إحدى الصعوبات الأساسية التي تواجهها أحكاماً تجرم المواد المعادية للأجانب[1773] هو الحفاظ على التوازن بين ضمان حرية التعبير من ناحية، ومنع انتهاك حقوق الأفراد أو الجماعات من ناحية أخرى. ودون الخوض في التفاصيل، فإن الصعوبات التي نشأت في المفاوضات بشأن الاتفاقية المتعلقة بالجريمة السيبرانية[1774] وحالة التوقيعات/التصديقات على البروتوكول الإضافي[1775] تثبت أن اختلاف مدى حماية حُرية التعبير يعوق عملية التنسيق.[1776] وفيما يتعلق بالمبدأ المشترك للجُرم المزدوج بالتحديد،[1777] يؤدي غياب التنسيق إلى صعوبات في الإنفاذ في الحالات التي تأخذ بُعداً دولياً.[1778]

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.

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 ارتُكب 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 أغسطس 1945، أو أي محكمة دولية أخرى أنشئت بموجب صكوك دولية ذات صلة ويعترف الطرف بولايتها.

2 يجوز لأي طرف إما

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

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

الأفعال المشمولة

تُجرّم المادة 3 التوزيع المتعمد للمواد المعادية للأجانب وإتاحتها للجمهور من خلال نظام حاسوبي. وبالتالي، فإن الطرق التقليدية للتوزيع التي لا تنطوي على أنظمة حاسوبية (مثل الكتب والمجلات) غير مشمولة.[1779] واستناداً إلى التعريف الوارد في المادة 2، تشير المواد العنصرية والمعادية للأجانب إلى أي مادة مكتوبة أو صورة أو أي تمثيل آخر للأفكار أو النظريات التي تدعو أو تشجع أو تحرض على الكراهية أو التمييز أو العنف، ضد أي فرد أو مجموعة من الأفراد، استناداً إلى العرق أو اللون أو النسب أو الأصل القومي أو الإثني، فضلاً عن الدين إذا ما استخدمت كذريعة لأي من هذه العوامل. ويعني "التوزيع" النشر الفعال للمواد.[1780] ويغطي التعبير "إتاحة" القيام بوضع المواد على الخط. فهو يقتضي أن يتمكن المستعملون من الوصول إلى هذه المواد. ويمكن أن يُرتكب الفعل من خلال وضع المواد على مواقع إلكترونية أو التوصيل بأنظمة تقاسم الملفات وتمكين الآخرين من الوصول إلى هذه المواد بواسطة قدرات أو مجلدات تخزين غير مسدودة.[1781] ويشير التقرير التفسيري إلى الحاجة إلى أن تكون عملية استحداث أو تجميع روابط مرجعية مشمولة أيضاً.[1782] ونظراً لأن الروابط المرجعية تسهل فقط النفاذ إلى المواد، فإن هذا التفسير يتجاوز نص الحكم. ويشمل التوزيع أفعال إعادة توجيه المواد العنصرية والتي

تحض على كراهية الأجانب للآخرين. وبالإضافة إلى ذلك يقتضي التجريم أن يشمل توزيع المواد وإتاحتها التفاعل مع الجمهور، وبذلك يستبعد الاتصال الخاص.[1783]

تتبع المادة 6 نهجاً مماثلاً للمادة 3، تجريم توزيع أو إتاحة من خلال نظام حاسوبي للجمهور،[1784] مواد تنفي أو تقلل إلى أدنى حد أو توافق أو تبرر أفعالاً تشكل جريمة الإبادة الجماعية أو جرائم ضد الإنسانية، كما يحددها القانون الدولي وتقرها قرارات نهائية وملزمة للمحكمة العسكرية الدولية المنشأة بموجب اتفاق لندن بتاريخ 8 أغسطس 1945، أو أي محكمة دولية أخرى منشأة بموجب صكوك دولية ذات صلة يعترف الطرف المعني بولايتها القضائية.

وتجرم المادة 4 تهديد الأشخاص، بواسطة نظام حاسوبي، بارتكاب جريمة جنائية خطيرة، بحكم انتمائهم إلى مجموعة متميزة العرق أو اللون، أو النسب أو الأصل القومي أو الإثني، فضلاً عن الدين، أو إلى مجموعة من الأشخاص يتميزون بأي من هذه السمات. وتشير إلى التهديدات التي تخلق الشعور بالخوف لدى الأشخاص الموجه إليهم هذا التهديد بحيث أنهم سيتعرضون لارتكاب جريمة.[1785] وخلافاً عن المادة 3 لا يتطلب التعبير "تهديد" أي تفاعل مع الجمهور ولذلك فهو يغطي أيضاً إرسال رسائل بالبريد الإلكتروني إلى الضحية.

تعتمد المادة 5 نهجاً مماثلاً للمادة 4، تجريم إهانة الأشخاص بحكم انتمائهم إلى مجموعة متميزة العرق أو اللون أو النسب أو الأصل القومي أو الإثني، فضلاً عن الدين، إذا ما استخدمت كذريعة لأي من هذه العوامل، أو إلى مجموعة من الأشخاص يتميزون بأي من هذه السمات. ويشير التعبير "إهانة" إلى أي تعبير هجومي أو قدحي أو يمس كرامة الشخص ويتصل مباشرة بالشخص المهان الذي ينتمي إلى هذه المجموعة. ولتجنب التعارض مع مبدأ حرية التعبير،[1786] من الضروري تحديد فعل الإهانة بصورة ضيقة. والفرق الرئيسي بين المادتين 4 و5 هو أن الحكم يقتضي فقط الإهانة علناً، ولذلك لا يشمل الاتصال الخاص (مثل البريد الإلكتروني).[1787]

مشروع اتفاقية ستانفورد الدولية

لا يتضمن مشروع اتفاقية ستانفورد الدولية غير الرسمي[1788] لعام 1999 ("مشروع ستانفورد) حكماً يجرِّم خطاب الكراهية. وأشار واضعو مشروع ستانفورد إلى أنه ليس من الضروري معاملة أي نوع من الخطاب أو المنشورات باعتبارها إجرامية بموجب مشروع ستانفورد.[1789] ومع الاعتراف بمختلف النُهج الوطنية ترك واضعو مشروع ستانفورد للدول اتخاذ قرار بشأن هذا الجانب من التجريم.[1790]

11.2.6 *الجرائم الدينية*

تختلف شدة حماية الأديان ورموزها من بلد لآخر.[1791] يتم الإعراب عن عدد من الشواغل فيما يتعلق بالتجريم. ويشير الإعلان المشترك لعام 2006 للمقرر الخاص للأمم المتحدة بشأن حرية الرأي والتعبير وممثل منظمة الأمن والتعاون بشأن حرية وسائل الإعلام والمقرر الخاص لمنظمة الدول الأمريكية المعني بحرية التعبير، إلى أنه في "العديد من البلدان، يساء استخدام القواعد الفضفاضة في هذا المجال من جانب الأقوياء للحد من الأصوات غير التقليدية أو المعارضة أو الناقدة أو أصوات الأقليات أو مناقشة القضايا الاجتماعية الصعبة".[1792] ويشير الإعلان المشترك لعام 2008 إلى أن المنظمات الدولية، بما في ذلك الجمعية العامة للأمم المتحدة ومجلس حقوق الإنسان، يجب عليها أن تمانع اعتماد المزيد من البيانات المؤيدة لفكرة تجريم التشهير بالأديان.

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (البروتوكول الإضافي)

واجهت المفاوضات بشأن هذا الموضوع بين أطراف الاتفاقية المتعلقة بالجريمة السيبرانية نفس الصعوبات التي ظهرت بشأن مواد كراهية الأجانب.[1793] ومع ذلك، فإن البلدان التي تفاوضت بشأن أحكام البروتوكول الإضافي الأول للاتفاقية المتعلقة بالجريمة السيبرانية وافقت على إضافة الدين كموضوع للحماية في اثنين من الأحكام.

الحكم

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 ارتُكب 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 لأيٍّ 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 عبارات 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[1794]، ولكن تم حذف تلك الأحكام عندما أعيد إدخال مشروع القانون كقانون منع الجرائم الإلكترونية في 2007،[1795] الذي أعلن عنه في ديسمبر 2007.[1796]

*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.*

*21 **استعمال عبارات 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 التي تجرّم الجرائم الدينية هو مبدأ حرية التعبير.[1797] وكما أُشير من قبل يمثِّل اختلاف مدى حماية حرية التعبير عائقاً يعترض عملية التنسيق.[1798] وفيما يتصل بصورة خاصة بالمبدأ المشترك بازدواج الجُرم[1799] يؤدي غياب التنسيق إلى صعوبات في الإنفاذ في الحالات التي تأخذ بُعداً دولياً.[1800]

12.2.6 المقامرة غير القانونية

هناك قلق من تزايد عدد مواقع شبكة الويب التي تعرض المقامرة غير القانونية[1801]، نظراً لإمكانية استعمال ذلك للالتفاف على حظر المقامرة المطبَّق في بعض البلدان.[1802] 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.[1803]

مثال من التشريعات الوطنية

لا تتضمن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية حظراً على المقامرة على الخط. ومن أمثلة النُهُج الوطنية في هذا الصدد المادة 284 من قانون العقوبات الألماني:

مثال

الفقرة 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.

(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[1804] على المقامرة من خلال تحديد إجراءات لتنظيم هذه الألعاب.[1805] ولا يركِّز صراحة على ألعاب الحظ المتصلة بالإنترنت، ولكنه يشملها أيضاً.[1806] 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.[1807] وهذا التجريم يتجاوز عواقب المساعدة والتحريض، نظراً لأن مرتكبي الجرائم قد يواجهون عقوبات أعلى.[1808]

ولتجنُّب التحقيقات الجنائية يستطيع مشغِّل مواقع المقامرة غير القانونية أن ينقل مادياً أنشطته[1809] إلى بلدان لا تجرِّم المقامرة غير القانونية.[1810] وهذا الانتقال إلى أماكن أخرى يمثِّل تحدياً لوكالات إنفاذ القانون لأن وجود المخدِّم خارج أراضي البلد[1811] لا يؤثر عموماً على إمكانيات نفاذ المستعمل داخل البلد إلى الموقع.[1812] ولتحسين إمكانيات وكالات إنفاذ القانون لمكافحة المقامرة غير القانونية وسَّعت الحكومة الألمانية التجريم ليشمل المستعملين.[1813] 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:

الفقرة 285 – المشاركة في ألعاب حظ بدون إذن

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

وإذا استعمل الجناة مواقع المقامرة لأنشطة غسيل الأموال، فإن تحديد هوية الجناة يكون عسيراً في كثير من الأحيان.[1814] ومن أمثلة النُهج المتبعة[1815] لمنع المقامرة غير القانونية وأنشطة غسيل الأموال قانون إنفاذ المقامرة غير القانونية على الإنترنت في الولايات المتحدة لعام 2005.[1816]

البند 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.

البند 5364 – سياسات وإجراء تعيين ومنع الصفقات المقيَّدة

أ) 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 تعينها 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.

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 مشاركاً 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.

البند 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 أمراً 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[1817] (عبر الحدود). ويتضمن لائحتين هامتين: أولاً، 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.[1818] ويمكن أن يؤدي انتهاك هذا الحظر إلى عقوبات جنائية.[1819] وثانياً، 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 (GATS)[1820] يجري بحثه في الوقت الحاضر.[1821]

13.2.6 القذف والتشهير

القذف ونشر المعلومات الزائفة أفعال لا يقتصر ارتكابها في الشبكات. ولكن كما أشير من قبل، فإن إمكانية الإرسال مجهول الهوية[1822] والتحديات اللوجستية التي تتصل بالحجم الهائل من المعلومات المتوفِّرة في الإنترنت[1823] هي باراميترات مجرَّدة تدعم تلك الأفعال.

وقد ثارت مناقشات خلافية[1824] 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.[1825] وقد صرّح المقرر الخاص للأمم المتحدة المعني بحُرية الرأي والتعبير وممثل منظمة الأمن والتعاون في أوروبا المعني بحُرية وسائط الإعلام عن الآتي: "لا يمثِّل التشهير الجنائي تقييداً مبرَّراً لحُرية التعبير؛ وينبغي إلغاء جميع قوانين التشهير الجنائي واستبدالها عند الضرورة بقوانين ملائمة للتشهير المدني".

ورغم هذا القلق قامت بعض البلدان[1826] بتطبيق أحكام في القانوني 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،[1827] فإن الإحصاءات الجنائية الألمانية تسجِّل 187 527 جريمة تشهير في عام 2006.[1828] ولا تتضمن اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية ولا قانون الكومنولث النموذجي ولا مشروع اتفاقية ستانفورد أي أحكام تعالج هذه الأفعال بصورة مباشرة.

مثال 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.[1829]

الحكم

365 – التشهير الجنائي[1830]

(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

الفقرة 185 – الإهانة

تعاقب الإهانة بالحبس لمدة 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.

14.2.6 الرسائل الاقتحامية

نظراً لما يتردَّد من أن نسبة تصل إلى 75 في المائة[1831] من جميع رسائل البريد الإلكتروني هي رسائل اقتحامية،[1832] فقد نوقشت بكثافة[1833] ضرورة فرض جزاءات جنائية على رسائل البريد الإلكتروني الاقتحامية. وتختلف الحلول التشريعية الوطنية التي تعالج مشكلة الرسائل الاقتحامية.[1834] 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.[1835] 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.[1836] 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.[1837]

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، يمثِّل 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 وتقلِّل إنتاجية المستعمل.

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

لا تتضمن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية تجريماً صريحاً للرسائل الاقتحامية.[1838] ويشير واضعو الاتفاقية بأن يقتصر تجريم هذه الأفعال على الإعاقة الخطيرة والمتعمَّدة للاتصالات.[1839] ولا يركِّز هذا النهج على رسائل البريد الإلكتروني غير المطلوبة ولكن على آثار ذلك على المنظومة الحاسوبية أو الشبكة. واستناداً إلى النهج القانوني في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، يمكن أن تستند مكافحة الرسائل الاقتحامية إلى التداخل غير القانوني في الشبكات والنُظم الحاسوبية فقط:

المادة 5 – التدخل في النظم الحاسوبية

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 نظام حاسوبي عن طريق إدخال أو إرسال، أو إتلاف، أو محو، أو تغيير، أو تبديل، أو تدمير بيانات حاسوبية.

مشروع اتفاقية ستانفورد الدولية

لا يشمل مشروع اتفاقية ستانفورد غير الرسمي[1840] لعام 1999 نصاً يجرِّم الرسائل الاقتحامية. ومشروع ستانفورد، مثله مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، يجرِّم فقط الرسائل الاقتحامية إذا كانت رسائل البريد الإلكتروني غير المطلوبة تؤدي إلى تداخل متعمَّد في النظام.

تنسيق سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR)

هناك مثال لنهج محدد لتنسيق سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية[1841] في المادة 15 من النص التشريعي للجريمة السيبرانية.[1842]

الرسائل الاقتحامية

15 (1) *أي شخص يقوم، عمداً دون عذر أو مبرر مشروع:*

أ) بالبدء عمداً بإرسال رسائل بريد إلكتروني متعددة من نظام حاسوبي أو عن طريقه؛ أو

ب) باستخدام نظام حاسوبي يتمتع بالحماية لإرسال أو إعادة إرسال رسائل بريد إلكتروني متعددة بقصد خداع أو تضليل المستعملين، أو أي موفر لخدمة البريد الإلكتروني أو أي خدمة للإنترنت، عن مصدر هذه الرسائل، أو

ج) بتزييف مادي لمعلومات الرأسية في رسائل بريد إلكتروني متعددة ويبدأ عن عمد في إرسال هذه الرسائل، يرتكب جريمة يعاقب عليها، في حالة الإدانة، بالسجن لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.

(2) ويمكن لبلد تقييد التجريم فيما يتعلق بإرسال رسائل إلكترونية متعددة في إطار العلاقة بين العملاء أو العلاقات التجارية. ويجوز أن يقرر بلد عدم تجريم السلوك في القسم 15 (1) أ)، شريطة توفر سبل انتصاف فعالة أخرى.

يتضمن الحكم ثلاثة أفعال مختلفة. تغطي الفقرة (1) *أ)* من المادة 15 عملية الشروع في إرسال رسائل بريد إلكتروني متعددة. وتعرّف الفقرة 14(3) رسائل البريد الإلكتروني المتعددة كرسالة بريدية، بما في ذلك رسائل البريد الإلكتروني والرسائل الفورية، المرسلة إلى أكثر من ألف متلقٍ. وفي هذا السياق، تشير المذكرة التفسيرية إلى أن قصر التجريم على الأفعال التي تنفذ بدون عذر أو مبرر مشروع يؤدي دوراً هاماً في التمييز بين المراسلات المشروعة (مثل الرسائل الإخبارية) والرسائل الاقتحامية غير المشروعة.[1843] وتجرّم الفقرة (1) *ب)* من المادة 15 الالتفاف على تكنولوجيا مكافحة الرسائل الاقتحامية بإساءة استعمال أنظمة الحاسوب المحمية لإرسال رسائل إلكترونية أو نقلها. وتغطي الفقرة (1) *ج)* من المادة 15 الالتفاف على تكنولوجيا مكافحة الرسائل الاقتحامية بتزييف معلومات الرأسية. وتشير المذكرة التفسيرية إلى أن المادة 15 تتطلب أن ينفذ الجاني الجرائم عن قصد ودون عذر أو مبرر مشروع.[1844]

قانون الولايات المتحدة

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.[1845]

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،

(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 المسجّل 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 المسجّل أو بالخلف الشرعي لمصلحة المسجّل 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.[1846] والقصد من القانون هو إقامة معيار وطني وحيد بغرض السيطرة على البريد الإلكتروني التجاري.[1847] 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.[1848] 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 (الفَلترة).[1849] وبالإضافة إلى ذلك، يُجرِّم الحكم النفاذ غير المسموح إلى حاسوب متمتع بحماية وبدء إرسال رسائل بريد إلكتروني تجارية عديدة.

15.2.6 إساءة استخدام الأجهزة

هناك قضية خطيرة أخرى وهي وجود أدوات برمجيات وعتاد مخصصة لارتكاب الجرائم.[1850] فإلى جانب تكاثر "أجهزة القرصنة" يعتبر تبادل كلمات المرور الذي يمكّن المستعمِلين غير المأذون لهم من النفاذ إلى الأنظمة الحاسوبية تحدياً خطيراً.[1851] وتوفُّر هذه الأجهزة وتهديدها 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.[1852]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

مع مراعاة مبادرات مجلس أوروبا الأخرى قرّر واضعو الاتفاقية المتعلقة بالجريمة السيبرانية 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[1853]:

الحكم

المادة 6 – إساءة استخدام الأجهزة

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

أ) الإنتاج أو البيع، والحصول بغرض الاستخدام، أو الجلب أو التوزيع أو بالأحرى التوفير:

'1' لجهاز يشمل برنامج حاسوبي، صُمِّم أو طُوِّع ابتداءً، بغرض ارتكاب أيٍ من الجرائم المنصوص عليها أعلاه في المواد من 2-5؛

'2' لكلمة سر خاصة بحاسوب، أو شفرة دخول، أو بيانات مماثلة يمكن بواسطتها الدخول على كامل أو جزء من نظام حاسوبي، 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' بفعاليه، بغرض ارتكاب أيٍ 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 نظام حاسوبي أو حمايته 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.

الأغراض المشمولة

تعيِّن الفقرة 1 أ) الأجهزة[1854] 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.[1855] "كلمة السر الخاصة بالحاسوب، أو شفرات النفاذ 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.[1856] 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.

الأفعال المشمولة

تُجرِّم الاتفاقية بشأن الجريمة السيبرانية مجموعة واسعة من الأفعال. فبالإضافة إلى الإنتاج، تعاقِب الاتفاقية أيضاً على بيع الأجهزة وكلمات السر 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.[1857] وطبّق عدد من البلدان أحكاماً مشابهة في قوانينها الجنائية.[1858] "التوزيع" ويغطّي الأفعال النشطة في تحويل الأجهزة أو كلمات السر إلى آخرين.[1859] وفي سياق المادة 6، يصف "البيع" الأنشطة الداخلة في بيع الأجهزة وكلمات السر مقابل المال أو مقابل تعويض آخر. ويغطي "الحصول بغرض الاستخدام" الأفعال المتصلة بالأفعال النشطة للحصول على كلمات السر والأجهزة.[1860] ونظراً لأن فعل الحصول يرتبط باستعمال هذه الأدوات عموماً يتطلب وجود قصد من جانب الجاني للحصول على الأدوات لاستعمالها بطريقة تتجاوز القصد "العادي" أي بغرض ارتكاب أيٍ من الجرائم المنصوص عليها في المواد من 2–5". ويغطي الجلب أفعال الحصول على الأجهزة وشفرات النفاذ من بلدان أجنبية.[1861] 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 إلا إذا ارتبط باستعمالها، فإنه من المشكوك فيه أن مجرّد جلب الأدوات دون قصد البيع أو الاستعمال يقع تحت طائلة المادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. ويشير "التوفير" إلى فعل يمكِّن المستعمِلين الآخرين من الحصول على الأصناف.[1862] ويشير التقرير التفسيري بأن مصطلَح "التوفير" يقصد أيضاً إلى تغطية إنشاء أو تجميع الوصلات الإلكترونية من أجل تسهيل النفاذ إلى هذه الأجهزة.[1863]

أدوات الاستعمال المزدوج

بعكس نهج الاتحاد الأوروبي في تنسيق حقوق الطبع،[1864] لا يقتصر انطباق هذا الحكم على الأجهزة المخصصة حصرياً لتسهيل ارتكاب الجريمة السيبرانية – بل إن الاتفاقية بشأن الجريمة السيبرانية تغطي أيضاً الأجهزة التي تستعمل عادةً 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.[1865]

ولكفالة الحماية الصحيحة للأنظمة الحاسوبية، فإن الخبراء يستعملون ويملكون أدوات برمجية مختلفة تجعل منهم مجال تركيز محتمل لإنفاذ القانون. وتفحص الاتفاقية بشأن الجريمة السيبرانية هذه الانشغالات بثلاث طرق[1866]: 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.[1867] ويشير التقرير التفسيري إلى أن هذا القصد الخاص قد أُدرج "لتجنّب خطر الإفراط في التجريم عند إنتاج هذه الأجهزة وبيعها في السوق لأغراض مشروعة، وذلك مثلاً لمكافحة الهجمات ضد الأنظمة الحاسوبية".[1868] وأخيراً، يعلن واضعو الاتفاقية بشأن الجريمة السيبرانية 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.[1869] 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.[1870] وتمكِّن الاتفاقية بشأن الجريمة السيبرانية 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تقتضي المادة 6 أن يرتكب الجاني جريمته عمداً.[1871] وبالإضافة إلى القصد العادي بشأن الأفعال المشمولة بالمادة 6 تقتضي الاتفاقية المتعلقة بالجريمة السيبرانية إضافة قصد خاص لاستعمال الجهاز بغرض ارتكاب أيٍ من الجرائم المقرّرة في المواد من 2 إلى 5 من الاتفاقية.[1872]

بغير حق

يجب ارتكاب الأفعال "بغير حق"،[1873] 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 بشأن الجريمة السيبرانية إلى أن القيام بهذه الأفعال لا يعتَبر "بغير حق".[1874]

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.[1875]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مماثل للمادة 6 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في المادة 9 من قانون الكومنولث النموذجي لعام 2002.[1876]

الأجهزة غير القانونية

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.

وعلى الرغم من أن الأجهزة المشمولة بالحكم والأفعال المذكورة هي ذاتها، فإن الاختلاف الرئيسي مع اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية هو أن قانون الكومنولث النموذجي يُجرِّم الأفعال التي تجري باستهتار إضافة إلى الأفعال المتعمدة في حين أن الاتفاقية بشأن الجريمة السيبرانية تتطلب وجود نية في جميع الحالات. 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.[1877] واقتَرحت كندا نهجاً مشابهاً بدون تحديد مُسبَق لعدد البنود التي من شأنها أن تؤدّي إلى التجريم.[1878]

مشروع اتفاقية ستانفورد الدولية

يتضمن مشروع اتفاقية ستانفورد الدولية غير الرسمي[1879] لعام 1999 (مشروع ستانفورد) حكماً يُجرّم الأفعال المتصلة ببعض الأجهزة غير القانونية.

> ***المادة 3 – الجرائم***
>
> *1 تُرتكَب جرائم تندرج تحت طائلة هذه الاتفاقية إذا باشر أي شخص بطريقة غير قانونية وعمداً أي سلوك مما يلي بدون سلطة أو إذن أو موافقة معترَف 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 مشروع ستانفورد بأنه ليس من المطلوب عموماً معاملة أي نوع من الخطاب أو النشر باعتباره إجرامياً بموجب مشروع اتفاقية ستانفورد.[1880] وكان الاستثناء الوحيد يتصل بالأجهزة غير القانونية.[1881] وفي هذا السياق أبرز واضعو الاتفاقية أن التجريم ينبغي أن يقتصر على الأفعال المذكورة وألاّ يشمل مثلاً مناقشة أوجه ضعف النظام.[1882]

النص التشريعي للجريمة السيبرانية في إطار تنسيق سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR)

يمكن العثور على نهج مفيد في النص التشريعي الذي أعدته الدول المستفيدة في إطار مبادرة تنسيق سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية.[1883]

> ***الأجهزة غير القانونية***
>
> ***10***
>
> *[...]*
>
> *(3) ألف قد يقرر بلد عدم تجريم مجرد النفاذ غير المصرح به شريطة توفر سبل انتصاف فعالة أخرى. وعلاوة على ذلك، قد يقرر بلد قصر التجريم على الأجهزة المدرجة في جدول.*

لمنع التجريم المفرط، قرر واضعو الاتفاقية إدراج إمكانية الحد من التجريم بإدخال قائمة سوداء. وفي هذه الحالة، تكون الأجهزة المدرجة في القائمة فقط مشمولة بالحكم. وهذا النهج يحد من مخاطر تجريم الأفعال التي تكون مرغوبة من وجهة نظر الأمن السيبراني. ومع ذلك، من المرجح جداً أن يتطلب الاحتفاظ بهذه القائمة موارد كبيرة.

16.2.6 *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.[1884] 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".[1885]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تُجرِّم معظم أنظمة القانون الجنائي جريمة التزوير في وثائق ملموسة.[1886] وأشار واضعو الاتفاقية بشأن الجريمة السيبرانية إلى تباين هيكل القواعد المتصلة في النُهج القانونية الوطنية.[1887] وفي حين يستند أحد المفاهيم إلى صحة شخصية كاتب الوثيقة يستند مفهوم آخر إلى صحة البيان الوارد فيها. وقرّر واضعو الاتفاقية 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 إلكترونياً.[1888]

الحكم

> ***المادة 7 – جريمة التزوير المتعلقة بالحاسوب***
>
> *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 حاسوبية، 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 عما إن كانت مقروءة و/أو مفهومة بصورة مباشرة. وتُعرَّف البيانات الحاسوبية في الاتفاقية بأنها[1889] "أية عمليات عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية معالجة داخل نظام حاسوبي، بما في ذلك برنامج مناسب لجعل النظام الحاسوبي يؤدي وظائفه". 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[1890] – ولا يشمل الحكم تزييف البيانات التي لا يمكن استعمالها في أغراض قانونية.

الأفعال المشمولة

يجب أن يناظر "إدخال" البيانات[1891] إنتاج وثيقة ملموسة زائفة.[1892] يشير مصطَلح "تبديل" إلى تعديل بيانات موجودة.[1893] ويشير التقرير التفسيري خاصة إلى التباينات والتغييرات الجزئية.[1894] ويشير مصطَلح "تدمير" البيانات الحاسوبية إلى عمل يؤثّر على توفّر البيانات.[1895] ويشير واضعو الاتفاقية خاصة في التقرير التفسيري إلى حجب أو إخفاء البيانات.[1896] 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.[1897] ويشير التقرير التفسيري فقط إلى إزالة معلومات من وسيط بيانات.[1898] 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.[1899]

العنصر الذهني

كما يحدث في حالة جميع الجرائم الأخرى المعرَّفة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تقتضي المادة 3 أن يرتكب الجاني جريمته عمداً.[1900] ولا تتضمن الاتفاقية بشأن الجريمة السيبرانية تعريفاً لمصطلح "عمداً". وفي التقرير التفسيري يشير واضعو الصياغة إلى أن التعبير "عمداً" ينبغي أن يُعرف على صعيد وطني.[1901]

بغير حق

لا يمكن ملاحقة أفعال التزييف بموجب المادة 7 من الاتفاقية إلا إذا ارتُكبت "بغير حق".[1902]

التقييدات والتحفّظات

تتيح المادة 7 إمكانية إبداء تحفّظ من أجل الحدّ من التجريم، وذلك باقتضاء عناصر إضافية مثل قصد التزييف قبل إنشاء المسؤولية الجنائية.[1903]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

لا يتضمن قانون الكومنولث النموذجي لعام 2002 أي حكم يُجرِّم التزييف المتصل بالحاسوب.[1904]

مشروع اتفاقية ستانفورد الدولية

يتضمن مشروع اتفاقية ستانفورد الدولية غير الرسمي[1905] لعام 1999 حكماً يُجرِّم 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية 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 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية هذا الفعل. ويكفي أن يقوم الجاني بفعله بقصد اعتبار الفعل أو التصرّف حياله في الأغراض القانونية كما لو كان قصرياً.

17.2.6 انتحال الهوية

إذا وضعنا في الاعتبار التغطية الإعلامية،[1906] ونتائج الدراسات الاستقصائية الأخيرة[1907] والمنشورات العديدة القانونية والتقنية[1908] في هذا الميدان، فسوف يبدو من الملائم الإشارة إلى انتحال الهوية باعتبارها ظاهرة واسعة الانتشار.[1909] ورغم الجوانب العالمية لهذه الظاهرة لم تُطبِّق جميع البلدان بعد أحكاماً في نظام قانونها الجنائي الوطني لتجريم جميع الأفعال المتصلة بانتحال الهوية. وقد أعلنت مفوضية الاتحاد الأوروبي مؤخراً أن انتحال الهوية لم يخضع بعد للتجريم في جميع الدول الأعضاء في الاتحاد الأوروبي.[1910] وأعربت المفوضية الأوروبية عن رأيها بأن "التعاون في إنفاذ القوانين في الاتحاد الأوروبي سيكون أكثر

فعالية لو تم تجريم انتحال الهوية في جميع الدول الأعضاء" وأعلنت أنها ستبدأ قريباً في مشاورات لتقييم ما إن كان من الملائم تطبيق تشريع من هذا القبيل.[1911]

ومن المشاكل المتصلة بمقارنة الصكوك القانونية القائمة في مكافحة انتحال الهوية أن هذه الصكوك تختلف اختلافاً هائلاً.[1912] والعنصر الثابت الوحيد في النُهُج القائمة هو أن السلوك المدان يتصل بمرحلة أو أخرى من المراحل التالية[1913]:

- 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 انتحال 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).

أمثلة لنُهُج 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 بانتحال 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 بانتحال الهوية – ولا يغطي خاصة تلك الأنشطة التي يكون الضحية هو الذي يتصرف وليس الجاني.

البند 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؛

(3) عن علم بامتلاك – بقصد الاستعمال غير القانوني أو النقل غير القانوني – خمس وثائق هوية أو أكثر (خلاف الوثائق الصادرة قانونياً 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 تعرُّف 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.

[...]

البند 1028 ألف– انتحال 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 بانتحال الهوية إلى التوصل إلى حيازة البيانات المتصلة بالهوية.[1914] ومن خلال تجريم "نقل" وسيلة إثبات الهوية بقصد ارتكاب جريمة، فإن الأحكام تجرِّم الأفعال المتصلة بالمرحلة 1 بطريقة عريضة جداً.[1915] وبسبب تركيز الأحكام على فعل النقل فإنها لا تغطي الأفعال التي يقوم بها الجاني قبل بدء عملية النقل.[1916] 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 بانتحال الهوية.[1917] وحيازة البيانات المتصلة بالهوية بدون قصد استعمالها ليس مشمولاً.[1918]

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).

وهناك مثال آخر يتمثل في المادة 4 من النص التشريعي للجريمة السيبرانية الذي أعدته الدول المستفيدة في إطار مبادرة سياسات تكنولوجيا المعلومات والاتصالات والإجراءات التشريعية والتنظيمية.[1919]

الجرائم المتصلة بانتحال الهوية

14

أي شخص يقوم عمداً وبدون عذر أو مبرِّر مشروع أو تجاوزاً لعذر أو مبرر مشروع بواسطة استخدام نظام حاسوبي في أي مرحلة من مراحل الجريمة، بنقل أو حيازة أو استخدام عمداً، دون عذر أو مبرر مشروع، وسيلة تعرف هوية شخص آخر بقصد ارتكاب أو المساعدة أو التحريض على ارتكاب أي نشاط غير مشروع أو فعل يتصل به يشكل جريمة، يرتكب جريمة يعاقب عليها في حالة الإدانة بالحبس لمدة لا تزيد عن [الفترة] أو غرامة لا تزيد عن [المبلغ] أو كلاهما.

يغطي الحكم المراحل الرئيسية للجرائم المتعلقة بالهوية النموذجية الموصوفة أعلاه. والمرحلة الأولى فقط، التي يحصل فيها الجاني على المعلومات المتعلقة بالهوية، غير مشمولة. و"نقل" وسائل الهوية يغطي عمليات نقل البيانات من حاسوب إلى نظام حاسوبي آخر. وهذا القانون هام بشكل خاص لتغطية بيع (ونقل) المعلومات المتعلقة بالهوية. وتشير "الحيازة" إلى التحكم الذي يمارسه شخص عمداً على المعلومات المتصلة بالهوية.[1920] ويغطي "الاستخدام" مجموعة واسعة من الممارسات مثل تقديم هذه المعلومات للشراء عبر الإنترنت. وفيما يتعلق بالعنصر الذهني، يتطلب الحكم أن يتصرف الجاني عمداً فيما يتعلق بجميع العناصر الموضوعية وأن تكون لديه أيضاً نية محددة للقيام بالنشاط لارتكاب أي نشاط غير مشروع يتجاوز نقل المعلومات المتصلة بالهوية أو حيازتها أو استخدامها والمساعدة على ارتكابه أو التحريض على ارتكابه.

مثال نهج متعدد الأحكام

الفرق الرئيسي بين اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية ونُهج الحكم الوحيد (مثل نهج الولايات المتحدة على سبيل المثال) هو أن الاتفاقية بشأن الجريمة السيبرانية لا تحدِّد جريمة سيبرانية منفصلة للاستعمال غير القانوني للمعلومات المتصلة بالهوية.[1921] وعلى نسق الحالة في صدد تجريم الحصول على المعلومات المتصلة بالهوية، لا تغطي الاتفاقية بشأن الجريمة السيبرانية كل الأفعال الممكنة المتصلة بالاستعمال غير القانوني للمعلومات الشخصية.

المرحلة 1

تتضمن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية[1922] عدداً من الأحكام التي تجرِّم أفعال انتحال الهوية المتصلة بالإنترنت في المرحلة 1. وهذه الأحكام بالتحديد هي:

- النفاذ غير المشروع (المادة 2)[1923]
- الاعتراض غير المشروع (المادة 3)[1924]
- التدخل في البيانات (المادة 4)[1925]

ومع مراعاة مختلف الطرق المختلفة التي يستطيع بها الجاني النفاذ إلى البيانات، ويجب 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 انتحال الهوية ولكنها غير مشمولة باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

المرحلة 2

لا يمكن بسهولة أن تغطي اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية 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 بشأن الجريمة السيبرانية.

المرحلة 3

تعرِّف الاتفاقية المتعلقة بالجريمة السيبرانية 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 انتحال الهوية.[1926] وتشير الدراسات الاستقصائية بشأن انتحال الهوية إلى أن معظم البيانات التي يتم الحصول عليها تُستعمل في الغش المتصل ببطاقات الائتمان.[1927] وفي حالة ارتكاب الغش المتصل ببطاقات الائتمان على الخط، فمن المرجح أن يمكن ملاحقة الجاني استناداً إلى المادة 8 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. 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.

18.2.6 الغش المتصل بالحاسوب

الغش جريمة شائعة في الفضاء السيبراني.[1928] وهو أيضاً مشكلة شائعة خارج الإنترنت، ولهذا تتضمن معظم القوانين الوطنية أحكاماً تجرِّم الغش.[1929] ومع ذلك، فإن تطبيق الأحكام الحالية على الحالات المتصلة بالإنترنت قد يكون عسيراً، حيث تستند أحكام القانون الجنائي الوطنية التقليدية إلى تزييف الشخص.[1930] 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.[1931]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تسعى الاتفاقية إلى تجريم أي تلاعب غير صحيح بمجرى تجهيز البيانات بقصد إحداث نقل غير قانوني للممتلكات من خلال النص على مادة بشأن الغش المتصل بالحاسوب.[1932]

الحكم

> ***المادة 8 – جريمة النصب المتعلقة بالحاسوب***
>
> *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 حاسوب؛*
>
> *ب) أي تدخل في وظيفة نظام حاسوبي،*
>
> *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.[1933] 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.[1934] ويشير مصطلح "تبديل" إلى تعديل البيانات الموجودة.[1935] ويشير مصطلح "تدمير" البيانات الحاسوبية إلى فعل يؤثر على توفر البيانات.[1936] ويناظر مصطلح "محو" تعريف المصطلح في المادة 4 التي تغطي أفعال إزالة معلومات.[1937]

وبالإضافة إلى قائمة الأفعال تتضمن الفقرة ب) من المادة 8 بنداً عاماً يجرِّم "أي تدخل في وظيفة نظام حاسوبي" فيما يتصل بالغش. وقد أُضيف البند العام إلى قائمة الأفعال المشمولة من أجل فتح هذا الحكم ليشمل أي تطورات أخرى.[1938]

ويشير التقرير التفسيري إلى أن أي "تدخل في وظيفة نظام حاسوبي" يغطي الأفعال من قبيل التلاعب بالعتاد وأفعال تدمير الصفحات المطبوعة والأفعال التي تؤثر على تسجيل أو تدفق البيانات أو تتابع تسيير البرامج.[1939]

الخسارة الاقتصادية

تنص معظم القوانين الجنائية الوطنية على أن الفعل الجنائي يجب أن يؤدي إلى خسارة اقتصادية. وتتبع الاتفاقية بشأن الجريمة السيبرانية مفهوماً مشابهاً وتقصر التجريم على تلك الأفعال التي ينجم فيها التلاعب عن خسارة اقتصادية أو حيازية مباشرة لممتلكات شخص آخر بما فيها الأموال والأصول المادية والأصول غير المادية ذات القيمة الاقتصادية.[1940]

العنصر الذهني

كما حدث في حالة الجرائم المذكورة الأخرى تقتضي المادة 8 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية أن يرتكب الجاني جريمته عمداً. ويشير هذا العمد إلى التلاعب وكذلك إلى الخسارة المالية.

وبالإضافة إلى ذلك، تقتضي الاتفاقية بشأن الجريمة السيبرانية أن يتصرف الجاني بقصد احتيالي أو غير أمين للحصول على فوائد اقتصادية أو فوائد أخرى لنفسه أو للغير.[1941] ومن أمثلة الأفعال المستبعدة من المسؤولية الجنائية بسبب عدم توفُّر 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.[1942]

بغير حق

لا يمكن ملاحقة الغش المتصل بالحاسوب بموجب المادة 8 من الاتفاقية إلا إذا تم ارتكابه "بغير حق".[1943] ويشمل ذلك اقتضاء أن الفائدة الاقتصادية يجب الحصول عليها بغير حق. وأشار واضعو الاتفاقية بشأن الجريمة السيبرانية إلى أن الأفعال لا تعتبر قد جرت بغير حق إذا كانت قد جرت عملاً بعقد صحيح بين الأشخاص المتأثرين.[1944]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

لا يتضمن قانون الكومنولث النموذجي لعام 2002 حكماً يجرِّم الغش المتصل بالحاسوب.[1945]

مشروع معاهدة ستانفورد الدولية

لا يتضمن مشروع معاهدة ستانفورد الدولية غير الرسمي[1946] لعام 1999 حكماً يجرِّم الغش المتصل بالحاسوب.

19.2.6 جرائم حقوق الطبع

كان التحوُّل من التوزيع التماثلي إلى التوزيع الرقمي للمحتوى الخاضع لحماية حقوق الطبع نقطة تحول في انتهاكات حقوق الطبع.[1947] 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.[1948]

وقد استجابت صناعة الترفيه لذلك بتنفيذ تدابير تقنية (إدارة الحقوق الرقمية لمنع الاستنساخ)،[1949] ولكن حتى الآن يتم الالتفاف على هذه التدابير نمطياً بعد فترة قصيرة من تطبيقها.[1950] 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.[1951]

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تتضمن الاتفاقية بشأن الجريمة السيبرانية حكماً يغطي جرائم حقوق الطبع ويسعى هذا الحكم إلى تنسيق مختلف اللوائح في القوانين الوطنية. وتبين أن هذا الحكم من العقبات الرئيسية التي تحول دون استخدام الاتفاقية بشأن الجريمة السيبرانية خارج أوروبا.

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 المنقِّحة 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 نظام حاسوبي.

(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 نظام حاسوبي.

(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، وألا يخل هذا التحفُّظ بالالتزامات الدولية للطرف بموجب الاتفاقيات الدولية المشار إليها بالفقرتين 1 و2 من هذه المادة.

ويخضع التعدي على حقوق الطبع للتجريم في بعض البلدان[1952] وتعالجه عدة معاهدات دولية.[1953] وتهدف الاتفاقية بشأن الجريمة السيبرانية 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.[1954]

الإحالة إلى اتفاقات دولية

بعكس الأُطر القانونية الأخرى لا تسمي الاتفاقية بشأن الجريمة السيبرانية صراحة الأفعال التي يتعيَّن تجريمها، ولكنها تحيل إلى عدد من الاتفاقات الدولية.[1955] 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 لاحقاً فقد أثير السؤال بشأن ما إن كانت الاتفاقية بشأن الجريمة السيبرانية تفرض على الدول الموقِّعة التوقيع أيضاً على الاتفاقات الدولية المذكورة في المادة 10. ويشير واضعو الاتفاقية المتعلقة بالجريمة السيبرانية إلى أن اتفاقية المجلس الأوروبي بشأن الجريمة السيبرانية لا تفرض التزاماً من هذا القبيل.[1956] 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 إلا على الأطراف التي وقَّعت أحد هذه الاتفاقات الدولية.

