الأمم المتحدة

A/CONF.213/9

Distr.: General
22 January 2010
Arabic
Original: English

مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية

سلفادور، البرازيل، ١٢-١٩ نيسان/أبريل ٢٠١٠

البند ٨ من جدول الأعمال المؤقت*

التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية

التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما في ذلك الجرائم الحاسوبية

ورقة عمل من إعداد الأمانة

أولا- مقدمة

١- إنَّ احتلال الجريمة الحاسوبية موقعاً بارزاً في جدول أعمال مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية يؤكِّد أهميتها التامَّة والتحديات الخطيرة التي تطرحها، على الرغم من أنَّ مناقشة المسألة بقيت متواصلة طوال نحو نصف قرن.

٢- وعلى مدى السنوات الخمسين الماضية، نوقشت ووُضعت حلول مختلفة لمعالجة مسألة الجريمة الحاسوبية. ويبقى الموضوع مثيراً للتحدي جزئياً، لأنَّ التكنولوجيا ما انفكّت تتطور، ولأن الأساليب المستخدَمة في ارتكاب الجرائم الحاسوبية تتغيَّر أيضاً.

٣- ومنذ ستِّينات القرن الماضي حتى ثمانيناته، واجهت الدول أفعالاً جديدة، منها التلاعب الحاسوبي والتجسُّس على البيانات، اللذان لم يكونا غالباً مشمولين بالتشريعات الجنائية. وقد تركَّزت المناقشة آنذاك على وضع تدابير تصد قانونية.[١]

---

* A/CONF.213/1.

(١) انظر Susan H. Nycum, *The Criminal Law Aspects of Computer Abuse: Applicability of the State Penal Laws to Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1976) and Ulrich Sieber, *Computerkriminalität und Strafrecht* (Cologne, Karl Heymanns Verlag, 1977).

050310 V.10-50380 (A)

الرجاء إعادة الاستعمال

٤- وقد أدى استحداث واجهات تطبيق ذات رسومات بيانية في تسعينات القرن الماضي، وما أعقبه من تزايد متسارع في عدد مستخدمي الإنترنت، إلى تحدِّيات جديدة. فالمعلومات التي يجيز القانون نشرها في أحد البلدان، تتاح على نطاق عالمي، حتى في بلدان يكون فيها نشر تلك المعلومات مخالفا للقانون. وثمة شاغل آخر يتعلق بالخدمات المتاحة بالاتصال الحاسوبي المباشر، وهو سرعة تبادل المعلومات، التي ثبت أنها مثيرة للتحدِّي، وبخاصة في التحقيق في الجريمة ذات الأبعاد عَبْر الوطنية.(٢)

٥- وقد سادت في العقد الأول من القرن الحادي والعشرين أساليب جديدة ومعقَّدة في ارتكاب الجرائم (مثل "التصيد الاحتيالي"،(٣) و"الاعتداءات بواسطة شبكة بوتنت")(٤) واستخدام تكنولوجيات يتعذّر كثيراً على ضباط إنفاذ القانون معالجتها من خلال التحقيقات (مثل بروتوكول التواصل الصوتي عبر الإنترنت و"الحوسبة السحابية").

ثانيا- تحديات الجريمة الحاسوبية

ألف- عدم اليقين بمداها

٦- على الرغم من التحسينات التكنولوجية والتحقيقات المكثَّفة، فإنّ مدى استخدام تكنولوجيا المعلومات لأغراض غير مشروعة يبقى ثابتاً أو ربما يتنامى. وقد أفاد بعض مُقدّمي خدمات البريد الإلكتروني أنّ ما مقداره ٧٥ إلى ٩٠ في المائة من جميع الرسائل الإلكترونية هي رسائل تطفلية.(٥) وهناك أرقام مماثلة لأعداد ثابتة أو متزايدة، منشورة بشأن سلوك

---

(٢) فيما يتعلق بأثر السرعة الشديدة التي تمّ بها تبادل البيانات على التحقيقات في الجرائم الحاسوبية، انظر: فهم الجريمة السيبرانية: دليل البلدان النامية (جنيف، ٢٠٠٩). متاح على الموقع http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

(٣) كما حدّده الاتحاد الدولي للاتصالات في فهم الجريمة السيبرانية: دليل (انظر الحاشية ٢)، "التصيد الاحتيالي" بأنه فعل يجري تنفيذه لجعل الضحية تكشف معلومات شخصية أو سرِّية. وقد استخدم مصطلح "التصيد الاحتيالي" (phishing) أصلاً لوصف استخدام الرسائل الإلكترونية "لاصطياد" كلمات السر والبيانات المالية من بحر من مستعملي الإنترنت. واستخدام "الحرفين "ph" مرتبط بأعراف شائعة للتسميات في أوساط المتسللين.

(٤) يُقصد بشبكة "البوتنت" مجموعة من الحواسيب المدسوس فيها برنامج يخضع لتحكُّم خارجي. انظر Clay Wilson, "Botnets, cybercrime and cyberterrorism: vulnerabilities and policy issues for Congress", Congressional Research Service Report RL32114، حُدِّث في ٢٩ كانون الثاني/يناير ٢٠٠٨، ومتاح على الموقع www.fas.org/sgp/crs/terror/RL32114.pdf.

(٥) أفاد الفريق العامل المعني بمكافحة إساءة استعمال المراسَلة الإلكترونية عام ٢٠٠٩ أنّ ما بين ٨٥ و٩٠ في المائة من الرسائل الإلكترونية كانت تطفيلية (http://www.maawg.org/sites/maawg/files/news/2009_MAAWG-Consumer_Survey-Part1.pdf).

جنائي آخر أكثر انتشاراً أيضاً. فعلى سبيل المثال، تُظهر مؤسسة "إنترنت ووتش" في تقريرها السنوي والخيري لعام ٢٠٠٨ عددا مستقراً نسبياً لمواقع الاستغلال التجاري المؤكَّدة للأطفال في المواد الإباحية على الإنترنت بين عامي ٢٠٠٦ و٢٠٠٨.

٧- ومع أنّ المعلومات الإحصائية مفيدة لجذب الانتباه إلى الأهمية القائمة أو المتزايدة للمسألة، فإنّ أحد التحديات الكبرى المتعلقة بالجريمة الحاسوبية، هو عدم توافر المعلومات الموثوقة بشأن حجم المشكلة، فضلاً عن عدم توافرها بشأن الاعتقالات والمحاكمات والإدانات. وإحصاءات الجريمة لا تذكر غالباً الجرائم بشكل منفصل، بينما الإحصاءات القليلة المتوافرة بشأن الجريمة الحاسوبية غير مفصّلة بشكل كافٍ عموماً لتزويد مقرِّري السياسات العامة بمعلومات موثوقة بشأن حجم الجرائم أو مداها.[٦] وبدون تلك البيانات، يصعب حساب أثر الجريمة الحاسوبية كمياً على المجتمع واستحداث استراتيجيات لمعالجة المسألة.[٧]

٨- ومن الأسباب المؤدية إلى عدم توافر المعلومات الإحصائية أنّ من الصعب تقدير حجم الخسائر المالية وعدد الجرائم التي يرتكبها الجناة في الفضاء الإلكتروني. وتُقدِّر بعض المصادر خسائر الأعمال والمؤسسات التجارية الناجمة عن الجريمة الحاسوبية في الولايات المتحدة[٨] بما قيمته ٦٧ بليون دولار أمريكي في السنة؛ ولكن، من غير المؤكّد ما إذا كان الاستقراء الخارجي المستنِد إلى نتائج الاستقصاء بالعيِّنات مُبرَّراً.[٩] ولا يقتصر تطبيق هذا النقد المنهجي على الخسائر، وإنما ينطبق أيضاً على الجرائم المعترَف بها.[١٠] كما إنّ من غير المؤكّد مدى إبلاغ الضحايا عن الجرائم الحاسوبية. فمع أنَّ السلطات المعنية بمكافحة الجرائم الحاسوبية تشجِّع الضحايا على الإبلاغ عن تلك الجرائم، هناك قلق بشأن عدم قيام الضحايا في القطاع المالي خصوصاً (مثل المصارف) بالإبلاغ عن وقوع تلك الجرائم، خوفاً من أن يُسيء الإعلان السلبي إلى سمعة أولئك الضحايا.[١١] فحين تُعلن شركة أن متسلِّلين وصلوا إلى

(٦) الولايات المتحدة الأمريكية، Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO report GAO-07-705 (Washington, D.C., June 2007), p. 22; and Ian Walden, *Computer Crimes and Digital Investigations* (Oxford, Oxford University Press, 2007).

(٧) Walden, *Computer Crimes and Digital Investigations*.

(٨) الولايات المتحدة، مكتب التحقيقات الاتحادي، *2005 FBI Computer Crime Survey*, p. 10.

