Distr.: General
18 August 2015
Arabic
Original: English

مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية

الفريق العامل المعني بالتعاون الدولي
فيينا، ٢٧ و٢٨ تشرين الأول/أكتوبر ٢٠١٥
البند ٢ من جدول الأعمال المؤقَّت*
جمع وتبادل الأدلة الإثباتية الإلكترونية

جمع وتبادل الأدلة الإثباتية الإلكترونية

ورقة معلومات أساسية من إعداد الأمانة

أولاً- مقدِّمة

١- تطرح الجرائم التي تنطوي على أدلة إثباتية إلكترونية تحديات فريدة أمام السلطات التي يُعهد إليها باتخاذ تدابير التصدي المناسبة لها سواء على الصعيد الداخلي (المشرِّعون والمحقِّقون والمدَّعون العامّون والقضاة) أو على مستوى التعاون الدولي.

٢- وبصفة عامة، يمكن أن تشمل الأدلة الإثباتية الإلكترونية أيَّ بيانات مولَّدة أو مخزَّنة في شكل رقمي كلما استُخدم الحاسوب. وهي تشمل المعلومات التي يُدخلها أيُّ فرد يدويًّا في جهاز إلكتروني أو المعلومات المولَّدة في معاملة حاسوبية أو استجابة لطلب، حيث يولِّد جهاز إلكتروني معلومات كما لو كان إنساناً آليًّا أو معلومات منتَجة ومخزَّنة حيثما يعالج جهاز ما معلومات ضمن مصفوفته. ومن ثمَّ، فإنَّ الأدلة الإثباتية الإلكترونية هي أيُّ معلومات مدرَجة أو مولَّدة أو محفوظة في قواعد بيانات أو نظم تشغيلية أو برامج تطبيقات

* CTOC/COP/WG.3/2015/1.

أو نماذج مولَّدة حاسوبيًّا تستنبط بالاستقراء نتائج ورسائل بريد إلكتروني وصوتي بل وحتى تعليمات محتفَظاً بها في صورة خامدة ضمن مصرف ذاكرة حاسوبية.[1]

٣- وقد أَعدت الأمانةُ هذه الورقة بغية تقديم معلومات أساسية عن مفاهيم وجوانب رئيسية تتعلق بالأدلة الإثباتية الإلكترونية ومساعدة الفريق العامل في المناقشات التي سيجريها بشأن بند جدول الأعمال ذي الصلة من اجتماعه.

ثانياً- جمع وتبادل الأدلة الإثباتية الإلكترونية: مجالات للنظر فيها والاستجابة لها على الصعيدين الوطني والدولي

٤- توجد صلة وثيقة بين جمع الأدلة الإثباتية الإلكترونية وتبادلها، ومن ثمَّ فإنَّ التشريعات الوطنية والاتفاقات أو الترتيبات الإقليمية والدولية كثيراً ما تنص على صلاحيات تحقيقية لجمع الأدلة الإثباتية الإلكترونية وعلى آليات التعاون لتبادلها.

ألف- جمع الأدلة الإثباتية الإلكترونية

١- الأطر القانونية الوطنية

٥- تتضمن قوانين الإجراءات الجنائية التقليدية في العادة أحكاماً بشأن جمع الأدلة الإثباتية وقبولها. وعندما يتعلق الأمر بأدلة في شكل إلكتروني، يمكن تحريف البيانات الحاسوبية والسجلات الإلكترونية بسهولة. ومن ثمَّ، ينبغي لجمع الأدلة الإثباتية الإلكترونية وتناولها أن يضمنا الصحة والسلامة والاستمرارية طوال الفترة الزمنية الكاملة التي تفصل بين ضبطها واستخدامها في المحاكمة.

(أ) الصلاحيات القانونية لجمع الأدلة الإثباتية الإلكترونية ومناولتها

٦- إنَّ للصلاحيات التحقيقية الوطنية دوراً رئيسيًّا في جمع الأدلة الإثباتية الإلكترونية. وكما جاء في الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة بشأن الجريمة السيبرانية، يجوز للدول، في سبيل إجراء تحقيقات فعّالة وجمع الأدلة الإثباتية الإلكترونية، أن تسنَّ تشريعات إجرائية تمنح صلاحيات لسلطات إنفاذ القانون ذات الصلة.

(١) Ireland Law Reform Commission, "Documentary and Electronic Evidence", Consultation paper, December 2009, p. 8.