العنصر الذهني

تُقصر الاتفاقية بشأن الجريمة السيبرانية التجريم على الأفعال التي ارتُكبت بواسطة منظومة حاسوبية، نظراً لطابعها العام.[1957] 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 بشأن الجريمة السيبرانية ويراعي المصطلح المستعمل في المادة 61 من الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (TRIPS)،[1958] التي تحكم الالتزام بتجريم انتهاكات حقوق الطبع.[1959]

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.[1960]

بغير حق

عموماً تتطلب أحكام القانون الجنائي الموضوعي المحدَّدة في الاتفاقية المتعلقة بالجريمة السيبرانية أن يكون ارتكاب الأفعال "بدون حق".[1961] وأشار واضعو الاتفاقية إلى أن مصطلح "انتهاك" ينطوي بالفعل على أن الفعل قد أرتُكب بدون إذن.[1962]

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 ("مشروع ستانفورد") غير الرسمي[1963] لعام 1999 حكماً يجرِّم انتهاكات حقوق الطبع. وأشار واضعو هذه الاتفاقية إلى أن جرائم حقوق الطبع لم تُدرج نظراً لأن ذلك قد يكون عسيراً.[1964] وبدلاً من ذلك أشاروا بصورة مباشرة إلى الاتفاقات الدولية القائمة.[1965]

20.2.6 استخدام الإرهابيين للإنترنت

مثلما ذُكر أعلاه، يستخدم مصطلح "استخدام الإرهابيين للإنترنت" من أجل وصف مجموعة من الأنشطة التي تتراوح بين الدعاية والهجمات المتعمّدة. وفيما يخص الاستجابة القانونية، من الممكن التمييز بين ثلاثة نُهُج نظامية مختلفة.

النُّهُج النظامية

استخدام التشريعات القائمة المتعلقة بالجريمة السيبرانية

يتعلق النهج الأول باستخدام التشريعات القائمة المتعلقة بالجريمة السيبرانية (التي وُضعت من أجل معالجة الأفعال غير الإرهابية) لتجريم استخدام الإرهابيين للإنترنت. وفي هذا السياق، لا بد من أخذ ثلاثة عناصر بعين الاعتبار. أولاً، من الممكن أن تُطبق في الحالات المتصلة بالإرهاب أحكام القانون الجنائي الموضوعي التي كانت تطبق بشأن الأفعال غير الإرهابية مثل التدخل في الأنظمة،[1966] لكن في أغلب الأحيان سيكون مدى الأحكام مختلفاً عما تنص عليه التشريعات المحددة الخاصة بالإرهاب. وقد يؤثر هذا في القدرة على استخدام أدوات التحقيق المتطورة التي تقتصر على التحقيق في الجرائم الإرهابية أو المنظمة. ثانياً، فإن استخدام أدوات التحقيق الخاصة بالجريمة السيبرانية في حالات استخدام الإرهابيين للإنترنت

يواجه تحديات أقل، مادامت أغلبية البلدان لا تقصر استخدام أدوات التحقيق المتطورة على الجرائم السيبرانية التقليدية، بل إنها تغطي أي جريمة تدخل فيها بيانات حاسوبية. وأخيراً، فإن الأدوات القانونية الإقليمية المستحدثة من أجل التصدي لتحديات الجريمة السيبرانية، لكنها لا تستهدف بالتحديد استخدام الإرهابيين للإنترنت، تتضمن غالباً استثناءات تتعلق بالتعاون الدولي فيما يخص الجرائم السياسية. وأحد الأمثلة على ذلك الفقرة 4أ) من المادة 27 من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.[1967]

المادة 27 – الإجراءات المتعلقة بطلبات المساعدة المبادلة في حالة عدم وجود اتفاقات دولية مطبقة

[...]

4 يجوز للطرف المتلقي لطلب تقديم العون، بالإضافة إلى أسباب الرفض المحددة في الفقرة 4 من المادة 25، أن يرفض تقديم المساعدة:

أ) إذا تعلق الطلب بجريمة يعتبرها الطرف المتلقي للطلب جريمة سياسية أو جريمة متصلة بجريمة سياسية،

ب) أو إذا كان يرى أن تنفيذ الطلب قد يلحق الضرر بسيادته أو أمنه أو نظامه العام أو مصالحه الأساسية الأخرى.

[...]

ويسمح هذا الحكم للأطراف في الاتفاقية برفض طلبات المساعدة المتبادلة إذا تعلقت بجريمة يعتبرها الطرف المتلقي للطلب جريمة سياسية أو جريمة متصلة بجريمة سياسية. ومن الممكن أن يعرقل هذا الأمر إلى حد كبير إجراء التحقيقات. ولذلك، تتضمن الأطر القانونية الخاصة بالإرهاب مثل اتفاقية مجلس أوروبا لمنع الإرهاب لعام 2005[1968] استبعاداً للبند الاستثناء السياسي.

المادة 20 – استبعاد بند الاستثناء السياسي

1 لا تُعتبر أي جريمة من الجرائم المشار إليها في المواد من 5 إلى 7 والمادة 9 من هذه الاتفاقية، لأغراض تسليم المطلوبين أو المساعدة القانونية المتبادلة، كجريمة سياسية، أو جريمة متصلة بجريمة سياسية أو كجريمة مستحثة بدوافع سياسية. وبالتالي، لا يجوز رفض طلب تسليم أو مساعدة قانونية متبادلة على أساس جريمة كهذه للسبب الوحيد المتمثل في أن الطلب يتعلق بجريمة سياسية أو جريمة متصلة بجريمة سياسية أو جريمة مستحثة بدوافع سياسية.

[...]

استخدام التشريعات القائمة لمكافحة الإرهاب

يتمثل النهج الثاني في استخدام تشريعات مكافحة الإرهاب القائمة من أجل تجريم استخدام الإرهابيين للإنترنت وملاحقتهم. وأحد الصكوك التقليدية، على سبيل المثال، اتفاقية مجلس أوروبا لمنع الإرهاب لعام 2005[1969].

المادة 5 – التحريض العلني على ارتكاب جريمة إرهابية

1 لأغراض هذه الاتفاقية، يعني التحريض العلني على ارتكاب جريمة إرهابية توزيع رسالة على الجمهور، أو إتاحتها له بشكل آخر، بقصد الحث على ارتكاب جريمة إرهابية، عندما يتسبب هذا السلوك، سواء كان يدعو بشكل مباشر أو غير مباشر إلى جرائم إرهابية، في خطر يتمثل في احتمال ارتكاب جريمة أو أكثر من هذه الجرائم.

2 ويعتمد كل طرف تدابير على النحو الذي قد يكون ضرورياً للإقرار بأن التحريض العلني على ارتكاب جريمة إرهابية، مثلما تعرفه الفقرة 1، عندما يرتكب بشكل غير مشروع وعن قصد، يُعدّ بمثابة جريمة جنائية بموجب القانون المحلي للطرف.

المادة 6 – التجنيد لأغراض الإرهاب

1 لأغراض هذ الاتفاقية، يعني التجنيد لأغراض الإرهاب إغراء شخص آخر لارتكاب جريمة إرهابية أو المشاركة في ارتكابها، أو الانضمام إلى جمعية أو مجموعة بغرض المساهمة في ارتكاب جريمة أو أكثر من الجرائم الإرهابية على يد تلك الجمعية أو المجموعة.

2 ويعتمد كل طرف تدابير على النحو الذي قد يكون ضرورياً للإقرار بأن التجنيد لأغراض الإرهاب، مثلما تعرفه الفقرة 1، عندما يرتكب بشكل غير مشروع وعن قصد، يعتبر جريمة جنائية بموجب القانون المحلي لهذا الطرف.

وتتضمن اتفاقية منع الإرهاب العديد من الجرائم مثل التحريض العلني على ارتكاب جريمة إرهابية والتجنيد لأغراض الإرهاب، لكنها لا تتضمن، على سبيل المثال، أحكاماً تجرم الهجمات المتصلة بالإرهاب ضد الأنظمة الحاسوبية. وفضلاً عن هذا، لا تتضمن الاتفاقية أحكاماً إجرائية. وعند التحقيق في الجرائم المتصلة بالإنترنت، على نحو خاص، فإن من الضروري في أغلب الأحيان وجود أحكام إجرائية محددة. فالكشف عن هوية مجرم يحرض على الإرهاب باستخدام مواقع شبكية يتطلب أدوات متطورة مثل الاحتفاظ السريع ببيانات الحركة.

تشريعات محددة

النهج الثالث هو سن تشريعات محددة تتصدى لاستخدام الإرهابيين للإنترنت.

أمثلة على التشريعات المحددة

مثلما ذُكر أعلاه، يستخدم مصطلح "استخدام الإرهابيين للإنترنت" من أجل وصف مجموعة من الأنشطة التي تتراوح بين نشر الدعاية والهجمات المتعمّدة. وفيما يخص الاستجابة القانونية، هناك مجالان رئيسيان للتنظيم، هما: الهجمات المتصلة بالحاسوب والمحتوى غير القانوني.

الهجمات المتصلة بالحاسوب

أحد النهج المتعلقة بوضع حكم يعالج الهجمات الحاسوبية الإرهابية تحديداً هو الفصل 66F من قانون تكنولوجيا المعلومات في الهند لعام 2000، المعدل في عام 2008:

66F المعاقبة على الإرهاب السيبراني– قانون تكنولوجيا المعلومات لعام 2000. [مثلما عُدل بقانون تكنولوجيا المعلومات (المعدل) لعام 2008]

(1) كل من،–

أ) لديه نية تهديد وحدة أو سلامة أو أمن أو سيادة الهند أو بث الرعب بين الشعب أو أي شريحة من الشعب عن طريق –

'1' حرمان أو التسبب في حرمان أي شخص مرخّص له بالنفاذ إلى مورد حاسوبي من النفاذ إلى ذلك المورد؛

'2' أو محاولة اختراق أو النفاذ إلى مورد حاسوبي بدون ترخيص أو تجاوز النفاذ المرخّص به؛

'3' أو إدخال ملوث حاسوبي أو التسبب في إدخاله.

ويتسبب أو من المحتمل أن يتسبب من خلال هذا السلوك في وفاة أو إصابة أشخاص أو في إعطاب أو تدمير ممتلكات أو يتسبب في أي شكل من أشكال الخلل أو كان يعرف أنه من المحتمل أن يتسبب في إلحاق الضرر أو عرقلة إمدادات أو خدمات أساسية لحياة المجتمع أو أن يؤثر تأثيراً ضاراً في البُنى التحتية الأساسية للمعلومات المحددة في إطار الفصل 70،

ب) أو يخترق أو ينفذ إلى مورد حاسوبي عن علم أو عن قصد دون ترخيص أو يتجاوز النفاذ المرخص به، ويتمكن عن طريق هذا السلوك من النفاذ إلى معلومات أو بيانات أو قواعد بيانات حاسوبية يكون النفاذ إليها مقيداً لأسباب تتعلق بأمن الدولة أو علاقاتها الخارجية؛ أو إلى أي معلومات أو بيانات أو قواعد بيانات حاسوبية يقيد النفاذ إليها لوجود أسباب تدعو إلى الاعتقاد بأنه إذا تم الحصول على هذه المعلومات أو البيانات أو قواعد البيانات الحاسوبية على هذا النحو، فقد تستخدم لإلحاق الضرر أو احتمال إلحاق الضرر بالمصالح المتعلقة بسيادة الهند وسلامتها، أو أمن الدولة أو علاقات الصداقة مع الدول الأجنبية، أو النظام العام، أو الآداب أو الأخلاق، أو لانتهاك حرمة المحكمة، أو للتشهير أو التحريض على ارتكاب جريمة، أو لفائدة أي دولة أجنبية، أو مجموعة من الأفراد أو لأغراض أخرى، فإنه يرتكب جريمة من جرائم الإرهاب السيبراني.

(2) ويُعاقب كل من يرتكب جريمة من جرائم الإرهاب السيبراني أو يتآمر على ارتكابها بعقوبة السجن التي قد تصل إلى السجن المؤبد".

ولا يقتضي الفصل 66F من قانون تكنولوجيا المعلومات في الهند فقط أن يتصرف الجاني بنية متصلة بالإرهاب ("نية تهديد وحدة أو سلامة أو أمن أو سيادة الهند أو بث الرعب بين الشعب وبين شريحة من الشعب") بل إذا أسفرت الجريمة كذلك عن ضرر بالغ مثل الوفاة أو الإصابة أو عرقلة الخدمات التي تلحق الضرر بالبنى التحتية الحرجة للمعلومات.

المحتوى غير القانوني

يشكل المحتوى غير القانوني مثل الدعاية الإرهابية مجالاً تتمسك فيه الدول بشكل خاص بنهج محايدة تكنولوجياً. وأحد الأمثلة على هذه النهج المحايدة تكنولوجيا هو المادة 10 من القانون الفيدرالي الروسي رقم 149-FZ المؤرخ 27 يوليو 2006 والمتعلق بالمعلومات وتكنولوجيا المعلومات وحماية المعلومات.

المادة 10 – نشر المعلومات أو إتاحة المعلومات

[...]

6 يُمنع نشر المعلومات التي تستهدف الدعاية للحروب والتمييز والعداء على أساس قومي أو عنصري أو ديني، وغيرها من المعلومات التي يخضع نشرها للمسؤولية الجنائية أو الإدارية.

ولا يتناول هذا الحكم بالتحديد توزيع المحتوى غير القانوني عن طريق الشبكات الحاسوبية أو إتاحة المحتوى على هذه الشبكات، بل إنه صيغ ليكون محايداً تكنولوجيا.

وأحد الأمثلة الأخرى على النهج المحايدة تكنولوجياً المادة 3 من تعديل عام 2008 للمقرر الإطاري للاتحاد الأوروبي[1970] بشأن مكافحة الإرهاب[1971].

المادة 3 – الجرائم المتصلة بالأنشطة الإرهابية

1 لأغراض هذا المقرر الإطاري:

أ) يعني "التحريض العلني على ارتكاب جريمة إرهابية" توزيع رسالة على الجمهور، أو إتاحتها له بشكل آخر، بقصد الحث على ارتكاب جريمة من الجرائم المدرجة في المادة 1(1) من أ) إلى ح)، عندما يسبب هذا السلوك، سواء كان يدعو بشكل مباشر أو غير مباشر إلى جرائم إرهابية، خطراً يتمثل في احتمال ارتكاب جريمة أو أكثر من هذه الجرائم؛

ب) يعني "التجنيد لأغراض الإرهاب" دفع شخص آخر إلى ارتكاب جريمة من الجرائم المدرجة في المادة 1(1) من أ) إلى ح) أو في المادة 2(2)؛

ج) يعني "التدريب لأغراض الإرهاب" تقديم إرشادات بشأن صنع أو استخدام المتفجرات أو الأسلحة النارية أو غيرها من الأسلحة أو المواد الضارة أو الخطرة، أو بشأن أساليب أو تقنيات محددة أخرى، بغرض ارتكاب جريمة من الجرائم المدرجة في المادة 1(1) من أ) إلى ح) مع إدراك أن المراد من توفير هذه المهارات هو استخدامها لهذا الغرض.

2 وتتخذ كل دولة عضو التدابير اللازمة لضمان أن تشمل الجرائم المتصلة بالأنشطة الإرهابية الأفعال العمدية التالية:

أ) التحريض العلني على ارتكاب جريمة إرهابية

ب) التجنيد لأغراض الإرهاب

ج) التدريب لأغراض الإرهاب

د) السطو المتفاقم بهدف ارتكاب جريمة من الجرائم المدرجة في المادة 1(1)؛

هـ) الابتزاز بهدف ارتكاب جريمة من الجرائم المدرجة في المادة 1(1)؛

و) إعداد وثائق إدارية مزيفة بهدف ارتكاب جريمة من الجرائم المدرجة في المادة 1(1) من أ) إلى ح) وفي المادة 2(2) ب).

3 وليس من الضروري أن تُرتكب بالفعل جريمة إرهابية للمعاقبة على فعل من الأفعال المبينة في الفقرة '2'.

ويؤكد واضعو القرار الإطاري المذكور في المقدمة أن الإطار القانوني القائم يجرم المساعدة في الإرهاب والتحريض والحث عليه لكنه لا يجرم نشر الخبرات الإرهابية باستخدام الإنترنت. وفي هذا السياق، أشار واضعو القرار الإطاري إلى أن "الإنترنت يستخدم لحث وحشد الشبكات الإرهابية المحلية والأفراد في أوروبا كما أنها تُستخدم كمصدر معلومات عن الوسائل والأساليب الإرهابية، وهي تُعدّ بالتالي بمثابة 'معسكر تدريبي افتراضي'".[1972] ورغم الإشارة إشارة صريحة إلى استخدام الإرهابيين للإنترنت في المقدمة، فقد صيغ الحكم المذكور على نحو محايد تكنولوجياً ونتيجة لذلك فإنه يغطي أفعال التدريب على الخط وخارج الخط لأغراض الإرهاب.[1973] وأحد التحديات المتصلة بتطبيق الحكم في الحالات المتعلقة بالإنترنت هو صعوبة إثبات أن الجاني يتصرف وهو يعلم أن المراد من المهارات المقدمة هو استخدامها لهذا الغرض. ومن المرجح إلى حد كبير أن تحد الحاجة إلى إثبات ذلك من قابلية تطبيق الحكم على إرشادات استخدام الأسلحة، التي تتاح على الخط. وبما أن من الممكن استخدام معظم الأسلحة والمتفجرات من أجل ارتكاب الجرائم العادية وكذلك الجرائم المتصلة بالإرهاب، فإن مجرد نشر هذا النوع من المعلومات لا يثبت أن ناشرها على علم بالطريقة التي ستُستخدم بها. ولذا، لا بد من النظر في سياق النشر (كأن تُنشر المعلومات على موقع شبكي تشغّله منظمة إرهابية). وقد يطرح هذا الأمر تحديات إذا نُشرت المعلومات خارج سياق المحتويات الأخرى المتصلة بالإرهاب، كأن تُنشر مثلاً عن طريق أنظمة تبادل الملفات وخدمات استضافة الملفات.

وأحد الأمثلة على نهج خاص بالإنترنت هو المادة 5 من اللوائح الصينية بشأن أمن وحماية وإدارة شبكات المعلومات الحاسوبية والإنترنت.

*"**المادة 5 –** لا يجوز لأي وحدة أو فرد استخدام الإنترنت من أجل استحداث أو نسخ أو استعادة أو إرسال الأنواع التالية من المعلومات:*

(1) التي تحرض على معارضة الدستور أو القوانين أو تنفيذ اللوائح الإدارية أو التي تنتهك الدستور أو القوانين أو تنفيذ اللوائح الإدارية؛

(2) التي تحرض على الإطاحة بحكومة النظام الاشتراكي؛

(3) التي تحرض على تقسيم البلاد، مما يضر بالوحدة الوطنية؛

(4) التي تحرض على الكراهية أو التمييز بين القوميات أو التي تضر بوحدة القوميات؛

(5) التي تقدم أكاذيب أو تشوه الحقيقة أو تنشر إشاعات أو تدمر نظام المجتمع؛

(6) التي تروج للخرافات، أو مواد ذات إيحاءات جنسية، أو القمار أو العنف أو القتل؛

(7) المتعلقة بالإرهاب، أو التي تحرض الآخرين على نشاط إجرامي، أو التي تسبّ علناً أشخاصاً آخرين أو التي تشوه الحقيقة للتشهير بأشخاص؛

(8) التي تسيئ إلى سمعة الهيئات الحكومية؛

(9) المتعلقة بأنشطة أخرى مناهضة للدستور أو القانون أو اللوائح الإدارية."

الحرب السيبرانية

رغم أن التهديدات المتصلة بالحرب السيبرانية نُوقشت خلال عدة عقود، فإن النقاش حول الاستجابة القانونية لم يبدأ إلا مؤخراً. وتخضع الحرب السيبرانية، ربما أكثر من الجريمة السيبرانية، لأحكام القانون الدولي. وتشكل اتفاقيتا لاهاي وجنيف وميثاق الأمم المتحدة صكوكاً مهمة من صكوك القانون الدولي التي تتضمن لوائح لتنظيم قوانين الحروب. وفي حين هناك ممارسة طويلة في تطبيق هذه الصكوك في النزاعات المسلحة العادية، فإن من الصعب تطبيقها على الهجمات الحاسوبية والقائمة على الشبكة. ويمكن توضيح هذا من خلال تحليل قابلية تطبيق المادة 2(4) من ميثاق الأمم المتحدة، حظر استخدام القوة.

***المادة 2 –** ميثاق الأمم المتحدة*

تعمل الهيئة وأعضاؤها في سعيها وراء المقاصد المذكورة في المادة الأولى وفقاً للمبادئ الآتية:

[...]

(4) يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة.

[...]

ويرمي منع استخدام القوة إلى إنفاذ حظر شامل لجميع أنواع القوة، باستثناء الأنواع التي تتماشى مع ميثاق المتحدة.[1974] وفي العقود الأخيرة، واجه منع استخدام القوة الوراد في المادة 2(4) تحديات عدة مرات. وكان أحد التحديات هو الانتقال من الحروب الكبرى التي شكلت محور التركيز عند صياغة ميثاق الأمم المتحدة بعد الحرب العالمية الثانية، إلى الحروب الصغرى التي أصبحت أكثر تواتراً إلى حد كبير في الوقت الراهن.[1975] وتضيف تغطية الهجمات المتصلة بالحاسوب بُعداً آخر إلى

التحديات، ليس فقط من حيث الحجم، بل أيضاً من حيث اختلاف الأساليب والأدوات المستخدمة في النزاع.[1976] ونتيجة لذلك، فإن الصعوبة الرئيسية المتصلة بتطبيق المادة 2 هي تفسير مصطلح "استخدام القوة". وليس هناك أي تعريف واضح لمصطلح "استخدام القوة" لا في ميثاق الأمم المتحدة ولا في أي صك دولي آخر ذي صلة. ومن المقبول به على نطاق واسع أن جميع أشكال الأفعال العدائية محظورة بموجب ميثاق الأمم المتحدة. ويشمل الحظر الهجمات بالأسلحة التقليدية، على سبيل المثال، لكنه لا يشمل التهديد باستخدام القوة والإكراه الاقتصادي.[1977]

والعنصران المكونان لاستخدام القوة هما استخدام الأسلحة ومشاركة جهات فاعلة حكومية. وعلى الرغم من أن أهمية هذه الأخيرة كانت موضوع جدل، على نحو خاص، في قرارات مجلس الأمن بعد هجمات 11 سبتمبر، يظل العنصران أساسيين فيما يخص حظر استخدام القوة.

استخدام الأسلحة/تدمير الأرواح والممتلكات

العنصر المكوّن الأول هو استخدام الأسلحة. ولا يمكن بأي حال من الأحوال أن تسمى التكنولوجيا الحاسوبية المستخدمة في تنفيذ الهجمات المتصلة بالإنترنت سلاحاً تقليدياً، طالما أن هذه الأسلحة تنطوي عموماً على أثر حركي.[1978] ومع هذا، فإن ضرورة إدراج أسلحة كيماوية وبيولوجية تطلبت بالفعل انتقالاً من تعريف موجه نحو الإجراءات إلى نهج موجه نحو التأثيرات. وفي إطار نهج أوسع كهذا، يمكن تعريف الأسلحة كأداة لتدمير الأرواح والممتلكات.[1979]

لكن، حتى بالاستناد إلى تفسير واسع من هذا النوع، من الصعب النظر إلى الهجمات الحاسوبية والقائمة على الشبكة بوصفها استخداماً للقوة وتناول التكنولوجيا الحاسوبية بوصفها أسلحة، بما أن أثر الهجمات مختلف.[1980] ولا تختلف الأساليب المستخدمة فقط، بل إن الآثار أيضاً تختلف مقارنة بالنزاعات المسلحة التقليدية.[1981] وتركز الاستراتيجيات العسكرية التقليدية التي يدخل فيها استخدام الأسلحة على الإنهاء المادي لقدرات العدو العسكرية. أما الهجمات الحاسوبية والقائمة على الشبكة فيمكن تنفيذها بقدر أدنى من الضرر المادي والخسارة في الأرواح.[1982] وعلى عكس هجمة باستخدام القذائف، لا تتسبب هجمة بالحرمان من الخدمة توقف موقعاً شبكياً حكومياً عن العمل بشكل مؤقت، في أي ضرر مادي فعلي. لكن سيكون من المضلل ادعاء أنه من غير الممكن أن تسفر الهجمات الحاسوبية عن ضرر بالغ. فقد تشكل هجمة بالحرمان من الخدمة ضد النظام الحاسوبي لمستشفى أو بنك للدم تهديداً خطيراً على الصحة وقد تعرض حياة عدد كبير من الأشخاص للخطر. ولعلّ اكتشاف الأثر المادي المحتمل لبرمجية ستوكسنت (Stuxnet) مثال آخر يظهر أن الهجمات الحاسوبية لا تؤدي بالضرورة إلى نتائج غير مادية. وإذا كان للهجمات الحاسوبية والقائمة على الشبكة مثل هذا الأثر المادي، فمن الممكن اعتبارها مماثلة للأسلحة التقليدية.[1983]

النزاع بين الدول

مثلما ذُكر أعلاه، فإن الشرط الثاني لتطبيق المادة 2 من ميثاق الأمم المتحدة هو أن يكون استخدام القوة على يد دولة ضد دولة أخرى. ورغم الاتجاهات الحديثة الرامية إلى توسيع نطاق تطبيق ميثاق الأمم المتحدة، فإن الأفعال التي ترتكبها جهات فاعلة غير حكومية لا تندرج في إطار المادة 2 من ميثاق الأمم المتحدة. ولهذا صلة كبيرة بتغطية الحرب السيبرانية، بما أنه في هذه الحرب تضطلع جهات غير حكومية بدور أهم – على عكس ما يجري في الحروب التقليدية. وهناك بواعث قلق كبيرة بشأن الانتشار، لأن بإمكان جهات غير حكومية الحصول على موارد فعالة قد تفوق الموارد التي تتحكم فيها الدول.[1984] وتضم أكبر البرمجيات الروبوتية عدة ملايين من الأنظمة الحاسوبية. ومن المحتمل أن يكون هذا العدد أكبر من عدد الأنظمة الحاسوبية التي تتحكم فيها الدول والمتاحة للتدخلات العسكرية في معظم الدول. وتكتسي قدرات الجهات غير الحكومية أهمية عالية، بما أن هذه الجهات تعمل أساساً خارج الإطار القانوني الدولي الملزم للدول. وتنشأ عن ذلك شواغل بشأن تحديد القائم بالهجمات. وحتى الآن يتطلب تطبيق المادة 2 من ميثاق الأمم المتحدة أن تُنسب أي هجمة حاسوبية إلى دولة ما. وتؤكد التجارب المتصلة بالحادثين اللذين شهدتهما إستونيا في عام 2007 وجورجيا في عام 2008 أن تحديد مصدر هجمة من الهجمات والتحقق منه قد يكون في معظم الحالات تحدياً لا يمكن التغلب عليه.

3.6 الأدلة الرقمية

Bibliography (selected): *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf; *Gercke*, Impact of Cloud Computing on the work of law enforcement agencies, published in *Taeger/Wiebe*, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4; *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No.3; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002; *Hayes*, Forensic Handwriting Examination, 2006; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2; *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010; *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No.1; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*,

Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1; *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

نظراً للسّعات المتزايدة لمحركات الأقراص الصّلبة، على نحو خاص،[1985] وتدني أسعار[1986] تخزين الوثائق الرقمية مقارنة بتخزين الوثائق المادية، فإن عدد الوثائق الرقمية في تزايد.[1987] ويخزن حالياً قدر كبير من البيانات في الصيغة الرقمية فقط.[1988] وإلى جانب هذا، أصبحت التكنولوجيات الحاسوبية والشبكية جزءاً من الحياة اليومية في البلدان المتقدمة وباتت تشهد نمواً في البلدان النامية. ونتيجة لذلك، تستأثر الوثائق الإلكترونية من قبيل الوثائق النصية والتسجيلات الفيديوية الرقمية والصور الرقمية[1989] بدور في التحقيقات المتعلقة بالجريمة السيبرانية والإجراءات ذات الصلة في المحاكم.[1990]

بيد أن أثر الرقمنة وأهمية الأدلة الرقمية بات يمتد ليتجاوز نطاق التحقيق في الجرائم السيبرانية: حتى في حالة ارتكاب جرائم تقليدية، يمكن أن يترك الجناة آثاراً رقمية،[1991] مثل المعلومات المتعلقة بتحديد موقع هواتفهم الخلوية أو طلباتهم المشتبه فيها على محركات البحث.[1992] ولذا، تعتبر القدرة على استغلال أدوات للتحقيق متعلقة ببيانات محددة وتقديم أدلة رقمية في المحكمة أمراً أساسياً بالنسبة للتحقيق في الجرائم السيبرانية والجرائم التقليدية على حدّ سواء.[1993]

وتطرح عملية التعامل مع 'الأدلة الرقمية' عدداً من التحديات،[1994] لكنها تفسح المجال أمام إمكانيات جديدة للتحقيق ولعمل خبراء الأدلة الجنائية والمحاكم. وقد تغير بالفعل عمل المحققين في المرحلة الأولى، أي جمع الأدلة، بسبب ضرورة أن يكون هؤلاء قادرين على التعامل مع الأدلة الرقمية. فلا بد لهم من أدوات معينة للتحقيق من أجل إنجاز التحقيقات. ويكون توافر هذه الأدوات مهما بالأخص إذا لم تتوفر الأدلة التقليدية مثل بصمات الأصابع أو الشهود. وفي هذه الحالات، قد تستند القدرة على تحديد الجاني وملاحقته إلى جمع الأدلة الرقمية وتقييمها على النحو الصحيح.[1995] لكن فضلاً عن جمع الأدلة، تؤثر الرقمنة أيضاً في الطريقة التي تتعامل بها وكالات إنفاذ القانون والمحاكم مع الأدلة.[1996] ففي حين تُقدَّم الوثائق الأصلية من خلال تسليم الوثيقة الرسمية في المحكمة، تتطلب الأدلة الرقمية في بعض الحالات إجراءات محددة لا تسمح بتحويل هذه الأدلة إلى أدلة تقليدية، على سبيل المثال عن طريق تقديم نسخ مطبوعة من الملفات والبيانات الأخرى المكتشفة.[1997]

ويقدم الفصل التالي لمحة عامة عن الجوانب العملية والقانونية للأدلة الرقمية والتحقيقات في الجرائم السيبرانية.

1.3.6 تعريف الأدلة الرقمية

تؤثر الرقمنة والاستخدام الناشئ لتكنولوجيا المعلومات والاتصالات تأثيراً كبيراً في الإجراءات المتعلقة بجمع الأدلة واستخدامها في المحاكم.[1998] ونتيجة لهذا التطوّر، أُدرجت الأدلة الرقمية كمصدر جديد للأدلة.[1999] وليس هناك تعريف واحد للأدلة الإلكترونية أو الرقمية.[2000] ويعرف قانون الشرطة والأدلة الجنائية في المملكة المتحدة (UK) الأدلة الرقمية بأنها "جميع المعلومات التي يتضمنها حاسوب".[2001] ويعرف نهج أوسع الأدلة الرقمية بأنها أي بيانات تخزن أو ترسل باستخدام التكنولوجيا الحاسوبية من شأنها أن تدعم نظرية الطريقة التي ارتكبت بها جريمة ما.[2002]

2.3.6 أهمية الأدلة الرقمية في التحقيقات المتعلقة بالجرائم السيبرانية

للأدلة الرقمية دور هام في مختلف مراحل التحقيقات في الجرائم السيبرانية. ويمكن التمييز عموماً بين مرحلتين رئيسيتين، هما[2003]: مرحلة التحقيق (تحديد الأدلة المناسبة[2004]، وجمع الأدلة والاحتفاظ بها[2005]، وتحليل التكنولوجيا الحاسوبية والأدلة الرقمية) ومرحلة تقديم الأدلة واستخدامها في الإجراءات في المحاكم.

وترتبط المرحلة الأولى بالأدلة الجنائية الحاسوبية وهو ما سيُناقش بمزيد من التفصيل أدناه. [2006]ويصف مصطلح "الأدلة الجنائية الحاسوبية"[2007] تحليل معدات تكنولوجيا المعلومات بهدف البحث عن أدلة رقمية.[2008] ويبرز النمو المستمر في كمية البيانات المخزنة في نسق رقمي التحديات اللوجيستية الماثلة أمام التحقيقات. وتستأثر نهج إجراءات الأدلة الجنائية المؤتمتة،[2009] مثل استخدام عمليات البحث القائمة على قيم الفرم (قيم هاش) للحصول على صور الأطفال المستغلين في المواد الإباحية أو عمليات البحث بواسطة كلمات رئيسية،[2010] بدور هام إلى جانب التحقيقات اليدوية.[2011] وتتضمن عملية تحديد الأدلة الجنائية الحاسوبية تحقيقات من قبيل تحليل العتاد والبرمجيات التي يستخدمها المشتبه فيه،[2012] أو استرجاع الملفات الملغاة،[2013] أو فك تجفير الملفات،[2014] أو تحديد مستخدمي الإنترنت عن طريق تحليل بيانات الحركة.

وتتعلق المرحلة الثانية بتقديم الأدلة الرقمية في المحكمة. وترتبط ارتباطاً وثيقاً بالإجراءات المحددة اللازمة لأن المعلومات الرقمية لا يمكن أن تصبح مرئية إلا عند طباعتها أو عرضها باستخدام التكنولوجيا الحاسوبية.

3.3.6 تزايد أهمية الأدلة الرقمية في التحقيقات المتعلقة بالجرائم التقليدية

إن قدرة المحققين على البحث عن البيانات والعثور على أدلة وكذلك قدرة المحاكم على التعامل مع الأدلة الرقمية لا تقتصران على التحقيقات المتعلقة بالجريمة السيبرانية. ونظراً لتزايد دخول التكنولوجيا الحاسوبية في حياة الأشخاص اليومية، باتت الأدلة الرقمية مصدراً مهما للأدلة حتى في التحقيقات التقليدية. ومن أمثلة ذلك محاكمة بشأن جريمة قتل في الولايات المتحدة، استُخدمت فيها تسجيلات لطلبات على محركات البحث مخزنة في حاسوب المشتبه فيه لإثبات أن المشتبه فيه كان يستخدم بشكل مكثف، قبل القتل، محركات البحث للحصول على معلومات بشأن السموم التي لا يمكن انكشافها.

4.3.6 فرص جديدة لعملية التحقيقات

بحسب تكنولوجيا المعلومات والاتصالات وخدمات الإنترنت التي يستخدمها المشتبه فيه، تُترك مجموعة كبيرة من الآثار الرقمية.[2015] وإذا استخدم المشتبه فيه، على سبيل المثال، محركات البحث للحصول على مواد إباحية يستغل فيها الأطفال، يسجل طلب بحثه وعناوين بروتوكول الإنترنت وحتى بعض المعلومات الإضافية المتصلة بالهوية في بعض الحالات (مثل معرف الهوية على غوغل).[2016] وأحياناً تشمل الكاميرات الرقمية المستخدمة لإنتاج صور الأطفال المستغلين في المواد الإباحية معلومات جغرافية في الملف تمكن المحققين من تحديد الموقع الذي أخذت فيه الصور إذا ضُبطت مثل هذه الصور على مخدم.[2017] كما يمكن في بعض الحالات تعقب المشتبهين الذين يقومون بتحميل محتوى غير قانوني من شبكات تبادل الملفات، وذلك عن طريق معرف الهوية الفريد الذي يتولد عند تثبيت برمجية تبادل الملفات.[2018] وقد ينتج عن تزوير وثيقة إلكترونية بيانات شرحية تمكن كاتب الوثيقة الأصلي من إثبات التلاعب.[2019]

وهناك جانب آخر يستشهد بها مراراً وتكراراً كمزية يتمثل في حياد وموثوقية الأدلة الرقمية.[2020] ومقارنة ببعض الفئات الأخرى من الأدلة مثل أقوال الشهود، فإن الأدلة الرقمية أقل عرضة بالتأكيد للتأثير الذي قد يكون له وقع على الاحتفاظ بالأدلة.[2021]

5.3.6 التحديات

في الأيام الأولى للتكنولوجيا الحاسوبية، كانت قدرة وكالات إنفاذ القانون على إنجاز تحقيقات تتضمن بيانات حاسوبية قدرة محدودة بسبب الافتقار إلى المعدات والخبرة في مجال الأدلة الجنائية الحاسوبية.[2022] وقد أدت الأهمية المتزايدة للأدلة الرقمية إلى

نشأة عدد متنام من معاملة الأدلة الجنائية الحاسوبية. لكن إذا كان من الممكن حل الجوانب اللوجيستية على نحو سهل إلى حد ما، يظل هناك عدد من التحديات.

والسبب الأساسي وراء هذه التحديات هو أنه على الرغم من وجود عدد من أوجه التشابه بين الأدلة الرقمية والفئات الأخرى من الأدلة، هناك اختلافات رئيسية بينها. وتظل بعض المبادئ العامة صالحة[2023]، مثل شرط أن تكون الأدلة مستَيقنة وكاملة وموثوقة ودقيقة وأن تجري عملية الحصول على الأدلة وفقاً للشروط القانونية.[2024] لكن إلى جانب أوجه التشابه، هناك عدد من الجوانب التي تجعل من الأدلة الرقمية[2025] أدلة فريدة من نوعها وتستدعي بالتالي اهتماماً خاصاً عند التعامل معها في التحقيقات الجنائية.

الحاجة إلى البحث العلمي والتدريب

الأدلة الرقمية هي فئة جديدة نسبياً من الأدلة ويشهد هذا المجال تطوراً سريعاً. ورغم الإطار الزمني المحدود جداً المتاح للبحث العلمي الأساسي، أصبحت إجراءات البحث عن الأدلة الرقمية والتوصل إليها وتحليلها تحتاج حالياً إلى مبادئ وإجراءات موثوقة علميا.[2026] وعلى الرغم من البحث المكثف الذي تم بالفعل، هناك مجالات مختلفة تتطلب اهتمام العلماء. ولذا من المهم مواصلة البحث العلمي في المجالات المثيرة للجدل مثل موثوقية الأدلة بوجه عام[2027] أو التقدير الكمي لمعدلات الخطأ المحتمل.[2028] ولا يقتصر تأثير التطور المستمر فقط على ضرورة البحث العلمي المتواصل.[2029] وبما أن التطورات قد تثير تحديات جديدة أمام التحقق من الأدلة الجنائية، فمن الضروري تدريب الخبراء بشكل مستمر.

الحاجة إلى وجود معايير قانونية ملزمة

رغم استخدام التكنولوجيات الحاسوبية والشبكية على المستوى العالمي وتشابه التحديات المتصلة بمقبولية الأدلة الرقمية في المحاكم– مع اختلاف الأنظمة القانونية، فإن المعايير القانونية الملزمة التي تتناول الأدلة الرقمية لم تطبق على نطاق واسع.[2030] وحتى الآن، لم تشرع سوى بعض البلدان في تحديث تشريعاتها ذات الصلة لتمكين المحاكم من التعامل مع الأدلة الرقمية بشكل مباشر.[2031] ومثلما هو الحال بالنسبة للقانون الجنائي الموضوعي والقوانين الإجرائية في مجال مكافحة الجريمة السيبرانية، هناك افتقار إلى مواءمة المعايير القانونية على الصعيد العالمي أيضاً في مجال الأدلة الرقمية.

الجوانب الكمية

مثلما ذُكر أعلاه، تزايد عدد الوثائق الرقمية بسبب أسعار تخزينها المتدنية[2032] مقارنة بتخزين الوثائق المادية.[2033] وعلى الرغم من توافر أدوات لأتمتة عمليات البحث[2034]، فإن تحديد الأدلة الرقمية المناسبة على جهاز للتخزين يمكنه حمل ملايين من الوثائق يشكل تحدياً لوجيستياً بالنسبة للمحققين.[2035]

الاعتماد على إفادات الخبراء

يتطلب تحليل الأدلة الرقمية وتقييمها مهارات خاصة وفهماً تقنياً لا يدخل بالضرورة ضمن التعليم الذي يتلقاه القضاة والمدعون العامون والمحامون. ولهذا، فإنهم يعتمدون أكثر فأكثر على دعم الخبراء في استرجاع الأدلة الرقمية.[2036] وفي حين لا تختلف هذه الحالة اختلافاً كبيراً عن تقنيات التحقيق المتطورة، مثل تسلسل الحمض النووي، فإنها تبرز الحاجة إلى نقاش ضروري بشأن نتائج هذا الاعتماد.[2037] ولتفادي أي أثر سلبي، تشجَّع المحاكم على أن تتأكد من موثوقية الأدلة وأن تطلب تحديد مدى ما يقترن بها من عدم التيقن.