(٩) فهم الجريمة السيبرانية: دليل (انظر الحاشية ٢).

(١٠) المرجع نفسه.

(١١) Neil Mitchison and Robin Urry, "Crime and abuse in e-business", *IPTS Report*, vol. 57, September 2001.

خادومها، قد يفقد الزبائن الثقة بها، وقد تكون التكاليف والعواقب الكاملة أكبر حتى من الخسائر الناجمة عن الهجوم المتسلِّل. وبالإضافة إلى ذلك، قد لا يعتقد المستهدَفون أنَّ أجهزة إنفاذ القانون ستكون قادرة على معرفة الجناة. ولكن إذا لم يجر الإبلاغ عن الجناة وملاحقتهم قضائياً، فقد يكرِّرون ارتكاب جرائمهم.

٩- وهناك صعوبة أخرى تتعلق بالمعلومات الإحصائية وهي أنَّه غالباً جداً ما يجري تكرار اقتباس معلومات غير موثوقة وغير قابلة للتحقق. ويتعلق أحد الأمثلة على ذلك بالمعلومات الإحصائية بشأن الجوانب التجارية من استغلال الأطفال في المواد الإباحية على الإنترنت. وقد ذُكر في عدة تحليلات أنّ ذلك الاستغلال يدرُّ سنوياً ٢.٥ بليون دولار على نطاق العالم.[١٢] لكنّ مصدر هذا الرقم (www.toptenreviews.com) لا يُقدِّم أية معلومات مرجعية بشأن الكيفية التي أُجري بها البحث. ومع العلم بأنّ الشركة تذكر في موقعها على الإنترنت أنها "تعطيك المعلومات التي تحتاج إليها للقيام بعملية شراء ذكية. ونحن نقدِّم توصية بأفضل منتَج في كل فئة. ومن خلال خرائطنا للمقارنة المتوازية، وأخبارنا ومقالاتنا وأشرطتنا المصوَّرة، فإننا نُبسِّط عملية الشراء للمستهلكين"، هناك شواغل جدية بشأن موثوقية البيانات. وفي مثال آخر، استنتج صحافي في وول ستريت جورنال[١٣] عام ٢٠٠٦، كان يحقِّق في الادِّعاء بأنّ استغلال الأطفال في المواد الإباحية عمل تجاري قيمته ٢٠ بليون دولار في السنة، أنّ الوثيقتين الرئيستين اللتين تشملان معلومات عن عائدات تتراوح من ٣ بلايين إلى ٢٠ بليون دولار (منشوران صادران عن المجلس الوطني للأطفال المفقودين والمستغَلِّين في الولايات المتحدة وعن مجلس أوروبا) أشارتا إلى مؤسسات لم تؤكد هذه الأرقام.

باء- البعد عَبْر الوطني

١٠- إنّ الجريمة الحاسوبية هي بطبيعتها عبر وطنية إلى حدٍّ كبير. فقد صُمِّمت شبكة الإنترنت أصلاً لتكون شبكة عسكرية تقوم على بنية شبكة لامركزية. وغالبا ما يكون للجريمة الحاسوبية بُعدٌ دولي ناجم عن بنيتها الأساسية وعن التوافر العالمي للخدمات.

---

(١٢) Kim-Kwang Choo, Russel G. Smith and Rob McCusker, “Future directions in technology-enabled crime: 2007-09”, Research and Public Policy Series, No. 78 (Canberra, Australian Institute of Criminology, 2007), p. 62; ECPAT International, *Violence against Children in Cyberspace* (Bangkok, 2005), p. 54; Council of Europe, *Organised Crime Situation Report 2005: Focus on the Threat to Economic Crime* (Strasbourg, December 2005), p. 41.

(١٣) Carl Bialik, “Measuring the child-porn trade”, *Wall Street Journal*, 18 April 2006.

والرسائل الإلكترونية ذات المضمون غير القانوني تُبعَث بسهولة إلى المتلقين في عدد من البلدان، حتى في الحالات التي يكون فيها المرسِل الأصلي والمتلقِّي الأخير كلاهما في البلد نفسه، أو إذا كان أيّ من المرسِل أو المتلقِّي يستعمل خدمة بريد إلكتروني يديرها مزوِّد خارج البلد. ولدى بعض مزوِّدي خدمة البريد الإلكتروني المجانية الشائعة ملايين المستخدمين في جميع أرجاء العالم، مما يبرز البُعد عبر الوطني للجريمة الحاسوبية.

١١- والتحديات التي يفرضها العنصر عبر الوطني على التحقيق في الجريمة الحاسوبية مماثلة لتلك المرتبطة بجرائم عبر وطنية أخرى. ونتيجة لمبدأ السيادة الوطنية الأساسي، الذي بمقتضاه لا يمكن إجراء تحقيقات في أقاليم أجنبية، بدون إذن السلطات المحلية، فإنّ التعاون الوثيق بين الدول المعنية أمر بالغ الأهمية في التحقيقات في الجرائم الحاسوبية. والتحدي الرئيسي الآخر يتعلق بالوقت القصير المتاح لإجراء التحقيقات في الجرائم الحاسوبية. وخلافاً للمخدرات غير المشروعة، التي يمكن أن يستغرق وصولها إلى مقصدها أسابيع، بحسب وسائط نقلها، يمكن إيصال الرسائل الإلكترونية في ثوانٍ، كما يمكن تنزيل ملفات كبرى في دقائق، عند توافر عرض النطاق الكافي.

١٢- والتعاون الآني والفعّال بين السلطات في مختلف البلدان بالغ الأهمية أيضاً، لأنه في قضايا الجريمة الحاسوبية، تحذف الأدلَّة غالباً بشكل تلقائي وضمن أُطُر زمنية قصيرة. ويمكن للإجراءات الرسمية المطوَّلة أن تُعيق التحقيقات إعاقة خطيرة.

١٣- ولا يزال عدد كبير من اتفاقات المساعدة القانونية المتبادلة القائمة يستند إلى إجراءات رسمية معقَّدة ومستهلِكة للوقت غالباً. ولذا، يُعتبَر من الحيوي استحداث إجراءات للتصدي سريعاً للحوادث والاستجابة سريعاً لطلبات التعاون الدولي.

١٤- وترد في الفصل الثالث من اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي إحدى مجموعات المبادئ لإعداد إطار قانوني للتعاون الدولي في تحقيقات الجرائم الحاسوبية.[١٤] ويتناول هذا الفصل الأهمية المتزايدة للتعاون الدولي (المواد ٢٣-٢٥)، ويروِّج لاستخدام وسائط الاتصال السريعة، بما فيها الفاكس والبريد الإلكتروني (المادة ٢٥، الفقرة ٣). وبالإضافة إلى ذلك، يُدعى الأطراف في الاتفاقية إلى تعيين نقطة اتصال تعمل على مدار الساعة طيلة أيام الأسبوع للاستجابة لطلبات المساعدة من الدول (المادة ٣٥). ويمكن إيجاد نُهُج أخرى في مشروع الاتفاقية الدولية لتعزيز الحماية من الجريمة الحاسوبية والإرهاب، وفي مشروع عُدَّة الاتحاد الدولي للاتصالات المتعلقة بتشريعات الجريمة الحاسوبية.

---

(١٤) مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٨٥. انظر أيضاً "التقرير التوضيحي" (explanatory report) لتلك الاتفاقية.

جيم- الاختلافات في النُهُج القانونية الوطنية

١٥- إنّ أحد الآثار العملية لبنية شبكة الإنترنت هو أنّ المجرمين الذين يرتكبون الجرائم الحاسوبية ليسوا بحاجة إلى أن يكونوا في مسرح الجريمة. ولذا، فقد أصبح منع توفير الملاذات الآمنة للمجرمين جانباً رئيسياً في منع الجريمة الحاسوبية.(١٥) وسيستخدم المجرمون الملاذات الآمنة لإعاقة التحقيقات. ومن الأمثلة الشائعة على ذلك الدودة الحاسوبية "لوف باغ" (Love Bug)، التي أُعدَّت في الفلبين عام ٢٠٠٠،(١٦) وقيل إنها عطّلت ملايين الحواسيب في جميع أرجاء العالم.(١٧) وأُعيقت التحقيقات المحلية بسبب أنّ ذلك العمل المؤذي ونشر البرمجية الضارّة لم يكن آنذاك مجرَّماً بشكل كافٍ في الفلبين.