ويمكن لصلاحيات التحقيق أن تتراوح بين تطبيق الصلاحيات الإجرائية التقليدية، والصلاحيات التحقيقية العامة بمعناها الواسع، والصلاحيات التحقيقية العامة المصمَّمة بحيث تنطبق على مجموعة من التدابير الخاصة بالفضاء السيبراني، والصلاحيات التحقيقية الشاملة المنفَّذة من أجل الحصول على الأدلة الإثباتية الإلكترونية.(٢)

٧- وكما تبيِّنه الدراسة عن الجريمة السيبرانية بمزيد من الوضوح، يكشف فحص الأساس القانوني للصلاحيات التحقيقية المستخدمة في الجرائم التي تنطوي على أدلة إثباتية إلكترونية أنَّ ثمة تنوعاً كبيراً في النُّهُج المتبعة على الصعيد الوطني. وترتبط تلك النُّهُج أولاً بمدى إمكانية تفسير الصلاحيات "التقليدية" على أنها تنطبق على البيانات غير الملموسة، وكذلك بمدى وجود سلطة قانونية فيما يخص التدابير التدخُّلية بصفة خاصة، من قبيل تحقيقات التحليل الجنائي عن بُعد.

٨- ومع ذلك، ففي حين تتباين الصلاحيات القانونية، يبدو أنَّ هناك درجة جيِّدة من التوافق في الآراء بين الدول التي قدَّمت تقارير لأغراض الدراسة عن الجريمة السيبرانية بشأن أنواع التدابير التحقيقية التي ينبغي أن تكون متاحة من أجل جمع الأدلة الإثباتية الإلكترونية. ويمكن أن تشمل تلك التدابير التعجيل بحفظ البيانات الحاسوبية؛ وأوامر الحصول على بيانات المحتوى المخزَّنة؛ وأوامر الحصول على بيانات الاتصالات المخزَّنة؛ وأوامر الحصول على معلومات عن المشتركين؛ وجمع بيانات المحتوى في الوقت الحقيقي؛ وجمع بيانات الاتصالات في الوقت الحقيقي؛ والبحث عن المعدات أو البيانات الحاسوبية؛ ومصادرة المعدات أو البيانات الحاسوبية؛ والوصول عبر الحدود إلى النظم أو البيانات الحاسوبية؛ واستخدام أدوات التحليل الجنائي عن بُعد.(٣)

٩- ولكي تتولى سلطات إنفاذ القانون التحقيق بفعالية في الجريمة السيبرانية وجمع الأدلة الإثباتية الإلكترونية ذات الصلة، اكتسب التعاون مع الجهات الفاعلة المعنية الأخرى، بما في ذلك من القطاع الخاص، أهمية خاصة على مدى السنوات الأخيرة. وبصفة عامة، يضطلع

(٢) مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، مشروع دراسة أعدها المكتب لكي ينظر فيها فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، UNODC, Comprehensive Study on Cybercrime: Draft — 2013, prepared by UNODC for the consideration of the Expert Group to Conduct a Comprehensive Study on Cybercrime (www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_ .STUDY_210213.pdf), Chapter 5, p. 125

(٣) ترد أمثلة على القوانين الوطنية بشأن هذه التدابير التحقيقية في مستودع الجريمة السيبرانية (http://cybrepo.unodc.org) وبوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة "شيرلوك" (http://sherloc.unodc.org).

مقدِّمو خدمات الإنترنت بدور مهم في إتاحة الوصول إلى الأدلة الإثباتية الإلكترونية. وقد يكون للقوانين الوطنية بشأن الخصوصية أثر أيضاً على قدرة مقدِّمي خدمات الإنترنت على تبادل المعلومات مع السلطات المعنية أثناء التحقيق. فعلى سبيل المثال، يجوز للدول أن تفرض قيوداً على نوع البيانات التي يمكن الوصول إليها، وأن تفرض حدوداً زمنية، وأن تضع متطلبات بشأن "السبب المحتمل"، وأن تفرض إشرافاً من جانب أجهزة النيابة العامة والقضاء.[٤] ونتيجة لإجراءات الحماية المستندة إلى الخصوصية الواردة في التشريعات الوطنية، قد يتعين على مقدِّمي خدمات الإنترنت الالتزام بعدم الإفصاح عن المعلومات الخاصة بالبيانات الشخصية للمشترك وبيانات المحتوى وبيانات الاتصالات. وبالإضافة إلى القوانين الوطنية، يضع القانون الدولي لحقوق الإنسان معايير محدَّدة للحقوق المتعلقة بالخصوصية للأشخاص الخاضعين لتحقيقات أجهزة إنفاذ القوانين.