الطبيعة الهشة للأدلة الرقمية

إن الأدلة الرقمية هشة إلى حد كبير ويمكن حذفها[2038] أو تعديلها[2039] بسهولة، وهو ما يعتبره الخبراء أمراً مُقلقاً.[2040] وشأنها شأن الفئات الأخرى من الأدلة، تنطوي الأدلة الرقمية على درجة ما من عدم اليقين.[2041] ولتفادي أي وقع سلبي على الموثوقية، يخضع جمع الأدلة الرقمية في معظم الأحيان لبعض الشروط التقنية. وعلى سبيل المثال، من شأن إغلاق نظام

حاسوبي أن يؤدي إلى فقدان كل الذاكرة المخزنة في ذاكرة النفاذ العشوائي للنظام[2042] ما لم تطبق تدابير تقنية خاصة لمنع هذه العملية.[2043] وفي الحالات التي تخزن فيها البيانات في ذاكرة مؤقتة، يمكن أن تكون تقنية جمع الأدلة مختلفة عن عملية جمع الأدلة الرقمية التقليدية.[2044] وقد يتعيّن وجود نهج متطور كهذا، على سبيل المثال، إذا كان المشتبه فيه يستخدم تكنولوجيا التجفير وأراد المحققون التأكد مما إذا كانت المعلومات المخزنة في ذاكرة النفاذ العشوائي تساعدهم على النفاذ إلى المعلومات المجفرة.[2045]

وقد تُجرى التعديلات عمداً على يد الجاني أو بالخطأ على يد المحققين. ويمكن أن يؤدي فقدان البيانات أو تعديلها في أسوأ الحالات إلى إدانة خاطئة.[2046]

وكنتيجة لهشاشة الأدلة الرقمية، فإن أحد أهم المبادئ الأساسية في مجال الأدلّة الجنائية الحاسوبية هو الحفاظ على سلامة الأدلة الرقمية.[2047] ويمكن تعريف السلامة في هذا السياق بأنها الخاصية التي لم تتغير بها البيانات الرقمية بأسلوب غير مرخص به منذ وقت استحداثها أو إرسالها أو تخزينها على يد مصدر مرخص له.[2048] ومن الضروري حماية سلامة البيانات لضمان موثوقيتها ودقتها.[2049] ويتطلب التعامل مع أدلة من هذا النوع معايير وإجراءات للإبقاء على نظام فعال للجودة. ويشمل ذلك جوانب عامة مثل سجلات الدعاوى، واستخدام التكنولوجيا والإجراءات المقبولة على نطاق واسع، وإجراء العمليات على يد خبراء مؤهلين فقط،[2050] وكذلك تطبيق أساليب معينة مثل المجموع التدقيقي وخوارزمية الفرم (هاش) والتوقيعات الرقمية.[2051] والأساليب اللازمة مكلفة ولا يمكنها أن تستبعد تماماً مخاطر التغيير.[2052]

الكمية المحدودة من البيانات المسجلة

بالنسبة للعديد من مستعملي الإنترنت، فإن كمية المعلومات المسجلة بشأن أنشطتهم تتسم بالإثارة. وقد لا يدرك المستعمل العادي أنه عندما ينفذ إلى الإنترنت أو يقوم بأفعال معينة مثل استخدام محرك للبحث،[2053] فإنه يترك آثاراً وراءه. ويمكن أن تكون هذه الآثار مصدراً قيّماً للأدلة الرقمية في التحقيق بشأن الجرائم السيبرانية. وعلى الرغم من ذلك، فإن المعلومات الرقمية الناتجة خلال استخدام التكنولوجيا الحاسوبية لا تُخزَّن جميعها. فالعديد من الأفعال والكثير من المعلومات مثل النقرات ولمسات المفاتيح لا تُحفظ إلا إذا رُكِّبت برمجية خاصة للمراقبة.[2054]

طبقة التجريد

حتى في الحالات التي تولد فيها أنشطة لمشتبه فيه أدلة رقمية، فإن هذه الأدلة تعزل زمنياً عن الأحداث التي تسجِّلها وتكون بالتالي سجلاً تاريخياً بالأحرى أكثر مما هي رصد حي.[2055] وإلى جانب هذا، لا تكون هذه الأدلة بالضرورة شخصية. وعلى سبيل المثال، إذا كان مشتبه فيه يستخدم مقهى عام للإنترنت من أجل النفاذ إلى صور الأطفال المستغلين في المواد الإباحية، فإن الآثار التي يتركها لا تتضمن بالضرورة معلومات عن الهوية يمكن من خلالها كشف هويته، إلا إذا أنزل المشتبه فيه في الوقت نفسه بريده الإلكتروني أو استعمل الخدمات التي تتطلب تسجيلا، وفي هذه الحالة يُستحدث رابط. لكن بما أن الوضع ليس كذلك، فإن الخبراء يشيرون إلى إنتاج هذا لطبقة تجريد قد تولد أخطاء.[2056]

الشروط المتصلة بالبنى التحتية

لقد اتبع تصميم قاعات المحاكم مبادئ مماثلة لعقود بل حتى لقرون في بعض البلدان. وبغض النظر عن الجوانب الأمنية (كأجهزة استشعار المعادن وآلات الأشعة السينية المثبتة) ووسائل الراحة (كمكيف الهواء)، يظل من الممكن استخدام قاعة محكمة مصممة ومجهزة منذ مئة سنة من أجل الإجراءات الجنائية.[2057] وتثير الحاجة إلى التعامل مع الأدلة الرقمية تحديات فيما يخص طبقة التجريد، كما أن عدم إمكانية تقديم الأدلة الرقمية دون استخدام أدوات مثل الطابعات والشاشات ينطوي على تبعات بالنسبة لتصميم قاعات المحاكم.[2058] ولا بد من تركيب الشاشات لضمان أن يستطيع القضاة والمدعي العام ومحاميو الدفاع والمتهم وهيئة المحلفين بطبيعة الحال متابعة عرض الأدلة. وتنجم عن تركيب وصيانة هذه المعدات تكاليف كبيرة بالنسبة للأنظمة القضائية.

البيئة التقنية المتغيرة

ومثلما ذُكر أعلاه، فإن التكنولوجيا في تغير مستمر. ويستدعي ذلك مراجعة مستمرة للإجراءات والمعدات والتدريب ذي الصلة من أجل ضمان ملاءمة وفعالية التحقيقات.[2059] ومع إنتاج نسخ جديدة باستمرار لأنظمة التشغيل أو المنتجات البرمجية، من الممكن أن تتغير الطريقة التي تُخزن بها البيانات المناسبة للتحقيقات. وتجري تطورات مماثلة فيما يخص العتاد.[2060] ففي الماضي كانت البيانات تُخزّن على الأقراص المرنة. أما اليوم، فسيكتشف المحققون أن المعلومات المناسبة قد تُخزن على أجهزة تشغيل الوسائط MP3 أو في ساعات تضم جهاز تخزين من نوع USB. ولا تنحصر التحديات في مواكبة آخر الاتجاهات في التكنولوجيا الحاسوبية.[2061] ولا بد لخبراء الأدلة الجنائية أيضاً من الاحتفاظ بمعدات للتعامل مع التكنولوجيا المتقادمة، كالأقراص المرنة من حجم 5.25 بوصة. وعلاوةً على التغييرات في العتاد، لا بد من القدرة على النفاذ إلى البرمجيات المتقادمة: فمن الممكن ألا يتسنى فتح الملفات من أدوات برمجية متقادمة دون استخدام البرمجية الأصلية.

ومن الضروري أيضاً دراسة التغييرات الأساسية في سلوك المستعمل دراسة متأنية. فقد أثر توافر النفاذ عريض النطاق ومخدمات التخزين عن بُعد، على سبيل المثال، في الطريقة التي تخزن بها المعلومات. وإذا كان بمقدور المحققين في الماضي التركيز على مقر المشتبه فيه عند البحث عن الأدلة الرقمية، فاليوم لا بد لهم من مراعاة احتمال أن يخزن المشتبه فيه ملفات في شكل مادي في الخارج وأن ينفذ إليها عن بُعد عند الضرورة.[2062] ويشكل الاستخدام المتزايد للتخزين بالحوسبة السحابية تحديات جديدة بالنسبة للمحققين.[2063]

6.3.6 أوجه التكافؤ بين الأدلة الرقمية والأدلة التقليدية

سلّطت الأبحاث التي أجريت في أوروبا في عامي 2005 و2006 الضوء على مجالات مختلفة من التكافؤ بين الأدلة الرقمية والتقليدية في 16 بلداً خضعت للدراسة.[2064] ويوجد التكافؤ الأكثر شيوعاً بين الوثائق الإلكترونية والوثائق الورقية. وأوجه التكافؤ الإضافية التي تُلاحظ في أغلب الأحيان هي البريد الإلكتروني والبريد التقليدي، والتوقيع الإلكتروني والتوقيعات الخطية التقليدية، وسندات التوثيق العدلي الإلكترونية وسندات التوثيق العدلي التقليدية.[2065]

7.3.6 العلاقة بين الأدلة الرقمية والأدلة التقليدية

فيما يخص العلاقة بين الأدلة الرقمية والأدلة التقليدية، يمكن التمييز بين عمليتين، هما: استبدال الأدلة التقليدية بالأدلة الرقمية، وإدراج الأدلة الرقمية كمصدر إضافي يكمل الأشكال التقليدية من الأدلة مثل الوثائق والشهود.

وأحد الأمثلة على الأدلة الرقمية التي تحل محل الأدلة التقليدية هو الاستخدام المتزايد للبريد الإلكتروني بدلاً من الرسائل.[2066] وفي الحالات التي لا تُرسل فيها أي رسائل مادية، لا بد أن تركز التحقيقات على الأدلة الرقمية. ولهذا انعكاسات فيما يخص الأساليب المتاحة لتحليل الأدلة وتقديمها. وفي الماضي، عندما كانت الرسائل المكتوبة باليد هي الوسيلة السائدة للاتصال غير الشفوي، كان تحليل الأدلة الجنائية يركز على التحقيق بواسطة الأدلة الجنائية لخط اليد.[2067] وقد سبق في الماضي عند انتشار الآلات الكاتبة، أن تغيرت الأساليب التي يستخدمها خبراء الأدلة الجنائية من تحليل الأدلة الجنائية للخط إلى تحليل الآلة الكاتبة.[2068] ومع التحول الجاري من الرسائل التقليدية إلى الرسائل الإلكترونية، لا بد للمحققين من أن يتعاملوا مع الأدلة الجنائية للبريد الإلكتروني[2069] في المقابل.[2070] وإذا كان ما ينتج من عدم القدرة على استخدام الوثائق المادية يحد من إمكانية إجراء التحقيقات ذات الصلة من جهة، فإن بإمكان المحققين الآن، من جهة أخرى، أن يستخدموا أدوات لأتمتة التحقيقات المتعلقة بالبريد الإلكتروني.[2071]

ورغم أن من المحتمل في أغلبية الحالات التي تتعلق باتصالات إلكترونية أن ينصب التركيز على الأدلة الرقمية،[2072] فمن الممكن أن تستمر فئات أخرى من الأدلة في القيام بدور مهم في تحديد هوية الجاني. وهذا مهم بالأخص لأن العمليات الحاسوبية لا تترك جميعها آثاراً رقمية ولأن من غير الممكن ربط جميع الآثار التي تُركت بالمشتبه فيه.[2073] وإذا استُعملت مطاريف الإنترنت العامة من أجل تنزيل المواد الإباحية التي يستغل فيها الأطفال، فقد يكون من غير الممكن ربط عملية

التنزيل بشخص يمكن تحديد هويته إذا لم يتمّ تسجيله[2074]، أو لم يترك أي معلومات شخصية؛ لكن قد تكون تسجيلات كاميرا المراقبة الفيديوية أو بصمات الأصابع على لوحة المفاتيح مفيدة، إذا أُتيحت. وفي المقابل، من الممكن في الجرائم التقليدية التي تستأثر فيها بصمات الأصابع وآثار الحمض النووي والشهود بدور مهيمن، أن تشكل الأدلة الرقمية مصدراً إضافياً قيّماً للأدلة. وقد تمكن المعلومات المتعلقة بموقع هاتف المشتبه فيه وكالات إنفاذ القانون من تحديد موقعه[2075] كما يمكن أن تدل الطلبات المشتبه فيها على محركات البحث على موقع ضحية مفقودة.[2076] وفيما يخص الجرائم التي تتضمن معاملات مالية (مثل التبادل التجاري لمواد إباحية يُستغل فيها أطفال[2077])، قد تشمل التحقيقات أيضاً سجلات تحتفظ بها منظمات مالية من أجل الكشف عن هوية الجاني. وفي عام 2007، اعتمد تحقيق عالمي بشأن المواد الإباحية التي يستغل فيها الأطفال على الكشف عن هوية المشتبه فيهم بالاستناد إلى سجلات معاملات مالية تتصل بشراء مواد إباحية يستغل فيها أطفال.[2078]

8.3.6 مقبولية الأدلة الرقمية

هناك مجالان مهمان للنقاش فيما يخص الأدلة الرقمية، هما: عملية جمع الأدلة الرقمية، ومقبولية الأدلة الرقمية في المحاكم. وستُناقش شروط محددة تتعلق بجمع الأدلة الرقمية مناقشة مستفيضة في الفصل الوارد أدناه المتعلق بالقانون الإجرائي. وفيما يتعلق بمقبولية الأدلة الرقمية، فإن المبادئ الأساسية هي نفسها على الرغم من الاختلافات القائمة بالمقارنة مع الأدلة التقليدية. بَيد أن تلخيص هذه المبادئ يشكل تحديا، بما أنه ليس هناك افتقار فقط إلى اتفاقات دولية ملزمة، بل إن هناك أيضاً اختلافات جوهرية في النهج الفعلي للتعامل مع الأدلة الرقمية. وفي حين تمنح بعض البلدان سلطة تقديرية للقضاة بشأن قبول الأدلة الرقمية أو رفضها، بدأت بلدان أخرى في وضع إطار قانوني لمعالجة مقبولية الأدلة في المحاكم.[2079]

الشرعية

إن أحد الشروط الأساسية الأهم لمقبولية الفئات التقليدية من الأدلة[2080] والأدلة الرقمية على حد سواء هو شرعية الأدلة.[2081] ويشترط هذا المبدأ أن تكون الأدلة الرقمية قد جُمعت وحللت وحفظت وقدمت في نهاية المطاف في المحكمة وفقاً للإجراءات المناسبة ودون انتهاك الحقوق الأساسية للمشتبه فيه.[2082] وتختلف الشروط المتصلة بجمع الأدلة وتحليلها وحفظها وتقديمها في نهاية المطاف في المحكمة من بلد لآخر، وكذلك النتائج الناجمة عن انتهاك حقوق المشتبه فيه. وتتراوح المبادئ والقواعد الممكن انتهاكها ما بين حقوق المشتبه فيه الأساسية مثل الخصوصية[2083] وعدم احترام الشروط الإجرائية. ونظراً لعدم كفاية التشريعات في معظم الأحيان، تطبق عادةً المبادئ العامة للأدلة على الأدلة الرقمية.[2084]

وتحدَّد شروط جمع الأدلة الرقمية بالأساس عن طريق القانون الإجرائي الجنائي. وفي معظم البلدان يقتضي اعتراض بيانات محتوى على سبيل المثال أمراً من المحكمة، كما يقتضي تمديد نطاق البحث ليشمل أجهزة التخزين عن بُعد أن تكون تلك الأجهزة في البلد نفسه. وإذا جرى الاعتراض دون أمر من المحكمة، يكون هناك خرق للإجراءات المناسبة، ومن ثم قد يتعارض التحقيق مع حقوق المشتبه فيه. ويحدد القانون على نحو أقل شروط حفظ الأدلة.[2085] بيد أن المبدأ الأساسي المتمثل في ضرورة حماية سلامة الأدلة الرقمية هو مبدأ توجيهي دون شك.[2086] ولا بد للمحققين من أن يتأكدوا أن الأدلة لم تُغير بأي طريقة غير مرخص بها منذ وقت استحداثها أو إرسالها أو تخزينها على يد مصدر مرخص له.[2087] ومن الضروري حماية سلامة الأدلة لضمان الموثوقية والصحة والالتزام بمبدأ الشرعية.[2088] ونادراً ما يحدد القانون إجراءات تقديم الأدلة في المحاكم.

ومثلما ذُكر أعلاه، لا تختلف الشروط وحدها اختلافاً كبيراً بل حتى النتائج الناجمة عن انتهاك الإجراءات وحقوق المشتبه فيه.[2089] وفي حين تعتبر بعض البلدان الأدلة غير مقبولة فقط إذا جُمعت بطريقة تنتهك انتهاكاً جسيماً حقوق المشتبه فيه (وليس، على سبيل المثال، إذا انتهكت فقط الشروط الشكلية) ولا تستبعد هذه الأدلة، تطبق بلدان أخرى– لا سيما تلك التي تطبق مبدأ ما بُني على باطل فهو باطل– معايير أخرى للمقبولية.[2090]

قاعدة أفضل الأدلة

بالنسبة للولايات القضائية القائمة على القانون العام، تكتسي قاعدة تطبيق أفضل الأدلة أهمية كبيرة.[2091] وهناك بعض الإحالات، في القضايا القديمة في الغالب، إلى "قاعدة أفضل الأدلة"، التي تقضي في إطار القانون العام بألا تُقبل سوى أفضل الأدلة المتاحة فيما يخص مسألة معينة. لكن، أياً كان الوضع الذي ربما تكون هذه القاعدة قد تمتّعت به في الماضي، هناك الآن إمكانية جد ضعيفة حالياً من أجل استمرار بقائها وبعض التأكيدات الصريحة لنهايتها.[2092]

والقاعدة العامة الآن على ما يبدو هي أنه سواء كان ثمة دليل معين هو أفضل الأدلة المتاحة أم لا فإن هذا لا يؤثر إلا في قيمته وليس في مقبوليته.[2093] وتتصل صلة وثيقة بقاعدة أفضل الأدلة "قاعدة الأدلة الأولية" التي كانت تقضي فيما سبق أنه في حالة الأدلة الوثائقية، فإن الوثيقة الأصلية أو نسخة "مسجلة" من الوثيقة هي المقبولة فقط لإثبات محتوياتها وصحتها. لكن المحاكم أبعدت بالفعل القاعدة القديمة، وتحصر التشريعات أي آثار متبقة من هذه القاعدة في الإجراءات الجنائية (التي تسمح الآن عموماً باستخدام نسخ مصدقة).[2094]

المنطق وراء اشتراط إصدار وثيقة أصلية عندما تكون متاحة بدلاً من الاعتماد على نسخ قد لا تكون مرضية، أو على مجموعات أقوال الشهود هو منطق واضح،[2095] على الرغم من أن التقنيات الحديثة تضع اعتراضات على اعتبار البديل الأول ضعيفا. وفي ظل الانعدام الذي لا مناص منه لأفضل الأدلة أو للأدلة الأولية في شكل وثائق، ستقبل المحاكم الأدلة الثانوية. وتوحي هذه الأدلة، في ظاهرها، بأن هناك أدلة غيرها وأفضل منها. ويجري إثبات الوثائق العامة والقضائية عادة بتقديم نسخ منها، دون تبرير غياب النسخ الأصلية؛ كما يجوز الآن إثبات أي بيان تتضمنه أي وثيقة عن طريق إصدار نسخة مصدقة من الوثيقة.[2096] والمبدأ الذي يقوم عليه هذا هو تقليص مخاطر الخطأ في التدوين وفي الإفادة بالشهادات فيما يخص مضمون الوثيقة واحتمالات التلاعب غير المكشوف.[2097] وتسمح القاعدة في تفسيرها الصارم باستخدام الأدلة الثانوية (في شكل نسخة) في حالة فقدان الأدلة الأصلية.

وفيما يخص الأدلة الرقمية، يثير هذا عدداً من الأسئلة، طالما كان من الضروري تحديد ماهيّة النسخة الأصلية.[2098] وبما أن من الممكن عموماً نسخ البيانات الرقمية دون فقدان الجودة ولأن تقديم البيانات الأصلية في المحكمة أمر غير ممكن في جميع القضايا، فإن قاعدة أفضل الأدلة تبدو غير متوافقة مع الأدلة الرقمية. لكن المحاكم بدأت تفتح هذه القاعدة لتطورات جديدة من خلال قبول نسخة إلكترونية والوثيقة الأصلية معاً.[2099] ولا تشترط قاعدة تطبيق أفضل الأدلة في هذا التفسير الأوسع شهادة خطية أو شهادة الشهود في كل حالة، لكنها تشترط استخدام أفضل الأدلة التي يمكن الحصول عليها من المحتويات.[2100] كما أن قاعدة أفضل الأدلة كانت مكرسة في معظم الأنظمة القانونية في منطقة الكومنولث.[2101]

القاعدة المضادة للشهادة بالسمع

القاعدة المضادة للشهادة بالسّمع هي مبدأ آخر مهم بشكل خاص بالنسبة لبلدان الكومنولث.[2102] وتتمثل الأدلة القائمة على الشهادة بالسمع في الأدلة التي يدلي بها شاهد في المحكمة بشأن قول جاء على لسان شخص آخر خارج المحكمة، عندما تُقدَّم هذه الأدلة لإثبات صحة القول.[2103] وبموجب القانون العام كانت الأدلة القائمة على الشهادة بالسمع غير مقبولة بوجه عام؛ لكن في الإجراءات المدنية، أُلغيت هذه القاعدة في المملكة المتحدة بموجب قانون الأدلة المدنية في عام 1995، الذي ينص على مقبولية الأدلة القائمة على الشهادة بالسمع رهناً بوجود ضمانات قانونية، ويحتفظ بعدد من الاستثناءات في القانون العام بشأن القاعدة المضادة للشهادة بالسّمع.[2104]

وحسب قاعدة القانون العام المتعلقة بالشهادة بالسّمع، لا يقبل تصريح غير تصريح أدلى به شخص عند تقديم أدلة شفوية في الإجراءات وقدمه كدليل على الوقائع المصرح بها.[2105] ولأغراض القاعدة المذكورة، يعني تصريح خارج المحكمة أي تصريح غير تصريح أدلى به شاهد أثناء تقديم أدلته، وقد يشمل، على سبيل المثال، قولاً أُدلي به في إجراءات قانونية سابقة. وبالتالي، من الممكن أن يكون القول قد قُدم دون يمين أو مشفوعاً بيمين، سواء في صيغة خطية أو حتى عن طريق علامات

أو حركات، من أي شخص، سواء سُمي شاهد أم لا في الإجراءات المعنية.[2106] وإلى جانب هذا، ترمي القاعدة إلى التمكين من استجواب الشاهد الحقيقي وإظهار مواطن الضعف في قول معين.[2107] وفي المقابل، من الضروري أن يثبت ذلك شاهد لديه معرفة شخصية مباشرة. وليست شهادة الشاهد هي وحدها التي يمكن أن تتضمن شهادة بالسمع غير مقبولة، بل إن مستندات أيضاً قد تتضمن شهادة بالسمع غير مقبولة.[2108] وقد قُدم عدد من الأسباب لتبرير قاعدة القانون العام ضد الشهادة بالسماع، مثل خطر تقديم أدلة مصطنعة، الذي يتصل باحتمال ألا تكون الأدلة القائمة على الشهادة بالسمع أدلة موثوقة. وتطبق حالياً القواعد التي تنظم مقبولية الأدلة القائمة على الشهادة بالسمع عندما (وفقط عندما) يبدو للمحكمة أن غرض أو أحد أغراض الشخص الذي يدلي بالتصريح هو جعل شخص آخر يؤمن بالأمر أو جعل شخص آخر يتصرف أو آلة تعمل على أساس أن الأمر هو مثلما جاء في التصريح.[2109]

وبالنظر إلى أن الهدف من البيانات التي تجمع خلال التحقيق (مثل ملفات التسجيل) هو إثبات حقيقة الأمر الذي جاء في الأدلة الرقمية نفسها، فإن التطبيق الدقيق للقاعدة مثير للمشاكل في عصر تشكل فيه الأدلة الرقمية في معظم الأحيان الفئة الأكثر ملاءمة من الأدلة في إجراءات المحاكم. وقد بدأت بعض البلدان التي تطبق القانون العام في تنفيذ استثناءات قانونية بشأن قاعدة الشهادة بالسمع.[2110] ولا يمكن أن تكون الأدلة الناتجة عن الحواسيب أو الكاميرات أو غيرها من الآلات دون أن تشمل أي تصريح بشري أدلة قائمة على الشهادة بالسمع.[2111] وبموجب القانون العام، كان من المسلم به أن الصور المرئية، حتى وإن كانت من صنع أيادي بشرية، لا تشكل "بيانات" لأي وقائع زُعم أنها تمثلها وبالتالي فهي لم تكن شهادة بالسمع. لكن هناك الآن حكماً واضحاً عكس ذلك.[2112]

وعندما لا تكون هناك أي استثناءات قانونية، فإن تطبيق القاعدة على الأدلة الرقمية يثير الجدل من خلال الإشارة إلى أنها لا تطبق إلا على التصريحات التي تتضمن أقوالاً لأشخاص بشريين. وعلى هذا الأساس، لن تعتبر المعلومات المولَّدة آلياً دون تدخل بشري كأدلة ممكنة قائمة على شهادة بالسمع،[2113] إلا إذا استخدمت عملية استحداث البرمجية كحجة لتطبيق القاعدة حتى في هذه الحالات.[2114]

الملاءمة/الفعالية

إن الملاءمة والفعالية شرطان من الشروط الأخرى الشائعة لمقبولية الأدلة الرقمية.[2115] وبأخذ كمية البيانات المخزنة حتى على حاسوب شخصي في الاعتبار، والتي قد يكون جزء ضئيل فقط منها ملائماً للقضية، يمكن إدراك الأهمية العملية لهذا المعيار في التحقيقات المتعلقة بالجريمة السيبرانية. وتطبيق هذا المعيار مهم من أجل تقييد تجميع الأدلة ومن أجل تقديمها في المحكمة. وعلى عكس ما يجري مع الأدلة التقليدية، إذ إنه يمكن خلال عملية التجميع إغفال الأجزاء غير المناسبة من الأدلة بدون أي مشاكل، فإن عملية الاختيار تنطوي على تحديات أكثر عندما يتعلق الأمر بالأدلة الرقمية،[2116] بما أنه في الوقت الذي يُحتجز فيه العتاد الحاسوبي، يكاد يكون من المستحيل الحسم إن كانت أدوات التخزين المعنية تتضمن المعلومات المطلوبة أم لا.

الشفافية

على عكس عمليات البحث والمصادرة التقليدية، التي تجري علناً وتضمن بالتالي أن يكون المشتبه فيه على علم بإجراء التحقيق، فإن أدوات التحقيق المتطورة مثل اعتراض الاتصالات في الوقت الفعلي لا تتطلب هذا الكشف. وعلى الرغم من القدرة التقنية، لا تسمح جميع البلدان لوكالات إنفاذ القانون بإنجاز عمليات سرية، أو تشترط على الأقل إخبار المشتبه فيه بهذه العمليات فيما بعد. وتمنح الشفافية خلال جميع مراحل عملية جمع الأدلة ومعالجتها واستخدامها في المحكمة، للمشتبه فيه إمكانية طرح أسئلة بشأن شرعية الأدلة المجمعة وملاءمتها.

9.3.6 الإطار القانوني

في حين يمكن وجود أحكام القانون الجنائي الموضوعي التي تغطي أشكال الجرائم الحاسوبية الأكثر شيوعاً في عدد كبير من البلدان، فإن الوضع يختلف فيما يخص الأدلة الرقمية. فحتى الآن، لم تعالج جوانب محددة من الأدلة الرقمية سوى بلدان قليلة، كما أن هناك افتقار إلى معايير دولية ملزمة. [2117]

قانون الكومنولث النموذجي بشأن الأدلة الإلكترونية (2002)

في عام 2000، قرر وزراء العدل في الولايات القضائية الصغيرة لبلدان الكومنولث إنشاء فريق للعمل من أجل وضع تشريعات نموذجية بشأن الأدلة الإلكترونية. والنتيجة الرئيسية التي خرج بها فريق الدراسات من تحليل القانون المقارن هي أنه، فيما يخص مقبولية الأدلة الرقمية، تكتسي موثوقية النظام الذي تستحدث به الأدلة الرقمية أهمية أكبر من الوثيقة نفسها. ويبرز القانون النموذجي لعام 2002،[2118] الذي ارتكز على تشريعات من سنغافورة[2119] وكندا[2120]، هذه النتائج ويغطي أهم جوانب الأدلة الرقمية فيما يخص البلدان التي تطبق القانون العام، مثل تطبيق قاعدة أفضل الأدلة[2121] وسلامة الأدلة الرقمية.

المقبولية بصفة عامة

3 لا يطبق أي حكم من أحكام قواعد الأدلة للحيلولة دون قبول تسجيل إلكتروني في الأدلة لمجرد أنه تسجيل إلكتروني.

يتضمن الفصل 3 عنصراً مشتركاً بين الأُطر القانونية التي تعمل على تنظيم جوانب الأدلة الرقمية، يمكن العثور عليه في شكل مماثل، على سبيل المثال، في المادة 5 من توجيه الاتحاد الأوروبي لعام 1999 بشأن التوقيعات الرقمية.[2122] ويرمي هذا الحكم إلى ضمان ألا تكون الأدلة الرقمية غير مقبولة في حد ذاتها. وفي هذا الصدد، يوفر الفصل 3 الأساس لاستخدام الأدلة الرقمية في إجراءات المحاكم. لكن لا تُكفل مقبولية الأدلة لمجرد أنها رقمية. فمن الضروري أن تستوفي الأدلة الرقمية قواعد الأدلة المعمول بها. وإذا كانت الأدلة مواداً قائمة على الشهادة بالسّمع، فإنها لا تصبح مقبولة بسبب الفصل 3.

نطاق القانون

4 (1) لا يعدل هذا القانون أي حكم من أحكام القانون العام أو أي قاعدة قانونية فيما يتعلق بمقبولية التسجيلات، باستثناء القواعد المتعلقة بالاستيقان وأفضل الأدلة.

(2) ويجوز لأي محكمة أن تأخذ بالأدلة المقدمة بموجب هذا القانون عند تطبيق أي حكم من أحكام القانون العام أو أي قاعدة قانونية فيما يتعلق بمقبولية التسجيلات.

تطبيق قاعدة أفضل الأدلة

6 (1) في أي إجراء قانوني، خاضع لأحكام الفقرة الفرعية (ب)، تطبق فيه قاعدة أفضل الأدلة بشأن التسجيلات الإلكترونية، تُنفذ القاعدة بعد إثبات سلامة نظام التسجيلات الإلكترونية الذي تُسجل أو تُخزن فيه أو من خلاله البيانات.

(2) في أي إجراء قانوني، يجري فيه على نحو واضح أو متسق التصرف بناء على تسجيل إلكتروني في شكل نسخة مطبوعة أو الاعتماد عليه أو استخدامه باعتباره تسجيل المعلومات المسجلة أو المخزنة على النسخة المطبوعة، تكون النسخة المطبوعة هي التسجيل لأغراض تطبيق قاعدة أفضل الأدلة.

وقد تتعارض بعض خصائص الأدلة الرقمية، مثلما وُصف أعلاه، مع المبادئ التقليدية المتعلقة بمقبولية الأدلة. ويتصل هذا بالأخص بقاعدة أفضل الأدلة، التي تكتسي أهمية كبيرة بالنسبة للبلدان التي تطبق القانون العام.[2123] والهدف من قاعدة أفضل الأدلة هو تقليص المخاطر المحتملة في التدوين وفي الإفادة بالشهادات فيما يخص مضمون الوثيقة واحتمالات التلاعب غير المكشوف.[2124] ويتطلب قبول الأدلة أن تكون الأدلة الوثائقية أفضل الأدلة المتاحة للطرف. وتحديد ما إذا كانت هذه الأدلة تستبعد الأدلة الرقمية في حد ذاتها هو أمر مثير للجدل.[2125] ويشكل الفصل 4 والفصل 6 من القانون النموذجي للكومنولث الدول المستقلة مثالين على استثناء قانوني. وفي هذا السياق، يوضح الفصل 4 بادئ ذي البدء أن القانون النموذجي لا يعدل سوى مبادئ التصديق وأفضل الأدلة. ووفقاً لهذا التوضيح العام، يعدل الفصل 6 قاعدة أفضل الأدلة لضمان ألا تكون الأدلة الرقمية غير مقبولة في حد ذاتها. وبالاستناد إلى الفصل 6، لا تُعدّ الأدلة الرقمية غير مقبولة بناءً على قاعدة أفضل الأدلة شريطة القدرة على إثبات سلامة النظام الذي استحدث البيانات.

قانون الكومنولث النموذجي المتعلق بالجرائم الحاسوبية والجرائم المتصلة بالحاسوب (2002)

في عام 2002، قُدم مشروع القانون النموذجي لبلدان الكومنولث بشأن الحاسوب والجريمة الحاسوبية.[2126] ويتضمن إلى جانب أحكام القانون الجنائي الموضوعي والمواد الإجرائية حكماً محدداً يتناول الأدلة الرقمية.

الأدلة

20 في الإجراءات المتعلقة بجريمة ضد قانون [دولة مشترعة]، فإن:

أ) ادعاء أن هناك جريمة تدَخل في نظام حاسوبي قد ارتُكبت؛

ب) وحقيقة أن الأدلة قد نتجت من ذلك النظام الحاسوبي؛

أمر لا يمنع في حد ذاته من قبول تلك الأدلة.

وهذا النهج مشابه للمادة 3 من القانون النموذجي لبلدان الكومنولث الأكثر تحديداً والمتعلق بالأدلة الإلكترونية لعام 2002.

4.6 الولاية القضائية

Bibliography (selected): *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004. *Hirst,* Jurisdiction and the Ambit of the Criminal Law, 2003; *Inazumi,* Universal Jurisdiction in Modern International Law, 2005; *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf; *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 69 et seq; *Sachdeva*, International Jurisdiction in Cyberspace: A Comparative Perspective, Computer and Telecommunications Law Review, 2007,, page 245 et seq; *Scassa/Currie*, New First Principles? Assessing the Internet's Challenges to Jurisdiction, Georgetown Journal of International Law, Vol. 42, 2001, page 117 et seq, available at: http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF; United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm; *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at:

www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf; *Van Dervort*, International Law and Organizations: An Introduction, 1998; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

1.4.6 مقدمة

إن الجريمة السيبرانية جريمة نمطية عابرة للحدود تضم ولايات قضائية مختلفة. ومن الطبيعي أن تتأثر بها عدة بلدان. وقد يتصرف الجاني من البلد A، باستخدام خدمة للإنترنت في البلد B في حين يكون الضحية في البلد C. ويشكل هذا تحدياً في مجال تطبيق القانون الجنائي[2127] ويؤدي إلى طرح أسئلة عن البلد الذي لديه الولاية القضائية والبلد الذي ينبغي أن يبدأ بالتحقيق وما هي طريقة تسوية النزاعات. وفي حين تبدو هذه المسألة مليئة بالتحديات بالفعل، فإن من الضروري مراعاة أنه إذا دخلت في الجريمة، على سبيل المثال، خدمات الحوسبة السحابية فقد يصل الأمر إلى شمول عدد أكبر من الولايات القضائية.[2128]

ويُستخدم مصطلح "الولاية القضائية" لوصف أمور قانونية مختلفة ومتنوعة.[2129] وبالاستناد إلى مبادئ القانون الدولي العام، تصف "الولاية القضائية" سلطة دولة ذات سيادة بشأن تنظيم سلوك معين.[2130] وهي بالتالي أحد جوانب السيادة الوطنية.[2131] لكن في إطار التحقيق المتعلق بالجريمة السيبرانية، تشير "الولاية القضائية" إلى سلطة دولة من أجل إنفاذ قانونها المحلي.[2132] وعموما، سيكون بإمكان وكالات إنفاذ القانون إجراء تحقيق فقط إذا كان لدى البلد الولاية القضائية.

2.4.6 المبادئ المختلفة للولاية القضائية

من الممكن التمييز بين المبادئ المختلفة من الولاية القضائية.

3.4.6 مبدأ الإقليمية/مبدأ الإقليمية الموضوعية

يتمثل المبدأ الأساسي الأهم والأساس الأكثر شيوعاً للولاية القضائية في مبدأ الإقليمية.[2133] ويطبق هذا المبدأ إذا ارتكبت جريمة داخل إقليم دولة ذات سيادة،[2134] بغض النظر عن جنسية الجاني أو الضحية. وتتضح أهمية هذا المبدأ من كون الولاية القضائية لا تفيد عموماً إلا إذا أمكن إنفاذها وإذا تطلب إنفاذ القانون المراقبة (المقتصرة عموماً على الإقليم). وأحد نهج تدوين مبادئ الإقليمية الخاصة بالحاسوب هو المادة 22(1)*أ)* من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

> **المادة 22 – الولاية القضائية**
>
> *1 يعتمد كل طرف تشريعات وغيرها من التدابير على النحو اللازم لتحديد الولاية القضائية بشأن أي جريمة محددة وفقاً للمواد من 2 إلى 11 من هذه الاتفاقية، عندما ترتكب الجريمة:*
>
> *أ) في إقليم الطرف؛*
>
> *ب) أو على متن سفينة عليها علم ذلك الطرف؛*
>
> *ج) أو على متن طائرة مسجلة بموجب قوانين ذلك الطرف؛*
>
> *د) أو على يد مواطن من مواطنيه، إذا كانت الجريمة جريمة يعاقب عليها بموجب القانون الجنائي للمكان الذي ارتكبت فيه أو إذا ارتُكبت الجريمة خارج الولاية القضائية الإقليمية لأي دولة.*
>
> *[...]*

ويخص هذا الحكم بالتحديد الحاسوب بما أنه يشير إلى الجرائم المذكورة في المواد من 2 إلى 11 من اتفاقية الجريمة السيبرانية.

بيد أن التطبيق فيما يخص قضايا الجريمة السيبرانية يسير جنباً إلى جنب مع التحديات. وترتكب جريمة بالتأكيد إذا كان الجاني والضحية حاضرين جسدياً في البلد عندما ينفذ الجاني بطريقة غير مشروعة إلى نظام الضحية الحاسوبي. لكن هل تكون الجريمة قد ارتُكبت داخل إقليم دولة إذا تصرف الجاني من الخارج عند نفاذه إلى نظام الضحية الحاسوبي في البلد؟

وتشمل هذه القضايا عنصراً خارجاً عن الإقليم. بيد أن محاكم العدل الدولية أعربت في قضية "لوتوس" (Lotus) أنه حتى في القضايا التي تطبق فيه البلدان الولاية القضائية فقط على أساس الإقليمية، يجوز مع ذلك اعتبار التصرف الذي يُرتكب خارج الإقليم كما لو أنه ارتُكب في الإقليم إذا وقع عنصر من العناصر المكونة للجريمة (لا سيما أثرها) في البلد.[2135] وإن هذا المذهب، الذي يُشار إليه أيضاً "بمبدأ الإقليمية الموضوعية"[2136]، ملائم للغاية في قضايا الجريمة السيبرانية.[2137] لكن مع الأخذ في الاعتبار إمكانية تضرر نظم حاسوبية في بلدان مختلفة ببرمجية خبيثة أرسلها أحد الجناة، تؤكد أن هذا التعريف الواسع للإقليمية يقود بسهولة إلى نزاعات محتملة بشأن الولايات القضائية.[2138] وتزداد مخاطر حدوث نزاعات محتملة أكثر في حالة تطبيق مبدأ الإقليمية على قضايا لا يكون فيها الجاني ولا الضحية داخل البلد لكن فقط البنية التحتية الموجودة في البلد هي التي استخدمت في ارتكاب الجريمة، ومثال ذلك إرسال بريد إلكتروني فيه محتوى غير قانوني باستخدام مورِّد خدمة البريد الإلكتروني في بلد ما أو تخزين موقع شبكي فيه محتويات غير قانونية في مخدم للمورِّد المستضيف في البلد.

وهناك تدوين لهذا النهج الواسع في الفقرة 11 (3) (ب) من قانون سنغافورة المتعلق بسوء استخدام الحاسوب لعام 2007.

النطاق الإقليمي للجرائم المرتكبة في إطار هذا القانون

[...]

11- (1) رهناً بأحكام الفقرة الفرعية (2)، تكون أحكام هذا القانون نافذة، بشأن أي شخص، أياً كانت جنسيته أو كان وطنه، خارج وداخل سنغافورة.

(2) عندما ترتكب جريمة يغطيها هذا القانون على يد أي شخص في أي مكان خارج سنغافورة، يجوز التعامل معه كما لو ارتكبت الجريمة داخل سنغافورة.

(3) لأغراض هذا الفصل، يطبق هذا القانون، فيما يخص الجريمة المعنية، إذا –

أ) كان المتهم في سنغافورة في وقت الواقعة؛

ب) أو إذا كان الحاسوب أو البرنامج أو البيانات في سنغافورة في وقت الواقعة.

ومن المحتمل جداً أن يؤدي هذا النهج الواسع إلى قابلية لتطبيق تشريعات سنغافورة فيما يخص البيانات المرسلة فقط من خلال الأنظمة الحاسوبية في سنغافورة.[2139]

4.4.6 المبدأ الرئيسي

يرتبط المبدأ الرئيسي ارتباطاً وثيقاً بمبدأ السيادة الإقليمية ولكنه يوسع نطاق تطبيق القوانين المحلية لتطول الطائرات والسفن. ومع الأخذ في الاعتبار، أن تيسر حلول النفاذ إلى الإنترنت في خدمات النقل البحري والجوي[2140] أفرز مسائل تتعلق بتطبيق القانون الجنائي على قضايا لا تتواجد فيها الأنظمة الحاسوبية المعتدية والمعتدى عليها داخل الأراضي ولكن خارج الحدود على متن سفينة أو طائرة.

ومن أمثلة النهج المستعملة لتنظيم هذه الحالات المادة 22 (1) ب) وج) من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

المادة 22 – الولاية القضائية

1 يعتمد كل طرف التدابير التشريعية وغيرها من التدابير التي قد تكون ضرورية لبسط الولاية القضائية على أي جريمة ترتكب طبقاً للمواد من 2 إلى 11 من هذه الاتفاقية، عندما ترتكب:

أ) داخل أراضيه؛

ب) أو على متن سفينة ترفع علم هذا الطرف؛

ج) أو على متن طائرة مسجلة طبقاً لقوانين هذا الطرف؛

د) أو يرتكبها أحد مواطني هذا الطرف، إذا كانت من الجرائم التي يعاقب عليها طبقاً للقانون الجنائي في البلد الذي وقعت فيه أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة.

[...]

5.4.6 مذهب التأثيرات/مبدأ وقائي

يتناول مذهب التأثيرات بسط الولاية القضائية في الجرائم التي يرتكبها أجانب وتقع خارج الحدود الإقليمية بكاملها دون وقوع أي عنصر داخل الحدود الإقليمية غير أن تأثيرها يظل كبيراً داخل الحدود الإقليمية.[2141] ويرتبط بذلك ارتباطاً وثيقاً بالمبدأ الوثائق الذي يبسط الولاية القضائية في قضايا مماثلة عندما تبرز مصلحة وطنية أساسية. ونتيجة لغياب الجاني والمجني عليه والبنية التحتية المستخدمة، لا تكون هناك إلا علاقات ضعيفة ببلد ما وتطبيق المبدأ يصبح مثيراً للجدل.[2142]

6.4.6 مبدأ الجنسية الفاعلة

يشير مبدأ الجنسية إلى الولاية القضائية المطبقة على الأنشطة التي يقوم بها المواطنون خارج الوطن.[2143] وهي تتعلق بسلطة الدولة في تنظيم سلوك مواطنيها ليس فقط داخل أراضيها ولكن في الخارج أيضاً. وهذا المبدأ أكثر شيوعاً في البلدان ذات القوانين المدنية من تلك ذات القوانين العامة.[2144] ونتيجةً لذلك تميل البلدان ذات القوانين العامة إلى تعويض النقص في التشريعات على أساس مبدأ الجنسية بتأويل أكثر اتساعاً لمبدأ الإقليمية.

وبالنسبة لحقيقة أن الجرائم المتعلقة بالإنترنت يمكن ارتكابها دون مغادرة البلد، فإن هذا المبدأ يكون أقل ارتباطاً عندما يتصل الأمر بقضايا الجريمة السيبرانية، ومع ذلك، يمكن أن تكون أكثر ارتباطاً في سياق إنتاج المواد التي يستغل فيها الأطفال جنسياً لأغراض توزيعها عبر الشبكات الحاسوبية.[2145]

ومن أمثلة النهج المستخدمة في تنظيم مبدأ الجنسية، المادة 22 (1) د) من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية.