١٦- وتكتسب مسألة التقارب بين التشريعات أهمية كبرى، لأنّ بلدانا عديدة تستند في نظام مساعدتها القانونية المتبادلة إلى مبدأ ازدواجية التجريم، الذي بمقتضاه يجب اعتبار الاعتداء جريمة في الدولة التي تطلب المساعدة والدولة التي تقدِّمها كلتيهما.(١٨) وتنحصر التحقيقات على صعيد عالمي عموماً في الأفعال المجرَّمة في جميع البلدان المتأثرة. ومع أن هناك عدداً من الجرائم التي يمكن مقاضاة مرتكبيها في أي مكان في العالم، فإن الاختلافات الإقليمية تؤدي دوراً هاماً. فعلى سبيل المثال، تجرَّم أنواع مختلفة من المحتوى في بلدان

---

(١٥) سلطت كل من الجمعية العامة، في قرارها ٥٥/٦٣، ومجموعة الثماني، في المبادئ وخطة العمل لمكافحة جريمة التكنولوجيا العالية، التي أقرت في اجتماع وزراء العدل والداخلية لمجموعة الثماني، الذي عُقد في واشنطن العاصمة في ١٠ كانون الأول/ديسمبر ١٩٩٧ (متاحة على الموقع www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf)، الضوء على ضرورة القضاء على الملاذات الآمنة لمن يُسيؤون استخدام المعلومات التكنولوجية بشكل إجرامي.

(١٦) الولايات المتحدة، مكتب المساءلة العام General Accountability Office, *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*، شهادة أُدلي بها أمام اللجنة الفرعية المعنية بالمؤسسات المالية، واللجنة المعنية بالمصارف والإسكان والشؤون الحضرية، مجلس الشيوخ الأمريكي، تقرير مكتب المساءلة العام، GAO report GAO/T-AIMD-00-181 (واشنطن العاصمة، أيار/مايو ٢٠٠٠).

(١٧) "Police close in on Love Bug culprit" *BBC News*, 6 May 2000. متاح على الموقع http://news.bbc.co.uk/2/hi/science/nature/738537.stm.

(١٨) فيما يتعلق بمبدأ ازدواجية التجريم في التحقيقات بشأن الجرائم الحاسوبية، انظر دليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسيب ومكافحتها (المجلة الدولية للسياسات الجنائية، العددان ٤٣ و٤٤: منشورات الأمم المتحدة، رقم المبيع E.94.IV.5) الصفحة ٢٦٩، وورقة المعلومات الخلفية التي أعدّها شتاين شيولبيرغ وأماندا هوبارد بعنوان "Harmonizing national legal approaches on cybercrime"، الصفحة ٥، والتي عُرضت في الاجتماع المواضيعي للاتحاد الدولي للاتصالات بشأن الأمن الحاسوبي، الذي عُقد في جنيف من ٢٨ حزيران/ يونيه إلى ١ تموز/يوليه ٢٠٠٥.

مختلفة،[١٩] مما يعني أنّ المادة التي يمكن توفيرها قانونياً على خادوم في أحد البلدان، قد تُعتبَر غير قانونية في بلد آخر.[٢٠]

١٧- وتكنولوجيا الحواسيب والشبكات المستخدَمة حالياً هي نفسها، بشكل أساسي، في العالم قاطبة. وباستثناء مسائل اللغة ومُهايئات الطاقة، هناك فرق ضئيل جداً بين أنظمة الحواسيب والهواتف الخلوية المباعة في آسيا وتلك التي تباع في أوروبا. ونشأ وضع مشابه فيما يتعلق بالإنترنت. وبفضل التوحيد القياسي، فإن البروتوكولات المستخدَمة في أفريقيا هي نفسها تلك المستخدَمة في الولايات المتحدة. فالتوحيد القياسي يمكِّن المستخدمين في جميع أرجاء العالم من الحصول على الخدمات نفسها عَبْر الإنترنت.[٢١]

١٨- وتتناول الفقرات التالية نهجَين مختلفَين للتعامل مع البعد عَبْرَ الوطني للجرائم الحاسوبية والمعايير القانونية المختلفة.

١- توافق التشريعات

١٩- إنّ أحد النُهُج لمعالجة البعد عَبْر الوطني للجرائم الحاسوبية وتحسين التعاون الدولي هو وضع وتوحيد التشريعات ذات الصلة. وقد اتخذت عدة نُهُج إقليمية في السنوات الأخيرة.

٢٠- فقد أعدَّت رابطة الكومنولث عام ٢٠٠٢ قانوناً نموذجياً بشأن الحواسيب والجرائم المتصلة بها، بهدف تحسين تشريعات مكافحة الجرائم الحاسوبية في الدول الأعضاء في الكومنولث، وتحسين التعاون الدولي. وبدون تلك التحسينات، ستكون هناك حاجة إلى ما لا يقل عن ١ ٢٧٢ معاهدة ثنائية بين دول الكومنولث، لتتعاون عَبْر الحدود بشأن هذه المسألة.[٢٢] ويشمل القانون النموذجي أحكاما تتعلق بالقانون الجنائي الموضوعي، والقانون

(١٩) تُعدَّ النُهُج القانونية المختلفة لتنظيم المحتوى أحد الأسباب لعدم إدراج جوانب معيَّنة من المحتوى غير القانوني في الاتفاقية المتعلقة بجرائم الحاسوب، ولكنها عولجت في بروتوكول إضافي. انظر أيضاً فهم الجريمة السيبرانية: دليل، الفصل ٢-٥ (انظر الحاشية ٢).

(٢٠) فيما يتعلق بالنُهُج الوطنية المختلفة إزاء تجريم استغلال الأطفال في المواد الإباحية، انظر، مثلاً، Ulrich Sieber, *Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet: eine strafrechtsvergleichende Untersuchung* (Bonn, Forum Verlag Godesberg, 1999).

(٢١) فيما يتعلق بأهمية المعايير التقنية الوحيدة، وكذلك المعايير القانونية الوحيدة، انظر Marco Gercke, "National, regional and international approaches in the fight against cybercrime", *Computer Law Review International*, 2008, p. 7.

(٢٢) Richard Bourne, "2002 Commonwealth Law Ministers' Meeting: policy brief"، وثيقة أُعدِّت لاجتماع وزراء العدل في رابطة الكومنولث الذي عُقد في كينغز تاون، سانت فنسنت وجزر غرينادين، من ١٨ إلى ٢١ تشرين الثاني/نوفمبر ٢٠٠٢ (لندن، معهد دراسات الكومنولث، ٢٠٠٢)، الصفحة ٩.

الإجرائي والتعاون الدولي. وبسبب التركيز الإقليمي للقانون النموذجي، فإن الأثر على المواءمة يقتصر على الدول الأعضاء في الكومنولث.

٢١- وقد بذل الاتحاد الأوروبي جهوداً أيضاً لتنسيق التشريعات بشأن الجريمة الحاسوبية في إطار دُوله الأعضاء الـ٢٧، من خلال ما يلي على سبيل المثال: التوجيه 2000/31/EC الصادر عن البرلمان الأوروبي والمجلس بشأن جوانب قانونية معيَّنة من خدمات مجتمع المعلوماتية، ولا سيما التجارة الإلكترونية في السوق الداخلية؛ والقرار الإطاري لمجلس الاتحاد الأوروبي 2000/413/JHA بشأن مكافحة الاحتيال وتزوير وسائط الدفع غير النقدي؛ والقرار الإطاري لمجلس الاتحاد الأوروبي 2004/68/JHA بشأن مكافحة الاستغلال الجنسي للأطفال، واستغلالهم في المواد الإباحية؛ والقرار الإطاري لمجلس الاتحاد الأوروبي 2005/222/JHA بشأن الهجمات على النُظُم المعلوماتية؛[٢٣] والتوجيه 2006/24/EC الصادر عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي بشأن الاحتفاظ بالبيانات التي تستخلص أو تعالج في إطار توفير خدمات الاتصالات الإلكترونية المتاحة للجمهور، وتعديل التوجيه 2002/58/EC؛ والقرار الإطاري الصادر عن مجلس الاتحاد الأوروبي 2008/919/JHA بتعديل القرار الإطاري 2002/475/JHA بشأن مكافحة الإرهاب. وخلافاً لمعظم النُهُج الإقليمية الأخرى، فإنّ تنفيذ الصكوك التي يعتمدها الاتحاد الأوروبي إلزامي على جميع الدول الأعضاء. ورغم سريان الصكوك، فقد كانت العقبة الرئيسية أمام جهود المواءمة داخل الاتحاد الأوروبي، حتى مطلع عام ٢٠١٠ على الأقل، هي الصلاحية المحدودة للتشريعات في مجال القانون الجنائي.[٢٤] وقد نتج تنوّع النهُج عن أنّ قدرة الاتحاد الأوروبي على تنسيق القانون الجنائي الوطني كانت تقتصر على مجالات خاصة.[٢٥] وقد غيَّرت معاهدة لشبونة المعدِّلة لمعاهدة الاتحاد الأوروبي والمعاهدة المنشئة للجماعة الأوروبية هذا الوضع، وهي تعطي الآن الاتحاد الأوروبي ولاية أقوى لمواءمة التشريعات بشأن الجرائم المتعلقة بالحاسوب في المستقبل - لكنّ هذا الأمر يقتصر على الدول الأعضاء الـ٢٧.