١٠- وقد اعتُمدت "المبادئ التوجيهية للتعاون بين أجهزة إنفاذ القانون ومقدِّمي خدمات الإنترنت من أجل مكافحة الجرائم السيبرانية" التي أعدها مجلس أوروبا استجابةً لأهمية مقدِّمي خدمات الإنترنت في جمع الأدلة الإثباتية الإلكترونية. وتهدف المبادئ التوجيهية إلى مساعدة سلطات إنفاذ القانون ومقدِّمي خدمات الإنترنت على هيكلة تفاعلاتهم على النحو الصحيح عند التصدي للمسائل المتعلقة بالجرائم السيبرانية. ويتوخى أن تتسم المبادئ التوجيهية بالمرونة وأن تُطبق في أيِّ بلد وفقاً للتشريعات الوطنية واحترام حقوق المواطنين الأساسية. وتُشجَّع سلطات إنفاذ القانون ومقدِّمو خدمات الإنترنت على اتخاذ جملة خطوات، من بينها تبادل المعلومات؛ وتعزيز ثقافة التعاون؛ ووضع إجراءات مكتوبة للتعاون المتبادل؛ والنظر في إنشاء شراكات رسمية؛ وحماية الحقوق الأساسية للمواطنين.[٥]

(ب) بناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية على مناولة الأدلة الإثباتية الإلكترونية

١١- الأدلة الإثباتية الإلكترونية هشّة بطبيعتها. فهي قابلة للتحريف أو الإتلاف أو التدمير من خلال سوء المناولة أو الفحص بطريقة غير سليمة. ولهذا السبب، ينبغي اتخاذ احتياطات

(٤) Cybercrime Study, Chapter 5, p. 134.

(٥) المبادئ التوجيهية للتعاون بين أجهزة إنفاذ القانون ومقدِّمي خدمات الإنترنت من أجل مكافحة الجرائم السيبرانية، متاحة في الرابط:
www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

خاصة من أجل توثيق هذا النوع من الأدلة الإثباتية وجمعه والحفاظ عليه وفحصه. وقد يؤدي عدم القيام بذلك إلى جعل هذه الأدلة غير صالحة للاستعمال أو يُفضي إلى استنتاجات غير دقيقة.

١٢- ومن ثمَّ، يتسم بناء القدرات على صعيد أجهزة إنفاذ القانون ونظم العدالة الجنائية الوطنية بأهمية حاسمة. ومع أنَّ غالبية البلدان شَرَعت في إنشاء هياكل متخصِّصة للتحرِّي عن الجرائم السيبرانية والجرائم المنطوية على أدلة إثباتية إلكترونية، فإنَّ هذه الهياكل تعاني في كثير من البلدان من نقص التمويل والقدرات. ومع زيادة انتشار الأدلة الإثباتية الرقمية في مجال التحرِّي عن الجرائم "التقليدية"، فقد يتعيَّن على سلطات إنفاذ القانون أن تميِّز بوضوح بين الجهات المعنية بالتحقيق في الجرائم السيبرانية وتلك المعنية بمختبرات التحليل الجنائي الرقمي، وأن تحدِّد بوضوح تسلسل سير عملهما. وقد يحتاج موظفو الخطوط الأمامية في أجهزة إنفاذ القانون، بصورة متزايدة، إلى اكتساب واستخدام مهارات أساسية، مثل المهارات اللازمة لإنتاج صورة طبق الأصل لجهاز تخزين إلكتروني لأغراض الاستدلال الجنائي.

١٣- ومع شيوع التطوُّرات التكنولوجية الجديدة مثل الشبكات المُخفية للهوية والتشفير العالي الدرجة والعملات الافتراضية في الجرائم التي تشمل أدلة جنائية إلكترونية، سوف يتعيَّن أيضاً على المحقِّقين أن يعتمدوا استراتيجيات جديدة. فعلى سبيل المثال، يمكن لسلطات إنفاذ القانون أن تعمل على تدعيم الشراكات مع أفرقة البحث الأكاديمي التي تركِّز على استحداث منهجيات تقنية في مجالات مثل تحديد سمات المعاملات التي تُجرى بالعملات الافتراضية ودراستها.[٦] وربما يتعيَّن أيضاً على المحقِّقين أن ينظروا في كيفية استخدام أساليب التحرِّي الخاصة، مثل المراقبة والعمليات المستترة واستخدام المُخبِرين والتسليم المراقب، في حالة بيع سلع غير مشروعة عبر الإنترنت، جنباً إلى جنب مع التحرِّيات الخاصة بالإنترنت وتقنيات التحليل الجنائي الرقمي من أجل جمع الأدلة الإثباتية الإلكترونية الحساسة والهشة. ومن الواضح إجمالاً أنَّ بناء قدرات الجهات المعنية بإنفاذ القانون والعدالة الجنائية في مجال مكافحة الجريمة السيبرانية و/أو الجريمة التي تنطوي على أدلة إثباتية إلكترونية سيكون عمليةً جاريةً ومتواصلةً، مع استمرار ظهور الابتكارات التكنولوجية والإجرامية بإيقاع سريع.[٧]

(٦) انظر، مثلاً، Sarah Meiklejohn and others, “A fistful of bitcoins: characterizing payments among men with no names”, in Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference (New York, ACM, 2013).