المادة 22 – الولاية القضائية

1 يعتمد كل طرف التدابير التشريعية وغيرها من التدابير التي قد تكون ضرورية لبسط الولاية القضائية على أي جريمة ترتكب طبقاً للمواد من 2 إلى 11 من هذه الاتفاقية، عندما ترتكب:

أ) داخل أراضيه؛

ب) أو على متن سفينة ترفع علم هذا الطرف؛

ج) أو على متن طائرة مسجلة طبقاً لقوانين هذا الطرف؛

د) أو يرتكبها أحد مواطني هذا الطرف، إذا كانت من الجرائم التي يعاقب عليها طبقاً للقانون الجنائي في البلد الذي وقعت فيه أو إذا ارتكبت الجريمة خارج الولاية الإقليمية لأي دولة.

[...]

7.4.6 مبدأ الجنسية المنفعلة

يشير مبدأ الجنسية المنفعلة إلى الولاية القضائية القائمة على جنسية الضحية. ومع مراعاة التداخل مع مبدأ الإقليمية، فهو يكون ذا صلة فقط عندما يصبح مواطن ضحية لجريمة عندما يكون خارج البلاد. ويخضع تطبيق المبدأ لمناقشات جدلية – [2146] لا سيما لكونه يضم القانون الأجنبي بعدم الكفاية لحماية الأجانب – غير أنه اكتسب المزيد من القبول في العقود الأخيرة.[2147]

ومن أمثلة تقنين هذا المبدأ – في حالات لا تتعلق بالإنترنت – القسم 7 من قانون العقوبات الألماني.

المادة 7

الجرائم المرتبكة خارج البلاد – حالات أخرى

(1) يطبق القانون الجنائي الألماني على الجرائم التي ترتكب خارج البلاد ضد أي ألماني، إذا كان الجرم عملاً جنائياً في مكان ارتكابه أو إذا كان مكان الجريمة لا يخضع لأي تشريعات جنائية.

8.4.6 مبدأ العالمية

يؤسس مبدأ العالمية ولاية قضائية لبعض الجرائم التي تهم المجتمع الدولي.[2148] ويتعلق هذا المبدأ على نحو خاص بجرائم خطيرة مثل الجرائم ضد الإنسانية وجرائم الحرب.[2149] ومع ذلك، فإن كثير من البلدان التي تعترف بالمبدأ أدخلت عليه المزيد من التطوير.[2150] ونتيجة لذلك، أصبح المبدأ، في ظل ظروف معينة قابلاً للتطبيق حتى على الجريمة السيبرانية.

ومن أمثلة الأحكام التي يمكن تطبيقها على قضايا الجريمة السيبرانية، القسم 6 (6) من قانون العقوبات الألماني.

المادة 6

الجرائم المرتكبة خارج البلاد ضد مصالح قانونية محمية دولياً

يطبق القانون الجنائي الألماني أيضاً على الجرائم التالية المرتكبة خارج البلاد، بغض النظر عن مكان وقوعها:

1 (ملغى)؛

2 الجرائم التي تشمل الطاقة النووية والمتفجرات والإشعاع طبقاً للقسم 307 والأقسام 308 (1) إلى (4) والقسم 309 (2) والقسم 310؛

3 الهجمات على الحركة الجوية والبحرية (القسم 316 ج)؛

4 الاتجار بالبشر لأغراض الاستغلال الجنسي ولأغراض الاستغلال في العمل والمساعدة على الاتجار بالبشر (الأقسام من 232 إلى 233 أ))؛

5 التداول غير القانوني للمخدرات؛

6 توزيع المواد التي يستغل فيها الأطفال جنسياً المحددة في الأقسام 184 أ) و184 ب) (1) إلى (3) والأقسام 184 ج) (1) إلى (3) وكذلك بالاقتران مع العبارة الأولى بالقسم 184 د).

[...]

وطبقاً للقسم 6 (6) يمكن لألمانيا أن تمارس ولاية قضائية على مواقع الإنترنت الإلكترونية التي توفر المواد التي يستغل فيها الأطفال جنسياً لتحميلها حتى لو لم يكن مشغل الموقع الإلكتروني مقيماً في ألمانيا، أو كانت المخدمات غير موجودة في ألمانيا وحتى إن لم يدخل على الموقع أي من مستعملي الإنترنت في ألمانيا.

5.6 القانون الإجرائي

Bibliography (selected): ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1; *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801; *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*; *Gercke/Tropina*, From Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf; *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery,

Richmond Journal of Law & Technology, 2004, Vol. X, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1.

1.5.6 مقدمة

كما يتضح من الأقسام الواردة أعلاه تتطلَّب مكافحة الجريمة السيبرانية وجود أحكام كافية في القانون الجنائي الموضوعي.[2151] 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.[2152] فالقيام بتحقيقات يتطلب منها– بالإضافة إلى التدريب والمعدات – الاضطلاع بأدوات إجرائية تمكِّنها من اتخاذ التدابير اللازمة لتعيين الجاني وجمع الأدلة المطلوبة لإقامة الدعاوى الجنائية.[2153] 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 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.[2154]

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.[2155] فإذا كان مقر الجاني في بلد مختلف،[2156] 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.[2157]

وقد وضعت بعض البلدان بالفعل أدوات جديدة تمكِّن وكالات إنفاذ القوانين من التحقيق في الجرائم السيبرانية، وكذلك الجرائم التقليدية التي تتطلب تحليل البيانات الحاسوبية.[2158] وكما حدث في حالة القانون الجنائي الموضوعي تتضمن الاتفاقية المتعلقة بالجريمة السيبرانية التي وضعها مجلس أوروبا مجموعة من الأحكام التي تعبِّر عن المعايير الدنيا المقبولة قبولاً واسعاً في شأن الأدوات الإجرائية المطلوبة للتحقيقات في الجرائم السيبرانية.[2159] 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.

2.5.6 التحقيقات المتصلة بالحاسوب والإنترنت (التحليل الجنائي الحاسوبي)

يستعمل مصطلح "التحليل الجنائي الحاسوبي" في وصف التجميع النظامي للبيانات وتحليلها في تكنولوجيا الحاسوب بغرض التوصل إلى أدلة رقمية[2160]. ويتم هذا التحليل عادة بعد ارتكاب الجريمة[2161]. وبالتالي فهو جزء رئيسي في التحريات المتصلة بجرائم الحاسوب والجريمة السيبرانية. ويواجه المحققون الذي يقومون بهذه التحريات تحديات عديدة، يرد شرحها في الفصل 3.

ويُثبت مدى المشاركة المحتملة من جانب خبراء التحليل الجنائي الحاسوبي أهمية هذا التحليل في عملية التحقيق. وبالإضافة إلى ذلك، فإن توقف نجاح تحقيقات الإنترنت على توفر موارد التحليل الجنائي يبرز ضرورة التدريب في هذا المجال. ولا يمكن إجراء تحقيق فعال وملاحقة فعالة في الجريمة السيبرانية إلا إذا كان المحققون حاصلين على تدريب في مجال التحليل الجنائي الحاسوبي أو يستطيعون الاستفادة من الخبراء في هذا المجال.

التعريف

هناك تعاريف مختلفة لمصطلح "التحليل الجنائي الحاسوبي".[2162] إذ يمكن تعريف هذا المصطلح بأنه يعني "فحص معدات وأنظمة تكنولوجيا المعلومات من أجل الحصول على معلومات لأغراض التحقيقات الجنائية والمدنية".[2163] فالجناة يتركون آثاراً تدل عليهم أثناء ارتكابهم جرائمهم.[2164] 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.[2165] ويتطلب هذا التحليل. بالإضافة إلى أدوات إجرائية كافية، قدرة السلطات على إدارة وتحليل البيانات ذات الصلة. وتختلف المتطلبات المتعلقة بأداة التحقيق الإجرائي وتصاحب تقنيات التحقيق الجنائي الحاسوبي[2166] تحديات فريدة[2167] حسب الجرائم المرتكبة والتكنولوجيا الحاسوبية المستخدمة.

مراحل التحقيقات الجنائية الحاسوبية

يمكن عادة التفريق بين مرحلتين رئيستين:[2168] مرحلة التحقيق (تحديد الأدلة ذات الصلة[2169] وجمعها وحفظها[2170] وتحليل تكنولوجيا الحاسوب والأدلة الرقمية)، وعرض واستعمال الأدلة في إجراءات المحاكمة. ومن أجل شرح الأنشطة المختلفة، يوسع الفصل التالي النموذج إلى أربع مراحل.

إجراءات تحديد الأدلة

تؤدي الزيادة في سعة الأقراص الصلبة[2171] وانخفاض تكلفة[2172] تخزين الوثائق الرقمية مقارنة بالوثائق المادية إلى زيادة مطردة في أعداد الوثائق الرقمية[2173]. ومع الحاجة إلى تركيز التحريات على الأدلة ذات الصلة لتفادي عدم قبول الدعوى، يجب إيلاء عناية خاصة بتحديد الأدلة[2174]. وبناء على ذلك، يقوم خبراء التحليلات القضائية بدور هام في وضع استراتيجيات التحريات واختيار الأدلة ذات الصلة. فبوسعهم، على سبيل المثال، تحديد موقع الأدلة المطلوبة في أنظمة التخزين الضخمة. ويتيح ذلك للمحققين حصر نطاق التحريات في أجزاء البنية التحتية الحاسوبية ذات الصلة بالتحريات وتفادي التحفظ على ما لا يلزم أو على كم كبير من العتاد الحاسوبي[2175]. وترتبط عملية الاختيار هذه بمدى تنوع أجهزة التخزين المتاحة مما يجعل من عملية تحديد موقع تخزين الأدلة ذات الصلة عملية مرهقة[2176]. وينطبق ذلك بشكل خاص إذا كان المشتبه فيه لا يخزن المعلومات محلياً، بل يستعمل وسائل التخزين عن بُعد. وقد أثر تيسر النفاذ عريض النطاق ومخدمات التخزين عن بُعد على أسلوب تخزين المعلومات. فإذا كان المشتبه فيه يخزن المعلومات على مخدم موجود في بلد آخر، فإن عملاً بسيطاً كهذا يمكن أن يصعب كثيراً من الحصول على الأدلة. ويمكن في هذه الحالة استعمال التحليلات القضائية الحاسوبية لتحديد ما إذا كان قد تم استعمال خدمات تخزين عن بُعد[2177]. ولا ينحصر تحديد المعلومات الرقمية ذات الصلة في الملفات في حد ذاتها. فقواعد بيانات أدوات البرمجيات التي توفرها أنظمة التشغيل لتحديد الملفات بسرعة يمكنها أن تتضمن هي الأخرى معلومات ذلة صلة[2178]. حتى الملفات التي يولدها النظام مؤقتاً ربما تحتوي هى الأخرى على أدلة لأعمال إجرامية[2179].

ومن الأمثلة الأخرى لتحديد الأدلة، مشاركة خبراء التحليلات القضائية الحاسوبية في تحديد الصكوك الإجرائية السليمة. فهناك عدد من البلدان يمكن وكالات إنفاذ القانون من إجراء نوعين من أنواع المراقبة في الوقت الفعلي. وعملية اعتراض بيانات المحتوى بوجه عام تتسم بقدر أكبر من الاقتحام مقارنة بعملية جمع بيانات الحركة. ويمكن لخبراء التحليلات القضائية الحاسوبية تحديد ما إذا كان جمع بيانات الحركة كافياً لإثبات ارتكاب الجريمة ومن ثم مساعدة المحققين في تحقيق التوازن المطلوب بين الحاجة إلى التوصل إلى الدليل القوي والالتزام بحماية حقوق المشتبه فيه باختيار أقل الوسائل صرامة من بين خيارات متساوية في الأثر. ويبين المثالان أن دور المحققين القضائيين الحاسوبيين لا يقتصر على الجوانب التقنية في التحقيق، بل يمتد ليشمل مسؤولية حماية الحقوق الأساسية للمشتبه فيهم وبالتالي تفادي عدم قبول الأدلة المتحصل عليها في الدعوى[2180].

جمع الأدلة وحفظها

يتطلب العمل في جمع الأدلة الرقمية مهارات متقدمة نظراً إلى أن التقنيات المستعملة في جمع أدلة مخزنة في القرص الصلب لحاسوب منزلي والتقنيات المستخدمة في اعتراض عملية إرسال البيانات تختلف اختلافاً كبيراً. وعندما يتعلق الأمر بشكل خاص بجناة على مستوى عال من الحرفية، يواجه المحققون عادة مواقف تتطلب قرارات سريعة. ومن الأمثلة على ذلك، هل ينبغي إبطال نظام حاسوبي في وضع تشغيل أم لا، وكيف يمكن القيام بهذا الإجراء. ولتفادي الإخلال بسلامة الأدلة الرقمية المطلوبة، هناك توجيه عام يتمثل في فصل مصدر الطاقة الكهربائية، مما يمنع تعديل الملفات[2181]. بيد أن هذا الفصل للطاقة الكهربائية

يمكن أن ينشط التجفير[2182] ومن ثم يحول دون النفاذ إلى البيانات المخزنة[2183]. ويتحمل المحققون الأوائل الذين يقومون بالخطوات الأولى في جمع الأدلة الرقمية مسؤولية كبيرة تجاه عملية التحقيق بأكملها حيث إن أي قرار خاطئ قد يكون له أثر خطير على القدرة على حفظ الأدلة المطلوبة[2184]. فإذا اتخذ هؤلاء قرارات غير سليمة بشأن الحفظ، يمكن فقد خيوط هامة.

ويتعين على خبراء التحقيقات القضائية الحاسوبية التأكد من تحديد كافة الأدلة المطلوبة[2185]. وقد يتعذر ذلك إذا أخفى الجناة الملفات في جهاز تخزين لمنع وكالات إنفاذ القانون من تحليل محتويات الملفات. ويمكن للتحقيقات القضائية الحاسوبية أن تحدد الملفات المخفاة والنفاذ إليها[2186]. ويحتاج الأمر إلى عمليات استعادة مماثلة إذا ما تم حذف المعلومات الرقمية[2187]. فالملفات التي يتم حذفها بمجرد نقلها إلى سلة المهملات الافتراضية لا يمكن بالضرورة اعتبارها غير متاحة لوكالات إنفاذ القانون حيث يمكن استعادتها باستعمال أدوات برمجيات خاصة بالأدلة الحاسوبية[2188]. بيد أنه إذا كان الجناة يستعملون أدوات لضمان حذف الملفات بصورة آمنة عن طريق تحرير معلومات جديدة على المعلومات المخزنة، فإن الاستعادة في هذه الحالة تكون مستحيلة بوجه عام[2189]. ويمكن لعملية جمع الأدلة أن تواجه تحديات إذا ما حاول الجناة منع النفاذ إلى المعلومات المطلوبة باستعمال تكولوجيا التجفير، التي يتزايد استعمالها بصورة مطردة.[2190] وحيث إن هذا الأمر يحول دون نفاذ وكالات إنفاذ القانون إلى المعلومات المجفرة وفحصها، فإن استعمال تكنولوجيات التجفير ينطوي على تحديات كبيرة بالنسبة إلى وكالات إنفاذ القانون.[2191] ويمكن لخبراء التحقيقات القضائية الحاسوبية محاولة فك تجفير الملفات المجفرة[2192]. وإذا تعذر ذلك، يمكنهم دعم وكالات إنفاذ القانون في وضع استراتيجيات للحصول على نفاذ إلى الملفات المجفرة، باستعمال أدوات رصد لوحة المفاتيح مثلاً[2193].

ويشمل العمل في جمع الأدلة تقييم الأدوات الجديدة وتنفيذها[2194]. ومن أمثلة النهج الجديدة، المناقشة بشأن أدوات التحقيقات القضائية الحاسوبية عن بُعد[2195]، أو مراقبة نشاط المشتبه فيه عن بُعد[2196] دون علم المشتبه فيه بالتحريات الجارية على نظامه. وإذا ما توفرت هذه الأداة، فإنها يمكن أن تقوم بدور في وضع استراتيجية لجمع الأدلة الرقمية.

الاتصال بموردي الخدمات

يقوم موردو خدمات الإنترنت (ISP) بدور هام في كثير من تحقيقات الجريمة السيبرانية، نظراً لاستخدام معظم المستعملين لخدماتهم من أجل النفاذ إلى الإنترنت أو من أجل تخزين مواقع الويب. وحقيقة أن موردي خدمات الإنترنت يملكون في بعض الحالات القدرات التقنية للكشف عن الجرائم ومنعها ودعم وكالات إنفاذ القانون في تحقيقاتها كان الحافز لمناقشة مكثفة بشأن دور موردي خدمات الإنترنت في تحقيقات الجريمة السيبرانية. وقد تراوحت الالتزامات التي نوقشت من التنفيذ الإجباري للتكنولوجيات الوقائية إلى الدعم الطوعي للتحقيقات[2197]. ويمكن لخبراء التحقيقات القضائية الحاسوبية أن يدعموا أيضاً أي تحقيق بإعداد الطلبات التي تقدم لموردي الخدمات[2198] ومساعدة المحققين في إعداد سجلات تاريخية وافية للقضايا[2199] التي تعد ضرورية لإثبات اعتمادية الأدلة المتوفرة. ويتطلب التعاون بين وكالات إنفاذ القانون وموردي خدمات الإنترنت في هذه التحقيقات تطبيق بعض الإجراءات[2200]. والمبادئ التوجيهية الصادرة عن مجلس أوروبا بشأن التعاون بين وكالات إنفاذ القانون وموردي خدمات الإنترنت[2201] تتضمن مجموعة من الإجراءات الضرورية من بينها أمور مثل تقديم تفسيرات ومساعدات بشأن تقنيات التحقيق[2202] وترتيب الأولويات[2203]

ومساعدة خبراء التحقيقات القضائية الحاسوبية قد تكون مفيدة في هذا الصدد لتحسين كفاءة الإجراءات والتعاون الوثيق مع موردي خدمات الإنترنت يكتسي بأهمية خاصة في تحديد المشتبه فيه. حيث يترك المشتبه في ارتكابهم جرائم سيبرانية في الغالب آثار تدل عليهم[2204]. وتحليل بيانات الحركة، مثل فحص ملفات التسجيل التي تحتفظ بها موردو خدمات الإنترنت يمكن أن تقود المحققين إلى التوصيل الذي استخدمه الجاني للدخول إلى الإنترنت[2205]. ويمكن للجناة محاولة إعاقة التحقيقات بالاستفادة من تكنولوجيا الاتصالات التي تغفل فيها الهوية[2206]. غير أنه حتى في هذه الحالة، لا تكون التحقيقات مستحيلة، إذا ما جرى تعاون وثيق بين المحققين وموردي خدمات الإنترنت[2207]. ومن الأمثلة على ذلك، أداة التحقيق القضائي الحاسوبي المسماة بالمتحقق من عنوان الحاسوب وبروتوكول الإنترنت (CIPAV) التي استعملت في الولايات المتحدة لتحديد مشتبه فيه كان

يستعمل خدمات الاتصالات التي تغفل فيها الهوية[2208]. ومن المثلة الأخرى للتعاون بين موردي خدمات الإنترنت والمحققين تحري البريد الإلكتروني. فقد أصبح البريد الإلكتروني وسيلة من وسائل الاتصالات واسعة الانتشار[2209]. ولمنع التعرف عليهم، يستعمل الجناة في بعض الأوقات عناوين عامة للبريد الإلكتروني تمكنهم من التسجيل باستعمال معلومات شخصية زائفة. بيد أنه حتى في هذه الحالة، يمكن تحديد المشتبه فيه بفحص معلومات الرأسية[2210] وملفات سجلات مورد خدمة البريد الإلكتروني.

ولا تقتصر الحاجة إلى التعاون والتواصل مع الموردين على موردي خدمات الإنترنت. حيث إنه نتيجة إلى أن بعض الجرائم مثل الاحتيال[2211] والتوزيع التجاري للمواد التي يستغل فيها الأطفال جنسياً تتضمن معاملات مالية، فإن من بين استراتيجيات تحديد الجناة الحصول على بيانات من المؤسسات المالية المشاركة في المعاملات[2212]. ومن أمثلة ذلك، تحقيق جرى في ألمانيا حيث تم تحديد الجناة الذين قاموا بتحميل مواد يستغل فيها الأطفال جنسياً من موقع إلكتروني تجاري بواسطة سجلات بطاقة الائتمان. وبطلب من المحققين، قامت شركات بطاقات الائتمان بتحليل سجلات العملاء لتحديد العملاء الذين قاموا باستعمال بطاقاتهم لشراء مواد يستغل فيها الأطفال جنسياً من موقع إلكتروني محدد[2213]. وتكون هذه التحقيقات أصعب في حالة استعمال وسائل الدفع التي تغفل فيها الهوية[2214].

فحص تكنولوجيا المعلومات والاتصالات

تتمثل الخطوة الأولى في معظم التحقيقات في إثبات أن الجاني لديه القدرة على ارتكاب الجريمة. ومن بين المهام الرئيسية لخبراء التحليلات القضائية الحاسوبية، فحص العتاد والبرمجيات المتحفظ عليها[2215]. ويمكن إجراء الفحص أثناء البحث في منشآت المشتبه به[2216] أو بعد التحفظ على هذه الأشياء. وللقيام بذلك، يقوم المحققون الأوائل عادة بالتحفظ على جميع أجهزة التخزين المطلوبة – حيث يمكن أن يحمل كل منها ملايين الملفات وهو ما يفرض في الغالب تحدياً لوجستياً[2217]. وكما ورد آنفاً، فإن مبادئ الارتباط والفعالية تكتسي بأهمية كبيرة بقبول الأدلة الرقمية[2218]. ومن ثم، فإن تحديد العتاد المطلوب واختياره يعد من المهام الرئيسية في أي تحقيق[2219].

ويمكن من خلال تحليل لمكونات العتاد المتاحة إثبات، على سبيل المثال، أن حاسوب المشتبه به قادر على تنفيذ إحدى هجمات رفض الخدمة[2220]، أو مزود برقاقة تمنع التلاعب بنظام التشغيل. وقد يكون تحليل العتاد ضرورياً كذلك في تحديد المشتبه به. وتقوم بعض أنظمة التشغيل بتحليل تشكيلة عتاد أي حاسوب أثناء عملية التثبيت وتقدم هذا التحليل إلى منتج البرمجيات. إذا تسنى الكشف عن مواصفة عتاد المشتبه به استناداً إلى معلومات من شركة البرمجيات، يمكن لتحليل العتاد أن يساعد في التحقق من أن نظام الحاسوب المتحفظ عليه يفي بالغرض. ولا يعني تحليل العتاد بالضرورة التركيز على المكونات المادية الملحقة بالنظام الحاسوبي حيث تحتفظ معظم أنظمة التشغيل بسجلات للعتاد الملحق بنظام حاسوبي أثناء اي عملية تشغيل[2221]. وعلى أساس الملفات المدرجة في ملفات السجلات مثل سجل ويندوز، يمكن للمحللين القضائيين الحاسوبيين حتى، تحديد العتاد الذي استعمل في الماضي وغير الموجود أثناء إجراءات البحث والتحفظ.

وإلى جانب تحليل العتاد، فإن تحليل البرمجيات من الأعمال الاعتيادية في تحقيقات الجريمة السيبرانية. والبرمجيات الحاسوبية ضرورية لتشغيل أي نظام حاسوبي. فإلى جانب أنظمة التشغيل، يمكن تثبيت أدوات برمجيات أخرى لإدارة وظائف أنظمة الحاسوب حسب احتياجات المستعمل. ويمكن لخبراء التحليلات القضائية الحاسوبية تحليل أداء أدوات البرمجيات لوظائفها من أجل إثبات أن المشتبه به قادر على ارتكاب على ارتكاب جريمة محددة. ويمكنهم، على سبيل المثال، التحقق مما إذا كان النظام الحاسوبي للمشتبه به يتضمن برمجية تسمح بتجفير البيانات في الصور (تقنية إخفاء المعلومات[2222]). ويمكن لقائمة للأدوات البرمجية المثبتة على حاسوب المشتبه به أن تساعد أيضاً في حذف الملفات بصورة مؤمنة، يمكنهم البحث تحديداً عن دليل مشفر أو محذوف[2223]. ويمكنهم أيضاً تحديد وظائف الفيروسات الحاسوبية أو أي أشكال أخرى من البرمجيات الضارة وإعادة بناء عمليات تشغيل البرمجيات[2224]. وفي بعض الحالات التي يتم فيها العثور على محتويات غير قانونية على حواسيب المشتبه بهم، أو على المشتبه بهم أنهم لم يقوموا بتحميل الملفات ولكنها حملت بواسطة فيروس حاسوبي. ويمكن للمحققين في هذه الحالات محاولة تحديد البرمجيات الضارة المثبتة في النظام الحاسوبي وتحديد وظائفها. ويمكن إجراء تحليلات مشابهة إذا كان من الجائز أن

يكون نظام الحاسوب قد تعرض للإصابة بفيروس ما وأصبح جزءاً من برمجية روبوتية[2225]. ويمكن لتحليل البرمجيات أن يكون مهماً لتحديد ما إذا كانت البرمجية قد انتجت خصيصاً لارتكاب جرائم أم يمكن استعمالها في أغراض شرعية وقانونية (استعمال مزدوج). وهذا التمييز قد يكون هاماً، طالما هناك بعض البلدان التي تقصر تجريم إنتاج الأجهزة غير الشرعية على الأجهزة المصممة فقط أو في الأساس لارتكاب جرائم[2226].

ولا تقتصر التحقيقات المتعلقة بالبيانات على وظائف البرمجيات، بل تشمل أيضاً، إجراء تحليل للملفات ذات الطابع غير التقليدي مثل الوثائق بالنسق PDF أو ملفات الفيديو. وتتراوح هذه التحليلات بين تحليل المحتوى لبعض الملفات والبحث الأوتوماتي بكلمات رئيسية[2227] لملفات النصوص والبحث بالصور للصور المعروفة في حاسوب المشتبه به[2228]. ويشمل تحليل الملفات أيضاً فحص الوثائق الرقمية التي ربما تكون زُيفت[2229] إلى جانب تحليل البيانات الشرحية[2230]. ويمكن لهذا التحليل أن يحدد آخر توقيت[2231] فتحت فيه الوثيقة أو عُدلت[2232]. كما يمكن اللجوء إلى تحليل البيانات الشرحية لتحديد مؤلف الملف الذي يحتوي على رسالة تهديد أو الرقم التسلسلي لآلة التصوير التي استعملت في إنتاج صورة مستغل فيها الأطفال جنسياً. ويمكن تحديد المؤلفين أيضاً استناداً إلى تحليل لغوي يمكن أن يساعد في تحديد ما إذا كان المشتبه به في كتب مقالات من قبل وترك معلومات يمكن أن تساعد في التعرف عليه في هذا السياق[2233].

التتبُّع والإبلاغ

من أبرز التحديات المتعلقة بالأدلة الرقمية أنها هشة للغاية ويمكن حذفها بسهولة[2234] أو تعديلها[2235]. وكما ورد آنفاً، من بين تبعات هشاشة الأدلة الرقمية ضرورة الحفاظ على سلامتها[2236]. ومن ثم يتعين وجود سجلات للحالات. ومشاركة خبراء مؤهلين[2237] لوضع سجلات الحالات تعد من نهج الحفاظ على سلامة الأدلة التي يمكن لخبراء التحليلات القضائية الحاسوبية المشاركة فيها[2238]. غير أن لهؤلاء الخبراء دور أيضاً عندما يتعذر التحفظ على العتاد أو عندما يكون غير كاف. وفي هذه الحالات، تسمح بعض البلدان للمحققين بنسخ الملفات. ومن ثم يتعين إيلاء عناية خاصة لحماية الملفات المنسوخة من أي شكل من أشكال التعديل أثناء عملية النسخ[2239].

عرض الأدلة في المحكمة

تتمثل المرحلة النهائية للتحقيق بوجه عام في عرض الأدلة في المحكمة. ففي حين يقوم بعرض الأدلة في المحكمة عادة إما ممثلو الادعاء أو محامو الدفاع، يمكن لخبراء التحليلات القضائية الحاسوبية القيام بدور هام في الإجراءات الجنائية كخبراء شهود يمكنهم مساعدة الأشخاص المشاركين في إجراءات المحاكمة على فهم عمليات استنباط الأدلة[2240]. ونظراً لتعقد الأدلة الرقمية، تتزايد أهمية إشراك خبراء التحليلات القضائية الحاسوبية، وهو ما يؤدي إلى اعتماد القضاة والمحلفين والمدعين والمحامين على إفادات هؤلاء الخبراء[2241].

عمليات فحص الأدلة الجنائية

على الرغم من أن الأدلة الجنائية الحاسوبية تتعامل بدرجة كبيرة مع العتاد الحاسوبي ومع البيانات الحاسوبية، فإنه لا توجد ضرورة عادة لأتمتتها، حيث تظل الأدلة الجنائية الحاسوبية عملاً يدوياً[2242] إلى حد كبير. وينطبق هذا الأمر على نحو خاص بالنسبة لوضع الاستراتيجيات والبحث عن أدلة محتملة خلال إجراءات البحث والتحفظ. والوقت اللازم لهذه العمليات اليدوية وقدرة الجناة على أتمتة هجماتهم تفرض تحديات تواجهها وكالات إنفاذ القوانين، خاصة في التحقيقات التي تشمل عدداً كبيراً من المشتبه بهم وكميات كبيرة من البيانات[2243]. ومع ذلك، هناك بعض العمليات مثل البحث عن الكلمات الرئيسية للمشتبه بهم أو استعادة الملفات المحذوفة، يمكن أتمتتها باستخدام أدوات خاصة لتحليل الأدلة الجنائية الحاسوبية[2244].

3.5.6 الضمانات

أبرزت وكالات إنفاذ القانون في أنحاء العالم خلال السنوات القليلة الماضية الحاجة الماسة لوجود أدوات كافية لإجراء التحقيقات.[2245] ومع وضع ذلك في الاعتبار فقد يكون من المدهِش أن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية

تعرضت للنقد في صدد الأدوات الإجرائية.[2246] ويركّز النقد أساساً على جانب أن الاتفاقية المتعلقة بالجريمة السيبرانية تتضمن عدداً من الأحكام لإثبات أدوات التحقيق (المواد من 16 إلى 21) ولكنها تتضمن حكماً واحداً فقط (المادة 15) يتناول الضمانات.[2247] وبالإضافة إلى ذلك، يمكن أن يلاحَظ أنه بعكس أحكام القانون الجنائي الموضوعي في الاتفاقية المتعلقة بالجريمة السيبرانية لا توجد سوى احتمالات قليلة جداً لإدخال تعديلات وطنية في تطبيق الاتفاقية.[2248] ويركّز النقد لذلك على الجوانب الكمّية أساساً. ومن الصحيح أن الاتفاقية المتعلقة بالجريمة السيبرانية 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.

وكانت اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية قد صُمِّمت منذ بدايتها لتكون إطاراً وصكّاً دوليين لمكافحة الجريمة السيبرانية دون أن يقتصر ذلك فقط على البلدان الأعضاء في مجلس أوروبا.[2249] وأثناء التفاوض على الأدوات الإجرائية اللازمة أدرك واضعو الاتفاقية، المتعلقة بالجريمة السيبرانية 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.[2250] ولذلك قرّر واضعو الاتفاقية المتعلقة بالجريمة السيبرانية عدم إدراج قواعد تنظيمية محدّدة في نصّ الاتفاقية والاكتفاء بدلاً من ذلك بمطالبة الدول الأعضاء بكفالة تطبيق المعايير الوطنية والدولية الأساسية للضمانات.[2251]

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 تتضمن 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 تطبّق 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.[2252] 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 المتعلقة بالجريمة السيبرانية 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،[2253] فإن اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تعرِّف المعايير الدنيا بإشارتها إلى الأُطر الأساسية مثل: 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.

ونظراً لأن الاتفاقية المتعلقة بالجريمة السيبرانية يمكن أن تكون مفتوحة للتوقيع والتصديق من جانب بلدان ليست أعضاء في مجلس أوروبا،[2254] فمن المهم التأكيد على أن تقييم أنظمة الضمانات في الدول الموقّعة غير الأعضاء في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية 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 اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية 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 إلا وفقاً 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.[2255] ويراعي قانون السوابق القضائية بالتحديد خطورة التدخل في التحقيق[2256]، وغرضه[2257] وتناسبه.[2258] والمبادئ الأساسية التي يمكن استخراجها من قانون السوابق القضائية هي: ضرورة وجود أساس قانوني كافٍ لأدوات التحقيق،[2259] ويجب أن يكون الأساس القانوني واضحاً بشأن الموضوع،[2260] ويتعيَّن أن تكون اختصاصات وكالات إنفاذ القانون معروفة سلفاً،[2261] لا يمكن تبرير مراقبة الاتصالات إلا في سياق الجرائم الخطيرة.[2262]

وبالإضافة إلى ما سبق، فإن المادة 15 من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تأخذ في الاعتبار مبدأ التناسب.[2263] 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 اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية صراحة إلى بعض أهم الضمانات[2264]، بما فيها الإشراف، ومبررات التطبيق، وتقييد الإجراء فيما يتعلق بالنطاق والمدة.

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 ضرورياً.[2265]

وهناك جانب هام يتصل بنظام الضمانات المنصوص عليه في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، 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 المتعلقة بالجريمة السيبرانية 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 اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تمكِّن الأطراف من مواصلة صياغة نظام للضمانات المتدرجة. وتشمل هذه الأمثلة ما يلي: التمييز بين اعتراض بيانات المحتوى

(المادة 21)[2266] وجمع بيانات الحركة (المادة 20)[2267]. وعلى العكس من جمع بيانات الحركة، يقتصر اعتراض بيانات المحتوى على الجرائم الخطيرة.[2268] والتمييز بين الأمر العاجل بحفظ بيانات الحاسوب المخزونة (المادة 16)[2269] وتقديم بيانات الحاسوب التي تم الاحتفاظ بها استناداً إلى أمر الإبراز (المادة 18)[2270] فالمادة 16 تمكِّن وكالات إنفاذ القانون فقط من إصدار أوامر حفظ البيانات دون الكشف عنها.[2271] وفي النهاية، التمييز بين الالتزام بتقديم "معلومات المشترِك"[2272] و"بيانات الحاسوب"[2273] في المادة 18.[2274]

وإذا تم تقييم شدة أداة التحقيق والأثر المحتمل على المشتبه فيه تقييماً صحيحاً وصُمِّمت الضمانات بحيث تتماشى مع نتائج التحليل، فإن نظام الضمانات المتدرجة لن يؤدّي إلى اختلال نظام الأدوات الإجرائية.

4.5.6 الحفظ العاجل لبيانات الحاسوب المخزونة والإفصاح عنها (إجراء التجميد السريع)

في كثير من الأحيان يتطلب تعيين الجاني الذي ارتكب جريمة إلكترونية تحليلاً لبيانات الحركة.[2275] ويمكن أن يساعد عنوان بروتوكول إنترنت الذي استعمله الجاني، بوجه خاص، 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.[2276]

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 تولَّدت أثناء العملية والتي تمكّن من إجراء العملية. ومن منظور اقتصادي يهتم معظم مقدمي الإنترنت بحذف المعلومات بأسرع ما يمكن نظراً لأن تخزينها لفترات طويلة يتطلب سعة تخزينية كبيرة جداً ومكلِّفة.[2277]

ومع ذلك، فإن الجوانب الاقتصادية لا تشكِّل 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.[2278]

المادة 6 – بيانات الحركة

1 يجب مسح بيانات الحركة المتصلة بالمشتركين والمستعملين التي يعالجها ويخزنها مقدِّم شبكة اتصالات عمومية أو خدمة اتصالات إلكترونية متوفِّرة 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 يمثِّل 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 من 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[2279]، وهما استبقاء البيانات، وحفظ البيانات ("إجراء التجميد السريع").

ويفرض التزام استبقاء البيانات على مقدِّم خدمات الإنترنت حفظ بيانات الحركة لفترة معيَّنة من الوقت[2280] ويتعيَّن في أحدث النُهج التشريعية إبقاء السجلات لمدة تصل إلى 24 شهراً.[2281] ويمكِّن ذلك وكالات إنفاذ القانون من النفاذ إلى البيانات اللازمة لتحديد الجاني حتى بعد ارتكابها بشهور عديدة.[2282] وقد اعتمد البرلمان الأوروبي مؤخراً التزام استبقاء

البيانات[2283] ويجري مناقشة هذا الالتزام أيضاً في الولايات المتحدة في الوقت الحاضر.[2284] وفيما يتعلق بمبادئ استبقاء البيانات، يمكن الاطلاع أدناه على مزيد من المعلومات.

الاتفاقية المتعلقة بالجريمة السيبرانية

حفظ البيانات نهج مختلف لكفالة عدم فشل التحقيق في الجريمة السيبرانية لا لسبب سوى حذف بيانات الحركة أثناء إجراءات التحقيق الطويلة.[2285] 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.[2286] وقرَّر واضعو اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية التركيز على "التحفظ على البيانات" بدلاً من "استبقاء البيانات".[2287] ويمكن الاطلاع على القاعدة التنظيمية في المادة 16 من الاتفاقية المتعلقة بالجريمة السيبرانية.

المادة 16 – سرعة الحفاظ على بيانات الحاسوب المخزونة

1 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك حتى يمكن لسلطاتها المختصة الأمر أو طلب العمل بصورة عاجلة على حفظ بيانات بعينها على حاسوب، بما في ذلك خط سير البيانات المخزَّنة بواسطة نظام حاسوبي، وخاصة في حالة وجود أُسس للاعتقاد بإمكانية تعرُّض بيانات حاسوبية بصفة خاصة للفقد أو التعديل.

2 في حالة قيام طرف بتفعيل الفقرة 1 أعلاه بواسطة إصدار أمر إلى شخص ما بحفظ بيانات حاسوبية 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 ويحافظ على سلامة بيانات الحاسوب 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 يحفظ بيانات حاسوبية، 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.

ومن منظور مقدِّم خدمة الإنترنت، يعتبر حفظ البيانات أداة أقل تقييداً مقارنة باستبقاء البيانات.[2288] 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 طالما أنه 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 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.[2289] 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.[2290] 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 اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. ومزايا فصل التزام حفظ البيانات والتزام الإفصاح عنها هو أنه من المحتمل اقتضاء شروط مختلفة لتطبيقهما.[2291] وفيما يتعلق بأهمية التصرف الفوري، سيكون من المفيد مثلاً التنازل عن اقتضاء صدور أمر من القاضي وتمكين الادعاء أو الشرطة من إصدار أمر الحفظ.[2292] وسيمكِّن ذلك السلطات المختصة من التصرف بسرعة أكبر. ويمكن أن تتحقَّق حماية حقوق المشتبه فيهم باقتضاء صدور أمر للإفصاح عن البيانات.[2293]

والإفصاح عن البيانات المحتفظ بها هو جانب من الجوانب التي تنظمها المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية:

> ***المادة 18 – أوامر الإفصاح***
>
> *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 الحاسوب بحوزة ذلك الشخص أو تحت سيطرته، ومخزَّنة داخل نظام الحاسوب 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 حاسوبية 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 التقنية التي يتم اتخاذها في ذلك والفترة الزمنية للخدمة؛*
>
> *ب) هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم الهاتف 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 تتوفر بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.*

واستناداً إلى الفقرة الفرعية 1*أ)* من المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، يمكن إلزام مقدمي الخدمة الذين قاموا بحفظ البيانات بالإفصاح عنها.

والمادة 18 من الاتفاقية المتعلقة بالجريمة السيبرانية لا تنطبق فقط بعد إصدار أمر حفظ عملاً بالمادة 16 من الاتفاقية المتعلقة.[2294] وهذا الحكم هو أداة عامة تستطيع وكالات إنفاذ القانون أن تستعملها. وإذا قام متلقي الأمر الإبراز طوعاً بنقل البيانات المطلوبة، فإن دور وكالات إنفاذ القانون لا يقتصر على ضبط العتاد ولكنها تستطيع تطبيق أمر الإبراز الأقل تقييداً. ومقارنة بضبط العتاد فعلاً، فإن أمر تقديم المعلومات ذات الصلة هو أقل تقييداً بصورة عامة. لذلك كان تطبيقه هاماً بصفة خاصة في الحالات التي لا تتطلَّب فيها التحقيقات الجنائية النفاذ إلى العتاد.

وبالإضافة إلى الالتزام بتقديم بيانات الحاسوب تمكِّن المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية 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[2295] الذي استعمل عنوان بروتوكول إنترنت في وقت ارتكاب الجريمة. واستناداً إلى الفقرة 1 *ب)* من المادة 18 من الاتفاقية المتعلقة بالجريمة السيبرانية، يكون مقدِّم الخدمة ملزماً بتقديم معلومات المشترك المذكورة في الفقرة الفرعية 3 من المادة 18.[2296]

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 – الحفظ العاجل لبيانات الحركة والكشف الجزئي لها

1 يعتمد كل طرف، بالنسبة لبيانات الحركة المطلوب حفظها بموجب المادة 16، ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك:

أ) لضمان إمكانية سرعة حفظ بيانات الحركة 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 بيانات الحركة 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 المتعلقة بالجريمة السيبرانية فصلاً صارماً بين التزام حفظ البيانات بناءً على الطلب والتزام الإفصاح عنها للسلطات المختصة.[2297] 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 مسير الإرسال. وبدون هذا الإفصاح الجزئي لن تتمكَّن وكالات إنفاذ القانون في بعض الحالات من تعقُّب الجاني في حالة وجود أكثر من مقدِّم خدمة.[2298] ونظراً لتجمع الالتزامين اللذين يؤثران على حقوق المشتبه فيهم بطرق أخرى، فمن الضروري مناقشة نقطة تركيز الضمانات المتصلة بهذه الأداة.

قانون الكومنولث النموذجي المتعلق بالجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نُهج مشابهة في قانون الكومنولث النموذجي لعام 2002.[2299]

الحكم

تقديم البيانات

15 إذا اقتنع قاضي تحقيق استناداً إلى طلب مقدِّم من ضابط شرطة بأن بيانات حاسوبية محدَّدة، أو مطبوعة منها أو أي معلومات أخرى، مطلوبة بصورة معقولة لأغراض تحقيق جنائي أو دعوى جنائية يجوز للقاضي أن يأمر:

أ) شخصاً في إقليم [البلد الذي سن القانون] يسيطر على نظام حاسوبي أن يقدِّم من النظام بيانات حاسوبية محدَّدة أو مطبوعة أو غير ذلك من النواتج المفهومة الأخرى من تلك البيانات؛

ب) ومقدِّم خدمة إنترنت في [البلد الذي سن القانون] أن يقدِّم معلومات عن الأشخاص الذين يشتركون في الخدمة أو يستعملونها بشكل آخر؛ و

ج)[2300] وأي 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.