٢٢- وقد أعدَّ مجلس أوروبا ثلاثة صكوك رئيسية لتنسيق تشريعات الجريمة الحاسوبية. وأفضل صكٍّ معروف منها هو الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي، التي تمّ إعدادها بين عامي

---

(٢٣) للمزيد من المعلومات، انظر: Marco Gercke, "The EU framework decision on attacks against information systems", *Computer und Recht*, 2005, pp. 468 ff.، وفهم الجريمة السيبرانية: دليل (انظر الحاشية ٢)، الصفحة ٩٩.

(٢٤) Helmut Satzger, *Internationales und Europäisches Strafrecht* (Baden-Baden, Nomos, 2005), p. 84; and P.J.G. Kapteyn and Pieter Verloren van Themaat, *Introduction to the Law of the European Communities: After the Coming into Force of the Single European Act* (Boston, Kluwer Law International, 1989).

(٢٥) فيما يتعلق بتشريعات الجرائم الحاسوبية في بلدان الاتحاد الأوروبي: *Handbook of Legal Procedures of Computer Network Misuse in EU Countries* (Santa Monica, California, Rand Corporation, 2006).

١٩٩٧ و٢٠٠١. وتشمل تلك الاتفاقية بنوداً متعلقة بالقانون الجنائي الموضوعي، والقانون الإجرائي والتعاون الدولي. وبحلول كانون الأول/ديسمبر ٢٠٠٩، كانت قد وقَّعت عليها ٤٦ دولة وصدَّقت عليها ٢٦ دولة. ونظرا لعدم التوصّل إلى اتفاق بشأن تجريم العنصرية وتوزيع مواد تثير كراهية الأجانب، أثناء التفاوض بشأن هذه الاتفاقية، فقد استحدث البروتوكول الإضافي للاتفاقية المتعلقة بجرائم الفضاء الحاسوبي، والخاص بتجريم أفعال العنصرية وكراهية الأجانب المرتكَبة بوساطة نظم حاسوبية.[٢٦] وبحلول كانون الأول/ديسمبر ٢٠٠٩، كانت ٣٤ دولة[٢٧] قد وقَّعت على البروتوكول الإضافي و١٥ دولة[٢٨] قد صدَّقت عليه. وفي عام ٢٠٠٧، فتح باب التوقيع على اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي.[٢٩] وهي تشمل أحكاماً محددة تجرِّم تداول المواد الإباحية التي يُستغل فيها الأطفال، فضلاً عن تجريم سبل الحصول عن علم على تلك المواد من خلال تكنولوجيا المعلومات والاتصالات (المادة ٢٠، الفقرة ١ (و)). وحتى كانون الأول/ديسمبر ٢٠٠٩، كانت قد وقَّعتها ٣٨ دولة،[٣٠] بينها ثلاث دول[٣١] صدَّقت عليها.

٢٣- ويُضاف إلى ذلك مشروع الاتفاقية الدولية لتعزيز الحماية من الجرائم الحاسوبية والإرهاب، الذي أُعدّ على سبيل المتابعة لمؤتمر استضافته جامعة ستانفورد، الولايات المتحدة، عام ١٩٩٩، ومشروع عُدَّة الاتحاد الدولي للاتصالات بشأن تشريعات الجريمة الحاسوبية، الذي أعدَّه ممثلو رابطة المحامين الأمريكية وخبراء آخرون.

---

(٢٦) مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٨٩. انظر أيضاً "التقرير التوضيحي" للبروتوكول الإضافي.

(٢٧) أرمينيا، إستونيا، ألبانيا، ألمانيا، أوكرانيا، إيسلندا، البرتغال، بلجيكا، البوسنة والهرسك، بولندا، الجبل الأسود، جمهورية مقدونيا اليوغوسلافية سابقاً، جمهورية مولدوفا، جنوب أفريقيا، الدانمرك، رومانيا، سلوفينيا، السويد، سويسرا، صربيا، فرنسا، فنلندا، قبرص، كرواتيا، كندا، لاتفيا، لكسمبرغ، ليتوانيا، ليختنشتاين، مالطة، النرويج، النمسا، هولندا، اليونان.

(٢٨) أرمينيا، ألبانيا، أوكرانيا، البوسنة والهرسك، جمهورية مقدونيا اليوغوسلافية سابقا، الدانمرك، رومانيا، سلوفينيا، صربيا، فرنسا، قبرص، كرواتيا، لاتفيا، ليتوانيا، النرويج.

(٢٩) مجلس أوروبا، مجموعة المعاهدات، الرقم ٢٠١.

(٣٠) أذربيجان، إسبانيا، إستونيا، ألبانيا، ألمانيا، أوكرانيا، إيرلندا، إيسلندا، إيطاليا، البرتغال، بلجيكا، بلغاريا، بولندا، تركيا، الجبل الأسود، جمهورية مقدونيا اليوغوسلافية سابقا، جمهورية مولدوفا، جورجيا، الدانمرك، رومانيا، سان مارينو، سلوفاكيا، سلوفينيا، السويد، صربيا، فرنسا، فنلندا، قبرص، كرواتيا، لكسمبرغ، ليتوانيا، ليختنشتاين، المملكة المتحدة، موناكو، النرويج، النمسا، هولندا، واليونان.

(٣١) ألبانيا، الدانمرك، اليونان.

٢- الطابع الإقليمي

٢٤- إنّ التطورات الناشئة عن التوحيد القياسي التقني تتجاوز، نظرياً، عولمة التكنولوجيا والخدمات، ويمكن أن تؤدي إلى مواءمة القوانين الوطنية. لكنّ مبادئ القانون الوطني تتغيّر بوتيرة أبطأ بكثير من التطورات التقنية، كما يظهر من حالة التصديق على الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي، ومن التفاوض بشأن البروتوكول الإضافي للاتفاقية. وهذا يؤدي إلى تطور ثانٍ: نُهُج الطابع الإقليمي للإنترنت.

٢٥- ومع أنّ الإنترنت قد لا تعترف بضوابط الحدود، فهناك وسائط للحدّ من الحصول على معلومات معيّنة.(٣٢) وبناءً على ذلك، فإنّ واجبات مزوِّدي خدمة الإنترنت، بشأن منع الوصول إلى مواقع إلكترونية تشمل استغلال الأطفال في المواد الإباحية، أصبحت في دائرة اهتمام الحكومات الوطنية والمنظمات الدولية.(٣٣) ومن وجهة نظر تقنية، فإن مزوِّدي الخدمة قادرون، عموماً، على معرفة ما إذا كان الموقع الذي يريد المستخدِم الوصول إليه مُدرجاً على قائمة سوداء، وعلى منع ذلك الوصول. وتتفاوت الحلول التقنية من تلاعب بنظام اسم النطاق واستخدام خوادم وكيلة إلى حلول مختلطة تمزج نُهُجاً متنوعة.(٣٤) وتفيد

---

(٣٢) Jonathan Zittrain, "A history of online gatekeeping", *Harvard Journal of Law and Technology*, vol. 19, No. 2 (2006), p. 253.

(٣٣) فيما يتعلق بالواجبات والنُهُج الخاصة بالمرشِّحات، انظر: Ilaria Lonardo, "Italy: Service Provider's Duty to Block Content", *Computer Law Review International*, 2007, pp. 89 ff.; Ulrich Sieber and Malaika Nolde, *Sperrverfügungen im Internet: Nationale Rechtdurchsetzung im globalen Cyberspace?* (Berlin, Duncker and Humblot, 2008); W. Ph. Stol and others, *Filteren van kinderporno op internet: Een verkenning van technieken en reguleringen in binnen- en buitenland* (The Hague, Boom Juridische Uitgevers, WODC, 2008); Tom Edwards and Gareth Griffith, "Internet censorship and mandatory filtering", *NSW Parliamentary Library Research Service*, E-Brief 5/08, November 2008; Jonathan Zittrain and Benjamin Edelman, "Documentation of Internet filtering worldwide", October 2003، والمشروع المتاح على الموقع http://cyber.law.harvard.edu/filtering.

(٣٤) للاطلاع على استعراض شامل للجوانب التقنية، انظر Sieber and Nolde, *Sperrverfügungen im Internet*, pp. 50 ff.; Stol and others, *Filteren van kinderporno op internet*, pp. 10 ff.; Andreas Pfitzmann, Stefan Köpsell and Thomas Kriegelstein, *Sperrverfügungen gegen Access-Provider: Technisches Gutachten*, Technical University of Dresden, available from www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; Richard Clayton, Steven J. Murdoch and Robert N. M. Watson, "Ignoring the Great Firewall of China", paper presented at the 6th Workshop on Privacy Enhancing Technologies, Cambridge, June 2006; Lori Brown Ayre, *Internet Filtering Options Analysis: An Interim Report*, prepared for the InfoPeople Project, May 2001.