الكشف عن بيانات الحركة المخزنة

16[2301] 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.

حفظ البيانات

17 (1) إذا اقتنع ضابط شرطة بأن:

أ) البيانات المخزونة في نظام حاسوبي 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.

5.5.6 استبقاء البيانات

يفرض التزام استبقاء البيانات على مقدِّم خدمات الإنترنت الاحتفاظ ببيانات الحركة لفترة معيَّنة من الوقت.[2302] 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[2303] الذي أُعلن بطلانه في عام 2014.[2304]

المادة 3 – الالتزام باستبقاء 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؛

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 أثارت تغطية هذا التوجيه للمعلومات الرئيسية عن أي اتصال عن طريق الإنترنت نقداً حاداً من منظمات حقوق الإنسان.[2305] ويمكن أن يؤدّي ذلك بدوره إلى قيام المحاكم الدستورية بإعادة النظر في هذا التوجيه وتطبيقه.[2306] 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،[2307] إلى أنه من المشكوك فيه أن يمكن تطبيق التزام استبقاء البيانات بدون انتهاك الحقوق الأساسية.[2308] وقد سبقت الإشارة إلى الصعوبات في صدد تطبيق هذه القواعد التنظيمية في مجموعة الثمانية في 2001.[2309]

ولكن النقد لا ينصبّ على هذا الجانب وحده. فهناك سبب آخر يجعل استبقاء البيانات أقل فاعلية في مكافحة الجريمة السيبرانية وهو إمكانية الالتفاف حول الالتزامات. وتشمل أسهل الطرق للالتفاف حول التزام استبقاء البيانات، استعمال معدات طرفية عامة مختلفة للإنترنت أو خدمات البيانات الهاتفية المتنقلة المدفوعة سلفاً التي لا تتطلب أي تسجيل،[2310] واستعمال خدمات اتصال مجهولة الهوية يتم تشغيلها (جزئياً على الأقل) في بلدان لا تطبّق نظام استبقاء البيانات.[2311]

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.[2312]

وبالإضافة إلى ذلك، يستطيع الجناة الالتفاف حول التزام استبقاء البيانات باستعمال مقدمات اتصالات مجهولة الهوية.[2313] 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.[2314]

ونظراً للسهولة 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[2315] أو حظر استعمال تكنولوجيا الاتصالات مجهولة الهوية.[2316]

في عام 2014، أعلنت محكمة العدل الأوروبية أخيراً بطلان التوجيه.[2317] وبناءً على رأي المحكمة فإنه يفضي إلى تدخل واسع النطاق وخطير بشكل خاص في الحقوق الأساسية في احترام الحياة الخاصة وحماية البيانات الشخصية، دون أن يقتصر ذلك التدخل على ما هو ضروري قطعاً. ونتيجة لذلك لم تعد الدول الأعضاء مرتبطة بالتوجيه. والقوانين الوطنية التي نفذت وفقاً للتوجيه ليست باطلة تلقائياً. ومن غير المؤكد حالياً ما إذا كان الاتحاد الأوروبي سوف يقدم ويعتمد توجيهاً جديداً.

6.5.6 التفتيش والمصادرة

رغم أن أدوات التحقيق الجديدة مثل جمع بيانات المحتوى في الوقت الفعلي واستعمال برمجيات التحليل الجنائي عن بُعد لتعيين الجاني لا تزال موضع المناقشة ورغم تطبيقها بالفعل في بعض البلدان، يظل التفتيش والمصادرة يمثلان دائماً أداة من أهم أدوات التحقيق.[2318] وبمجرد تعيين الجاني وقيام وكالة إنفاذ القانون بمصادرة معداته الخاصة بتكنولوجيا المعلومات يستطيع خبراء التحليل الجنائي الحاسوبي تحليل الجهاز لجمع الأدلة اللازمة للادعاء.[2319]

وتجري في الوقت الحاضر مناقشة إمكانية استبدال أو تعديل إجراء التفتيش والمصادرة في بعض البلدان الأوروبية وفي الولايات المتحدة.[2320] وهناك أسلوب لتجنُّب ضرورة دخول مسكن المتهم تفتيشه وضبط جهازه الحاسوبي، وهذه الإمكانية هي إجراء التفتيش على الخط إلكترونياً.[2321] وتصف هذه الأداة، والتي 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.[2322] ورغم أن وكالات إنفاذ القانون تستطيع بوضوح أن تستفيد من عدم إدراك المتهم لوجود تحقيقات، فإن النفاذ المادي إلى العتاد يمكِّن من تطبيق تقنيات تحقيقيه أكثر كفاءة. ويبرز ذلك الدور الهام لإجراءات التفتيش والمصادرة في إطار تحقيقات الإنترنت.

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تتضمن معظم قوانين الإجراءات الجنائية الوطنية أحكاماً تمكِّن وكالات إنفاذ القانون من التفتيش وضبط الأشياء.[2323] والسبب في أن واضعي اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية قاموا رغم ذلك بإدراج أحكام تتناول التفتيش والمصادرة هو أن القوانين الوطنية لا تغطي في كثير من الأحيان إجراءات التفتيش والمصادرة المتصلة بالبيانات[2324]. إذ إن بعض البلدان، على سبيل المثال، تقصر تطبيق إجراءات[2325] المصادرة على الأشياء المادية. 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 والمصادرة التقليدية المطبَّقة على البنود الملموسة، وذلك عندما لا تعرف وكالات إنفاذ القانون الموقع المادي للمخدِّم ولكنها تستطيع الوصول إليه عن طريق الإنترنت.[2326] والمادة 19، شأنها شأن الأحكام الإجرائية الأخرى التي تنص عليها الاتفاقية المتعلقة بالجريمة السيبرانية، لا تحدد الشروط والمتطلبات التي يتعين على المحققين الالتزام بها لإجراء هذه التحقيقات.[2327] والحكم نفسه لا ينص على ضرورة وجود أمر من المحكمة ولا يحدد الظروف التي يُستثنى فيها شرط الحصول على أمر المحكمة ومع الأخذ في الاعتبار عملية التعدّي على الحريات والحقوق المدنية للمشتبه بهم والتي تستوجبها إجراءات التفتيش والمصادرة، فإن معظم البلدان تقيّد تطبيق هذا الصك[2328].

وتهدف الفقرة الفرعية 1 من المادة 19 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية إلى إقامة أداة تمكِّن من تفتيش الأنظمة الحاسوبية وتعادل في كفاءتها إجراءات التفتيش التقليدية.[2329]

> ***المادة 19 – تفتيش ومصادرة بيانات الحاسوب 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 حاسوبي 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 والمصادرة هو أداة يستعملها المحققون بصورة متكررة، فهناك عدد من التحديات التي تقترن بتطبيقها في التحقيقات في الجرائم السيبرانية.[2330] وتتمثَّل إحدى الصعوبات الأساسية في أن أوامر التفتيش تقتصر في كثير من الأحيان على أماكن بعينها (مثل مسكن المشتبه فيه).[2331] 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.[2332] ويتزايد إقبال مستعملي الإنترنت على مخدمات الإنترنت من أجل تخزين البيانات وتجهيزها

("الحوسبة السحابية"). 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.[2333] وتعالج اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية هذه القضية في الفقرة الفرعية 2 من المادة 19.

المادة 19 – تفتيش ومصادرة بيانات الحاسوب 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 حاسوب بعينه أو على جزء منه، وفقاً للفقرة 1 أ)، وقيام أسباب لديها للاعتقاد بأن البيانات المطلوبة مخزَّنة داخل نظام حاسوب 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 والمصادرة في صدد البيانات الحاسوبية المخزونة.[2334] ولا تقتصر الأدوات اللازمة على نسخ البيانات ذات الصلة.[2335] 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.[2336] وإذا لم يكن المحققون يملكون تصريحاً باتخاذ التدابير اللازمة لكفالة سلامة البيانات المنسوخة، فإن البيانات المنسوخة قد لا تكون مقبولة كدليل في الإجراءات الجنائية.[2337] 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 المصادرة، فإن المعلومات تظل في العتاد عموماً ولن يتمكَّن المحققون في التحقيقات المتصلة بالمحتوى غير القانوني خاصة[2338] (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.[2339] وتعالج اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية هذه القضايا المذكورة أعلاه في الفقرة الفرعية 3 من المادة 19.

المادة 19 – تفتيش ومصادرة بيانات الحاسوب المخزَّنة

[...]

3 يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لمنح سلطاته المختصة صلاحية ضبط أو تأمين بيانات الحاسوب التي يتم الدخول عليها طبقاً للفقرتين 1 أو 2، وتشمل هذه الإجراءات صلاحية:

أ) ضبط أو تأمين نظام الحاسوب أو جزء منه أو وسيط تخزين البيانات؛

ب) عمل نسخة من هذه البيانات الحاسوبية والاحتفاظ بها؛

ج) المحافظة على تجانس بيانات الحاسوب المخزَّنة ذات الصلة؛

د) جعل هذه البيانات الحاسوبية غير قابلة للدخول عليها أو إزالتها على نظام الحاسوب 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 كثير من الأحيان التعجيل بالتحقيقات السريعة.[2340] وفي هذه الحالات، تفرض التحقيقات صعوبات فريدة طالما كان لها بُعد دولي يتطلب تعاوناً دولياً في التحقيقات.[2341] 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.[2342] ولكن حتى إذا تمكنوا من تعيين المحرك الصلب المحدَّد، فإن تدابير الحماية قد تمنعهم من البحث عن البيانات ذات الصلة. وقرَّر واضعو المتعلقة بالجريمة السيبرانية 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 والمصادرة. ففي كثير من البلدان لا ترغم أوامر التفتيش والمصادرة الأشخاص المتأثرين بالتحقيق إلا على تحمُّل الإجراءات - ولا يتعيَّن عليهم دعم التحقيق دعماً نشطاً. وفيما يتعلق بأي شخص يملك معرفة خاصة مطلوبة للتحقيق، فإن تطبيق اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية 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.[2343] ولا تحدِّد الاتفاقية المتعلقة بالجريمة السيبرانية 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"*.[2344]

> ***المادة 19 – تفتيش ومصادرة بيانات الحاسوب 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 الحاسوب 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.[2345]

> ***تعاريف لهذا الجزء***
>
> ***11*** *في هذا الجزء:*
>
> *[...]*
>
> *تشمل "المصادرة":*
>
> *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.

[...]

مسوغات البحث والمصادرة

12[2346] (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.

[...]

مساعدة الشرطة

13[2347] (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؛

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.

7.5.6 أمر الإبراز

حتى إذا كان القانون الوطني لا يطبِّق التزاماً مثل الالتزام الوارد في الفقرة الفرعية 4 من المادة 19 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، 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 والمصادرة، فمن المرجح أنهم سيحتاجون في هذه الحالة إلى ضبط عتاد أكثر من اللازم بالفعل. ولذلك سيعمد مقدمو الخدمة عموماً إلى دعم التحقيقات وتقديم البيانات اللازمة عندما تطلبها وكالات إنفاذ القانون. وتتضمن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية أدوات تسمح للمحققين بالعمل بدون أوامر التفتيش إذا قدَّم الشخص الذي يملك البيانات ذات الصلة هذه البيانات إلى المحققين.[2348]

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 يتمثل في إمكانية انتهاك مقدمي الخدمة التزاماتهم التعاقدية مع عملائهم إذا اتبعوا طلب تقديم بعض البيانات دون أن يكون الطلب مستنداً إلى أساس قانوني كافٍ.[2349]

المادة 18 – أمر الإبراز

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 الحاسوب بحوزة ذلك الشخص أو تحت سيطرته، ومخزَّنة داخل نظام الحاسوب 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.

وتتضمن المادة 18 التزامين اثنين. فالفقرة الفرعية 1*أ)* من المادة 18 تُلزم 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.[2350] 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 المتعلقة بالجريمة السيبرانية في التقرير التفسيري إلى أن مجرَّد وجود القدرة التقنية على الوصول عن بُعد إلى البيانات المخزَّنة لا يشكِّل سيطرة بالضرورة.[2351] ولذلك يقتصر تطبيق المادة 18 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية على الحالات التي تتجاوز فيها درجة سيطرة الشخص المشتبه فيه الإمكانية المحتملة للنفاذ إلى البيانات.

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.[2352] وفي معظم الحالات لا يقود عنوان بروتوكول إنترنت إلا إلى مقدِّم خدمة الإنترنت الذي قدَّم عنوان بروتوكول إنترنت إلى المستعمل. وقبل أن يمكن استعمال أي خدمة يلزم مقدمو خدمة الإنترنت المستعمل عادة بأن يسجِّل معلومات المشترك الخاصة به.[2353] وتتيح الفقرة الفرعية 1 *ب)* من المادة 18 للمحققين مطالبة مقدم الخدمة بتقديم معلومات المشترك هذه. وفي هذا السياق يكون من المهم أن نبرز أن المادة 18 من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية لا تفرض مع ذلك التزام استبقاء البيانات[2354] ولا التزام مقدِّمي الخدمة بتسجيل معلومات المشترك.[2355]

ولا يبدو أن التمييز بين "البيانات الحاسوبية" في الفقرة الفرعية 1*أ)* و"معلومات المشترك" في الفقرة الفرعية 1 *ب)* للوهلة الأولى ضرورياً مادامت 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 اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية السلطات القانونية المختصة من تقديم معلومات محفوظة في شكل غير رقمي.[2356]

المادة 1 – تعاريف

لأغراض هذه الاتفاقية:

[...]

ب) يُقصد "ببيانات الحاسوب" أية عمليات عرض للحقائق أو المعلومات أو المفاهيم في قالب مناسب لعملية معالجة داخل نظام حاسوبي، بما في ذلك برنامج مناسب لجعل نظام الحاسوب يؤدي وظائفه؛

المادة 18 – أمر الإبراز

[...]

3 لغرض هذه المادة – فإن مصطلح "معلومات المشترك" يعني أية معلومات في صورة بيانات حاسوبية أو أي صورة أخرى يتم حفظها من جانب مقدِّم الخدمة، والتي تتعلَّق بالمشتركين في الخدمات الخاصة به بخلاف حركة 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 الهاتف 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 تتوفر 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.[2357] إذ يمكن مثلاً فرض متطلبات أكثر صرامة[2358] فيما يتعلق بأمر إبراز طبقاً للفقرة الفرعية 1 ب)، نظراً لأن هذه الأدوات تسمح لوكالات إنفاذ القانون بالنفاذ إلى أي نوع من البيانات الحاسوبية بما فيها بيانات المحتوى.[2359] والتفريق بين جمع بيانات الحركة في الوقت الحقيقي (المادة 20)[2360] وجمع بيانات المحتوى في الوقت الحقيقي (المادة 21)[2361] يوضِّح أن واضعي الاتفاقية المتعلقة بالجريمة السيبرانية أدركوا أن وكالات إنفاذ القانون تستطيع النفاذ إلى مختلف الضمانات التي يتعيَّن تنفيذها حسب نوع البيانات.[2362] وبهذا التفريق بين "البيانات الحاسوبية" و"معلومات المشترك" تمكِّن المادة 18 من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية الدول الموقَّعة من إقامة نظام مشابه للضمانات المتدرجة بشأن أمر الإبراز.[2363]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في قانون الكومنولث النموذجي لعام 2002.[2364]

إعداد البيانات

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)[2365] 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.

8.5.6 جمع البيانات في الوقت الفعلي

المراقبة الهاتفية أداة تستعمل في التحقيقات في الجرائم الكبرى في كثير من البلدان.[2366] 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.[2367]

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).[2368] 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.[2369]

ونظراً لأن كثيراً من الجرائم الحاسوبية ينطوي على تبادل بيانات، فإن القدرة على اعتراض هذه العمليات أيضاً 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[2370] وكذلك بقضايا قانونية. ومن وجهة النظر القانونية لا يشمل التصريح بتسجيل المكالمات الهاتفية بالضرورة تصريحاً باعتراض عمليات نقل البيانات.

وتهدف اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية إلى سد الثغرات القائمة في قدرة وكالات إنفاذ القانون على رصد عمليات نقل البيانات.[2371] وفي إطار هذا النهج تميِّز الاتفاقية المتعلقة بالجريمة السيبرانية بين مجموعتين من مراقبة نقل البيانات. فالمادة 20 تصرِّح للمحققين بجمع بيانات الحركة. وتعرِّف الفقرة د) من المادة 1 من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية "بيانات الحركة".

المادة 1 – تعاريف

[...]

د) يُقصد بـ"بيانات الحركة" أي بيانات حاسوبية متعلقة باتصال عن طريق نظام حاسوبي وتنشأ عن نظام حاسوبي 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.[2372]

9.5.6 جمع بيانات الحركة

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

ومع الأخذ في الاعتبار أن تعريف بيانات الحركة يختلف من بلد لآخر،[2373] قرَّر واضعو اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية 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 شركاء الاتصال في أي اتصال عن طريق الإنترنت.[2374]

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 يمكِّن وكالات إنفاذ القانون من تحليل الاتصال بطريقة أكثر فعالية، فإن بيانات الحركة تؤدي دوراً هاماً في تحقيقات الجرائم السيبرانية.[2375] وفي حين أن النفاذ إلى بيانات المحتوى يمكِّن 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 تمكِّن المحققين من تعيين صفحة الويب التي يقوم الجاني فيها بتحميل صور أطفال فاضحة. ومن خلال رصد بيانات الحركة المتولِّدة أثناء استعمال خدمات الإنترنت تستطيع وكالات إنفاذ القانون من تعيين عنوان بروتوكول إنترنت للمخدِّم وتحاول بعد ذلك أن تحدِّد الموقع المادي.

المادة 20 – تجميع بيانات الحركة في الوقت الفعلي

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 التقنية، في إقليم ذلك الطرف؛

ب) وإجبار مقدِّم الخدمة، في نطاق قدرته التقنية على:

'1' جمع أو تسجيل، من خلال تطبيق الوسائل التقنية في إقليم ذلك الطرف؛

'2' أو التعاون مع السلطات المختصة ومساعدتها في جمع أو تسجيل، في الوقت الفعلي، بيانات الحركة المرتبطة باتصالات معيَّنة في إقليم ذلك الطرف التي تم نقلها بواسطة نظام الحاسوب.

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 في الوقت الفعلي بيانات المرتبطة باتصالات معيَّنة تم نقلها في إقليمه، من خلال تطبيق الوسائل التقنية 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.[2376]

النهج الأول هو فرض التزام على 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.[2377]

النهج الثاني هو تمكين وكالات إنفاذ القانون من إرغام مقدِّم خدمة الإنترنت على تجميع البيانات بناءً على طلبهم. ويمكِّن 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.[2378]

وقد وضعت اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية بدون تفضيل لأي تكنولوجيا محدَّدة وبدون أن تهدف إلى وضع معايير تستدعي ضرورة الدخول في استثمارات مالية عالية من جانب قطاع الصناعة المعني.[2379] ومن هذا المنظور يبدو أن الفقرة الفرعية 1 *أ*) من المادة 20 من الاتفاقية المتعلقة بالجريمة السيبرانية تمثِّل الحل الأفضل. ولكن القاعدة التنظيمية في الفقرة الفرعية 2 من المادة 20 توضح أن واضعي الاتفاقية المتعلقة بالجريمة السيبرانية 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[2380] يستطيع الجناة استعمال خدمات في الإنترنت تمكِّن من القيام بالإرسال مجهول الهوية. وإذا كان الجاني يستعمل خدمة إرسال مجهول الهوية مثل برمجية TOR[2381] لحماية الحركة، فإن المحققين في معظم الحالات لا يستطيعون القيام بتحليل بيانات الحركة أو تعيين شركاء الاتصال بنجاح. ويستطيع الجاني أن يحقِّق نتيجة مشابهة من خلال استعمال المعدات الطرفية العامة للإنترنت.[2382]

ومقارنة بإجراءات التفتيش والمصادرة التقليدية يتمثَّل أحد مزايا جمع بيانات الحركة في أن الشخص الذي يشتبه في ارتكابه جريمة لا يدرك بالضرورة وجود تحقيق بشأنه.[2383] 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 سيعملون على بقاء المعرفة بالتحقيقات الجارية سرية. وبالنسبة لمقدم الخدمة يقترن ذلك بميزة إعفاء مقدِّم الخدمة من الالتزام[2384] بإبلاغ المستعملين.[2385]

وقد صُمِّمت اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية لتحسين وتنسيق التشريعات بشأن القضايا المتصلة بالجريمة السيبرانية.[2386] 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. نظراً لعدم 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. وتعطي الفقرة الفرعية 3 من المادة 14 الأطراف الحق في إبداء تحفظات بشأن الحكم وقصر تطبيقه على بعض الجرائم.[2387]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في قانون الكومنولث النموذجي لعام 2002.[2388]

اعتراض بيانات الحركة

19 (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.

10.5.6 اعتراض بيانات المحتوى

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

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.[2389] 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 التقنية، في إقليم ذلك الطرف؛

ب) وإجبار مقدِّم الخدمة، في نطاق قدرته الفنية على:

'1' جمع أو تسجيل، من خلال تطبيق الوسائل التقنية، في إقليم ذلك الطرف؛

'2' أو التعاون مع السلطات المختصة ومساعدتها في جمع أو تسجيل، في الوقت الفعلي، لمحتوى البيانات المرتبطة باتصالات معيَّنة في إقليم ذلك الطرف التي تم نقلها بواسطة نظام الحاسوب

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 في الوقت الفعلي لمحتوى البيانات المرتبطة باتصالات معيَّنة تم نقلها في إقليمه، من خلال تطبيق الوسائل التقنية 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.

وبعكس ما يحدث في حالة بيانات الحركة، لا تقدِّم اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية تعريفاً لبيانات المحتوى. وكما ينص المصطلح المستعمل صراحةً، 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 بواسطة بروتوكول إنترنت.

ويعتبر استعمال تكنولوجيا التجفير من أهم الصعوبات في التحقيقات استناداً إلى المادة 21.[2390] وكما اقترحنا بالتفصيل من قبل، يمكن أن تمكِّن تكنولوجيا التجفير الجناة من حماية المحتوى المتبادل بطريقة تجعل من المستحيل على وكالات إنفاذ القانون النفاذ إلى ذلك المحتوى. وإذا قام المجرم بتجفير المحتوى الذي ينقله، فإن وكالات إنفاذ القانون لا يتسنّى لها سوى اعتراض اتصال مشفَّر دون إمكانية تحليل المحتوى. وبدون النفاذ إلى المفتاح المستعمل في تجفير الملفات، فإن إمكانية إزالة التجفير قد تستغرق وقتاً طويلاً جداً.[2391]

قانون الكومنولث النموذجي للجرائم الحاسوبية والجرائم المتصلة بالحاسوب

يمكن الاطلاع على نهج مشابه في قانون الكومنولث النموذجي لعام 2002.[2392]

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.

11.5.6 التنظيم المتصل بتكنولوجيا التجفير

كما جاء أعلاه يستطيع الجناة عرقلة تحليل بيانات المحتوى باستعمال تكنولوجيا التجفير. وتتوافر منتجات برمجيات مختلفة تمكِّن المستعملين من توفير حماية فعَّالة للملفات ولعمليات نقل البيانات من تعرضها للنفاذ غير المأذون به.[2393] وإذا استعمل المشتبه فيهم هذه المنتجات ولم تتمكَّن سلطات التحقيق من النفاذ إلى المفتاح المستعمل لتجفير الملفات، فإن التجفير المطلوب قد يتطلب وقتاً طويلاً.[2394]

ويمثِّل استعمال الجناة لتكنولوجيا التجفير تحدياً لوكالات إنفاذ القانون.[2395] وهناك نُهج وطنية ودولية مختلفة[2396] لمعالجة المشكلة.[2397] وبسبب اختلاف التقديرات بشأن التهديد الناجم عن تكنولوجيا التجفير لا يوجد حتى الآن أي نهج دولي مقبول بصورة واسعة في معالجة هذا الموضوع.

وهناك نهج يتمثل في تخويل وكالات إنفاذ القانون فك التجفير إذا استلزم الأمر.[2398] وبدون هذا التخويل، 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 مجفَّر من أجل حل التجفير.[2399]

وهناك نهج آخر يتمثل في تحديد مدى أداء برمجية التجفير من خلال تقييد طول المفتاح.[2400] ويمكِّن ذلك، حسب درجة التقييد، المحققين من كسر المفاتيح في غضون فترة معقولة من الوقت. ويخشى معارضو هذا الحل أن التقييد لن يمكِّن المحققين فقط من كسر التجفير ولكنه يمكِّن أيضاً الجواسيس الاقتصاديين الذين يحاولون النفاذ إلى المعلومات التجارية المجفَّرة.[2401] وبالإضافة إلى ذلك، فإن هذا التقييد سيؤدي فقط إلى منع الجناة عن استعمال تجفير أقوى في حالة عدم توفُّر أدوات البرمجيات المذكورة. ويتطلب ذلك في البداية وضع معايير دولية لمنع منتجي منتجات التجفير القوية من عرض برمجياتهم في البلدان التي لا يوجد فيها تقييدات ملائمة بشأن طول المفتاح. وعلى أي حال يستطيع الجناة بسهولة نسبية صياغة برمجيات تجفير خاصة بهم بدون أي قيود على طول المفتاح.

والإلزام بإنشاء نظام لاستيداع المفاتيح أو وضع إجراء لاستعادة المفتاح في حالة منتجات التجفير القوية هو نهج آخر.[2402] وتنفيذ هذه القواعد التنفيذية يمكِّن المستعملين من الاستمرار في استعمال تكنولوجيا التجفير 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.[2403] ويخشى معارضو هذا الحل أن يتمكَّن الجناة من النفاذ إلى المفاتيح المقدَّمة ويستطيعون بها فك تجفير معلومات سرية. وبالإضافة إلى ذلك، يستطيع الجناة بسهولة نسبية الالتفاف على هذا التنظيم من خلال صياغة برمجية تجفير خاصة بهم لا تتطلَّب تقديم المفتاح إلى السلطة.

في النهاية تحاول البلدان مواجهة هذا التحدّي بتنفيذ.[2404] ويصف هذا المصطلح التزام الإفصاح عن المفتاح المستعمل لتجفير البيانات. وقد نوقش تطبيق هذه الأداة في إطار اجتماع الثمانية في عام 1997 في دنفر.[2405] وطبَّق عدد من البلدان هذا الالتزام.[2406] ومن أمثلة التطبيق الوطني المادة 69 من قانون تكنولوجيا المعلومات لعام 2000 في الهند.[2407] ومن أمثلة هذا الالتزام الأخرى المادة 49 من لائحة سلطات التحقيق لعام 2000 في المملكة المتحدة[2408]:

الإشعارات التي تتطلب الإفصاح

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؛

(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.

عدم الالتزام بالإشعار

53 (1) أي شخص وجّه إليه إشعار بموجب المادة 49 يكون مذنباً بجريمة إذا أحجم 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.[2409]

وهناك قلق عام من أن الالتزام يؤدي إلى احتمال التنازع مع الحقوق الأساسية للمتهم ضد تجريم الذات.[2410] 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 الذي يفرضه التجفير.[2411]

وهناك قلق آخر من أن فقد 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 التجفير في إجراءات جنائية غير مرغوبة. ومع ذلك، فإن الفقرة الفرعية 2 من المادة 53 على وجه الخصوص تنطوي على احتمال التداخل مع عبء الإثبات.[2412]

وفي النهاية هناك حلول تقنية تمكِّن الجناة من الالتفاف على الالتزام بالإفصاح عن المفتاح المستعمل في تجفير البيانات. ومن أمثلة التفاف الجاني حول الالتزام استعمال برمجية التجفير على أساس مبدأ "قدرة الإنكار المقبولة".[2413، 2414]

12.5.6 برمجية التحقيقات الجنائية 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 يستتبعه ضرورة النفاذ إلى شقة المشتبه فيه أو بيته أو مكتبه. وفي هذه الحالة يعرف

المشتبه فيه بوجود تحقيق بمجرد أن يبدأ المحققون في أعمال البحث.[2415] ويمكن أن تؤدي هذه المعلومات إلى تغيُّر في السلوك.[2416] 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.[2417] 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.[2418] 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".[2419] وفي عام 2007، نُشرت تقارير تقول بأن وكالات إنفاذ القانون في الولايات المتحدة تستعمل برمجية لتعقُّب المشتبه فيهم الذين يستعملون أدوات الاتصال مجهول الهوية.[2420] وكانت التقارير تشير إلى أمر تفتيش حيث كان استعمال أداة تسمى CIPAV (جهاز التحقق من الحاسوب وعنوان بروتوكول إنترنت)[2421] مطلوباً فيه.[2422] وبعد أن قرَّرت المحكمة الاتحادية في ألمانيا أن أحكام قانون الإجراءات الجنائية الموجودة لا تسمح للمحققين باستعمال برمجية التحليل الجنائي عن بُعد للقيام سراً بتفتيش حاسوب المشتبه فيه بدأت مناقشة بشأن ضرورة تعديل القوانين القائمة في هذا المجال.[2423] وفي سياق المناقشة نُشرت معلومات تقول بأن سلطات التحقيق قد استعملت بصورة غير قانونية برمجية التحليل الجنائي عن بُعد في اثنين من التحقيقات.[2424]

ونُوقشت مختلف مفاهيم "برمجية البحث عن الأدلة الجنائية عن بُعد" وخاصة وظائفها المحتملة.[2425] ويمكن أن تؤدي هذه البرمجية الوظيفتين التاليتين من منظور نظري، وظيفة يمكن أن تكون وظيفة التفتيش وتمكِّن هذه الوظيفة وكالات إنفاذ القانون من البحث عن المحتوى غير القانوني وجمع المعلومات عن الملفات المخزونة في الحاسوب.[2426] والوظيفة الأخرى هي التسجيل حيث 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 عبر بروتوكول الإنترنت للاتصال بالأشخاص الآخرين المشتبه فيهم فلن يتم عموماً تخزين محتوى المحادثة.[2427] ويمكن أن تسجل برمجية البحث عن الأدلة الجنائية عن بُعد البيانات المعالجة للاحتفاظ بها كي يستعملها المحققون. مسجِّل المفتاح وإذا كانت برمجية البحث عن الأدلة الجنائية عن بُعد تتضمن وحدة لتسجيل ضربات المفاتيح، فإن هذه الوحدة يمكن استعمالها لتسجيل كلمات المرور التي يستعملها الشخص المشتبه به في تجفير الملفات.[2428] وعلاوةً على ذلك، يمكن لأداة كهذه أن تتضمن وظائف تحديد الهوية التي تمكّن المحققين من إثبات مشاركة المشتبه به في جريمة جنائية حتى لو استعمل خدمات اتصال مجهولة الهوية لعرقلة المحققين في تعيين هوية الجاني وذلك بتعقُّب عنوان بروتوكول إنترنت المستعمل.[2429] وفي النهاية يمكن للبرمجية التي تعمل عن بُعد أن تُستعمل لتشغيل آلة تصوير للإنترنت (ويبكام) أو ميكروفون لأغراض مراقبة الغرفة.[2430]

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 الجنائي 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 التي يمكن بواسطتها إرسال البرمجة 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 طرق.[2431] وبصدد تدابير الحماية مثل التفتيش عن الفيروسات وحوائط النيران التي تجهَّز بها معظم الحواسيب، فإن جميع أساليب التركيب عن بُعد تطرح بصعوبات تواجه المحققين.[2432]

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 الجنائي عن بُعد ستمكِّن المحققين فقط من تحليل أنظمة حاسوبية موصولة بالإنترنت.[2433] ومن العسير، بالإضافة إلى ذلك، الحفاظ على سلامة النظام الحاسوبي للشخص المشتبه فيه عند العمل عند بُعد.[2434] وفي صدد هذه الجوانب لن تكون برمجية البحث عن الأدلة الجنائية عن بُعد قادرة عموماً على أن تحلّ محلّ 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 الجنائي 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.[2435] 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.

مثال

ثمة نهج يمكن الاطلاع عليه في النصوص التشريعية للدول المستفيدة ضمن مبادرة تنسيق سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR).[2436]

برمجية التحليل الجنائي

27 *(1) إذا ما اقتنع أحد [القضاة] [قضاة التحقيق] طبقاً [لمعلومات تم الحصول عليها بعد قسم شفوي/خطي] بأنه في أحد التحقيقات المتعلقة بجريمة من الجرائم المدرجة في الفقرة 7 أدناه، توجد أسباب معقولة للاعتقاد بأن الأدلة الضرورية سيتعذر جمعها بتطبيق الأدوات الأخرى المدرجة في الجزء الرابع وأنها مطلوبة لدرجة ما من أجل تحقيق جنائي، [يجوز] [يجب] أن يخول [القاضي] [قاضي التحقيق] بناء على طلب أحد ضباط الشرطة استخدام برمجية للتحليل الجنائي عن بُعد بالمهمة المحددة اللازمة للتحقيق وتركيب هذه البرمجية على النظام الحاسوبي للمشتبه به من أجل جمع الأدلة المطلوبة. ويتعين أن يشمل الطلب المعلومات التالية:*

أ) المشتبه بارتكابه الجريمة، إن أمكن مع الاسم والعنوان؛

ب) وصف للنظام الحاسوبي المستهدف؛

ج) وصف الإجراء المزمع ومداه وفترة استخدامه؛

د) أسباب ضرورة الاستخدام.

(2) من الضروري في تحقيق كهذا ضمان أن تقتصر التعديلات المدخلة على النظام الحاسوبي للمشتبه به على التعديلات الضرورية للتحقيق وأن أي تغييرات يمكن، قدر الإمكان، إلغاؤها بعد انتهاء التحقيق. ومن الضروري أن يسجل ما يلي أثناء التحقيق:

أ) الوسيلة التقنية المستعملة وتوقيت وتاريخ استعمالها؛

ب) تعريف النظام الحاسوبي وتفاصيل التعديلات المنفذة أثناء التحقيق؛

ج) أي معلومات متحصل عليها.

يتعين حماية المعلومات المتحصل عليها عبر هذه البرمجية ضد أي تعديلات أو حذف أو نفاذ من قبل غير المخولين.

(3) تحدد مدة التخويل الواردة في الفقرة 27 (1) [بثلاثة أشهر]. وإذا لم تستوف شروط التخويل في أي وقت، يكون الإجراء المتخذ، التوقف في الحال.

(4) التخويل بتركيب البرمجية يتضمن النفاذ عن بُعد إلى النظام الحاسوبي للمشتبه به.

(5) إذا تطلبت عملية التركيب الوجود المادي في مكان ما، يتعين الوفاء بمتطلبات الفقرة 20.

(6) إذا تطلب الأمر، يجوز لأحد ضباط [إنفاذ القانون] [الشرطة]، بموجب أمر المحكمة الممنوح في البند (1) أعلاه، أن يطلب أن تكلف المحكمة أي من موردي خدمات الإنترنت بدعم عملية التركيب.

(7) [قائمة الجرائم]

(8) يجوز لأي بلد أن يقرر عدم تطبيق الفقرة 27.

وأشار واضعو النص التشريعي إلى أنهم يدركون أن تطبيق هذه الأداة يمكن أن يكون اقتحامياً بشكل كبير وربما يتداخل مع الحقوق الأساسية للمشتبه به.[2437] وقد تم بالتالي تطبيق العديد من الإجراءات الوقائية. أولاً، يتطلب استعمال هذه البرمجية، استحالة جمع الأدلة عن طريق عمليات أخرى. ثانياً، يتعين وجود أمر من قاض أو قاضي تحقيق. ثالثاً، يجب أن يشمل الطلب أربعة عناصر رئيسية. كما تقتصر الإجراءات القانونية على الوارد في الفقرتين 1 و2.

13.5.6 اشتراط الإذن

يستطيع أن يتخذ الجناة تدابير لتعقيد التحقيقات. فبالإضافة إلى استعمال برمجيات تمكِّن من الاتصال مجهول الهوية[2438] 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 تساعد وكالات إنفاذ القانون في إجراء التحقيقات بكفاءة أكبر. ومن أمثلة نُهج تقييد استعمال المحطات الطرفية العمومية في ارتكاب مخالفات جنائية المادة 7[2439] من المرسوم الإيطالي رقم 144،[2440] الذي تم تحويله في عام 2005 ليصبح قانوناً (القانون رقم 155/2005).[2441] ويفرض هذا الحكم على أي شخص يعتزم تقديم نفاذ عمومي إلى الإنترنت (مثل مقاهي الإنترنت أو الجامعات[2442] 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. ونظراً لعدم 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.[2443]

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. ويمكن لالتزام التسجيل أن يتداخل مع حق تشغيل خدمات الإنترنت بدون إذن وهو ما تأكد في الإعلان المشترك لعام 2005 للمقرر الخاص للأمم المتحدة المعني بحرية الرأي والتعبير، وممثل منظمة الأمن والتعاون في أوروبا المعني بحرية وسائط الإعلام والمقرر الخاص للمنظمة الدولية الأمريكية المعني بحرية التعبير.[2444] ومن المرجح أن اقتضاء تحديد الهوية سيؤثر على استعمال الإنترنت نظراً لأن مستعملي الإنترنت سيخشون في هذه الحالة أن يجري رصد استعمالهم للإنترنت. وحتى إذا كان المستعملون يعرفون أن أنشطتهم قانونية فسوف يظل ذلك عاملاً مؤثراً على تفاعلهم

واستعمالهم.[2445] وفي الوقت نفسه، فإن الجناة الذين يريدون 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.

وهناك شواغل مماثلة من فرض تشريع يستهدف خدمات الاتصالات القائمة على أساس إغفال الهوية. فهناك جدل مستمر بشأن تطبيق صكوك مماثلة نوقشت بشأن تكنولوجيا التجفير على تكنولوجيا الاتصالات وخدماتها القائمة على إغفال الهوية.[2446] وإضافة إلى التضارب بين حماية الخصوصية وضمان القدرة على تحري الجرائم، فإن الخلافات بشأن الملاءمة العملية للنهج القانونية المختلفة لمواجهة التحدي الخاص بالتجفير (خاصة الافتقار إلى القدرة على الإنفاذ) تنطبق بحذافيرها على الاتصالات القائمة على إغفال الهوية.

6.6 التعاون الدولي

Bibliography (selected): *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4; *Choo,* Trends in Organized Crime, 2008, page 273 *et seq.*; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005; *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992; *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2; *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296; *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931; *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9; *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

1.6.6 مقدمة

ينطوي عدد متزايد من الجرائم السيبرانية على بُعد دولي.[2447] وكما أُشير أعلاه يتمثَّل أحد أسباب هذه الظاهرة في عدم وجود حاجة كبيرة إلى تواجد الجناة بأنفسهم في مكان تقديم الخدمة.[2448] ومن ثم، لا يحتاج الجناة عموماً إلى التواجد في المكان الذي توجد فيه الضحية. وعموماً تقترن تحقيقات الجريمة السيبرانية بضرورة التعاون الدولي. ونظراً لعدم وجود إطار قانوني دولي شامل وعدم وجود هيئة فوق وطنية بوسعها التحقيق في هذه الجرائم، تحتاج الجرائم العابرة للحدود الوطنية إلى التعاون بين السلطات المعنية في البلدان الضالعة.[2449] وقدرة الجناة على التنقل وعدم اشتراط تواجدهم في مكان الجريمة وآثار الجريمة تجعل من الضروري بالنسبة إلى سلطات إنفاذ القانون والسلطات القضائية التعاون ومساعدة الدولة صاحبة الولاية القضائية.[2450] ونظراً للاختلافات بين القوانين الوطنية ومحدودية الصكوك، يعتبر التعاون الدولي أحد التحديات الرئيسية لعولمة الجريمة.[2451]

وينطبق هذا الأمر على الأشكال التقليدية للجرائم العابرة للحدود الوطنية وعلى الجريمة السيبرانية أيضاً. ومن المطالب الرئيسية للمحققين في التحقيقات عبر الوطنية وجود تفاعل فوري من جانب نظرائهم في البلد الذي يقع فيه مكان الجاني.[2452] وفي هذه المسألة على وجه الخصوص، فإن الصكوك التقليدية للتعاون القضائي الدولي في أمور القانون الجنائي لا تفي، عادة بالمقتضيات المتعلقة بسرعة إجراء التحقيقات في الإنترنت.[2453]

2.6.6 آليات التعاون الدولي

بالنسبة إلى التحقيقات المتعلقة بالجريمة السيبرانية، تتمثل الآليات الرسمية الأكثر ملائمة لدعم التعاون الدولي في ترتيبات متبادلة لتقيم المساعدة القانونية وتسليم الجناة. وهناك آليات أخرى أقل أهمية من الناحية العملية مثل نقل المساجين ونقل المحاكمات في الأمور الجنائية ومصادرة العائدات الإجرامية واسترداد الأصول. وإضافة إلى الآليات الرسمية، هناك أساليب غير رسمية للتعاون مثل تبادل المعلومات بين وكالات إنفاذ القانون في مختلف البلدان.

3.6.6 استعراض شامل للصكوك المطبقة

هناك ثلاثة سيناريوهات رئيسية لتحديد الصكوك المطبقة من أجل التعاون الدولية الأولي، يمكن للإجراءات المعنية أن تشكل جزءاً من الاتفاقات الدولية مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (UNTOC)[2454]، وبروتوكولاتها الثلاثة[2455] أو الاتفاقيات الإقليمية مثل اتفاقية البلدان الأمريكية للمساعدة المتبادلة في المسائل الجنائية[2456] والاتفاقية الأوروبية للمساعدة المتبادلة في المسائل الجنائية.[2457] واتفاقية مجلس أوروبا بشأن الجريمة السيبرانية[2458]. وتتمثل الإمكانية الثانية في تنظيم الإجراءات من خلال اتفاقات ثنائية. وتتعلق هذه الاتفاقات عادة بطلبات محددة يمكن أن تقدم لتحديد الإجراءات والأشكال الملائمة للتواصل إلى جانب حقوق والتزامات الطرفين.[2459] وقد وقعت استراليا، على سبيل المثال، أكثر من 30 اتفاقاً ثنائياً مع بلدان أخرى لتنظيم الجوانب المتعلقة بتسليم المجرمين.[2460] وقد تناولت بعض مفاوضات هذه الاتفاقات الجريمة السيبرانية كموضوع، غير أنه من غير المؤكد إلى مدى تتناول الاتفاقات القائمة الجريمة السيبرانية[2461] بصورة وافية. وفي حال عدم تطبيق اتفاقات متعددة الأطراف أو اتفاقات ثنائية، يتعين إرساء التعاون الدولي بوجه عام على أساس إرادة دولية تستند إلى مبدأ المعاملة بالمثل.[2462] ولما كان التعاون على الاتفاقات والإرادة الثنائية يعتمد كثيراً على ظروف الحالة الفعلية والبلدان الضالعة، يركز الاستعراض الشامل أدناه على الاتفاقيات الدولية الإقليمية.

4.6.6 اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

تُعدّ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (UNTOC)[2463] الصك الدولي الرئيسي للتعاون القضائي في المسائل الجنائية. وتشمل هذه الاتفاقية صكوكاً هامة للتعاون الدولي، غير أنها لم تصمم تحديداً لمعالجة المسائل المتصلة بالحرية السيبرانية كما أنها لا تتضمن أحكاماً محددة للتعامل مع الطلبات الملحة الخاصة بحفظ البيانات.

تطبيق اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

طبقاً للفقرة 1 من المادة 3، لا تنطبق الاتفاقية في حالات الجريمة السيبرانية، إلا على الحالات التي يكون فيها الجاني عضواً في جماعة إجرامية منظمة. وتعرف المادة 2 من الاتفاقية UNTOC الجماعة الإجرامية المنظمة بأنها جماعة مكونة من ثلاثة أشخاص أو أكثر.

المادة 2 – المصطلحات المستخدمة

لأغراض هذه الاتفاقية:

أ) يُقصد بتعبير "جماعة إجرامية منظمة" جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقاً لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى؛

[...]

المادة 3 – نطاق الانطباق

1 تنطبق هذه الاتفاقية، باستثناء ما تنص عليه خلافاً لذلك، على منع الجرائم التالية والتحقيق فيها وملاحقة مرتكبيها:

أ) الأفعال المجرمة بمقتضى المواد 5 و6 و8 و23 من هذه الاتفاقية؛

ب) الجريمة الخطيرة حسب التعريف الوارد في المادة 2 من هذه الاتفاقية؛ حيثما يكون الجرم ذا طابع عبر وطني وتكون ضالعة فيه جماعة إجرامية منظمة.

ولذا، فإن الاتفاقية تتعلق على نحو خاص بالحالات التي تضم أي من أشكال الجريمة المنظمة. ومما لا شك فيه أن الجريمة المنظمة تدخل في سياق الجريمة السيبرانية. ولذا لا يوجد يقين بشأن مدى ضلوع وبالتالي ارتباط الاتفاقية UNTOC بتحقيقات الجريمة السيبرانية عبر الوطنية. وفي الواقع يعتبر تحديد ضلوع الجريمة المنظمة أمراً بالغ الأهمية. وبالتالي، فإن تحليل العلاقة بين الجرائم المتعلقة بالهوية والجريمة المنظمة تكتنفه صعوبات. وتمثل العائق الرئيسي الأول في غياب البحوث العلمية الموثوقة في هذا المجال. وخلافاً للجوانب التقنية للجناة، يعد مكون الجريمة المنظمة لدى الجناة من الجوانب التي لم تحلل بكثافة. وقد كانت هناك تحقيقات ناجحة حددت العديد من العصابات الإجرامية الضالعة في الجريمة السيبرانية. بيد أن هيكل هذه الجماعات لا يقارن بالضرورة بهيكل الجماعات التقليدية للجريمة المنظمة حيث تنزع جماعات الجريمة السيبرانية إلى هيكل أكثر اتساعاً ومرونة[2464]. كما أن هذه الجماعات تكون أقل في العدد كثيراً مقارنة بالجماعات التقليدية للجريمة المنظمة.[2465] وتسمح شبكة الإنترنت بالتعاون الوثيق مع الآخرين وتنسيق الأنشطة دون الحاجة إلى الالتقاء وجهاً لوجه.[2466] وهذا الأمر يجعل من الأجدى للجناة العمل معاً في جماعات مخصصة سلسة[2467].

طلبات المساعدة القانونية المتبادلة

تحدد المادة 18 إجراءات المساعدة القانونية المتبادلة. ويتضمن هذا الحكم مجموعة كاملة من الإجراءات.

المادة 18 – المساعدة القانونية المتبادلة

1 تقدم الدول الأطراف، بعضها لبعض، أكبر قدر ممكن من المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية فيما يتصل بالجرائم المشمولة بهذه الاتفاقية، حسبما تنص عليه المادة 3، وتمد كل منها الأخرى تبادلياً بمساعدة مماثلة عندما تكون لدى الدولة الطرف الطالبة دواع معقولة للاشتباه في أن الجرم المشار إليه في الفقرة 1 أ) أو ب) من المادة 3 ذو طابع عبر وطني، بما في ذلك أن ضحايا تلك الجرائم أو الشهود عليها أو عائداً لها أو الأدوات المستعملة في ارتكابها أو الأدلة عليها توجد في الدولة الطرف متلقية الطلب وأن جماعة إجرامية منظمة ضالعة في ارتكاب الجرم.

2 تقدم المساعدة القانونية المتبادلة بالكامل بمقتضى قوانين الدولة الطرف متلقية الطلب ومعاهداتها واتفاقاتها وترتيباتها ذات الصلة، فيما يتصل بالتحقيقات والملاحقات والإجراءات القضائية المتعلقة بالجرائم التي يجوز تحميل هيئة اعتبارية المسؤولية عنها بمقتضى المادة 10 من هذه الاتفاقية في الدولة الطالبة.

[...]

وتتضمن المادة 18 (1)-(2) المبادئ العامة للتعاون الدولي.[2468] وهذه المبادئ ترتبط بتحقيقات الجريمة السيبرانية وبالتحقيقات التقليدية على السواء. كما تشمل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية أحكاماً مماثلة.

المادة 18 – المساعدة القانونية المتبادلة

[...]

3 يجوز أن تطلب المساعدة القانونية المتبادلة، التي تقدم وفقًا لهذه المادة، لأي من الأغراض التالية:

أ) الحصول على أدلة أو أقوال من الأشخاص؛

ب) تفعيل خدمة الوثائق القضائية؛

ج) تنفيذ عمليات التفتيش والضبط والتجميد؛

هـ) تقديم المعلومات والأدلة والتقييمات التي يقوم بها الخبراء؛

ز) التعرف على عائدات الجرائم أو الممتلكات أو الأدوات أو الأشياء الأخرى أو اقتفاء أثرها لأغراض الحصول على أدلة؛

ح) تيسير مثول الأشخاص طواعية في الدولة الطرف الطالبة؛

ط) أي نوع آخر من المساعدة لا يتعارض مع القانون الداخلي للدولة الطرف متلقية الطلب.

[...]

وتتضمن الفقرة 3 من المادة 18 (3) طلبات محددة للمساعدة القانونية المتبادلة. والقائمة معقدة وتتراوح من جمع الأدلة إلى إجراءات الملاحقة الخاصة بالجريمة. وكما ورد آنفاً، لا تشمل الاتفاقية UNTOC صياغة محددة بشأن الطلبات المتعلقة بالبيانات، مثل طلبات اعراض الاتصالات أو التحفظ على بيانات. بيد أن المادة 18(3) *ط)* تفتح الحكم لطلبات أخرى، لذا يمكن استعمال الاتفاقية UNTOC في الطلبات المتعلقة بالبيانات. وعلى الرغم من أنه جدير بوجه عام مناقشة مزايا التنظيم المحدد للطلبات، فإن الصكوك الإقليمية المقارنة التي تتضمن هذه الطلبات، مثل اتفاقية مجلس أوروبا بشأن الحرية والسيبرانية لا تشير في العادة إلاَّ إلى الأحكام الإجرائية في القانون الوطني دون تحديد إجراءات محددة لطلبات المساعدة القانونية المتبادلة.

المادة 18 – المساعدة القانونية المتبادلة

[...]

4 يجوز للسلطات المختصة للدولة الطرف، دون مساس بالقانون الداخلي، ودون أن تتلقى طلباً مسبقًا، أن تحيل معلومات متعلقة بمسائل جنائية إلى سلطة مختصة في دولة طرف أخرى حيثما ترى أن هذه المعلومات يمكن أن تساعد تلك السلطة على القيام بالتحريات والإجراءات الجنائية أو إتمامها بنجاح أو أنها قد تفضي إلى قيام الدولة الطرف الأخرى بصوغ طلب عملاً بهذه الاتفاقية.

5 تكون إحالة المعلومات، عملاً بالفقرة 4 من هذه المادة دون إخلال بما يجري من تحريات وإجراءات جنائية في الدولة التي تتبعها السلطات المختصة التي تقدم تلك المعلومات. وتمتثل السلطات المختصة التي تتلقى المعلومات لأي طلب بإبقاء تلك المعلومات طي الكتمان، ولو مؤقتاً، أو بفرض قيود على استخدامها. بيد أن هذا لا يمنع الدولة الطرف المتلقية من أن تفشي في إجرائها معلومات تبرئ شخصاً متهماً. وفي تلك الحالة، تقوم الدولة الطرف المتلقية بإخطار الدولة الطرف المحيلة قبل إفشاء تلك المعلومات، وتتشاور مع الدولة الطرف المحيلة إذا ما طلب ذلك. وإذا تعذر، في حالة استثنائية، توجيه إشعار مسبق، قامت الدولة الطرف المتلقية بإبلاغ الدولة الطرف المحيلة بذلك الإفشاء دون إبطاء.

[...]

وتتبادل المادة 18 (4)-(5) تبادل المعلومات. فهي تفرض شكلاً من أشكال التعاون[2469] على أساس طوعي دون أي التزام على الطرف المتلقي بتقديم طلب للمساعدة القانونية المتبادلة.[2470] وهي تغطي المعلومات المتعلقة بالمسائل الجنائية مثل معلومات عن المستهلكين المحتملين للمواد الإباحية المستغل فيها الأطفال المقيمين في بلد آخر تم اكتشافهم أثناء تحقيق ما. وفي التحقيقات المعقدة بشكل خاص، التي تستنزف فيها الإجراءات الرسمية المتبادلة الوقت وبالتالي، يمكن أن تعيق التحقيقات، تميل وكالات إنفاذ القانون إلى اللجوء إلى وسائل التعاون غير الرسمية. ومع ذلك، لا يمكن لعملية تبادل المعلومات أن تعمل كوسيلة بديلة إلا إذا كان بمقدور الدولة المتلقية للمعلومات جمع كافة الأدلة المطلوبة بمعرفتها. وفي كل الحالات الأخرى، يحتاج الأمر إلى التعاون الرسمي لضمان سلسلة الحفظ. وفي المناقشة بشأن تحويل التعاون الدولي من طلبات رسمية غلى تبادل غير رسمي للمعلومات، من الضروري الوضع في الاعتبار أن العملية الرسمية وضعت لحماية سلامة الدولة إلى جانب حقوق المتهمين. ومن ثم، ينبغي لتبادل المعلومات ألاّ يلتف حول الهيكل المحدد للمساعدة القانونية المتبادلة.

المادة 18 – *المساعدة القانونية المتبادلة*

[...]

6 ليس في أحكام هذه المادة ما يخل بالالتزامات الناشئة عن أية معاهدة أخرى، ثنائية أو متعددة الأطراف، تحكم أو ستحكم المساعدة القانونية المتبادلة كلياً أو جزئياً.

7 تنطبق الفقرات 9 إلى 29 من هذه المادة على الطلبات المقدمة عملاً بهذه المادة إذا كانت الدول الأطراف المعنية غير مرتبطة بمعاهدة لتبادل المساعدة القانونية. وإذا كانت تلك الدول الأطراف مرتبطة بمعاهدة من هذا القبيل، وجب تطبيق الأحكام المقابلة في تلك المعاهدة، ما لم تتفق الدول الأطراف على تطبيق الفقرات 9 إلى 29 من هذه المادة بدلاً منها. وتُشجع الدول الأطراف بشدة على تطبيق هذه الفقرات إذا كانت تسهل التعاون.

8 لا يجوز للدول الأطراف أن ترفض تقديم المساعدة القانونية المتبادلة وفقًا لهذه المادة بدعوى السرية المصرفية.

9 يجوز للدول الأطراف أن ترفض تقديم المساعدة القانونية المتبادلة بمقتضى هذه المادة بحجة انتفاء ازدواجية التجريم. بيد أنه يجوز للدولة متلقية الطلب، عندما ترى ذلك مناسباً، أن تقدم المساعدة، بالقدر الذي تقرره حسب تقديرها، بصرف النظر عما إذا كان السلوك يمثل جرماً بمقتضى القانون الداخلي للدولة الطرف متلقية الطلب.

10 يجوز نقل أي شخص محتجز أو يقضي عقوبته في إقليم دولة طرف ومطلوب وجوده في دولة طرف أخرى لأغراض التعرف أو الإدلاء بشهادة أو تقديم مساعدة أخرى في الحصول على أدلة من أجل تحقيقات أو ملاحقات أو إجراءات قضائية تتعلق بجرائم مشمولة هذه الاتفاقية إذا استوفي الشرطان التاليان:

أ) موافقة ذلك الشخص طوعاً وعن علم؛

ب) اتفاق السلطات المختصة في الدولتين الطرفين، رهناً بما تراه هاتان الدولتان الطرفان مناسباً من شروط.

11 لأغراض الفقرة 10 من هذه المادة:

أ) يكون للدولة الطرف التي ينقل إليها الشخص سلطة إبقائه قيد الاحتجاز، وعليها التزام بذلك، ما لم تطلب الدولة الطرف التي نقل منها الشخص غير ذلك أو تأذن بغير ذلك؛

ب) تنفذ الدولة الطرف التي ينقل إليها الشخص، دون إبطاء، التزامها بإعادته إلى عهدة الدولة الطرف التي نقل منها وفقًا لما يتفق عليه مسبقًا، أو بأية صورة أخرى، بين السلطات المختصة في الدولتين الطرفين؛

ج) لا يجوز للدولة الطرف التي ينقل إليها الشخص أن تطالب الدولة الطرف التي نقل منها ببدء إجراءات تسليم من أجل إعادة ذلك الشخص؛

د) تُحتسب المدة التي يقضيها الشخص المنقول قيد الاحتجاز في الدولة التي نقل منها ضمن مدة العقوبة المفروضة عليه في الدولة الطرف التي نقل إليها.

12 ما لم توافق على ذلك الدولة الطرف التي يتقرر نقل شخص ما منها، وفقاً للفقرتين 10 و11 من هذه المادة، لا يجوز ملاحقة ذلك الشخص، أياً كانت جنسيته، أو احتجازه أو معاقبته أو فرض أي قيود أخرى على حريته الشخصية، في إقليم الدولة التي ينقل إليها، بسبب أفعال أو إغفالات أو أحكام إدانة سابقة لمغادرته إقليم الدولة التي نقل منها.

[...]

وتتبادل المادة 18(6)-(12) الجوانب الإجرائية للمساعدة القانونية المتبادلة. والفقرتان 8 و9 تمثلان أهمية خاصة لقضايا الجريمة السيبرانية. وتمكن الفقرة 9 الدول من رفض طلبات المساعدة المتبادلة على أساس انتفاء ازدواجية التجريم. ويكتسي هذا الأمر بالأهمية نظراً إلى محدودية نطاق نهج توحيد الأحكام الجنائية الهامة الخاصة بالجريمة السيبرانية في الوقت الراهن. مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. وحتى منتصف 2010، لم تصدق على هذه الاتفاقية إلا 30 بلداً، حيث حددت المعايير الدنيا المقابلة بشأن الجرائم السيبرانية. ويمكن لذلك أن يعيق التعاون على أساس الاتفاقية UNTOC.

المادة 18 – المساعدة القانونية المتبادلة

[...]

13 تعين كل دولة طرف سلطة مركزية تكون مسؤولة ومخولة بتلقي طلبات المساعدة القانونية المتبادلة وتقوم بتنفيذ تلك الطلبات أو بإحالتها إلى السلطات المختصة لتنفيذها. وحيثما كان للدولة الطرف منطقة خاصة أو إقليم خاص ذو نظام مستقل للمساعدة القانونية المتبادلة، جاز لها أن تعين سلطة مركزية منفردة تتولى المهام ذاتها فيما يتعلق بتلك المنطقة أو بذلك الإقليم. وتكفل السلطات المركزية سرعة وسلامة تنفيذ الطلبات المتلقاة أو إحالتها. وحيثما تقوم السلطة المركزية بإحالة الطلب إلى سلطة مختصة لتنفيذه، تشجع تلك السلطة المختصة على تنفيذ الطلب بسرعة وبصورة سليمة. ويخطر الأمين العام للأمم المتحدة باسم السلطة المركزية المعينة لهذا الغرض وقت قيام كل دولة طرف بإيداع صك تصديقها على هذه الاتفاقية أو قبولها أو إقرارها أو الانضمام إليها. وتوجه طلبات المساعدة القانونية المتبادلة وأي مراسلات تتعلق بها إلى السلطات المركزية التي تعينها الدول الأطراف. ولا يمس هذا الشرط حق أية دولة طرف في أن تشترط توجيه مثل هذه الطلبات والمراسلات إليها عبر القنوات الدبلوماسية، وفي الحالات العاجلة، وحيثما تتفق الدولتان الطرفان المعنيتان، عن طريق المنظمة الدولية للشرطة الجنائية، إن أمكن ذلك.

14 تقدم الطلبات كتابة أو، حيثما أمكن، بأية وسيلة تستطيع إنتاج سجل مكتوب بلغة مقبولة لدى الدولة الطرف متلقية الطلب، وبشروط تتيح لتلك الدولة الطرف أن تتحقق من صحته. ويخطر الأمين العام للأمم المتحدة باللغة أو اللغات المقبولة لدى كل دولة طرف وقت قيام كل دولة طرف بإيداع صك تصديقها على هذه الاتفاقية أو قبولها أو إقرارها أو الانضمام إليها. وفي الحالات العاجلة، وحيثما تتفق الدولتان الطرفان على ذلك، يجوز أن تقدم الطلبات شفوياً، على أن تؤكد كتابةً على الفور.

15 يتضمن طلب المساعدة القانونية المتبادلة:

أ) هوية السلطة مقدمة الطلب؛

ب) موضوع وطبيعة التحقيق أو الملاحقة أو الإجراء القضائي الذي يتعلق به الطلب، واسم ووظائف السلطة التي تتولى التحقيق أو الملاحقة أو الإجراء القضائي؛

ج) ملخصاً للوقائع ذات الصلة بالموضوع، باستثناء ما يتعلق بالطلبات المقدمة لغرض تبليغ مستندات قضائية؛

د) وصفاً للمساعدة الملتمسة وتفاصيل أي إجراء معين تود الدولة الطرف الطالبة اتباعه؛

هـ) هوية أي شخص معني ومكانه وجنسيته، حيثما أمكن ذلك؛

و) الغرض الذي تلتمس من أجله الأدلة أو المعلومات أو التدابير.

16 يجوز للدولة الطرف متلقية الطلب أن تطلب معلومات إضافية عندما يتبين أنها ضرورية لتنفيذ الطلب وفقًا لقانونها الداخلي، أو عندما يكون من شأن تلك المعلومات أن تسهل ذلك التنفيذ.

[...]

وتحدد المادة 18(13)-(16) شكل ومضمون الطلبات، فضلاً عن قنوات الاتصال. وبالنسبة لقنوات الاتصال، تتبع الاتفاقية فكرة أن الطلبات ترسل من سلطة مركزية إلى سلطة مركزية نظيرة.[2471] وتشدد الاتفاقية على أهمية هذا الإجراء لضمان سرعة تنفيذ الطلب على الوجه الأمثل. وقد تختلف أدوار السلطات المركزية، وتتراوح بين المشاركة المباشرة في معالجة الطلبات وتنفيذها وإحالة هذه الطلبات إلى السلطات المختصة. وتترك الاتفاقية للدول تحديد ما إذا كانت الطلبات ترسل وجوباً عبر القنوات الدبلوماسية من عدمه. وهذا الخيار ينطوي على إبطاء العملية حيث سيبطئ كثيراً من إرسال الطلب ويعيق بشكل خاص تدابير متوقعة من شاكلة حفظ بيانات الحركة. وعلى النقيض من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية،[2472] لا تحدد الاتفاقية UNTOC وسائل التعاون المتوخى، بل تقدم إجراءً عاماً لحالات الطوارئ. فإذا وافقت الدول، يمكن استعمال المنظمة الدولية للشرطة الجنائية (الإنتربول) كقناة من قنوات الاتصال. ولتسهيل تحديد السلطة المعنية في بلد آخر، يحتفظ مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) بدليل إلكتروني في هذا الشأن.[2473] ويزود هذا الدليل سلطة الإصدار بالبيانات الأخرى ذات الصلة.[2474]

وعند تقديم الطلب، من الضروري الوفاء بالمتطلبات الأساسية المحددة في الفقرتين 14 و15. ولا يسمح بالطلبات الشفهية إلا في الحالات الطارئة ويتعين دعمها بطلب تحريري لاحقاً. وتقارير الدول الأطراف المعنية بتطبيق الاتفاقية تبين أنه على الرغم من أن لدى كثير من الدول تشريعات تلزم بتقديم طلبات المساعدة القانونية المتبادلة كتابةً، فإن عدد قليل فقط من البلدان أجاز قبول طلبات مقدمة مؤقتة تلحق بها فيما بعد رسائل إلكترونية.[2475] وفي هذا الصدد، تختلف الاتفاقية UNTOC عن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية التي تشجع الدول على استعمال وسائل الاتصالات الإلكترونية في الحالات الطارئة.[2476] ويوفر المكتب UNODC برمجته لصياغة هذه الطلبات من أجل ضمان اكتمال الطلبات (أداة تحرير طلب المساعدة القانونية المتبادلة).[2477]

المادة 18- المساعدة القانونية المتبادلة

[...]

17 يكون تنفيذ الطلب وفقًا للقانون الداخلي للدولة الطرف متلقية الطلب، وأن يكون، بالقدر الذي لا يتعارض مع القانون الداخلي للدولة الطرف متلقية الطلب وعند الإمكان، وفقًا للإجراءات المحددة في الطلب.

18 عندما يتعين سماع أقوال شخص موجود في إقليم دولة طرف، بصفة شاهد أو خبير، أمام السلطات القضائية لدولة طرف أخرى، ويكون ذلك ممكنًا ومتفقًا مع المبادىء الأساسية للقانون الداخلي، يجوز للدولة الطرف الأولى أن تسمح، بناء على طلب الدولة الأخرى، بعقد جلسة استماع عن طريق الفيديو إذا لم يكن ممكنًا أو مستصوبًا مثول الشخص المعني بنفسه في إقليم الدولة الطرف الطالبة. ويجوز للدول الأطراف أن تتفق على أن تتولى إدارة جلسة الاستماع سلطة قضائية تابعة للدولة الطرف الطالبة وأن تحضرها سلطة قضائية تابعة للدولة الطرف متلقية الطلب.

19 لا يجوز للدولة الطرف الطالبة أن تنقل المعلومات أو الأدلة التي تزودها بها الدولة الطرف متلقية الطلب، أو أن تستخدمها في تحقيقات أو ملاحقات أو إجراءات قضائية غير تلك المذكورة في الطلب، دون موافقة مسبقة من الدولة الطرف متلقية الطلب. وليس في هذه الفقرة ما يمنع الدولة الطرف الطالبة من أن تفشي في إجراءاتها معلومات أو أدلة تؤدي إلى تبرئة شخص متهم. وفي الحالة الأخيرة، تقوم الدولة الطرف الطالبة بإخطار الدولة الطرف متلقية الطلب قبل

حدوث الإفشاء وأن تتشاور مع الدولة الطرف متلقية الطلب، إذا ما طلب منها ذلك. وإذا تعذر، في حالة استثنائية، توجيه إشعار مسبق، قامت الدولة الطرف الطالبة بإبلاغ الدولة الطرف متلقية الطلب، دون إبطاء، بحدوث الإفشاء.

20 يجوز للدولة الطرف الطالبة أن تشترط على الدولة الطرف متلقية الطلب أن تحافظ على سرية الطلب ومضمونه، باستثناء القدر اللازم لتنفيذه. وإذا تعذر على الدولة الطرف متلقية الطلب أن تمتثل لشرط السرية، أبلغت الدولة الطرف الطالبة بذلك على وجه السرعة.

21 يجوز رفض تقديم المساعدة القانونية المتبادلة:

أ) إذا لم يقدم الطلب وفقًا لأحكام هذه المادة؛

ب) إذا رأت الدولة الطرف متلقية الطلب أن تنفيذ الطلب قد يمس سيادتها أو أمنها أو نظامها العام أو مصالحها الأساسية الأخرى؛

ج) إذا كان من شأن القانون الداخلي للدولة الطرف متلقية الطلب أن يحظر على سلطاتها تنفيذ الإجراء المطلوب بشأن أي جرم مماثل، لو كان ذلك الجرم خاضعاً لتحقيق أو ملاحقة أو إجراءات قضائية في إطار ولايتها القضائية؛

د) إذا كانت الاستجابة للطلب تتعارض مع النظام القانوني للدولة الطرف متلقية الطلب فيما يتعلق بالمساعدة القانونية المتبادلة.

22 لا يجوز للدول الأطراف أن ترفض طلب مساعدة قانونية متبادلة كرد اعتبار أن الجرم ينطوي أيضاً على مسائل مالية.

23 تبدي أسباب أي رفض لتقديم المساعدة القانونية المتبادلة.

24 تنفذ الدولة الطرف متلقية الطلب طلب المساعدة القانونية المتبادلة في أقرب وقت ممكن، وتراعي إلى أقصى حد ممكن أي مواعيد نهائية تقترحها الدولة الطرف الطالبة وتورد أسبابها، على الأفضل، في الطلب ذاته. وتستجيب الدولة الطرف متلقية الطلب للطلبات المعقولة التي تتلقاها من الدولة الطرف الطالبة بشأن التقدم المحرز في معالجة الطلب. وتبلغ الدولة الطرف الطالبة الدولة الطرف متلقية الطلب، على وجه السرعة، عندما تنتهي حاجتها إلى المساعدة الملتمسة.

25 يجوز للدولة الطرف متلقية الطلب تأجيل المساعدة القانونية المتبادلة لكونها تتعارض مع تحقيقات أو ملاحقات أو إجراءات قضائية جارية.

26 تتشاور الدولة الطرف متلقية الطلب، قبل رفض طلب بمقتضى الفقرة 21 من هذه المادة، أو قبل تأجيل تنفيذه بمقتضى الفقرة 25 من هذه المادة، مع الدولة الطرف الطالبة للنظر فيما إذا كان يمكن تقديم المساعدة رهناً بما تراه ضرورياً من شروط وأحكام. فإذا قبلت الدولة الطرف الطالبة المساعدة رهناً بتلك الشروط، وجب عليها الامتثال لتلك الشروط.

27 دون مساس بانطباق الفقرة 12 من هذه المادة، لا يجوز ملاحقة أي شاهد أو خبير أو شخص آخر يوافق، بناءً على طلب الدولة الطرف الطالبة، على الإدلاء بشهادته في إجراءات قضائية، أو على المساعدة في تحريات أو ملاحقات أو إجراءات قضائية في إقليم الدولة الطرف الطالبة، أو احتجاز ذلك الشاهد أو الخبير أو الشخص الآخر أو معاقبته أو إخضاعه لأي إجراء آخر يقيد حريته الشخصية في إقليم ذلك الطرف، بخصوص أي فعل أو إغفال أو حكم إدانة سبق مغادرته إقليم الدولة الطرف متلقية الطلب. وينتهي هذا الضمان إذا بقي الشاهد أو الخبير أو الشخص الآخر بمحض اختياره في إقليم الدولة الطرف الطالبة، بعد أن تكون قد أتيحت له فرصة المغادرة خلال مدة خمسة عشر يوماً متصلة، أو أية مدة تتفق عليها الدولتان الطرفان، اعتباراً من التاريخ الذي أبلغ فيه رسمياً بأن وجوده لم يعد مطلوباً من السلطات القضائية، أو في حال عودته إلى الإقليم بمحض اختياره بعد أن يكون قد غادره.

28 تتحمل الدولة الطرف متلقية الطلب التكاليف العادية لتنفيذ الطلب، ما لم تتفق الدولتان الطرفان المعنيتان على غير ذلك. وإذا كانت تلبية الطلب تستلزم أو ستستلزم نفقات ضخمة أو غير عادية، وجب على الدولتين الطرفين المعنيتين أن تتشاورا لتحديد الشروط والأحكام التي سينفذ الطلب بمقتضاها، وكذلك كيفية تحمل تلك التكاليف.

29 الدولة الطرف الطالبة

أ) توفر الدولة الطرف متلقية الطلب للدولة الطرف الطالبة نسخاً من السجلات أو الوثائق أو المعلومات الحكومية الموجودة في حوزتها والتي يسمح قانونها الداخلي بإتاحتها لعامة الناس؛

ب) يجوز للدولة الطرف متلقية الطلب، حسب تقديرها، أن تقدم إلى الدولة الطرف الطالبة، كلياً أو جزئياً أو رهناً بما تراه مناسباً من شروط، نسخاً من أي سجلات أو وثائق أو معلومات حكومية، موجودة في حوزتها ولا يسمح قانونها الداخلي بإتاحتها لعامة الناس.

30 تنظر الدول الأطراف، حسب الاقتضاء، في إمكانية عقد اتفاقات أو ترتيبات ثنائية أو متعددة الأطراف تخدم الأغراض المتوخاة من أحكام هذه المادة، أو تضعها موضع التطبيق العملي، أو تعززها.

5.6.6 اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

تتناول اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية ("اتفاقية الجريمة السيبرانية") الأهمية المتزايدة للتعاون الدولي في المواد من 23 إلى 35.

مبادئ عامة تتعلَّق بالتعاون الدولي

تحدد المادة 23 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية ثلاثة مبادئ عامة بخصوص التعاون الدولي بين الأعضاء في تحقيقات الجريمة السيبرانية.

المادة 23 – مبادئ عامة تتعلَّق بالتعاون الدولي

يتعاون الأطراف مع بعضهم البعض، وفقاً 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 حاسوبية، 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.[2478] ويلاحظ المبدأ الثالث أن الأحكام التي تتناول التعاون الدولي ليست بديلاً عن أحكام الاتفاقات الدولية المتعلقة بالمساعدة القانونية المتبادلة والتسليم أو الأحكام ذات الصلة في القوانين المحلية المتعلقة بالتعاون الدولي. وأكد واضعو اتفاقية الجريمة السيبرانية على أن المساعدة المتبادلة ينبغي أن تجري عموماً من خلال تطبيق المعاهدات ذات الصلة والترتيبات المماثلة المتعلقة بالمساعدة المتبادلة. ونتيجة لذلك، فإن اتفاقية الجريمة السيبرانية لا تقصد إنشاء نظام عام منفصل يتعلَّق بالمساعدة المتبادلة. ولذلك لا يطالَب كل طرف بوضع أساس قانوني لتمكين إجراء التعاون الدولي على النحو المعرَّف

في اتفاقية الجريمة السيبرانية إلا في الحالات التي لا تكون فيها المعاهدات والقوانين والترتيبات القائمة تتضمن فعلاً مثل هذه الأحكام.[2479]

تسليم المجرمين

يظل تسليم المواطنين جانباً من أصعب جوانب التعاون الدولي.[2480] 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 اتفاقية الجريمة السيبرانية ولا ينطبق في الحالات البسيطة (الحرمان من الحرية لفترة لا تزيد عن سنة واحدة على الأقل.[2481] ولتجنُّب النزاعات التي يمكن أن تحدث بشأن قدرة الأطراف على إبداء تحفظات، تستند المادة 24 إلى مبدأ ازدواج الجُرم.[2482]

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 الأمين العام لمجلس أوروبا باسم وعنوان كل سلطة مسؤولة عن إصدار أو تلقي طلبات التسليم، أو أوامر المصادرة التحفظية في حالة عدم وجود اتفاقية.*

ب) يقوم الأمين العام لمجلس أوروبا بإنشاء وتحديث سجل خاص بالسلطات المسؤولة التي يعيّنها الأطراف، ويلتزم كل طرف بالتأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت.

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.[2483] 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.[2484] 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 اتفاقية الجريمة السيبرانية هذه المشكلة بإبراز أهمية التمكين من استعمال وسائل سريعة للاتصال.[2485]

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 بنُظم وبيانات الحاسوب، 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 التجفير 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.

وخلال 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.[2486] 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.[2487]

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 رأى 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.

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.

وكما ورد آنفاً، هناك بعض الشواغل المتعلقة بالاستعاضة عن المساعدة القانونية المتبادلة بمعلومات تقدم بصورة غير رسمية. فلن يكون تبادل المعلومات ممكناً إلاّ إذا كان في مقدور الدولة متلقية المعلومات جمع كافة الأدلة المطلوبة بمعرفتها. وفي كل الحالات الأخرى، يحتاج الأمر إلى التعاون الرسمي لضمان سلسلة الحفظ. وفي المناقشة بشأن تحويل التعاون الدولي من طلبات رسمية إلى تبادل غير رسمي للمعلومات، من الضروري الوضع في الاعتبار أن العملية الرسمية وضعت لحماية سلامة الدولة إلى جانب حقوق المهتمين. ومن ثم، ينبغي لتبادل المعلومات ألا يلتفت حول الهيكل المحدد للمساعدة القانونية المتبادلة.

وتتصل واحدة من أهم القواعد في المادة 26 بسرية المعلومات. ونظراً إلى أن عدداً من التحقيقات لا يمكن أن تجري بنجاح إلا 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.

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 اتفاقية الجريمة السيبرانية وحدها. وقرَّر واضعو اتفاقية الجريمة السيبرانية عدم إقامة نظام منفصل للمساعدة القانونية المتبادلة الإلزامية في إطار اتفاقية الجريمة السيبرانية.[2488] 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 الالتزام بإقامة نقطة اتصال مسماة لطلبات المساعدة القانونية المتبادلة؛[2489] واقتضاء الاتصال المباشر بين نقاط الاتصال لتجنُّب الدخول في إجراءات تستغرق وقتاً طويلاً؛[2490] وقيام الأمين العام لمجلس أوروبا بإنشاء قاعدة بيانات لجميع نقاط الاتصال.

وبالإضافة إلى ذلك، تحدِّد المادة 27 قيوداً تتعلَّق بطلبات المساعدة. فأطراف اتفاقية الجريمة السيبرانية يستطيعون بصورة خاصة رفض التعاون بشأن القضايا السياسية، أو إذا كانت تعتبر أن التعاون سيمس بسيادتها أو أمنها أو نظامها العام أو مصالحها الجوهرية الأخرى.

ورأى واضعو اتفاقية الجريمة السيبرانية 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.[2491] ولذلك، فمن المهم بصفة خاصة تعريف مصطلح "المصالح الجوهرية الأخرى" تعريفاً ضيقاً. ويشير التقرير التفسيري للاتفاقية المتعلقة بالجريمة السيبرانية إلى أن ذلك قد يكون هو واقع الحال إذا كان من الممكن أن يؤدي

التعاون إلى صعوبات أساسية لدي الطرف المطلوب منه التعاون.[2492] ومن منظور واضعي الاتفاقية، فإن الانشغالات المتعلقة بعدم كفاية قوانين حماية البيانات لا تعتبر مصالح جوهرية.[2493]

المساعدة المتبادلة فيما يتعلق بالتدابير المؤقتة

تتضح في المواد 28-33 الأدوات الإجرائية الواردة في الاتفاقية المتعلقة بالجريمة السيبرانية.[2494] وتتضمن هذه الاتفاقية عدداً من الأدوات الإجرائية المصمَّمة لتحسين التحقيقات في الدول الأعضاء.[2495] وفيما يتعلق بمبدأ السيادة الوطنية،[2496] يمكن استعمال هذه الأدوات في التحقيقات على الصعيد الوطني فقط.[2497] 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 الحفاظ على بيانات الحاسوب المخزونة[2498]	المادة 29
المادة 17 – سرعة الحفاظ على بيانات الحركة والكشف الجزئي لها[2499]	المادة 30
المادة 18 – أمر الإبراز[2500]	لا شيء
المادة 19 – تفتيش ومصادرة بيانات الحاسوب المخزَّنة[2501]	المادة 31
المادة 20 – تجميع بيانات الحاسوب في الوقت الفعلي [2502]	المادة 33
المادة 21 – اعتراض محتوى البيانات[2503]	المادة 34

النفاذ عبر الحدود إلى البيانات الحاسوبية المخزنة

بالإضافة إلى التعبير البحت عن الأحكام الإجرائية، ناقش واضعو اتفاقية الجريمة السيبرانية الظروف التي يُسمح فيها لوكالات إنفاذ القانون بالنفاذ إلى البيانات الحاسوبية التي لا تكون مخزونة في أراضيها ولا تقع تحت سيطرة شخص في أراضيها. وقد تمكنوا 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.[2504] ولم يمكن التوصل إلى اتفاقات أخرى[2505] بل ولا يزال الحل الذي تم التوصل إليه موضعاً للنقد من جانب الدول الأعضاء في مجلس أوروبا.[2506]

والحالتان التي يُسمح فيهما لوكالات إنفاذ القانون بالنفاذ إلى البيانات المخزونة خارج أراضيها تتصلان بما يلي:

- معلومات متوفِّرة للجمهور؛ و/أو
- النفاذ بموافقة الشخص صاحب السيطرة.

المادة 32 – النفاذ عبر الحدود إلى بيانات مخزَّنة على حاسوب عن طريق الموافقة أو حيثما تكون متاحة علناً

يجوز لأي طرف، وبدون تفويض من أي طرف آخر:

أ) الدخول على بيانات حاسوب مخزَّنة ومتاحة علناً (مصدر مفتوح)، بغض النظر عن مكان وجود البيانات جغرافياً؛ أو

ب) النفاذ، أو تلقي، عن طريق نظام حاسوب في إقليمه، إلى بيانات حاسوبية مخزَّنة موجودة لدى 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 الحاسوب المذكور.

ولا تشمل المادة 32 الأشكال الأخرى للنفاذ عبر الحدود، ولكن هذه الأشكال الأخرى ليست مستبعدة أيضاً.[2507]

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.[2508]

ومن بين الشواغل الرئيسية أن الحكم بصياغته الحالية يمكن أن يتناقض مع المبادئ الأساسية للقانون الدولي.[2509] فطبقاً للقانون الدولي، يجب على المحققين احترام السيادة الوطنية أثناء التحقيق.[2510] فهو غير مسموح لهم بشكل خاص إجراء تحقيقات في دولة أخرى دون موافقة السلطات المختصة بهذه الدولة. وقرار منح هذا التصريح لا يتخذه شخص واحد، بل سلطات الدولة، لأن انهاك السيادة الوطنية لا يؤثر فقط على حقوق الأفراد، بل يؤثر أيضاً على مصالح الدول. وبالتصديق على اتفاقية الجريمة السيبرانية، تتجاوز البلدان هذا المبدأ جزئياً، وتسمح للبلدان الأخرى بإجراء تحقيقات في أراضيها.

وهناك شاغل آخر يتمثل في أن المادة وهناك شاغل آخر يتمثل في أن المادة لا 32(ب)، تحدد إجراءات التحقيق. فطبقاً لنص الحكم، لا يتحتم تطبيق نفس القيود الموجودة في القانون المحلي بالنسبة للتحقيقات المحلية المماثلة. ومن المثير أن هذا القيد كان موجوداً في مشروع نص اتفاقية الجريمة السيبرانية المقدم في أوائل عام 2000، غير أنه حذف في المسودة الثانية والعشرين.[2511]

وواضعي اتفاقية الجريمة السيبرانية ينتهكون، باستحداث المادة 32(ب)، الهيكل المتشدِّد لنظام المساعدة القانونية المتبادلة. فقد مكَّن واضعو اتفاقية الجريمة السيبرانية من خلال المادة 18 المحققين إصدار أمر لتقديم بيانات في التحقيقات المحلة. وإذا ما سمح لوكالات إنفاذ القانون باستخدام هذا الصك في التحقيقات الدولية، يتعين أن يكون الأمر متضمناً لمجموعة الصكوك المذكورة في سياق المساعدة الثانوية المتبادلة. ولا يمكن تطبيق هذه الأداة في التحقيقات الدولية لأن الحكم المناظر في الفصل 3 من اتفاقية الجريمة السيبرانية والذي يتناول التعاون الدولي 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.[2512]

ونوقش النفاذ العابر للحدود إلى البيانات الحاسوبية المخزنة أيضاً في موسكو في المؤتمر الوزاري لمجموعة البلدان الثمانية لعام 1999 بشأن مكافحة الجريمة المنظمة عبر الوطنية.[2513] وكان من نتاج هذا الاجتماع مجموعة من المبادئ بشأن النفاذ العابر للحدود.[2514] وكان هذا على الأرجح من كافة الجوانب نموذج التنظيم الذي استعمله واضعو اتفاقية الجريمة السيبرانية، ومن ثم فهو يظهر جوانب كثيرة متماثلة.

6 النفاذ العابر للحدود إلى البيانات المخزنة لا يستلزم مساعدة قانونية.

على الرغم مما تحويه هذه المبادئ، يتعين على أي دولة الحصول على ترخيص من أي دولة أخرى عندما تعمل طبقاً لقوانينها الوطنية بغرض:

أ) النفاذ إلى بيانات متاحة للجمهور (مفتوحة المصدر)، أياً كان موقعها الجغرافي؛

ب) النفاذ أو البحث أو النسخ أو الحفاظ على بيانات مخزنة في نظام حاسوبي موجود في دولة أخرى، إذا كان ذلك بموجب موافقة قانونية وطوعية من الشخص الذي له السلطة القانونية في الكشف عن هذه البيانات. ينبغي للدولة القائمة بالبحث مراعاة إخطار الدولة الجاري فيها البحث، إذا كان القانون الوطني يسمح بهذا الإخطار وإذا أظهرت البيانات انتهاكاً للقانون الجنائي أو إذا تبين أن الأمر في صالح الدولة الجاري فيها البحث.

ويمكن الاختلاف الأساسي في إجراء الإخطار الوارد في المادة 6(ب). ويهدف الحكم إلى تبادل المعلومات. بيد أنه يمكن لهذا الحكم، بعد تعديلات طفيفة، أن يضمن علم الدولة المتأثرة بإجراء تحقيقات على أراضيها. ولن يحول هذا الأمر دون التعارض مع القانون الدولي، غير أنه يضمن درجة معينة من الشفافية على أقل تقدير.