مبادرة الشبكة المفتوحة (OpenNet) بأن ما يزيد على عشرين[٣٥] بلدا يمارس هذا النوع من مراقبة المحتوى. كما تستخدم هذا النهج عدة بلدان أوروبية، منها إيطاليا والسويد وسويسرا والمملكة المتحدة والنرويج، فضلاً عن بلدان أخرى، منها إيران (جمهورية-الإسلامية) وتايلند والصين. ويناقش الاتحاد الأوروبي أيضاً تنفيذ تلك الواجبات.[٣٦] وتتركز الشواغل المتعلقة بهذا النهج على أنه يمكن الالتفاف على جميع الحلول التقنية المتوافرة حالياً، وأنّ هناك خطراً من الحماسة المفرطة في منع الوصول إلى المعلومات على الإنترنت.[٣٧] وقد أبرز مجلس أوروبا أهمية حماية الحقوق الأساسية، في توصية لجنة وزرائه، بشأن تدابير ترسيخ احترام حرية التعبير والمعلومات المتعلقة بمرشِّحات الإنترنت.

دال- الجريمة المنظمة

٢٦- مع أنّ الجرائم المتعلقة بالحاسوب تُرتكَب عموماً بأيدي أفراد، فإن الجماعات الإجرامية المنظمة ناشطة كذلك. ولهذا التطور أهمية خاصة لأنه يتيح إمكانية تطبيق الصكوك الموضوعة بغرض مكافحة الجريمة المنظمة، ومنها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.[٣٨]

٢٧- ولدى مناقشة الجريمة الحاسوبية والجريمة المنظمة من الضروري التمييز بين فئتين رئيسيتين من أساليب ضلوع الجماعات الإجرامية المنظمة، هما: استخدام تكنولوجيا المعلومات من جانب جماعات إجرامية منظمة تقليدية، وجماعات إجرامية منظمة تركِّز على ارتكاب جرائم حاسوبية.[٣٩]

٢٨- وتستخدم الجماعات الإجرامية المنظمة التقليدية، التي ليست لديها خلفية في الأنشطة الإجرامية المتعلقة بالإنترنت، تكنولوجيا المعلومات لتنسيق الأنشطة وتعزيز ارتكاب

---

(٣٥) Miklós Haraszti, "Preface", in *Governing the Internet: Freedom and Regulation in the OSCE Region*, C. Möller and A. Amouroux, eds. (Vienna, Organization for Security and Cooperation in Europe, 2007), pp. 5-6.

(٣٦) Commission of the European Communities, "Proposal for a Council framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing framework decision 2004/68/JHA", document COM(2009) 135, Brussels, 25 March 2009.

(٣٧) للمزيد من المعلومات بشأن حجب الإنترنت وتوازن الحريات الأساسية، انظر، Cormac Callanan and others *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Dublin, Aconite Internet Solutions, October 2009), chaps. 6 and 7.

(٣٨) الأمم المتحدة، مجموعة المعاهدات، المجلد ٢٢٢٥، الرقم ٣٩٥٧٤.

(٣٩) Kim-Kwang Raymond Choo, "Organised crime groups in cyberspace: a typology", *Trends in Organized Crime*, vol. 11, No. 3 (September 2008), pp. 270-295، يرى تشو في هذه المقالة أن هناك ثلاث فئات من الجماعات الإجرامية المنظمة التي تستغل تكنولوجيا المعلومات لاختراق الضوابط.

الجرائم.[٤٠] وفي هذه الحالات، تُستخدَم تكنولوجيا المعلومات لتحسين كفاءة الجماعة الإجرامية المنظمة في مجال أنشطتها التقليدية. وهذا يشمل التحوُّلَ إلى الاتصالات الإلكترونية، التي تمكِّن تلك الجماعات من الاستفادة من تكنولوجيا التشفير والتواصل خفية مثلاً. وبالإضافة إلى ذلك، يمكن استخدام الإنترنت لفتح أسواق جديدة، لأن الإنترنت، بحسب فرقة العمل المعنية بالجريمة المنظمة في المملكة المتحدة، أوجدت سوقاً جديدة وأكبر بكثير لأولئك المشاركين في بيع السلع المزيَّفة والمسروقة.[٤١]

٢٩- وتشير التقارير إلى توجُّه الجماعات الإجرامية المنظمة التقليدية نحو المشاركة في أشكال جديدة من الأنشطة الإجرامية في مجال جرائم التكنولوجيا العالية.[٤٢] ويشمل ذلك قرصنة البرامج وأشكالاً أخرى من انتهاك حقوق التأليف والنشر.[٤٣] ولكنّ مجالات أخرى من الجريمة الحاسوبية، ومنها استغلال الأطفال في المواد الإباحية[٤٤] والجريمة المتعلقة بالهوية، ترتبط غالباً بالجريمة المنظمة أيضاً. وفيما يتعلق بتنفيذ اتفاقية الجريمة المنظمة، لا بدَّ من أن تؤخذ في الاعتبار السمات الخاصة التالية فيما يتعلق بجماعات الجريمة الحاسوبية المنظمة:

(أ) تميل جماعات الجريمة الحاسوبية إلى امتلاك هياكل فضفاضة وأكثر مرونة، تتيح دمج الأعضاء في الجماعة لفترة محددة من الوقت؛[٤٥]

---

(٤٠) المرجع نفسه، الصفحة ٢٧٣؛ انظر أيضاً Eoghan Casey, *Digital Evidence and Computer Crime: Forenisc Science, Computers, and the Internet*, 2nd ed. (London, Academic Press, 2004), p. 9.

(٤١) United Kingdom, Organised Crime Task Force, *Annual Report and Threat Assessment 2007: Organised Crime in Northern Ireland* (2007), p. 34. Available from www.octf.gov.uk.

(٤٢) United Kingdom, Serious Organised Crime Agency, *The United Kingdom Threat Assessment of Organised Crime: 2009/10*, p. 10. Available from www.soca.gov.uk.

(٤٣) Canada, Canadian Security Intelligence Service, "Transnational criminal activity: a global context", *Perpectives*, 17 August 2000, available from www.csis-scrs.gc.ca/pblctns/prspctvs/200007-eng.asp; Choo, "Organised crime groups", p. 273 (see footnote 40).

(٤٤) Choo, "Organised crime groups", p. 281; European Police Office (Europol), "Child abuse in relation to trafficking in human beings", Serious Crime Overview, January 2008, p. 2; *Organised Crime Situation Report 2005*, p. 8; John Carr, *Child Abuse, Child Pornography and the Internet* (London, NCH, The Children's Charity, 2004), p. 17; Canada, Criminal Intelligence Service Canada, *Annual Report on Organized Crime in Canada 2007* (Ottawa, 2007), p. 4; "Annual report on organized crime in Greece for the year 2004", *Trends in Organized Crime*, vol. 9, No. 2 (2005), p. 5; United Nations, Commission on Human Rights, Report of the Special Rapporteur on the sale of children, child prostitution and child pornography (E/CN.4/2005/78), p. 8.

(٤٥) Choo, "Organised crime groups" p. 273 (انظر الحاشية ٤٠).

(ب) كثيرا ما تكون جماعات الجريمة الحاسوبية أصغر بكثير من الجماعات الإجرامية المنظمة التقليدية؛[٤٦]

(ج) كثيرا ما يتواصل أعضاء الجماعات بأسلوب إلكتروني حصريا، ولا يلتقون شخصياً.

ثالثا- تدابير التصدي للجريمة الحاسوبية

٣٠- إنّ المنظمات الدولية والإقليمية، والحكومات الوطنية، وأجهزة إنفاذ القانون والمنظمات غير الحكومية تعالج الجريمة الحاسوبية بوسائل مختلفة، بما في ذلك من خلال الوسائل التشريعية ووسائل إنفاذ القانون وبناء القدرات.

ألف- التشريعات

٣١- يجري حالياً وضع تشريعات الجرائم الحاسوبية على الصعيدين الوطني والإقليمي. وخلافاً للمعايير التقنية المستخدَمة في عمليات نقل البيانات، التي هي نفسها في جميع أرجاء العالم، لم تُبذَل حتى الآن جهود على الصعيد العالمي لتنسيق التشريعات بشأن الجريمة الحاسوبية.

١- الأثر المحدود للصكوك القائمة

٣٢- إنّ الأثر الشامل للنُهُج الإقليمية التي اعتمدتها رابطة الكومنولث والجماعة الاقتصادية لدول غرب أفريقيا (الإيكواس)، والاتحاد الأوروبي ومجلس أوروبا محدود، لأنّ النُهُج المعتمَدة لا تنطبق إلاّ على الدول الأعضاء في المنظمات المعنية. والصك الأوسع مدى حالياً هو الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي، التي تُعتبر ذات أهمية في مكافحة الجريمة الحاسوبية، والتي تؤيدها منظمات دولية مختلفة. وبالإضافة إلى ذلك، يمكن أن تنضم إلى الاتفاقية، عملاً بالمادة ٣٧ منها، أي دولة غير عضو في المجلس. وقد شاركت أربع دول غير أعضاء (جنوب أفريقيا وكندا والولايات المتحدة واليابان) في التفاوض بشأن الاتفاقية، منها ثلاث دول (كندا والولايات المتحدة واليابان) ترتبط ارتباطاً وثيقاً بالمجلس من خلال صفة المراقب التي تتمتع بها. وبحلول كانون الأول/ديسمبر ٢٠٠٩، كانت ٤٦ دولة[٤٧] (منها الدول غير

(٤٦) Susan W. Brenner, “Organized cybercrime? How cybercrime may affect the structure of criminal relationships”, North Carolina Journal of Law and Technology, No. 4 (2002), p. 27.

(٤٧) أذربيجان، أرمينيا، إسبانيا، إستونيا، ألبانيا، ألمانيا، أوكرانيا، إيرلندا، إيسلندا، إيطاليا، البرتغال، بلجيكا، بلغاريا، البوسنة والهرسك، بولندا، الجبل الأسود، الجمهورية التشيكية، جمهورية مقدونيا اليوغوسلافية سابقا، جمهورية مولدوفا، جنوب أفريقيا، جورجيا، الدانمرك، رومانيا، سلوفاكيا، سلوفينيا، السويد، سويسرا، صربيا، فرنسا، فنلندا، قبرص، كرواتيا، كندا، لاتفيا، لكسمبرغ، ليتوانيا، مالطة، المملكة المتحدة، النرويج، النمسا، هنغاريا، هولندا، الولايات المتحدة، اليابان، اليونان.

الأعضاء الأربع التي شاركت في التفاوض) قد وقَّعت الاتفاقية؛ وصدَّقت عليها حتى الآن ٢٦ دولة[٤٨] ودولة واحدة غير عضو في المجلس.

٣٣- ولا يمكن قياس أثر الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي بمجرّد عدد الدول التي وقّعتها أو صدّقت عليها. فالأرجنتين وباكستان وبوتسوانا والفلبين ومصر ونيجيريا، على سبيل المثال، قد عدّلت أجزاء من تشريعاتها وفقاً للاتفاقية دون الانضمام إليها رسمياً. ولكن مقارنة بالمعايير العالمية، يبقى عدد وسرعة التوقيع والتصديق مسألة مطروحة للتساؤل بالتأكيد. ففي السنوات التسع التي انقضت منذ توقيع أول ٣٠ دولة على الاتفاقية في ٢٣ تشرين الثاني/نوفمبر ٢٠٠١، لم يوقعها سوى ١٦ دولة إضافية. ومنذ عام ٢٠٠١، لم تنضم إلى الاتفاقية أي دولة غير عضو في مجلس أوروبا، مع أنّ الدعوة قد وُجِّهت إلى خمس دول (الجمهورية الدومينيكية وشيلي والفلبين وكوستاريكا والمكسيك) لكي تفعل ذلك. وكانت وتيرة التصديق بطيئة مثل التوقيع، حيث صدَّقت على الاتفاقية دولتان (ألبانيا وكرواتيا) عام ٢٠٠٢، ودولتان أخريان (إستونيا وهنغاريا) عام ٢٠٠٣، وأربع دول (جمهورية مقدونيا اليوغوسلافية سابقا ورومانيا وسلوفينيا وليتوانيا) عام ٢٠٠٤، وثلاث دول (بلغاريا والدانمرك وقبرص) عام ٢٠٠٥، وسبع دول (أرمينيا وأوكرانيا والبوسنة والهرسك وفرنسا والنرويج وهولندا والولايات المتحدة) عام ٢٠٠٦، وثلاث دول (إيسلندا وفنلندا ولاتفيا) عام ٢٠٠٧، ودولتان (إيطاليا وسلوفاكيا) عام ٢٠٠٨، وثلاث دول (ألمانيا وجمهورية مولدوفا وصربيا) عام ٢٠٠٩. وبما أنّ الاتفاقية بحاجة إلى التنفيذ فضلاً عن التصديق، فإن كفاءة الصك تعتمد على التعديل الكامل للقوانين الوطنية من جانب الدول التي صدَّقت على الاتفاقية. ولا بدَّ من إثبات على ذلك التعديل أيضاً.

٢- المناقشة العالمية

٣٤- الجانب الآخر من دور الأُطُر الإقليمية، بوصفها صكوكاً للمواءمة على الصعيد العالمي، هو قدرة غير الأعضاء على المشاركة فيها. وعلى الرغم من البعد عبر الوطني للجريمة الحاسوبية، فإن التأثير في أقاليم مختلفة من العالم متفاوت. وينطبق ذلك بشكل خاص على

(٤٨) أرمينيا، إستونيا، ألبانيا، ألمانيا، أوكرانيا، إيسلندا، إيطاليا، بلغاريا، البوسنة والهرسك، جمهورية مقدونيا اليوغوسلافية سابقا، جمهورية مولدوفا، الدانمرك، رومانيا، سلوفاكيا، سلوفينيا، صربيا، فرنسا، فنلندا، قبرص، كرواتيا، لاتفيا، ليتوانيا، النرويج، هنغاريا، هولندا، الولايات المتحدة.

البلدان النامية.[٤٩] والنُهُج الإقليمية المذكورة في الفقرة ٣٢ أعلاه لا تتيح فرصة مشاركة واسعة لغير الأعضاء. ومع أنّ اتفاقية جرائم الفضاء الحاسوبي هي الصك الأوسع عضوية حالياً، فإنها تحدّ من إمكانية مشاركة غير الأعضاء فيها. فقد جاء في المادة ٣٧ منها أنّ الانضمام إليها يتطلب من الدول أن تتشاور مع الدول المتعاقدة في الاتفاقية، وتحصل على موافقتها بالإجماع. ويضاف إلى ذلك أنّ المشاركة في المناقشة بشأن التعديلات المستقبلية الممكنة تقتصر على الأطراف في الاتفاقية (المادة ٤٤).

٣٥- وقد بيَّنت التجربة أنّ الدول تُحجم عموماً عن التصديق على اتفاقيات لم تُسهم في وضعها أو في التفاوض بشأنها وعن الانضمام إليها. وقد ثبتت صحة ذلك بغضِّ النظر عن موضوع الاتفاقيات.

٣٦- وقد وُجِّهت الدعوات إلى إعداد اتفاقية دولية بشأن الجريمة الحاسوبية في جميع الاجتماعات الإقليمية التحضيرية الأربعة لمؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة وللعدالة الجنائية.

٣٧- وصدرت دعوة مماثلة أخرى في اجتماعات رؤساء أجهزة إنفاذ القوانين الوطنية في أفريقيا الشرق الأدنى والأوسط وأوروبا، حيث جرت مناقشات بشأن الإنترنت، وجمع الأدلة الإلكترونية والتشريعات وسواها. وفي اجتماعات عُقدت في مناطق أخرى، خلص المشاركون إلى أنّ أجهزة إنفاذ القانون والسلطات القضائية كانت ضعيفة الإعداد وليست لديها القدرة الكافية على معالجة التطورات في مجال الجريمة الحاسوبية، وعلى جمع واستخدام الأدلة من التكنولوجيات الحاسوبية في التحضير للملاحقة القضائية. وكان هناك اتفاق شامل على أنّ القوانين الوطنية لم تكن مواكبة للتطورات، وعلى ضرورة إدخال تعديلات لدعم التحقيق مع الجناة ومقاضاتهم وإدانتهم على أساس الأدلة المستمدة من تكنولوجيا الحواسيب. وهناك حاجة ملحَّة إلى قواعد مشتركة وإلى التعاون بين الدول، بحيث يمكن للسلطات أن تعمل بفعالية عَبْر الاختصاصات لسَوق الجناة إلى العدالة. كما جاءت الدعوات إلى استحداث صك دولي من المؤسسات الأكاديمية.[٥٠]

---

(٤٩) انظر، على سبيل المثال، تقرير منظمة التعاون والتنمية في الميدان الاقتصادي، *Spam Issues in Developing Countries* (Paris, OECD, 2005), p. 4.، متاح على الموقع http://www.oecd.org/dataoecd/5/47/34935342.pdf؛ وكذلك فهم الجريمة السيبرانية: دليل، الصفحة ١٥ (انظر الحاشية ٢).