شبكة نقاط الاتصال على مدار الساعة طوال اليوم (24/7)

تتطلَّب تحقيقات الجرائم السيبرانية في كثير من الأحيان تصرفاً فورياً.[2515] 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.[2516] ولزيادة سرعة التحقيقات الدولية تُبرز الاتفاقية بالجريمة السيبرانية أهمية التمكين من استعمال وسائل الاتصال العاجلة في المادة 25. ولزيادة تحسين كفاءة طلبات المساعدة المتبادلة يُلزم واضعو الاتفاقية المتعلقة بالجريمة السيبرانية الأطراف بتسمية نقطة اتصال لطلبات المساعدة المتبادلة تكون حاضرة بدون أي حدود من ناحية الوقت.[2517] وأكد واضعو الاتفاقية المتعلقة بالجريمة السيبرانية على أن إقامة نقاط الاتصال هو أداة من أهم الأدوات التي تنص عليها الاتفاقية.[2518] أظهر استعراض جرى مؤخراً لاستعمال نقاط هذه الشبكة في البلدان التي صدّقت على الاتفاقية المتعلقة بالجريمة السيبرانية ومع ذلك محدودية استعمالها إلى حد كبير.

المادة 35 – شبكة 24/7

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 بنُظم وبيانات حاسوبية، أو من أجل جمع الأدلة الخاصة بجريمة جنائية في شكل إلكتروني، وتشمل هذه المساعدة تسهيل، أو إذا كان القانون الوطني والإجراءات المتّبعة 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.

وتستند فكرة شبكة 24/7 إلى شبكة جهات الاتصال الموجودة حالياً طوال 24 ساعة لخدمة مكافحة الجرائم الدولية ذات التكنولوجيا العالية المتعلقة بالحاسوب التابعة لمجموعة الثمانية.[2519] وبإنشاء شبكة لنقاط الاتصال تعمل على مدى اليوم طوال الأسبوع يهدف واضعو الاتفاقية المتعلقة بالجريمة السيبرانية إلى معالجة تحديات مكافحة الجريمة السيبرانية – وخاصة التحديات التي تتصل بسرعة عمليات تبادل البيانات[2520] والتي تنطوي على بُعد دولي.[2521] ويلتزم أطراف الاتفاقية المتعلقة بالجريمة السيبرانية بإنشاء نقاط الاتصال المذكورة وكفالة تمكنها من القيام بإجراءات فورية وكذلك الحفاظ على الخدمة. وكما جاء في الفقرة الفرعية 3 من المادة 35 من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، يشمل ذلك توفُّر العاملين المدرَّبين والمزوَّدين بالأجهزة.

وفيما يتعلق بعملية إقامة نقطة الاتصال وخاصة المبادئ الأساسية لهذا الهيكل، تسمح الاتفاقية المتعلقة بالجريمة السيبرانية 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 المتعلقة بالجريمة السيبرانية كذلك إلى أن نقطة شبكة 24/7 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، هما 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: حفظ البيانات وجمع الأدلة والاستدلال على مكان المشتبه فيهم.

ومن المهم أيضاً في هذا السياق أن نبرز أن الاتفاقية المتعلقة بالجريمة السيبرانية 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،[2522] 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.[2523]

وقد أُشير صراحة في الاجتماع الثاني للجنة الاتفاقية المتعلقة بالجريمة السيبرانية إلى أن مشاركة شبكة اتصالات 24/7 لا يتطلب التوقيع أو التصديق على الاتفاقية المتعلقة بالجريمة السيبرانية.[2524]

وفي عام 2008، نشر مجلس أوروبا دراسة تحلل فعالية التعاون الدولي في مكافحة الجريمة السيبرانية.[2525] وفي عام 2009، أُجريت دراسة عن تشغيل نقاط الاتصال 24/7 الخاصة بالجريمة السيبرانية.[2526] ومن بين النتائج التي أفرزتها الدراستان أن البلدان التي صدّقت على الاتفاقية بشأن الجريمة السيبرانية لم تُنشئ جميعها نقاطاً عاملة في الشبكة 24/7 كما تنص الاتفاقية. وهناك نتيجة أخرى مفادها أن البلدان التي أنشأت هذه النقاط لا تستخدمها عادة إلا في أضيق الحدود مثل حفظ بيانات الحركة.

6.6.6 التعاون الدولي في سياق مشروع اتفاقية ستانفورد الدولية

اعترف واضعو مشروع اتفاقية ستانفورد[2527] الدولية ("مشروع ستانفورد") 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

- 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 السيبرانية. والاختلاف الرئيسي هو أن القواعد التنظيمية المنصوص عليها في الاتفاقية المتعلقة بالجريمة السيبرانية أشد صرامة وأكثر تعقيداً وأكثر دقة في التحديد مقارنة بمشروع ستانفورد. وكما أشار واضعو مشروع ستانفورد، فإن نهج الاتفاقية المتعلقة بالجريمة السيبرانية عملي بقدر أكبر ولذلك ينطوي على بعض المزايا الواضحة من منظور التطبيق الفعلي.[2528] وقرّر واضعو مشروع 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.[2529]

7.6 مسؤولية مقدمي خدمات الإنترنت

Bibliography (selected): *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Luotonen*, Web Proxy Servers, 1997; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Naumenko*, Benefits of Active Caching in the WWW, available at: http://lcawww.epfl.ch/Publications/Naumenko/Naumenko99.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: http://www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: http://www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

1.7.6 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.[2530] وبالإضافة إلى مقدِّم خدمة البريد الإلكتروني ينطوي الإرسال على مقدمي خدمة النفاذ وكذلك جهات التسيير وإرسال البريد الإلكتروني إلى المتلقي. وينطبق الأمر نفسه 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.[2531] 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.[2532]

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.[2533] والإجابة على هذا السؤال تتسم بأهمية حاسمة في سياق التطوير الاقتصادي للبنية التحتية لتكنولوجيا المعلومات والاتصالات، إذ إن مقدمي الخدمة لن يشغِّلوا خدماتهم إلا 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، حيث إن 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.

2.7.6 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.[2534] 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 إلا 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 المتلقِّين المنتظرين ولم يتم الاحتفاظ بمثل هذه النُسخة في النظام أو الشبكة بطريقة تجعل المتلقِّين 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).

[...]

ويستند الحكم إلى قانون حقوق الطبع الرقمية للألفية (DMCA) الذي تم توقيعه ليصبح قانوناً في عام 1998.[2535] وبإقامة نظام للملاذ الآمن استبعد القانون مسؤولية مقدمي بعض الخدمات من انتهاكات حقوق الطبع التي يرتكبها طرف ثالث.[2536] ومن المهم أولاً لهذا السياق إبراز أن جميع مقدمي الخدمة غير مشمولين بهذا التقييد.[2537] إذ إن تقييد المسؤولية ينطبق فقط على مقدمي الخدمة[2538] ومقدمي خدمة الإخفاء.[2539] 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؛
- ألا يختار مقدِّم الخدمة الأشخاص الذين يتلقَّون المادة؛
- ألا 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[2540]:

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 وبنيّة حسنة لتقييد النفاذ أو الحصول على مواد يعتبرها المقدّم 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).*
>
> *[...]*

ما يشترك فيه هذان النهجان، أي البندان 512 *أ)* من العنوان 17 من مدونة الولايات المتحدة والبند 230 ج) من العنوان 47 من مدونة الولايات المتحدة هو 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 يتبناه الاتحاد الأوروبي الذي يتبع نهجاً أكثر اتساعاً.

3.7.6 توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية

يعتبَر توجيه الاتحاد الأوروبي الخاص بالتجارة الإلكترونية[2541] مثالاً من أمثلة النهج التشريعي لتنظيم مسؤولية مقدمي خدمة الإنترنت. وفي مواجهة التحديات الناشئة عن البُعد الدولي للإنترنت قرَّر واضعو التوجيه صياغة معايير قانونية توفِّر إطاراً قانونياً للتطوير الشامل لمجتمع المعلومات، وبذلك يتم دعم التنمية الاقتصادية الشاملة وأعمال وكالات إنفاذ القانون.[2542] وتستند القاعدة التنظيمية المتعلقة بالمسؤولية إلى مبدأ المسؤولية المتدرجة.

ويتضمن التوجيه عدداً من الأحكام التي تحد من مسؤولية بعض مقدّمي الخدمة.[2543] وهذه الحدود تتصل بمختلف فئات الخدمات التي يشغِّلها مقدِّم الخدمة.[2544] 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 محدودية الاحتمالات تقنية، 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.

4.7.6 مسؤولية مقدّم خدمة النفاذ (توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية)

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.[2545]

القسم 4: مسؤولية موردي الخدمات الوسطاء

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 ألا 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 المرسَلة 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 تؤثّر هذه المادة على إمكانية قيام محكمة أو سلطة إدارية، وفقاً للأنظمة القانونية للدول الأعضاء، بمطالبة مقدّم الخدمة بإنهاء أو منع أي انتهاك.

ويشبه هذا النهج البند 512أ) من العنوان 17 من مدوّنة الولايات المتحدة.[2546] 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.

5.7.6 مسؤولية التخزين المؤقت (توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية)

يُستعمَل مصطلَح "التخزين المؤقت" 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.[2547] ويتمثل أحد التقنيات المستعملة لتقليل عرض النطاق في إنشاء مخدِّمات وكيلة.[2548] 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 المعترَف بها على نطاق واسع بشأن تحديث المعلومات.

المادة 13

"التخزين المؤقت"

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 بشأن التجارة الإلكترونية هي مثال آخر لأوجه التشابه بين الهيكل المتشدد للولايات المتحدة والنهج الأوروبية. ويشبه نهج الاتحاد البند 512 ب) من العنوان 17 من مدونة الولايات المتحدة.[2549] وتهدف اللائحتان إلى النص على مسؤولية مقدّمي خدمة الإخفاء ويربط هذان التنظيمان تحديد المسؤولية بمقتضيات متشابهة. وفي صدد مسؤولية مقدّمي الخدمة،[2550] 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.

6.7.6 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.[2551]

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.[2552] والإخفاق في التصرّف الفوري يؤدي إلى تحقُّق مسؤولية مقدّم خدمة الاستضافة.[2553]

المادة 14

الاستضافة

1 عندما يتم تقديم خدمة من خدمات مجتمع المعلومات تتألف من تخزين معلومات مقدّمة من متلقي الخدمة، تكفل الدول الأعضاء ألا 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.[2554]

7.7.6 مسؤولية مقدم خدمة الاستضافة (تنسيق سياسات تكنولوجيا المعلومات والاتصالات وتشريعاتها وإجراءاتها التنظيمية (HIPCAR))

هناك نهج آخر بشأن مسؤولية مقدمي خدمات الاستضافة يمكن الاطلاع عليه في النص التشريعي الذي وضعته الدول المستفيدة داخل المبادرة HIPCAR.[2555]

مقدم خدمة الاستضافة

30 (1) يعتبر مقدم خدمة الاستضافة غير مسؤول جنائياً عن المعلومات المخزنة بطلب من مستعمل للخدمة بشرط:

أ) أن يقوم سريعاً بحذف هذه المعلومات أو منع النفاذ إليها بعد تلقيه أمراً من أي سلطة عامة أو محكمة بحذف معلومات غير قانونية محددة؛

ب) أو أن يقوم بمجرد حصوله على معلومات أو معرفته بشأن معلومات غير قانونية محددة مخزنة، وذلك من خلال أي أساليب أخرى خلاف صدور أمر من سلطة عامة، بإبلاغ السلطة العامة سريعاً لكي يتسنى لها تقييم طبيعة هذه المعلومات وإصدار أمر بحذف محتواها إذا لزم الأمر.

(2) لا تُطبق الفقرة 1 إذا كان مستعمل الخدمة يعمل في ظل سلطة وتحكم مقدم خدمة الاستضافة.

(3) إذا قام مقدم خدمة الاستضافة بحذف محتوى بعد استلام أمر طبقاً للفقرة 1، يُعفى من الالتزامات التعاقدية تجاه العمل لضمان تيسُّر الخدمة.

وعلى غرار نهج الاتحاد الأوروبي تماماً، يحدّ الفصل 30(1)أ) من المسؤولية إذا قام مقدم خدمة الاستضافة بحذف المحتوى سريعاً بعد استلام أمر من أي سلطة عامة أو محكمة. وتعني كلمة سريعاً بوجه عام أن يتم ذلك في غضون أقل من

24 ساعة.[2556] ويمكن الإشارة إلى أن الاختلاف الرئيسي عن نهج الاتحاد الأوروبي يكمن في الفصل 30(1) ب). وخلافاً لنهج الاتحاد الأوروبي، لا تقع على كاهل مقدم الخدمة مسؤولية تحديد ما إذا كان المحتوى مثار الاهتمام قانونياً أم لا. فإذا تلقّى معلومة، فإن التزامه ينحصر بادئ ذي بدء في إبلاغ السلطة العامة (المعنية) عن المحتوى الذي يحتمل أن يكون غير قانوني. وحدد واضعو الحكم أن السلطات هي التي ينبغي لها أن تقرر طبيعة الحكم وأن تُصدر أمراً بحذف المحتوى.[2557] وإذا ما اعتبرت المعلومات غير قانونية، يتعيّن على مقدم الخدمة حذفها لتفادي المسؤولية.

8.7.6 الاستبعاد من الالتزام بالرصد (توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية)

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.

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، بناءً على طلبها، بمعلومات تمكّنها من تعيين متلقّي خدماتهم الذين يبرمون معهم اتفاقات تخزين.

9.7.6 المسؤولية عن وصلات الإحالة الإلكترونية (قانون التجارة الإلكترونية – النمسا)

تؤدّي وصلات الإحالة الإلكترونية دوراً هاماً في الإنترنت. فهي تمكّن مقدِّم 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. وتوفِّر وصلة الإحالة أمر لمتصفح شبكة الويب بفتح عنوان الإنترنت الموضوع في الوصلة.

أثناء صياغة توجيه الاتحاد الأوروبي نوقشت ضرورة وضع قاعدة تنظيمية بشأن وصلات الإحالة مناقشة مكثّفة.[2558] 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.[2559] وإلى أن يتم تعديل قاعدة تنظيمية بشأن المسؤولية عن وصلات الإحالة في المستقبل، فإن للدول الأعضاء حرية صياغة حلول وطنية.[2560] وقد قرّرت بعض بلدان الاتحاد الأوروبي معالجة مسؤولية مقدّمي وصلات الإحالة في حكم خاص.[2561] واستندت هذه البلدان في تقرير مسؤولية مقدّمي وصلات الإحالة إلى نفس المبادئ التي يتضمنها التوجيه الأوروبي بشأن مسؤولية مقدّمي خدمة الاستضافة.[2562] وهذا النهج هو نتيجة منطقية لتشابه حالة مقدّمي خدمة الاستضافة ومقدّمي وصلات الإحالة. ففي الحالتين يسيطر مقدِّم 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:[2563]

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.

10.7.6 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 إلا 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".[2564]

وكما يحدث في حالة وصلات الإحالة الإلكترونية لا يتضمن توجيه الاتحاد الأوروبي معايير تحدّد مسؤولية مشغّلي محركات البحث. ولذلك قرّرت بعض بلدان الاتحاد الأوروبي معالجة مسؤولية مقدّمي محرّكات البحث في نصّ خاص.[2565] وبعكس حالة وصلات الإحالة الإلكترونية، لم تستند جميع البلدان في تنظيمها إلى نفس المبادئ.[2566] فإسبانيا[2567] والبرتغال استندتا في تنظيمهما المتعلق بمسؤولية مشغّلي محرّكات البحث إلى المادة 14 من التوجيه في حين استندت النمسا[2568] 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 يعدِّل المعلومات المتضمّنة في الإرسال.

1479 For an overview of legal approaches, see also: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 18 *et seq.*, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1480 *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.

1481 *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 255.

1482 Four definitions are included in Art. 1 and an additional provision was included in Art. 9, Council of Europe Convention on Cybercrime.

1483 For more information related to legal approaches regulating the liability of access provider see below: § 6.7.4

1484 With regard to the lawful interception of communication see below: § 6.5.9.

1485 With regard to the liability of caching provider see below: § 6.7.5.

1486 For more details related to different legal approaches to criminalize child pornography see below: § 6.2.8.

1487 With regard to the criminalization of such conduct see below: § 6.2.7.

1488 Art. 2(a) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

1489 Art. 3(a) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

1490 Sec. 3(3) HIPCAR Model Legislative Text on Cybercrime.

1491 With regard to details of the criminalization see below: § 6.2.8.

1492 For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

1493 See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

1494 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

1495 *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

1496 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1497 Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1498 Art. 2(c) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

1499 Art. 20(2) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

1500 With regard to different approaches to criminalize data interference see below: § 6.2.5.

1501 Regarding the criminalization of data espionage/illegal data acquisition see below: § 6.2.3.

1502 Art. 1(b) Council of Europe Convention on Cybercrime, ETS 185.

1503 Art. 1(b) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1504 Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

1505 Sec. 3(5) HIPCAR Model Legislative Text on Cybercrime.

1506 Sec.3 (7) HIPCAR Model Legislative Text.

1507 *Stair/Reynolds/Reynolds*, Fundamentals of Information Systems, 2008, page 167; *Weik*, Computer science and communications dictionary, 2000, page 826; *Stair/Reynolds*, Principles of Information Systems, 2011, page 15.

1508 Art. 1(a) Council of Europe Convention on Cybercrime, ETS 185.

1509 Art. 1(a) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The Framework Decision uses the term „information" system instead of computer system.

1510 Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

1511 Sec. 3(4) HIPCAR Model Legislative Text on Cybercrime.

1512 Regarding attacks against critical infrastructure see above: § 1.2

1513 Regarding the related challenges see above: § 3.2.14.

1514 With regard to the legal response see below: § 6.5.11.

1515 Draft African Union Convention on the Establishment of a credible Legal Framework for Cyber Security in Africa, Version 1, January 2011.

1516 See below: § 6.2.15.

1517 See Art. 10 (1)(a) HIPCAR Model Legislative Text on Cybercrime.

1518 See below: § 6.2.6.

1519 With regard to the liability of different types of provider see below: § 6.7.

1520 Regarding the liability of search engines see below: § 6.7.10.

1521 With regard to illegal interception, see below: § 6.2.4.

1522 For more details related to the interference with computer data see below: § 6.2.5.

1523 With regard to system interference see below: § 6.2.6.

1524 See in this regard below: § 6.2.14.

1525 See below: § 6.5.12.

1526 Regarding the different legal approaches to seize evidence see below: § 6.5.6.

1527 See in this regard Art. 19 (3) Council of Europe Convention on Cybercrime.

1528 Sec. 3 Commonwealth Model Law on Computer and Computer-related Crime.

1529 Sec. 3(17) HIPCAR Model Legislative Text on Cybercrime.

1530 See below: § 6.5.9.

1531 Art. 1 Council of Europe Convention on Cybercrime.

1532 Sec. 3(18) HIPCAR Model Legislative Text on Cybercrime.

1533 *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriontе*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

1534 These range from the simple proof that technical protection measures can be circumvented, to the intent to obtain data stored on the victim computer. Even political motivations have been discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

1535 Regarding the independence of place of action and the location of the victim, see above § 3.2.7.

1536 These can, for example, be passwords or fingerprint authorization. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of potential tools, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

1537 Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is also highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

1538 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 729.

1539 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "The need for protection reflects the interests of organizations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

1540 With regard to data espionage, see above, § 2.5.2 and below, § 6.1.3.

1541 With regard to data interference, see above, § 2.5.4 and below, § 6.1.5.

1542 *Sieber*, Informationstechnologie und Strafrechtsreform, page 49 *et seq.*

1543 For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

1544 Art. 2 of the Convention on Cybercrime enables the Member States to keep those existing limitations that are mentioned in Art. 2, sentence 2. Regarding the possibility of limiting criminalization, see also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

1545 An example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). This provision was changed in 2007. The following text presents the old version:

Section 202a – Data Espionage

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

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

1546 This approach is not only found in national legislation, but was also recommended by Council of Europe Recommendation No. (89) 9.

1547 For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

1548 Regarding the system of reservations and restrictions, see *Gercke*, The Convention on Cybercrime, Computer Law Review International, 2006, 144.

1549 *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1550 With regard to software tools that are designed and used to carry out such attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf. With regard to Internet-related social engineering techniques, see the information offered by the anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1551 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

1552 The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5 per cent of the respondents reported that 80-100 per cent of their losses were caused by insiders. Nearly 40 per cent of all respondents reported that between 1 per cent and 40 per cent of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: www.gocsi.com/.

1553 Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

1554 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

1555 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1556 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39

1557 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1558 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

1559 *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, page 7.

1560 See for example: World Information Technology And Services Alliance (WITSA), Statement On The Council Of Europe Draft Convention On Cybercrime, 2000, available at: www.witsa.org/papers/COEstmt.pdf. Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

1561 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62 (dealing with Article 4).

1562 *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

1563 This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

1564 *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1565 Article 42 – Reservations: By a written notification addressed to the Secretary-General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

1566 This limits the criminalization of illegal access to those cases where the victim used technical protection measures to protect its computer system. Access an unprotected computer system would therefore not be considered a criminal act.

1567 The additional mental element/motivation enables Member States to undertake a more focused approach rather than implementing a criminalization of the mere act of hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

1568 This enables Member States to avoid a criminalization of cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

1569 Framework Decision on Attacks against Information Systems – 19 April 2002 – COM (2002) 173. For more details, see above: § 5.2.1.

1570 Article 2 – Illegal access to information systems:

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

1571 Model Law on Computer and Computer Related Crime, LMM(02)17, available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1572 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1573 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1574 EU Directive 2013/40/EU on attacks against information systems.

1575 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78

1576 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1577 See *Sofaer/Goodman/Cuellar/Drozdova and others*. A Proposal for an International Convention on Cybercrime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1578 In this context, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

1579 Standalone computer systems are covered by Art. 1, paragraph 3, of the Draft Convention because they "control programs". This does not require a network connection.

1580 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1581 Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1582 The Explanatory Report points out that the provision intends to criminalize violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1583 See below: § 6.1.4.

1584 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

1585 One key indication of the limitation of application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet, which do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral*

telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights." See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1586 See in this context especially a recent case from Hong Kong, People's Republic of China. See above: § 2.5.2.

1587 ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1588 Regarding the challenges related to the use of encryption technology by offenders, see above: § 3.2.14; *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf; *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html. Regarding the underlying technology, see: *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

1589 One of the consequences related to this aspect is the fact that limitation of the criminalization of illegal access to those cases where the victim of the attack secured the target computer system with technical protection measures could limit the application of such a provision, insofar as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

1590 Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996). See in this context: *Chamblee*, Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 *et seq.*), 177 A.L.R. Fed. 609 (2002); *Fischer*, An Analysis of the Economic Espionage Act of 1996, 25 Seton Hall Legis. J. 239 (2001).

1591 *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 986, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

1592 For details, see: US CCIPS, Prosecuting Intellectual Property Crimes, 3rd Edition, 2006, page 138 *et seq.* available at: www.justice.gov/criminal/cybercrime/ipmanual/04ipma.pdf.

1593 *Loundy*, Computer Crime, Information Warfare, and Economic Espionage, 2009, page 55 *et seq.*; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.* available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

1594 *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 988, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

1595 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1596 The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1597 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1598 This provision has recently been modified and now even criminalizes illegal access to data. The previous version of the provision has been used here, because it is better suited for demonstrating the dogmatic structure.

1599 See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

1600 A similar approach of limiting criminalization to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention on Cybercrime: *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.* For more information, see above: § 6.1.1.

1601 This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement, self-protection measures.

1602 See in this context for example a recent case in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from

laptop tell a tawdry tale, The Sydney Morning Herald, 14.02.2008, available at: www.smh.com.au/news/web/stolen-photos-from-laptop-tell-a-tawdry-tale/2008/02/14/1202760468956.html; *Pomfret*, Hong Kong's Edision Chen quits after sex scandal, Reuters, 21.02.2008, available at: www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

1603 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1604 With regard to "phishing", see above: § 2.9.4 and below: § 6.1.15 and as well: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Phishing, Computer und Recht, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

1605 Regarding the risks related to the use of wireless networks, see above: § 3.2.3. Regarding the difficulties in cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

1606 Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1607 Regarding the underlying technology and the security related issues, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx. With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

1608 The computer magazine ct reported in 2004 that field tests proved that more than 50 per cent of 1 000 wireless computer networks that were tested in Germany were not protected. See: www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182.

1609 Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx.

1610 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1611 Regarding identity theft, see above: § 2.8.3 and below: § 6.1.16 and also: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1612 In the United States, the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes. Regarding offences related to social-security numbers, see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

1613 See: *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1, page 112.

1614 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1615 The Explanatory Report describes the technical means more in detail: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalization." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

1616 Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering".

1617 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

1618 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1619 See above: § 6.1.3.

1620 "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 55.

1621 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

1622 Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue, see Explanatory Report, No. 57: *"The creation of an offence in relation to "electromagnetic emissions" will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as "data" according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision"*, Explanatory Report to the Council of Europe Convention on Cybercrime, No. 57.

1623 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1624 *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1625 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 54.

1626 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39

1627 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1628 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1629 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1630 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1631 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1632 Cookies are data sent by a server to a browser and then sent back each time the browser is used to access the server. Cookies are used for authentication, tracking and keeping user information. Regarding the functions of cookies and the controversial legal discussion, see: *Kesan/Shah*, Deconstruction Code, Yale Journal of Law & Technology, 2003-2004, Vol. 6, page 277 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

1633 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1634 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1635 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1636 Model Law on Computer and Computer Related Crime" LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1637 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1638 The difficulty with offences against the integrity of data is that identification of these violations is often difficult to prove. Therefore, the Expert Group which drafted the Convention on Cybercrime identified the possibility of prosecuting violations regarding data interference by means of criminal law as a necessary strategic element in the fight against cybercrime. Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

1639 The 2007 Computer Economics Malware Report focuses on computer crime and analyses the impact of malware on the worldwide economy by summing up the estimated costs caused by attacks. It identified peaks in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion). For more information, see: 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code. A summary of the report is available at: www.computereconomics.com/article.cfm?id=1225.

1640 A number of computer fraud scams are including the manipulation of data – e.g. the manipulation of bank-account files, transfer records or data on smart cards. Regarding computer related fraud scams, see above: § 2.8.1 and below: § 6.1.17.

1641 Regarding the problems related to these gaps, see for example the LOVEBUG case, where a designer of a computer worm could not be prosecuted due to the lack of criminal law provisions related to data interference. See above: § 2.5.4 and: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1642 A similar approach to Art. 4 of the Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 – Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

1643 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

1644 As pointed out in the Explanatory Report, the two terms overlap. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1645 Regarding the more conventional ways to delete files using Windows XP, see the information provided by Microsoft, available at: www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

1646 Regarding the consequences for forensic investigations, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq.*, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1647 See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/05hb003.pdf.

1648 The fact that the Explanatory Report mentions that the files are unrecognizable after the process does not give any further indication with regard to the interpretation of the term. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1649 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1650 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf. In 2000 a number of well-known US e-commerce businesses were targeted by DoS attacks. A full list is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1651 With regard to the criminalization of DoS attacks, see also below: § 6.1.6.

1652 In addition, criminalization of DoS attacks is provided by Art. 5 of the Convention on Cybercrime. See below: § 6.1.6.

1653 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

1654 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Regarding the different recognized functions of malicious software, see above: § 2.5.4. Regarding the economic impact of malicious software attacks, see above: § 2.5.4.

1655 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1656 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1657 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report states: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1658 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62: "The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g., encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right." Regarding the liability of

Remailer, see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1659 For further information, see *du Pont*, The Time Has Come For Limited Liability For Operators Of True Anonymity Remailers In Cyberspace: An Examination Of The Possibilities And Perils, Journal Of Technology Law & Policy, Vol. 6, Issue 2, page 176 *et seq.*, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1660 With regard to the possible difficulties to identify offenders who have made use of anonymous or encrypted information, the Convention leaves the criminalization of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

1661 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1662 For further information, see: *Gercke*, The EU Framework Decision on Attacks against Information Systems, Computer und Recht 2005, page 468 *et seq.*

1663 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1664 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1665 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1666 Sec. 5 (Illegal access), Sec. 8 (Illegal interception) and Sec. 10 (Child pornography).

1667 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cybercrime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1668 ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1669 A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see above: § 2.5.4 and US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

1670 For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, Inferring Internet Denial-of-Service Activities, page 1, available at: www.caida.org/papers/2001/BackScatter/usenixsecurity01.pdf; CNN News, One year after DoS attacks, vulnerabilities remain, at: http://edition.cnn.com/2001/TECH/internet/02/08/ddos.anniversary.idg/index.html. *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1671 Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: Campbell/Gordon/Loeb/Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, pages 431-448.

1672 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding cyberterrorism, see above § 2.9.1 and *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyberterrorism and Cybersecurity, available at: www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeld*t, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: *Prados*, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 et *seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.* OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf; *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, pages 221-249.

1673 The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 65.

1674 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1675 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1676 The Explanatory Report gives examples for implementation of restrictive criteria for serious hindering: "Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate "denial-of-service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)" – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 67.

1677 *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Although the connotation of "serious" does limit the applicability, it is likely that even serious delays to operations resulting from attacks against a computer system can be covered by the provision.

1678 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

1679 Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection.

1680 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61. Regarding the fact that the definition does not distinguish between the different ways how information can be deleted, see above: § 6.1.15. Regarding the impact of the different ways of deleting data on computer forensics, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq*., available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

1681 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1682 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is therefore likely that the provision could cover unauthorized corrections of faulty information as well.

1683 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1684 "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam legislation worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: § 2.5.g.

1685 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

1686 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1687 Regarding legal approaches in the fight against spam, see above: § 6.1.l3.

1688 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

1689 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1690 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1691 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1692 See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

1693 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 68: "The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized by this article, even if it causes serious hindering."

1694 Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

1695 Article 3 – Illegal system interference: "Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor".

1696 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1697 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1698 Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), PC-CY (2000), 19, available at: www.iwar.org.uk/law/resources/eu/cybercrime.htm.

1699 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime

and Terror, page 225, available at: http://media.hoover.org/ documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1700 For an overview on hate speech legislation, see for example: the database provided at: www.legislationline.org. For an overview on other cybercrime-related legislation, see: the database provided at: www.cybercrimelaw.net.

1701 Regarding the challenges of international investigation, see above: § 3.2.4 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1702 For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

1703 *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 5.

1704 Regarding the influence of pornography on minors, see: *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact, and Prevention, Youth & Society, Vol. 34, 2003, page 330 *et seq.*, available at: www.unh.edu/ccrc/pdf/Exposure_risk.pdf; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002, available at: http://findarticles.com/p/articles/mi_m2372/is_1_39/ai_87080439.

1705 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".

1706 *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 28.

1707 The draft law was not in force by the time this publication was finalized.

1708 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1709 Regarding the challenges of international investigation, see above: § 3.2.4. See also: *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1710 *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.

1711 Regarding methods of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication, see above: § 3.2.14.

1712 It has been reported that some websites containing child pornography register up to a million hits per day. For more information, see: *Jenkins*, Beyond Tolerance: Child Pornography on the Internet, 2001, New York University Press; *Wortley/Smallbone*, Child Pornography on the Internet, page 12, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1713 Regarding the challenges related to investigations involving anonymous communication technology, see above: § 3.2.l.

1714 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

1715 *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 68.

1716 *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11, page 6, available at: http://jjlp.law.ucdavis.edu/archives/vol-11-no-1/07%20Liu%2011.1.pdf.

1717 *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 69.

1718 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

1719 *Akdeniz* in *Edwards/Waelde*, Law and the Internet: Regulating Cyberspace; *Williams* in *Miller*, Encyclopaedia of Criminology, page 7. Regarding the extent of criminalization, see: Child Pornography: Model Legislation & Global Review, 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalization of child pornography and freedom of speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws in terms of the criminalization of child pornography.

1720 Regarding differences in legislation, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 26, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

1721 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

1722 *Walden*, Computer Crimes and Digital Investigations, 2006, page 144.

1723 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 94.

1724 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, ETS 201.

1725 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 135.

1726 See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

1727 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 95.

1728 Regarding criminalization of the possession of child pornography in Australia, see: *Krone*, Does thinking make it so? Defining online child pornography possession offences, in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalization of child pornography.

1729 See: Child Pornography: Model Legislation & Global Review, 2006, page 2, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

1730 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 98.

1731 *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

1732 Based on the National Juvenile Online Victimization Study, only 3 per cent of arrested Internet-related child-pornography possessors had morphed pictures. *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

1733 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 102.

1734 *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

1735 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1736 Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1737 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.

1738 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)...".

1739 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.

1740 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, available at: http://conventions.coe.int.

1741 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

1742 For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

1743 See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

1744 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1745 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.

1746 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1747 *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

1748 Regarding the challenges related to the use of encryption technology, see above: § 3.2.14. One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

1749 See Explanatory Report to the Convention on the Protection of Children, No. 140.

1750 The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or is just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

1751 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1752 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].

1753 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.

1754 See the preface to the Optional Protocol.

1755 See Art. 2.

1756 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1757 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1758 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1759 See in this regard: *Powell*, Paedophiles, Child Abuse and the Internet, 2007; *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010, available at: www.cse.dmu.ac.uk/~bstahl/index_html_files/2010_grooming_ICIS.pdf.

1760 See: Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

1761 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

1762 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

1763 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 157.

1764 Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 159.

1765 International Mechanisms for Promoting Freedom of Expression, Joint Declaration, Challenges to Freedom of Expression in the New Century, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2001.

1766 For an overview of hate speech legislation, see the database provided at: www.legislationline.org.

1767 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1768 Regarding the criminalization of hate speech in Europe, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 781 *et seq.* available at: http://law.wlu.edu/deptimages/Law%20Review/62-2VanBlarcum.pdf. Regarding the situation in Australia, see: *Gelber/Stone*, Hate Speech and Freedom of Speech in Australia, 2007.

1769 Vienna Summit Declaration, 1993, available at: www.coe.int/t/dghl/monitoring/ecri/archives/other_texts/2-vienna/plan_of_action/plan_of_action_vienna_summit_EN.asp.

1770 Recommendation No. 1275 on the fight against racism, xenophobia, anti-Semitism and intolerance.

1771 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."

1772 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

1773 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1774 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

1775 Regarding the list of states that signed the Additional Protocol, see above: § 5.2.1.

1776 Regarding the difficulties related to the jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

1777 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at: www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1778 Regarding the challenges of international investigation, see above: § 3.2.5 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1779 Regarding possible reservations, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 792

1780 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

1781 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

1782 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

1783 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 29.

1784 Regarding the definition of "distributing" and "making available", see § 6.1.8 above.

1785 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 34.

1786 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of

Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1787 Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 36.

1788 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1789 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1790 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1791 Regarding legislation on blasphemy, as well as other religious offences, see: Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf.

1792 International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2006.

1793 See above: § 6.1.9, as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

1794 The draft law was not in force at the time this publication was finalized.

1795 Prevention of Electronic Crimes Ordinance 2007, available at: www.upesh.edu.pk/net-infos/cyber-act08.pdf.

1796 Prevention of Electronic Crimes Ordinance, 2007, published in the Gazette of Pakistan, Extraordinary, Part-I, dated 31 December 2007, available at: www.na.gov.pk/ordinances/ord2008/elect_crimes_10042008.pdf.

1797 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1798 Regarding the difficulties related to jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

1799 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

1800 Regarding the challenges of international investigation, see above: § 3.2.6 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1801 The 2005 e-gaming data report estimates total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm. Regarding the number of licensed Internet websites related to Internet gambling in selected countries, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 52, available at: www.gao.gov/new.items/d0389.pdf. Regarding the total numbers of Internet gambling websites, see: *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf.

1802 For an overview of different national Internet gambling legislation, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

1803 Regarding the situation in the People's Republic of China, see for example: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

1804 Regarding addiction, see: *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: www.european-lotteries.org/data/info_130/Wood.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

1805 See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

1806. See *Thumm*, Strafbarkeit des Anbietens von Internetglucksspielen gemaess § 284 StGB, 2004.

1807 Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which do not know that their services are abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

1808 For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously, criminalization is limited to those cases where the offender is intentionally making the equipment available.

1809 This is especially relevant with regard to the location of the server.

1810 Avoiding the creation of safe havens is a major intention of harmonization processes. The issue of safe havens has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 states that: "*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "*There must be no safe havens for those who abuse information technologies*".

1811 With regard to the principle of sovereignty, changing the location of a server can have a great impact on the ability of law-enforcement agencies to carry out an investigation. National Sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

1812 Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene, see above: §§ 3.2.6 and 3.2.7.

1813 For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

1814 Regarding the vulnerability of Internet gambling to money laundering, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 5, 34 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

1815 Regarding other recent approaches in the United States, see: *Doyle*, Internet Gambling: A Sketch of Legislative Proposals in the 108th Congress, CRS Report for Congress No. RS21487, 2003, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-4047: *Doyle*, Internet Gambling: Two Approaches in the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

1816 For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII, page 1183 *et seq.*, available at: http://law.fordham.edu/publications/articles/600flspub8956.pdf.

1817 *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

1818 *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm

1819 Based on Sec. 5366, criminalization is limited to the acceptance of financial instruments for unlawful Internet gambling.

1820 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.

1821 See: EU opens investigation into US Internet gambling laws, EU Commission press release, 10.03.2008, available at: http://ec.europa.eu/trade/issues/respectrules/tbr/pr100308_en.htm; *Hansen*, EU investigates DOJ internet gambling tactics, The Register, 11.03.2008, available at: www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

1822 See above: § 3.2.I.

1823 See above: § 3.2.2.

1824 See, for example: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US delegation to OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: 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: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf; *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

1825 See, for example, the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information, see: www.osce.org/documents/rfm/2004/10/14893_en.pdf. See in addition the statement of the representative on Freedom of the Media, Mr Haraszti, at the fourth Winder Meeting of the OSCE Parliamentary Assembly on 25 February 2005.

1826 Regarding various regional approaches to criminalization of defamation, see: *Greene* (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf.

1827 For more details, see: the British Crime Survey 2006/2007 published in 2007, available at: www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

1828 See: Crime Statistic Germany (Polizeiliche Kriminalstatistik), 2006, available at: www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

1829 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: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf.

1830 The full text of the Criminal Code of Queensland, Australia is available at: www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

1831 The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see: www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails are spam. See: http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

1832 For more information on the phenomenon, see above: § 2.6.7. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1833 Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf

1834 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.

1835 Regarding the availability of filter technology, see: *Goodman,* Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam Consumer Perspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

1836 Spam Issues in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1837 See Spam Issues in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

1838 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1839 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."

1840 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1841 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1842 The document available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1843 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1844 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1845 Regarding the US legislation on spam, see: *Sorkin*, Spam Legislation in the United States, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Warner*, Spam and Beyond: Freedom, Efficiency, and the Regulation of E-mail Advertising, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Alongi*, Has the US conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 *et seq.*, available at: www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

1846 For more details about the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM act 2003), see: www.spamlaws.com/f/pdf/pl108-187.pdf.

1847 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).

1848 For more details, see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

1849 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.

1850 Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

1851 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.

1852 One example is the 2001 EU Framework Decision combating fraud and counterfeiting of non-cash means of payment.

1853 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".

1854 With the definition of "distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report, No. 72), the drafters of the Convention restrict devices to software. Although the Explanatory Report is not definitive in this matter, it is likely that it covers not only software devices, but hardware tools as well.

1855 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1856 See, in this context: *Biancuzzi*, The Law of Full Disclosure, 2008, available at: www.securityfocus.com/print/columnists/466.

1857 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

1858 See for example one approach in the US legislation:

18 USC. § 1029 (Fraud and related activity in connection with access devices)

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both. […]

1859 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1860 This approach could lead to broad criminalization. Therefore Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

1861 Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

1862 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1863 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”.

1864 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society.

1865 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.

1866 Regarding the US approach to address the issue, see for example 18 USC. § 2512 (2):

(2) It shall not be unlawful under this section for –

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

1867 *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1868 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'."

1869 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 731.

1870 See, for example, the World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

1871 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1872 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

1873 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.

1874 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 77.

1875 For more information, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 78.

1876 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: 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: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1877 Expert Group's suggestion for an amendment:

Paragraph 3:

A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.

Official Note: Subsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.

1878 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.

1879 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1880 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1881 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1882 "Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating." See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1883 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1884 See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

1885 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.

1886 See for example 18 USC. § 495:

Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or

Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited –

Shall be fined under this title or imprisoned not more than ten years, or both.

Or Sec. 267 German Penal Code:

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:

1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;

2. causes an asset loss of great magnitude;

3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or

4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

1887 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 82.

1888 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."

1889 See Art. 1 (b) Convention on Cybercrime.

1890 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

1891 For example, by filling in a form or adding data to an existing document.

1892 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

1893 With regard the definition of "alteration" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1894 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1895 With regard the definition of "suppression" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1896 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1897 With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1898 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1899 If only part of a document is deleted the act might also be covered by the term "alteration".

1900. Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1901 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1902 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.

1903 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 85.

1904 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development,

Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1905 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1906 See, for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: http://edition.cnn.com/2006/US/05/18/identity.theft/; Identity Fraud, NY Times Topics, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html; *Stone*, US Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

1907 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.

1908 See, for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the US: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

1909 Regarding the phenomenon of identity theft, see above: § 2.8.3.

1910 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

1911 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

1912 *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.*

1913 *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

1914 This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data, see: *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007, available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1 ; ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

1915 The reason for the success is the fact that the provisions focus on the most relevant aspect of phase 1: transfer of the information from the victim to the offender.

1916 Examples of acts that are not covered include the illegal access to a computer system in order to obtain identity related information.

1917 One of the most common ways the information obtained is used is fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1918 Furthermore, it is uncertain whether the provisions criminalize possession if the offender does not intend to use the data but to sell them. Prosecution could in this case in general be based on fact that 18 USC. § 1028 not only criminalizes possession with the intent to use it to commit a crime, but also to aid or abet any unlawful activity.

1919 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1920 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1921 See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

1922 Similar provisions are included in the Commonwealth Model Law and the Stanford Draft International Convention. For more information about the Commonwealth model law, see: Model Law on Computer and Computer Related Crime, LMM(02)17. The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Stanford Draft International Convention, see: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1923 See above: § 6.1.1.

1924 See above: § 6.1.4.

1925 See above: § 6.1.5.

1926 *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

1927 See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

1928 See above: § 2.8.1.

1929. Regarding the criminalization of computer-related fraud in the UK, see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 *et seq.*

1930 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.

1931 A national approach that is explicitly address computer-related fraud is 18 USC. § 1030:

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

1932 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

1933 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.

1934 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

1935 With regard to the definition of "alteration" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1936 With regard to the definition of "suppression" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1937 With regard to the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1938 As a result, not only data-related offences, but also hardware manipulations, are covered by the provision.

1939 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 87.

1940 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 88.

1941 "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."

1942 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.

1943 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.