(٥٠) Joachim Vogel, "Towards a global convention against cybercrime", paper presented at the First World Conference of Penal Law, Guadalajara, Mexico, 19-23 November 2007; Stein Schjølberg and Solange Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and Security in Cyberspace* (Oslo, E-dit, 2009).

٣- تدابير التصدي للتوجُّهات الحديثة العهد

٣٨- إنّ الجريمة الحاسوبية تتغير باطِّراد. وحين أُعدَّت النُهُج الإقليمية، ومنها القانون النموذجي لرابطة الكومنولث بشأن الحواسيب والجرائم المتعلقة بها، والاتفاقية المتعلقة بجرائم الفضاء الحاسوبي، فإنّ "هجمات بوتنت" الواسعة النطاق، وعمليات "التصيد الاحتيالي" والاستخدام الإرهابي للإنترنت كانت إمَّا غير معروفة وإمَّا أنّ دورها لم يكن ذا أهمية كدورها اليوم. وبناءً على ذلك، لم تُعالج بأحكام محددة. وفي الاجتماعات الإقليمية التحضيرية للمؤتمر الثاني عشر، وُجِّهت المطالبة بمجابهة تلك الظواهر الجديدة، وبخاصة الاستخدام الإرهابي للإنترنت، الذي يتفاوت من الدعاية والاتصالات وتمويل الإرهاب بوساطة خدمات دفع متعلقة بالإنترنت إلى جمع المعلومات عن هدف محتمَل. وقد تناولت فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب[٥١] لتلك الظواهر في عدة مناسبات، فضلاً عن تدابير التصدي القانونية الممكنة لها.

٣٩- ومع أنه يمكن غالباً تغطية تلك الظواهر بتطبيق أحكام على التدخُّل في النظم أو التزوير المتعلق بالحواسيب، فيما يتعلق بالقانون الجنائي الموضوعي، فإن تطبيق الوسائل الإجرائية الواردة في الصكوك الإقليمية أصعب بكثير، وبخاصة لأنّ التكنولوجيات والخدمات المعروضة عَبْر الإنترنت (شبكة العلاقات الاجتماعية مثلاً) قد تغيرت بشكل كبير. فاعتراض اتصالات بروتوكول التواصل عَبْر الإنترنت، وقبول الأدلة الرقمية في الإجراءات القضائية الجنائية، وإجراءات التحقيق في قضايا تشمل تكنولوجيا التشفير أو وسائط الاتصال الخفيّ، هي مسائل ملحَّة، ولكن لا تجري معالجتها على الصعيد الإقليمي، إلاّ باستثناء بعض الحالات التي تجري معالجتها على الصعيد الوطني.[٥٢]

٤٠- وتعد معالجة هذه المسائل هامّة، لأنّ وسائل التحقيق التقليدية تفشل عندما يتعلق الأمر بالتحقيقات في الجرائم الحاسوبية. وأحد الأمثلة على ذلك اعتراض الاتصالات. وفي العقود الأخيرة، طوَّرت الدول وسائل التحقيق، ومنها التنصُّت الهاتفي، الذي مكَّنها من اعتراض الاتصالات الهاتفية عبر الهواتف المتنقلة والثابتة. ويجري عادة اعتراض المكالمات الهاتفية التقليدية من خلال مزوِّدي الاتصالات السلكية واللاسلكية. ولدى تطبيق أجهزة

---

(٥١) انظر، على سبيل المثال، فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب، "تقرير الفريق العامل المعني بمواجهة استخدام الإنترنت لأغراض إرهابية"، شباط/ فبراير ٢٠٠٩. متاح على الموقع www.un.org/terrorism/pdf/wg6-internet_rev 1.pdf.

(٥٢) للاطلاع على استعراض شامل للنهج الوطنية المختلفة التي تعالج هذه المسائل، انظر: فهم الجريمة السيبرانية، دليل، الفصل ٦ (انظر الحاشية ٢).

إنفاذ القانون المبدأ نفسه على اتصالات بروتوكول التواصل الصوتي عَبْر الإنترنت، فإنها تحتاج إلى التفاعل مع مزوِّدي خدمة هذا البروتوكول. أما إذا كانت خدمتهم قائمة على تكنولوجيا الاتصال بين النظراء،(٥٣) فقد يكون مزوِّدي الخدمة غير قادرين عموماً على اعتراض الاتصالات، لأن البيانات ذات الصلة تُنقَل مباشرة بين المشاركين في الاتصال.(٥٤) ولذا، قد تكون هناك حاجة إلى تقنيات جديدة، علاوة على الصكوك القانونية ذات الصلة.

٤١- ولا تتصل القدرة على إجراء تحقيقات متطوِّرة بجرائم جديدة فحسب، وإنما بجرائم حاسوبية ذات طابع تقليدي أكبر، منها استغلال الأطفال في المواد الإباحية. ومنذ منتصف تسعينات القرن الماضي، توافرت لموزِّعي المواد الإباحية ومستهلكيها إمكانية الحصول على خدمات الشبكة التي باتت تُستخدَم بكثافة أكبر.(٥٥) وقد أصبحت الإنترنت الوسيط الرئيسي لتبادل استغلال الأطفال في المواد الإباحية. والمشاكل المتعلقة بالتحرِّي والتحقيق في قضايا استغلال الأطفال في المواد الإباحية قد تم التسليم بها منذ تسعينات القرن الماضي؛ ومعظمها لا يزال موجوداً لأنّ باستطاعة المجرمين استخدام تكنولوجيا متطورة لإعاقة التحقيقات. فبحسب إحدى الدراسات، على سبيل المثال، استخدم ٦ في المائة من الأشخاص، الذين ضُبطوا متورطين في استغلال الأطفال في المواد الإباحية، تكنولوجيا التشفير، و١٧ في المائة منهم استخدموا برامج محمية بكلمة سرّ، و٣ في المائة استخدموا برنامجاً لإزالة الأدلة، و٢ في المائة استخدموا أنظمة تخزين نائية.(٥٦) وبالإضافة إلى ذلك، لوحظ تحوُّل فيما يتعلق بالتكنولوجيا: فبينما ساد التبادل في الأيام الأولى للإنترنت من خلال قنوات تقليدية، منها نقل

---

(٥٣) تتيح تكنولوجيا الاتصال بين النظراء الاتصال المباشر بين المشاركين في الشبكات، بدل إجبار المستخدمين على التواصل باستخدام هياكل مركزية تقليدية قائمة على الخوادم.

(٥٤) فيما يتعلق باعتراض أجهزة إنفاذ القانون لاتصالات بروتوكول التواصل الصوتي عبر الإنترنت، انظر Steven Bellovin and others, “Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP”, 13 June 2006, available from www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf; Matthew Simon and Jill Slay, “Voice over IP: forensic computing implications”, paper presented at the 4th Australian Digital Forensics Conference, Perth, Australia, December 2006.

(٥٥) United States, House of Representatives, “Sexual exploitation of children over the Internet” (2007), 109th Congress, p. 9.

(٥٦) انظر Janis Wolak, David Finkelhor and Kimberly J. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crime: Findings From the National Juvenile Online Victimization Study* (Alexandria, Virginia, National Center for Missing and Exploited Children, 2005), p. 9.

المحادثات عَبْر الإنترنت، بات استغلال الأطفال في المواد الإباحية هو ما يجري تبادله مؤخراً من خلال تكنولوجيا أخرى، مثل شبكات الاتصال بين النظراء.[٥٧]

باء- إنفاذ القانون

٤٢- بالإضافة إلى اعتماد إنفاذ القانون على الصكوك القانونية، فإنه يعتمد، بقدر كبير، على توافر أدوات التحقيق، ومنها البرامج الجنائية (لجمع الأدلة ورصد لوحة المفاتيح واستكشاف أو استرداد الملفات المحذوفة) وبرامج إدارة التحقيق أو قواعد البيانات (مثل القيم المختلطة من صور معروفة لاستغلال الأطفال في المواد الإباحية). وفي السنوات الأخيرة، طوِّرت ولا تزال تُطوَّر عدة أدوات منها.[٥٨] فعلى سبيل المثال، هناك مشروع بحث عنوانه " إعادة البناء التلقائي للأحداث من أجل التحليل الجنائي وتحليل التسلل"، يجري تنفيذه في كلية دبلن الجامعية (المعلومات متوافرة على الموقع http://cci.ucd.ie/?q=node/33)، وفي كانون الأول/ديسمبر ٢٠٠٩، استُحدثت في الولايات المتحدة تكنولوجيا جديدة لتعقُّب استغلال الأطفال في المواد الإباحية تُسمَّى الحمض النووي التصويري. ولا تزال إحدى المسائل الرئيسية المتعلقة بتلك الأدوات هي حاجة المطوِّرين إلى تنسيق الجهود بغية تلافي الازدواجية. وبالمثل، لا بدَّ من تنسيق جهود نقاط اتصال الشبكات (منها تلك المرتبطة بمجموعة الثماني والإنتربول، والشبكة المتصلة باتفاقية جرائم الفضاء الحاسوبي).