1944 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

1945 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers

Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1946 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1947 Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

1948 For more information on the effects of digitization on the entertainment industry, see above: § 2.7.1.

1949 The technology that is used is called digital rights management – DRM. The term digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies or other digital data. One of the key functions is copy protection, which aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

1950 Regarding the technical approach to copyright protection, see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

1951 For details see above: § 2.7.1.

1952 Examples are 17 USC. § 506 and 18 USC. § 2319:

Section 506. Criminal offenses

(a) Criminal Infringement. — Any person who infringes a copyright willfully either –

(1) for purposes of commercial advantage or private financial gain, or

(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.

[...]

Section 2319. Criminal infringement of a copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506(a)(1) of title 17 –

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;

(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.

(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements shall include –

(A) producers and sellers of legitimate works affected by conduct involved in the offense;

(B) holders of intellectual property rights in such works; and

(C) the legal representatives of such producers, sellers, and holders.

(e) As used in this section –

(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and

(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) an (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.

Regarding the development of legislation in the United States, see: *Rayburn*, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

1953 Regarding the international instruments, see: *Sonoda*, Historical Overview of Formation of International Copyright Agreements in the Process of Development of International Copyright Law from the 1830s to 1960s, 2006, available at: www.iip.or.jp/e/summary/pdf/detail2006/e18_22.pdf; *Okediji*, The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, 2006, available at: www.unctad.org/en/docs/iteipc200610_en.pdf. Regarding international approaches to anti-circumvention laws, see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

1954 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 109.

1955 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."

1956 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."

1957 Explanatory Report to the Council of Europe Convention on Cybercrime, Nos. 16 and 108.

1958 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

1959 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 113.

1960 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 114.

1961. 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.

1962 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.

1963 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1964 See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1965 See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

1966 See, for example, Art. 5 of the Convention on Cybercrime.

1967 Convention on Cybercrime, ETS 185.

1968 Council of Europe Convention on the Prevention of Terrorism, ETS 196.

1969 Council of Europe Convention on the Prevention of Terrorism, ETS 196.

1970 EU Framework Decision on Combating Terrorism, COM (2007) 650.

1971 EU Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

1972 EU Framework Decision 2008/919/JHA of 28 November 2008, No. 4.

1973 The intention of the drafters to cover online and offline activities was highlighted several times. See, for example: EU Framework Decision 2008/919/JHA of 28 November 2008, No. 11. "These forms of behavior should be equally punishable in all Member States irrespective of whether they are committed through the Internet or not."

1974 Regarding the motivation, see: *Russell*, A History of the United Nations Charter, 1958.

1975 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

1976 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 59.

1977 *Mani*, Basic Principles of Modern International Law: A Study of the United Nations Debates on the Principles of International Law Concerning Friendly Relations and Co-operation among States, 1993, page 263 *et seq.*

1978 *Bond*, Peacetime foreign Data Manipulations as one Aspect of Offensive Information Warfare, 1996.

1979 *Brownlie*, International Law and the Use of Force, 1993, page 362.

1980 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 80.

1981 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyber force, Alb. Law Journal of Science and Technology, Vol. 18, page 304.

1982 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

1983 *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1 000 Centrifuges at the Nataz Enrichment Plant?, Preliminary Assessment, Institute for Science and International Security, 2010.

1984 Regarding proliferation concerns, see: *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 58.

1985 With regard to the development, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

1986 *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.

1987 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 6.

1988 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

1989 Regarding the admissibility and reliability of digital images, see: *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy, page 267 *et seq.*

1990 *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7, page 71 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 14. Regarding the legal frameworks in different countries, see: *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 76; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213.

1991 See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

1992 For a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

1993 The Council of Europe Convention on Cybercrime therefore contains a provision that clarifies that the procedural instruments in the Convention shall not only be applicable with regard to cybercrime-related offences, but also to "other criminal offences committed by means of a computer system" and "the collection of evidence in electronic form of a criminal offence" (Art. 14).

1994 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

1995 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

1996 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

1997 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq*

1998 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 1.

1999 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

2000 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286. With more reference to national law: *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213; *Vaciago*, Digital Evidence, 2012, Chapter I.1 (with an overview about the discussion about digital evidence in different jurisdictions).

2001 Police and Criminal Evidence Code (PACE).

2002 *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

2003 Regarding the different models of cybercrime investigation, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

2004 This includes the development of investigation strategies.

2005 The second phase covers, in particular, the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2006 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.

2007 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

2008 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

2009 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.

2010 *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.

2011 This includes, for example, the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

2012 *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.

2013 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59

2014 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

2015 *Vaciago*, Digital Evidence, 2012, Chapter II.

2016 *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of

Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

2017 Regarding geo-recognition, see: *Friedland/Sommer*; Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, available at: www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf; *Strawn*, Expanding the Potential for GPS Evidence Acquisition, Small Scale Digital Device Forensics Journal, 2009, Vol. 3, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V3_1_Strawn.pdf; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

2018 See *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010, page 95 *et seq.*, available at: www.dfrws.org/2010/proceedings/2010-311.pdf.

2019 Regarding the use of metadata for investigations, see: *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf.

2020 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

2021 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217. Regarding the challenges of witnesses as a source of evidence, see: *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002.

2022 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2023 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.

2024 Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

2025 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161.

2026 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2027 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2028 Daubert v. Merrell Dow Pharmaceutical, Inc. (1993) 113 S. Ct. 2786, available at: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=509&invol=579.

2029 *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3, page 1.

2030 The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

2031 Regarding the status of national legislation, see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

2032 *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.

2033 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

2034 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

2035 *Casey*, Digital Evidence and Computer Crime, 2004, page 15.

2036 *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2Dpage 38F31AF079F9.pdf; With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2037 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf. Criteria for Admissibility of Expert Opinion, Utah Law Review, 1978, page 546 *et seq.*

2038 *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.

2039 See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39

2040 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

2041 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2042 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2043 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

2044 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 92.

2045 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

2046 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2047 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2048 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

2049 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2050 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2051 For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

2052 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2053 *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

2054 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

2055 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2056 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

2057 Regarding the design of courtrooms, see: *Youngblood*, Courtroom Design, 1976; *Smith/Larson*, Courtroom design, 1976.

2058 Scientific Evidence Review: Admissibility of Expert Evidence, ABA, 2003, page 159 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 169; *Nilsson*, Digital Evidence in the Courtroom, 2010; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12, Issue 1.

2059 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2060 See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 538.

2061 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

2062 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

2063 *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

2064 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 218

2065 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

2066 See in this context: *Nikali*, The Substitution of Letter Mail in Targeted Communication, 2007, available at: http://hsepubl.lib.hse.fi/pdf/diss/a136.pdf.

2067 See in this context *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Hayes*, Forensic Handwriting Examination, 2006.

2068 *Houck/Siegel*, Fundamentals of Forensic Science, 2010, page 512 *et seq.*; FBI Handbook of Crime Scene Forensics, 2008, page 111 *et seq.*; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962, Vol. 7, Issue 3, page 286 *et seq.*; *Miller*, An Analysis of the Identification Value of Defects in IBM Selectric Typewriters, American Academy of Forensic Science annual meeting, presented paper, Ohio, 1983; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007, page 207 *et seq.*

2069 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

2070 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

2071 *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No. 1, page 16 *et seq.*, available at: http://airccse.org/journal/nsa/0409s2.pdf.

2072 *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.

2073 Regarding approaches to link a suspect to stored computer records, see for example: *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 165.

2074 Regarding the obligation to register prior to the use of public Internet terminals in Italy, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, page 94.

2075 See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at

www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

2076 Regarding a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

2077 Regarding the extent of commercial child pornography, see: IWF 2007 Annual and Charity Report, page 7.

2078 See *Schnabel,* The Mikado Principle, Datenschutz und Datensicherheit, 2006, page 426 *et seq.*

2079 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 206.

2080 Regarding the legitimacy principle, see: *Grans/Palmer*, Australian Principles of Evidence, 2005, page 10.

2081 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 219.

2082 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.

2083 *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

2084 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

2085 Regarding necessary procedures, see: *Chawki*, The Digital Evidence in the Information Era, available at: www.droit-tic.com/pdf/digital_evid.pdf; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2086 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2087 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

2088 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2089 See in this context also: *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

2090 Regarding the consequences of the fruit of the poisonous tree doctrine for computer-crime investigations, see: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 563.

2091 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

2092 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.

2093 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332.

2094 *Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563, [2001] EMLR 654. The primary evidence rule was in any event inapplicable to recordings on film or tape, which may be proven by copies under common law (*Kajala v Noble* (1982) 75 Cr App Rep 149, DC; R v. Wayte (1982) 76 Cr App Rep 110, CA) and if lost or destroyed their contents may be proven by oral evidence from persons who have previously viewed or heard them (*Taylor v Chief Constable of Cheshire* [1987] 1 All ER 225, 84 Cr App Rep 191, DC). Also, see now the Criminal Justice Act 2003 s 133; and para 1464 post.

2095 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; *Permanent Trustee Co of New South Wales v Fels* [1918] AC 879, PC.

2096 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; The admission of documentary copies is subject to the Civil Evidence Act 1995: see PARA 808 *et seq.*

2097 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2098 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2099 With regard to different exemptions, see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 *et seq.*; Best Evidence Rule, California Law Review Commission, 1996, available at: www.clrc.ca.gov/pub/Printed-Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2100 For further reference, see: *Eltgroth*, Best Evidence and the Wayback Machine, Fordham Law Review, 2009, 193, available at: http://law.fordham.edu/assets/LawReview/Eltgroth_October_2009.pdf

2101 With regard to European common law countries (UK, Ireland), this development was especially supported by EU Directive 1999/93/EC. See also Sec. 4 and 6 of the Commonwealth model law on electronic evidence.

2102 *Munday*, Evidence, 2007, page 380; *Allen*, Practical Guide to Evidence, 2008, page 189.

2103 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567.

2104 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567 and *R v Sharp* [1988] 1WLR 7, HL; *R v Kearley* [1992] 2 AC 228, [1992] 2 All ER 345. HL. See also Civil Evidence Act 1995 ss1-7.

2105 Per Lord Havers in *R v Sharp* [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion.

2106 *Keane*, Modern Law of Evidence, 2005, pages 246-266.

2107 *Dennis*, The Law of Evidence, 2002, Chapters 16-17.

2108 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

2109 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006.

2110 See in this context, for example, Part II of the Irish Criminal Evidence Act 1992.

2111 R v Dodson [1984] 1 WLR 971, 79 CrApp Rep 220, CA (photographic evidence); R v Maqsud Ali [1966] 1 QB 688, 49 Cr App Rep 230, CCA (tape recorded conversation); R v Wood (1982) 76 Cr App Rep 23, CA; Castle v Cross [1984] 1 WLR 1372, DPP v McKeown [1997] 1 All ER 737, 2 Cr App Rep 155, HL (computer evidence).

2112 A "statement" is now defined as any representation of fact or opinion made by a person by whatever means; and it includes a representation made in a sketch, photo or other pictorial form: Criminal Justice Act 2003 ss 115(2), 134 (2).

2113 See in this context, for example, the Statue of Liberty case, [1968] 1 W.L.R. 739.

2114 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

2115 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

2116 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

2117 *Insa/Lazaro*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 214; *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 205.

2118 Model Law on Electronic Evidence (LMM(02)12.

2119 Singapore Evidence Act, Section 35.

2120 Canada Uniform Electronic Evidence Act.

2121 See above.

2122 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. For more information, see: *Dumortier*, The European Directive 1999/93/EC on a Community

Framework for Electronic Signatures, in Lodder/Kaspersen, eDirectives, 2000, page 33 *et seq.*, available at: www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf.

2123 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

2124 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2125 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2126 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2127 United Nations Report oft he International Law Commission, Fifty-eigth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm

2128 *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

2129 For a general overview see: *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

2130 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2131 National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2132 *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

2133 *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 6; *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

2134 *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

2135 International Court of Justice, Case of S.S."Lotus", Series A – No. 10, 1927, available at: www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

2136 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.html; Dunn/Krishna-Hensel/Mauer (eds), The Resurgence of the State, Trends and Progress in Cyberspace Governance, 2007, page 69.

2137 *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 8, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

2138 For an overview about relevant case examples for conflicts see: *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 10 et seq.

2139 *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 21.

2140 See in this regard for example: *Ali/Ragothaman/Bhagavathula/Pendse*, Security Issues in Airplane Data Networks, available at: http://soar.wichita.edu/dspace/bitstream/handle/10057/398/GRASP-4.pdf?sequence=1; The Developments in Satellite Hardware, Satellite Executive Briefing, Vol. 3, No. 12, 2010, available at: http://www.satellitemarkets.com/pdf/aug10.pdf.

2141 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm

2142 See *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Cameron*, Protective Principle of International Criminal Jurisdiction, 1994.

2143 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2144 *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72. Regarding the use of the principle within the US see for example United States v. Gallaxy Sports.

2145 See in this regard below: § 6.2.8.

2146 *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72.

2147 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2148 United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

2149 See: *Kobrick*, The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes, Columbia Law Review, Vol 87, 1987, page 1523 et seq; Regarding the discussion about scope and application of the principle of universal jurisdiction within the UN see the information provided by the Sixth Committee, available at: www.un.org/en/ga/sixth/64/UnivJur.shtml.

2150 For an overview about the implementation of the principle in European countries see: Universal Jurisdiction in Europe – The State of the Art, Human Rights Watch, 2006, available at: www.hrw.org/sites/default/files/reports/ij0606web.pdf.

2151 See above: §§ 4.5.4 and 6.1.

2152 This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132. Regarding the substantive criminal law provisions related to cybercrime, see above: § 6.1.

2153 Regarding the elements of an anti-cybercrime strategy, see above: § 4. Regarding user-based approaches in the fight against cybercrime, see: *Görling*, The Myth Of User Education, 2006, at http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

2154 Due to the protocols used in Internet communication and worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence, see above: § 3.2.7.

2155 Regarding the challenges of fighting cybercrime, see above: § 3.2.

2156 The pure fact that the offender is acting from a different country can result in additional challenges for law-enforcement agencies' investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases, the investigation nevertheless requires international cooperation between the authorities in both countries, which in general is more time consuming compared to investigations concentrating on a single country.

2157 See in this context also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 134.

2158 For an overview of the current status of the implementation of the Convention on Cybercrime and its procedural law provisions in selected countries, see the country profiles made available on the Council of Europe website: http://www.coe.int/cybercrime/.

2159 See Articles 15-21 of the Council of Europe Convention on Cybercrime.

2160 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.

2161 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21.

2162 *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

2163 *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

2164 For an overview of different kinds of evidence that can be collected by computer forensic experts, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2165 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

2166 For an overview of different forensic investigation techniques related to the most common technologies, see: *Carney/Rogers*, The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Vol. 2, Issue 4; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at:

www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Urnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, Vol. 5, Issue 1; *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2; *Gupta/Mazumdar*; Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4; Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Vol. 5, Issue 1; *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233; *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

2167 *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

2168 Regarding the different models of Cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

2169 This includes the development of investigation strategies.

2170 The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2171 With regard to developments, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

2172 *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.

2173 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

2174 *Vaciago*, Digital Evidence, 2012, Chapter II.1; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

2175 For guidelines on how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2176 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

2177 Regarding investigation techniques, see: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, page 283 *et seq.*

2178 *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No. 1.

2179 *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, Vol. 19, page 1227 *et seq.*; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 54.

2180 See below: § 6.3.8.

2181 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 171.

2182 Regarding the challenges of encryption, see § 3.2.14 as well as *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, Issue 3.

2183 Regarding possible counter strategies for law enforcement, see: *Haldeman/Schoen/Heninger* and other, Lest we Remember: Cold Boot Attacks on Encryption keys, 2008, available at: http://citp.princeton.edu/memory.

2184 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2185 *Vaciago*, Digital Evidence, 2012, Chapter II.1.

2186 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 59.

2187 *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.

2188 *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.

2189 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

2190 *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

2191 *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, page 297.

2192 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process in forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

2193 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the forensic software magic lantern, developed as a keylogger used by law enforcement in the US,

see: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

2194 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2195 *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2.

2196 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 52.

2197 For an overview of the debate, see: *Gercke*, The Role of Internet Service Providers in the Fight Against Child Pornography Computer Law Review International, 2009, page 65 *et seq.*

2198 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 15.

2199 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 24.

2200 See *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime – Toward common best-of-breed guidelines?, 2008, available at: www.coe.int/cybercrime/.

2201 For more information about the Guidelines, see: *Gercke,* The Council of Europe Guidelines for the Cooperation between LEAs and ISPs against Cybercrime, Computer Law Review International, 2008, page 97 *et seq.*

2202 See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 29.

2203 See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 30.

2204 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

2205 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

2206 Regarding the impact on tracing offenders, see: *Nicoll*, Concealing and Revealing Identity on the Internet in *Nicoll/Prins/Dellen*, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 *et seq.*

2207 *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

2208 For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2209 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, No. 4.

2210 For more information, see: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, § 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, page 149.

2211 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is

linked to popular hacker naming conventions. See *Gercke*, The criminalization of Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide: Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

2212 *Casey*, Digital Evidence and Computer Crime, 2004, page 19.

2213 For more information, see: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten, 08.01.2007, available at: www.spiegel.de/panorama/justiz/0,1518,457844,00.html.

2214 *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 472.

2215 *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.

2216 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 90, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2217 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

2218 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

2219 *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.

2220 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

2221 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 64, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2222 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

2223 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.

2224 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

2225 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

2226 With regard to the criminalization of illegal devices, see below: § 6.1.15..

2227 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.

2228 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

2229 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 29.

2230 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

2231 Regarding the ability to manipulate the time information and the response in forensic investigations, see: *Gladyshev/Patel*, Formalizing Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

Regarding dynamic time analysis, see: *Weil*, Dynamic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

2232 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

2233 *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2234 *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.

2235 See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

2236 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2237 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2238 For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

2239 Regarding the related procedural instrument, see: Art. 19, paragraph 3 Convention on Cybercrime.

2240 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 12.

2241 *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf. With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2242 *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.

2243 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 62.

2244 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

2245 See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801, for further reference.

2246 Taylor, The Council of Europe Cybercrime Convention – A civil liberties perspective, available at http://crime-research.org/library/CoE_Cybercrime.html; Cybercrime: Lizenz zum Schnueffeln Financial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at www.ccc.de.

2247 See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 *et seq.*

2248 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.

2249 See above: § 5.2.1.

2250 "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.

2251 "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.

2252 For the transformation of safeguards for Internet-related investigation techniques, see: *Taylor*, The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/taylor.pdf.

2253 This is especially relevant with regard to the protection of the suspect of an investigation.

2254 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.

2255 ABA International Guide to Combating Cybercrime, page 139.

2256 "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.

2257 "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.

2258 "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

2259 "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.

2260 "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.

2261 "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.

2262 "The cardinal issue arising under Article 8 (Art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (Art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

2263 "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.

2264 The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

2265 "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.

2266 See below: § 6.2.9

2267 See below: § 6.2.10.

2268 "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.

2269 See below: § 6.3.4.

2270 See below: § 6.3.7.

2271 As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorizes the law-enforcement agencies to prevent the deletion of the relevant data. The advantage of separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application.

2272 A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 of the Convention on Cybercrime.

2273 A definition of the term "computer data" is provided in Art. 1 of the Convention on Cybercrime.

2274 As described more in detail below, the differentiation between "computer data" and "subscriber information" in Art. 18 of the Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.

2275 "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 155. Regarding the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq*.

2276 *Gercke*, Preservation of User Data, DUD 2002, 578.

2277 The cost issue was especially raised within the discussion on data retention legislation in the EU. See, for example: E-communications service providers remain seriously concerned with the agreement reached by European Union Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005, available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

2278 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.

2279 The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report of the Workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001. A similar discussion took place during the negotiation of the Convention on Cybercrime. The drafters explicitly pointed out that the Convention does not establish a data retention obligation. See Explanatory Report to the Convention on Cybercrime, No. 151, available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

2280 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.*

2281 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.

2282 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."

2283 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.

2284 See, for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes – Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US, see: ABA International Guide to Combating Cybercrime, page 59.

2285 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2286 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.

2287 *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2288 See: *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

2289 "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.

2290 Explanatory Report, No. 152.

2291 Regarding the advantages of a system of graded safeguards, see above: § 6.3.3.

2292 "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.

2293 The drafters of the Convention on Cybercrime tried to approach the problems related to the need for immediate action from law-enforcement agencies on the one hand and the importance of ensuring safeguards on the other in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law-enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime, No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order

to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

2294 *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2295 An IP address does not necessary immediately identify the offender. If law-enforcement agencies know the IP address an offender used to commit an offence, this information only enables them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café), further investigations are necessary to identify the offender.

2296 If the offender is using services that do not require a registration or if the subscriber information provided by the user is not verified, Art. 18 Subparagraph 1b) will not enable the law-enforcement agencies to immediately identify the offender. Art. 18 Subparagraph 1b) is therefore especially relevant with regard to commercial services (like providing Internet access, commercial e-mail or hosting services).

2297 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2298 "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

2299 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2300 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.

2301 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."

2302 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.

2303 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.

2304 Judgement in Joined Cases C-293/12 and C-594/12.

2305 See, for example: Briefing for the Members of the European Parliament on Data Retention, available at: www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: www.vibe.at/aktionen/200205/data_retention_30may2002.pdf. Regarding the concerns relating to violation of the European Convention on Human Rights, see: *Breyer*, Telecommunications Data Retention and

Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

2306 See: Heise News, 13 000 determined to file suit against data retention legislation, 17.11.2007, available at: www.heise.de/english/newsticker/news/99161/from/rss09.

2307 Case C-275/06.

2308 See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

2309 In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

2310 Regarding the challenges for law-enforcement agencies related to the use of means of anonymous communication, see above: § 3.2.12.

2311 Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

2312 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2313 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.

2314 Regarding the impact of use of anonymous communication technology on the work of law-enforcement agencies, see above: § 3.2.12.

2315 Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2316 Regarding protection of the use of anonymous means of communication by the United States constitution, see: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 82, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

2317 Judgement in Joined Cases C-293/12 and C-594/12.

2318 A detailed overview of the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.* Regarding remote live search and possible difficulties with regard to the principle of chain of custody, see: *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law and Technology Vol. 9, Issue 2, 2005, available at: www.lawtechjournal.com/articles/2005/05_051201_Kenneally.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2319 Regarding the involvement of computer forensic experts in investigations, see above: § 6.3.2.

2320 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2321 See below: § 6.3.12.

2322 Apart from the fact that direct access enables the law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2323 See Explanatory Report to the Convention on Cybercrime, No. 184.

2324 "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.*

2325 Explanatory Report, No. 184.

2326 Regarding the difficulties of online search procedures, see below: § 6.3.12.

2327 See in this context: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

2328 Regarding the requirements in the US, see for example: *Brenner*, Michigan Telecommunications and Technology Law Review, 2001-2002, Vol. 8, page 41 *et seq.*; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2329 "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.

2330 *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2331 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2332 The importance of being able to extend the search to connected computer systems was already addressed by Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the recommendation is available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf.

2333 In this context, it is important to keep in mind the principle of national sovereignty. If the information is stored on a computer system outside the territory, an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be in its territory"– Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue, see also: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2334 For guidelines how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2335 Regarding the classification of the act of copying the data, see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*

2336 "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.

2337 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.

2338 See above: § 2.6.

2339 One possibility to prevent access to the information without deleting it is the use of encryption technology.

2340 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

2341 The fact that law-enforcement agencies are able to access certain data stored outside the country through a computer system in their territory does not automatically legalize the access. See Explanatory Report to the Convention on Cybercrime, No. 195. "This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation." Two cases of transborder access to stored computer data are regulated in Art. 32 Convention on Cybercrime:

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

2342 "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.

2343 "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.

2344 Explanatory Report to the Convention on Cybercrime, No. 202.

2345 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2346 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.

2347 Official Note: A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self-incrimination.

2348 Regarding the motivation of the drafters, see Explanatory Report to the Convention on Cybercrime, No. 171.

2349 "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.

2350 Explanatory Report to the Convention on Cybercrime, No. 173.

2351 "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.

2352 Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication, see above: § 3.2.12.

2353 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.

2354 See above: § 6.3.5.

2355 Explanatory Report to the Convention on Cybercrime, No. 172.

2356 This can be, for example, information that was provided on a classic registration form and kept by the provider as paper records.

2357 The Explanatory Report even points out that the parties to the Convention can adjust their safeguards with regard to specific data within each of the categories. See Explanatory Report to the Convention on Cybercrime, No. 174: "Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases." For example, the requirement of a court order.

2358 For example, the requirement of a court order.

2359 The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 21) shows that the drafters of the Convention realized the importance of separating instruments with different impact.

2360 See below: § 6.3.9.

2361 See below: § 6.3.10.

2362 Art. 21 of the Convention on Cybercrime obliges the signatory states to implement the possibility to intercept content data only with regard to serious offences ("Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law"). On the contrary, Art. 20 of the Convention on Cybercrime is not limited to serious offences. "Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

2363 Regarding the advantages of a graded system of safeguards, see above: § 6.3.3.

2364 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2365 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.

2366 Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel, see: Legal Opinion on Intercept Communication, 2006, available at: www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

2367 In these cases, other technical solutions for surveillance need to be evaluated. Regarding possible physical surveillance techniques, see: *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997, page 384 *et seq.*

2368 Regarding the interception of VoIP to assist law-enforcement agencies, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2369 Regarding the interception of VoIP to assist law-enforcement agencies, see: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 48, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.htm; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2370 In particular, lack of technical preparation of Internet providers to collect the relevant data in real time.

2371 Explanatory Report to the Convention on Cybercrime, No. 205.

2372 ABA International Guide to Combating Cybercrime, page 125.

2373 ABA International Guide to Combating Cybercrime, page 125.

2374 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.

2375 "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in cybercrime investigations, see also: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 *et seq.*

2376 "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.

2377 The Convention does not define technical standards regarding the design of such an interface. Explanatory Report to the Convention on Cybercrime, No. 220.

2378 Explanatory Report to the Convention on Cybercrime, No. 223.

2379 "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.

2380 See above: § 3.2.12.

2381 Tor is a software that enables users to protect against traffic analysis. For more information about the software, see: http://tor.eff.org/.

2382 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request an identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2383 This advantage is also relevant for remote forensic investigations. See below: § 6.3.12.

2384 Such obligation might be legal or contractual.

2385 Explanatory Report to the Convention on Cybercrime, No. 226.

2386 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."

2387 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.

2388 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at:

www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers,* Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2389 One possibility to prevent law-enforcement agencies from analysing the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures, see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

2390 Regarding the impact of encryption technology on computer forensic and criminal investigations, see: *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge, see below: § 6.3.11.

2391 *Schneier*, Applied Cryptography, page 185.

2392 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2393 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

2394 *Schneier*, Applied Cryptography, page 185.

2395 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:

2396 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."

2397 For more information, see: *Koops*, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

2398 The need for such authorization is mentioned, for example, in principle 6 of the 1997 Guidelines for Cryptography Policy: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

2399 This topic was discussed in the deliberations of the US District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow law-enforcement agencies to make use of a software to record keystrokes on a suspect's computer (keylogger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers). See: www.epic.org/crypto/scarfo/opinion.html.

2400 Export limitations on encryption software capable of processing strong keys are not designed to facilitate the work of law-enforcement agencies in the country. The intention of such regulations is to prevent the availability of the technology outside the country. For detailed information on import and export restrictions with regard to encryption technology, see: http://rechten.uvt.nl/koops/cryptolaw/index.htm.

2401 The limitation of the import of such powerful software is even characterized as "misguided and harsh to the privacy rights of all citizens". See, for example: The Walsh Report – Review of Policy relating to Encryption Technologies 1.1.16 available at: www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

2402 See: *Lewis*, Encryption Again, available at: www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

2403 The key escrow system was promoted by the United States Government and implemented in France for a period in 1996. For more information, see: Cryptography and Liberty 2000 – An International Survey of Encryption Policy, available at: http://www2.epic.org/reports/crypto2000/overview.html#Heading9.

2404 See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 *et seq.*

2405 "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management. which may allow, consistent with these guidelines. lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies", www.g7.utoronto.ca/summit/1997denver/formin.htm.

2406 See, for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf; Australia, Cybercrime Act, Art. 12, available at: http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf; Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at: http://staatsbladclip.zita.be/staatsblad/wetten/2001/02/03/wet-2001009035.html; France, Loi pour la confiance dans l'économie numérique, Section 4, Art. 37, available at: www.legifrance.gouv.fr/affichTexte.do;jsessionid=B78A2A8ED919529E3B420C082708C031.tpdjo12v_3?cidTexte=JORFTEXT000000801164&dateTexte=20080823; United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at: www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative à l'échange électronique de données juridiques, Chapter III, available at: http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/; Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: www.info.gov.za/gazette/acts/2002/a70-02.pdf; Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

2407 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.

2408 For general information on the Act, see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses, available at: www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

2409 For an overview of the regulation, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2410 Regarding the discussion of protection against self-incrimination under United States law, see for example: *Clemens*, No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private key, UCLA Journal of Law and Technology, Vol. 8, Issue 1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: www.richmond.edu/jolt/v2i1/sergienko.html; *O'Neil*, Encryption and the First Amendment, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art1.pdf; *Fraser*, The Use of Encrypted, Coded and Secret Communication is an "Ancient Liberty" Protected by the United States Constitution, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art2.pdf; *Park*, Protecting the Core Values of the First Amendment in an age of New Technology: Scientific Expression vs. National Security, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art3.pdf; Hearing before the Subcommittee on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary, United States Senate, 150 Congress, Second Session on Examining the Use of Encryption, available at: www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe on self-incrimination, in particular with regard to the European Convention on Human Rights (ECHR), see: *Moules*, The Privilege against self-incrimination and the real evidence, The Cambridge Law Journal, 66, page 528 *et seq.*; *Mahoney*, The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR, Judicial Studies Institute Journal, 2004, page 107 *et seq.*; *Birdling*, Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom, International Journal of Evidence and Proof, Vol. 12, Issue 1, 2008, page 58 *et seq.*; Commission of the European Communities, Green Paper on the Presumption of Innocence, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:pdf.

2411 Regarding the situation in the US, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

2412 In this context, see also: *Walker*, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: www.bileta.ac.uk/01papers/walker.html.

2413 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2414 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.

2415 A detailed overview of the elements of search procedures as well as the challenges of carrying them out is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.*

2416 Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an ongoing investigation based on Art. 20 confidential, see above: § 6.3.9.

2417 There are disadvantages related to remote investigations. Apart from the fact that direct access enables law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system it is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2418 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2419 See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.200, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

2420 See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: www.heise-security.co.uk/news/92950.

2421 Computer and Internet protocol address verifier.

2422 A copy of the search warrant is available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search, see: www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf. For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2423 Regarding the discussion in Germany, see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware "specialists" to bug terrorists, The Register, 21.11.2007, available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: www.spiegel.de/international/germany/0,1518,502955,00.html.

2424 See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: www.tagesspiegel.de/politik/;art771,1989104.

2425 For an overview, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

2426 The search function was the focus of the decision of the German Supreme Court in 2007. See: Online police searches found illegal in Germany, 14.02.2007, available at: www.edri.org/edrigram/number5.3/online-searches.

2427 Regarding investigations involving VoIP, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

2428 See: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf. Keylogging is the focus of the FBI software "magic lantern". See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf. See also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

2429 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.

2430. Regarding these functions, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

2431 Regarding the possible ways of infecting a computer system by spyware, see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

2432 With regard to the efficiency of virus scanners and protection measures implemented in the operating systems, it is likely that the functioning of a remote forensic software would require the cooperation of software companies. If software companies agree to prevent detection of remote forensic software, this could result in serious risks for computer security. For more information, see: *Gercke*, Computer und Recht 2007, page 249.

2433 If the offender stores illegal content on an external storage device that is not connected to a computer system, the investigators will in general not be able to identify the content if they only have access to the computer system via remote forensic software.

2434 Regarding the importance of maintaining integrity during a forensic investigation, see: *Hosmer*, Providing the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2435 National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2436 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2437 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2438 See above: § 3.2.12.

2439 Based on Art. 7, "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electrnic data transmission or other communications, are made available to the public, to customers or members" is obliged to require a licence from local authorities and identify persons using the service. For more information, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

2440 Decree 144/2005, 27 July 2005 ("Decreto-legge"). Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article, Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2441 For more details, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

2442 *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

2443 Regarding the related challenges, see: *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

2444 International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005.

2445 *Büllingen/Gillet/Gries/Hillebrand/Stamm*, Situation and Perspectives of Data Retention in an international comparison (Stand und Perspectiven der Vorratsdatenspeichung im internationalen Vergleich), 2004, page 10, available at: www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

2446 *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

2447 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

2448 See above: § 3.2.7.

2449 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2450 See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2451 *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

2452 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

2453 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."

2454 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

2455 The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

2456 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

2457 European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

2458 Council of Europe Convention on Cybercrime, ETS 185.

2459 See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2460 A full list of agreements is available at: www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

2461 Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

2462 See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, page 119.

2463 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.

2464 *Choo,* Trends in Organized Crime, 2008, page 273.

2465 *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4, page 27.

2466 See, for example: Great Britain Crown Prosecution Service, Convictions for internet rape plan, Media release, 01.12.2006.

2467 *Choo,* Trends in Organized Crime, 2008, page 273.

2468 For further details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2469 According to the report of the expert meeting held between 8 and 10 October 2008, there are certain states which require special provisions in their internal law to allow such spontaneous information, while others can transmit information spontaneously without such internal provisions in force: see CTOC/COP/2008/18 page 5.

2470 For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 226, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2471 For details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 225, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2472 See, for example, Art. 29 and Art. 35 Convention on Cybercrime.

2473 The directory is available at: www.unodc.org/compauth/en/index.html. Access requires registration and is reserved for competent national authorities.

2474 The directory indicates the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific requests of the receiving states and sometimes even extracts from domestic legislation of that state.

2475 See CTOC/COP/2008/18, paragraph 27.

2476 See Art. 25, paragraph 3 of the Convention on Cybercrime.

2477 The software is available at: www.unodc.org/mla/index.html.

2478 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).

2479 If, for example, two countries involved in a cybercrime investigation already have bilateral agreements in place that contain the relevant instruments, those agreements will remain a valid basis for the international cooperation

2480 Regarding the difficulties with the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

2481 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.

2482 Regarding the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

2483 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."

2484 See above: § 3.2.10.

2485 See Explanatory Report to the Convention on Cybercrime, No. 256.

2486 This information often leads to successful international investigations. For an overview of large-scale international investigations related to child pornography, see: *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296, page 4, available at: www.ecpat.se/upl/files/279.pdf.

2487 Similar instruments can be found in other Council of Europe conventions. For example, Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 28 of the Criminal Law Convention on Corruption. Council of Europe conventions are available at: www.coe.int.

2488 See Explanatory Report to the Convention on Cybercrime, No. 262.

2489 Regarding the 24/7 network points of contact, see below: § 6.4.12.

2490 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."

2491 See Explanatory Report to the Convention on Cybercrime, No. 268.

2492 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."

2493 See Explanatory Report to the Convention on Cybercrime, No. 269.

2494 See above: § 6.3.

2495 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).

2496 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2497 An exemption is Art. 32 of the Convention on Cybercrime – See below. Regarding the concerns related to this instrument, see: Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: " […] Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32b in particular in the light of experience gained from the use of this Article).

2498 See above: § 6.3.4.

2499 See above: § 6.3.4.

2500 See above: § 6.3.7.

2501 See above: § 6.3.6.

2502 See above: § 6.3.9.

2503 See above: § 6.3.10.

2504 See Explanatory Report to the Convention on Cybercrime, No. 293.

2505 "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.

2506 See below in this chapter.

2507 See Explanatory Report to the Convention on Cybercrime, No. 293.

2508 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

2509 See: Challenges and Best Practices in Cybercrime Investigation, 2008, available at: www.unafei.or.jp/english/pdf/PDF_rms/no79/15_P107-112.pdf.

2510 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2511 For more information, see: A Draft Commentary on the Council of Europe Convention, October 2000, available at: www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf.

2512 In this context, it is necessary to point out a difference between Art. 32 and Art. 18. Unlike Art. 18, Art. 32 does not enable a foreign law-enforcement agency to order the submission of the relevant data. It can only seek permission.

2513 Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, 19-20 October 1999.

2514 Principles on Transborder Access to Stored Computer Data, available at: www.justice.gov/criminal/cybercrime/g82004/99TransborderAccessPrinciples.pdf.

2515 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."

2516 See above: § 6.3.4.

2517 Availability 24 hours a day and 7 days a week is especially important with regard to the international dimension of cybercrime, as requests can potentially come from any time zone in the world. Regarding the international dimension of cybercrime and the related challenges, see above: § 3.2.6.

2518 See Explanatory Report to the Convention on Cybercrime, No. 298.

2519 Regarding the activities of the G8 in the fight against cybercrime, see above: § 5.1.1. For more information on the 24/7 Network, see: *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 484, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.

2520 See above: § 3.2.10.

2521 See above: § 3.2.6.

2522 Regarding the question of which authorities should be authorized to order the preservation of data, see above: § 6.3.4.

2523 Explanatory Report to the Convention on Cybercrime, No. 301.

2524 Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

2525 *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

2526 The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

2527 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

2528 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

2529 See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

2530 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.

2531. See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

2532 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2533 For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2534 In the decision Recording Industry Association Of America v. Charter Communications, Inc., the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the United States DMCA by pointing out the balance. In the opinion of the court, DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

2535 Regarding the history of DMCA and pre-DMCA case law in the United States, see: *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Salow*, Liability Immunity for Internet Service Providers – How is it working?, Journal of Technology Law and Policy, Vol. 6, Issue 1, 2001, available at: http://grove.ufl.edu/~techlaw/vol6/issue1/pearlman.html

2536 Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html.

2537 Regarding the application of DMCA to search engines, see: *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

2538 17 USC. § 512(a)

2539 17 USC. § 512(b)

2540 Regarding the Communications Decency Act, see: *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf;

2541 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union e-commerce regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*, available at: www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

2542. See *Lindholm/Maennel*, Computer Law Review International 2000, 65. Art. 12 – Art. 15 EU of the E-Commerce Directive.

2543 Art. 12 – Art. 15 EU of the E-Commerce Directive.

2544 With the number of different services covered, the E-Commerce Directive aims for a broader regulation than 17 USC. § 517(a). Regarding 17 USC. § 517(a).

2545 See Art. 12 paragraph 3 of the E-Commerce Directive.

2546 The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2547 Regarding traditional caching as well as active caching, see: *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

2548 For more information on proxy servers, see: *Luotonen*, Web Proxy Servers, 1997.

2549 The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2550 See above: § 6.5.4.

2551 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.

2552 This procedure is called "notice and takedown"

2553 The hosting provider is quite often in a difficult situation. On the one hand, it needs to react immediately to avoid liability; on the other hand, it has certain obligations to its customers. If it removes legal information that was just at first sight illegal, this could lead to claims for indemnity.

2554 By enabling their customers to offer products, they provide the necessary storage capacity for the required information.

2555 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2556 See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2557 See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2558 *Spindler*, Multimedia und Recht 1999, page 204.

2559 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.

2560 *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

2561. Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

2562 See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

2563 § 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.

2564 *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, page 5, available at: www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

2565 Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

2566 See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

2567 Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) – Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (Spain)

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No. tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

2568 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.

الاتحاد الدولي للاتصالات (ITU)
مكتب تنمية الاتصالات (BDT)
مكتب المدير

Place des Nations
CH-1211 Geneva 20
Email: mailto:bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

نائب المدير ورئيس دائرة الإدارة وتنسيق العمليات (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

دائرة البنية التحتية والبيئة التمكينية والتطبيقات الإلكترونية (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

دائرة الابتكارات والشراكات (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

دائرة دعم المشاريع وإدارة المعرفة (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

إفريقيا

إثيوبيا

المكتب الإقليمي للاتحاد
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia a

E-mail: itu-addis@itu.int
Tel.: +251 11 551 49 77
Tel.: +251 11 551 48 55
Tel.: +251 11 551 83 28
Fax: +251 11 551 72 99

الكاميرون

مكتب المنطقة للاتحاد
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

E-mail: itu-yaounde@itu.int
Tel.: + 237 22 22 92 92
Tel.: + 237 22 22 92 91
Fax: + 237 22 22 92 97

السنغال

مكتب المنطقة للاتحاد
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

E-mail: itu-dakar@itu.int
Tel.: +221 33 849 77 20
Fax: +221 33 822 80 13

زيمبابوي

مكتب المنطقة للاتحاد
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

E-mail: itu-harare@itu.int
Tel.: +263 4 77 59 41
Tel.: +263 4 77 59 39
Fax: +263 4 77 12 57

الأمريكتان

البرازيل

المكتب الإقليمي للاتحاد
SAUS Quadra 06 Bloco "E"
11 andar – Ala Sul
Ed. Luis Eduardo Magalhães (AnaTel)
70070-940 – Brasilia, DF – Brasil

E-mail: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

بربادوس

مكتب المنطقة للاتحاد
United Nations House
Marine Gardens
Hastings – Christ Church
P.O. Box 1047
Bridgetown – Barbados

E-mail: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

شيلي

مكتب المنطقة للاتحاد
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

E-mail: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

هندوراس

مكتب المنطقة للاتحاد
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT 4 Piso
P.O. Box 976
Tegucigalpa – Honduras

E-mail: ituteguciglapa@itu.int
Tel.: +504 2 2 201 074
Fax: +504 2 2 201 075

الدول العربية

مصر

المكتب الإقليمي للاتحاد
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

E-mail: itucairo@itu.int
Tel.: +20 2 35 37 17 77
Fax: +20 2 35 37 18 88

آسيا – المحيط الهادئ

تايلاند

المكتب الإقليمي للاتحاد
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

E-mail: itubangkok@itu.int
Tel.: +66 2 574 8565/9
Tel.: +66 2 574 9326/7
Fax: +66 2 574 9328

إندونيسيا

مكتب المنطقة للاتحاد
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

E-mail: itujakarta@itu.int
Tel.: +62 21 381 35 72
Tel.: +62 21 380 23 22
Tel.: +62 21 380 23 24
Fax: +62 21 389 05 521

كومنولث الدول المستقلة

الاتحاد الروسي

مكتب المنطقة للاتحاد
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation

E-mail: itumoskow@itu.int
Tel.: +7 495 926 60 70
Fax: +7 495 926 60 73

أوروبا

سويسرا

مكتب تنمية الاتصالات (BDT)
الاتحاد الدولي للاتصالات (ITU)
وحدة أوروبا (EUR)
Place des Nations
CH-1211 Geneva 20 – Switzerland
E-mail: eurregion@itu.int
Tel.: +41 22 730 5111

الاتحاد الدولي للاتصالات
مكتب تنمية الاتصالات
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN 978-92-61-15646-6 SAP id 39680
9 789261 156466

طبع في سويسرا
جنيف، 2014

11/2014