جيم- بناء القدرات

٤٣- إنّ الجريمة الحاسوبية مسألة لا تعني البلدان المتقدمة فحسب، ولكنها تعني البلدان النامية أيضا. وبحسب مؤسسة "ديفيلوبمانت غيتواي فاونديشن"، كان المستخدِمون في عام

---

(٥٧) United States, General Accountability Office, *File-Sharing Programs, Child Pornography is Readily Accessible over Peer-to-Peer Networks*, testimony before the Committee on Government Reform, House of representatives, GAO Report GAO-03-537T (Washington, D.C., March 2003); Gretchen Ruethling, "27 charged in international online child pornography ring", *New York Times*, 16 March 2006; Choo, "Organised crime groups", p. 282 (see footnote 40); United Kingdom, Stockport Safeguarding Children Board, *Safeguarding Children in Stockport: Policy and Practice Handbook* (May 2008), p. 299, available at http://www.safeguardingchildreninstockport.org.uk/documents/Section%2000%20-%20Preface%20and%20contents.pdf.

(٥٨) انظر، مثلا، مشروع البحث المعنون: "Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis"، الذي يجري تنفيذه في كلية دبلن الجامعية (المعلومات متاحة على الموقع htt://cci.ucd.ie/?q=node/33).

٢٠٠٥ في البلدان النامية أكثر منهم في البلدان المتقدِّمة.[٥٩] ومن العلامات الإيجابية أنّ الإيكواس قد اعتمدت مؤخراً توجيها بشأن الجريمة الحاسوبية، وأنّ جماعة شرق أفريقيا قد قدَّمت مشروع إطار للقوانين الحاسوبية. ويمكن للمزيد من الدعم أن يساعد أجهزة إنفاذ القانون على التأهب للجرائم التي قد تُرتكَب، حين يصبح الوصول الواسع النطاق مُتاحاً للمزيد من المستخدِمين في العالم النامي. ووجَّهت الجمعية العامَّة، في قرارها ٦٤/ ١٧٩، المعنْوَن "تعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولا سيما قدراته في مجال التعاون التقني"، النظر إلى المسائل المستجدة المتعلقة بالسياسة العامة التي حدَّدها الأمين العام (A/64/123) في مجال القرصنة والجرائم الحاسوبية والاستغلال الجنسي للأطفال والجريمة في المدن، ودعت المكتب إلى استكشاف سبُل ووسائل التصدي لهذه المسائل في إطار ولايته.

دال- التدريب

٤٤- بما أنّ التحقيق في الجرائم الحاسوبية ومقاضاة الضالعين في ارتكابها ينطوي على تحديات فريدة، فمن المهم توفير التدريب لضباط إنفاذ القانون والمدَّعين العامِّين والقضاة. وكما جرى التأكيد في اجتماعٍ بشأن الجريمة الحاسوبية عقده المكتب المعني بالمخدرات والجريمة لفريق من الخبراء، في فيينا، يومي ٦ و٧ تشرين الأول/أكتوبر ٢٠٠٩، فإن معظم المنظمات الدولية والإقليمية المعنية بالمسألة قد اتخذت خطوات لتدريب الخبراء المشاركين في إجراء تحقيقات بشأن الجرائم الحاسوبية وإعداد مواد تدريبية.[٦٠]

رابعا- الاستنتاجات والتوصيات

٤٥- إنّ التحقيق في الجرائم الحاسوبية وملاحقة مرتكبيها قضائياً يعدَّان مصدر تحدٍّ لجميع المؤسسات المعنية بهما. ومع مراعاة تعقُّد المسألة والتطور التقني المطَّرد، يبقى التدريب المستدام والمتَّسع دائما مسألة رئيسية لجميع السلطات المعنية. وقد بيَّنت المناقشة التي جرت في اجتماع فريق الخبراء الذي عقده المكتب المعني بالمخدرات والجريمة عام ٢٠٠٩ بشأن

(٥٩) المعلومات متاحة على الموقع http://topics.developmentgateway.org/special/informationsociety.

(٦٠) على سبيل المثال، نظمت رابطة التعاون الاقتصادي لآسيا والمحيط الهادئ عدة أنشطة تدريبية بشأن الجريمة الحاسوبية، بما في ذلك التشريع بشأنها؛ ونظَّمت رابطة الكومنولث دورات تدريبية قانونية وتقنية؛ وأسهم مجلس أوروبا في أنشطة تدريبية في أرجاء مختلفة من العالم، وأعدّ مواد تدريبية محددة للقضاة؛ ودعم الاتحاد الأوروبي إعداد دورات ومواد تدريبية بشأن الجريمة الحاسوبية لأجهزة إنفاذ القانون في الدول الأعضاء فيه، ونظَّم عدة دورات تدريبية داخل أوروبا وخارجها؛ كما نظَّمت الإنتربول عدة دورات تدريبية لأجهزة إنفاذ القانون، وأعدَّت مواد تدريبية؛ وأعدَّ الاتحاد الدولي للاتصالات مواد تدريبية بشأن الجريمة الحاسوبية، وهي متاحة بجميع لغات الأمم المتحدة، ووفّر تدريباً عاماً في عدة مناسبات إقليمية، وتدريباً خاصاً للقضاة.

الجريمة الحاسوبية أنّ بناء القدرات المؤسسية واستدامتها البعيدة المدى هما عاملان رئيسيان لقياس نجاح المبادرات المستقبلية.

٤٦- وللقضاء على الملاذات الآمنة وتحسين التعاون الدولي، ينبغي إيلاء الاهتمام لسد الثغرات في التشريعات القائمة، وتعزيز اتساق القوانين وتماسكها وتوافقها. ومع أخذ أهمية مواءمة التشريعات في الحسبان، والاستفادة من نتائج الاجتماعات التحضيرية لمؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، ينبغي النظر في وضع اتفاقية عالمية لمكافحة الجريمة الحاسوبية بعين التأني والقبول.

٤٧- وفي غضون ذلك، سيوفر المكتب المعني بالمخدرات والجريمة، بصفته جهة تعنى بوضع المعايير في مسائل منع الجريمة والعدالة الجنائية، منبراً متعدد الأطراف مع التركيز على البلدان النامية. وسيواصل اعتماد نهج شامل، وقائم على الشراكة ومتعدد التخصصات، بحشد خبرته الفنية القانونية والتقنية والمتعلقة بإنفاذ القانون، التي أثبتت جدواها، لمكافحة الأنشطة الإجرامية، وذلك إلى جانب الخبرات الفنية المحددة والمتطورة لدى الشركاء الرئيسيين، المنخرطين بالفعل في مكافحة الجريمة الحاسوبية. ويستهدف المكتب الشراكة بالأدوات والخبرات وتجميعها معاً، بما في ذلك من القطاع الخاص (ولا سيما من مزوِّدي خدمة الإنترنت)، لمعالجة المشكلة في بلد معين أو منطقة معيَّنة. وستُعطى الأولوية لتقديم المساعدة التقنية إلى الدول الأعضاء التي تحتاج إليها، بهدف معالجة النقص في القدرات والخبرات، وضمان الاستدامة البعيدة المدى في التعامل مع الجرائم المتعلقة بالحاسوب.

٤٨- وسيستهدف المكتب تحديداً القيام بما يلي: مساعدة الدول الأعضاء في اعتماد تشريعات للتحقيق الفعّال في الجرائم المتعلقة بالحاسوب وملاحقة الجناة قضائياً؛ وبناء المعرفة التشغيلية والتقنية للقضاة والمدّعين العامّين وضباط إنفاذ القانون، بشأن المسائل المتعلقة بالجريمة الحاسوبية، من خلال التدريب وتكييف/تطوير المواد التدريبية بشأن التحقيق في الجرائم المتعلقة بالحاسوب، وما شابهها، ومقاضاة مرتكبيها وتدريب سلطات إنفاذ القانون لكي تستخدم بفعالية آليات التعاون الدولي لمكافحة الجريمة الحاسوبية؛ ورفع مستوى الوعي لدى المجتمع المدني وإيجاد قوة دفع لدى متخذي القرارات لتوحيد الجهود لمنع الجريمة الحاسوبية ومكافحتها؛ واستبانة الممارسات الجيدة وتعميمها، وتعزيز الشراكات بين القطاعين العام والخاص في مجال منع الجريمة الحاسوبية ومكافحتها.