(٧) مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، ورقة معلومات أساسية من إعداد الأمانة بشأن حلقة العمل الثالثة: تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدِّي للأشكال المتطوِّرة للجريمة، مثل

(ج) دور الهياكل أو الوحدات المتخصصة في الجرائم السيبرانية: النُّهُج الداخلية

١٤- ما فتئ تخصُّص الأجهزة الوطنية لإنفاذ القانون في التحقيق في الجرائم السيبرانية و/أو الجرائم التي تنطوي على أدلة إثباتية إلكترونية يزداد شيوعاً ويؤدي دوراً حاسم الأهمية في تيسير عمليات جمع الأدلة الإثباتية الإلكترونية وتحليلها وتبادلها. ويرتبط هذا التخصص أساساً بالطبيعة الخاصة للجريمة السيبرانية التي تطرح تحديات محدَّدة فيما يتعلق بتعاريف الجريمة وإمكانية تطبيق القوانين وجمع الأدلة الإثباتية وتحليلها. ومن ثمَّ، فإنَّ مستوى المهارات والقدرات التقنية لدى هيئات إنفاذ القانون سيكون له أثر مباشر على فعالية التدابير المتخذة في مجال منع الجريمة والعدالة الجنائية لمواجهة الجريمة السيبرانية.[٨] وبالإضافة إلى ذلك، فبالنظر إلى زيادة انتشار الأجهزة الإلكترونية وشبكة الإنترنت والتواصلية العالمية في الحياة اليومية، صارت الأدلة الإثباتية الإلكترونية، مثل الرسائل النصّية ورسائل البريد الإلكتروني وبيانات تصفُّح الإنترنت، من الأمور المعتادة في كثير من التحقيقات الجنائية "التقليدية".[٩] ونتيجة لذلك، هناك أيضاً حاجة متزايدة إلى أن تكون لدى أجهزة إنفاذ القوانين على جميع المستويات – سواء المحلية أو الوطنية – قدرات أساسية على الأقل للتحقيق في الجريمة السيبرانية.

١٥- وكان أكثر المجالات ذكراً باعتباره يتطلب "تدخلات المساعدة التقنية" في الدراسة عن الجريمة السيبرانية هو عموماً مجال أساليب التحرِّي المتعلقة بالجرائم السيبرانية. ومن بين البلدان التي تحتاج إلى المساعدة، أشارت نسبة قدرها ٦٠ في المائة منها إلى أنَّ وكالات إنفاذ القانون فيها بحاجة إلى هذا النوع من المساعدة.[١٠] وأشارت الدول المبلِّغة لأغراض الدراسة عن الجريمة السيبرانية أيضاً إلى أنَّ مراكز الشرطة المحلية، في العديد من الحالات، تحيل قضايا الجرائم السيبرانية إلى جهة متخصصة في إنفاذ القانون على المستوى الوطني.[١١]

١٦- ويمكن للهياكل أو الوحدات المتخصصة في الجريمة السيبرانية داخل أجهزة إنفاذ القانون أن تسهِّل على الدول تركيز مواردها المحدودة في مكان واحد من أجل وضع أساليب التحري المتخصصة وجمع الأدلة الإثباتية الإلكترونية وتحليلها على نحو مناسب، بما في ذلك

الجرائم الإلكترونية (السيبرانية) والاتِّجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي، الوثيقة A/CONF.222/12، الفقرتان ٣٧ و٣٨.

(٨) Cybercrime Study, Chapter 5, p. 152.

(٩) انظر الحاشية ٧ أعلاه، الوثيقة A/CONF.222/12، الفقرة ١٦.

(١٠) Cybercrime Study, Executive Summary, p. xxiii.

(١١) Cybercrime Study, Chapter 5, p. 118.

إجراء فحوص التحليل الجنائي الرقمي. وفي الوقت نفسه، يمكن لهذه الهياكل أو الوحدات أن توفِّر التدريب لأجهزة إنفاذ القانون المحلية، وتنسق التدابير الوطنية للتصدي للجريمة السيبرانية، وتيسّر التعاون فيما بين الشركاء المشاركين في التحقيقات، وتستهدف أشكال الجريمة السيبرانية التي قد تكون مثيرة لقلق خاص لدى الدولة، مثل إيذاء الأطفال عبر شبكة الإنترنت والجرائم المتصلة بالهوية وعمليات الاحتيال والغش عبر شبكة الإنترنت، وما إلى ذلك.

(د) مقبولية الأدلة الإثباتية الإلكترونية في المحاكم

١٧- متى جُمعت الأدلة الإثباتية الإلكترونية وتُبُودِلَتْ، فإنها تصبح في الأحوال المثالية مقبولة في الإجراءات الجنائية. وإذا كان قانون الأدلة الإثباتية يعتمد تقليديًّا على السجلات الورقية، فإنَّ الشهادات الشفوية والأشياء المادية كانت دائماً جزءاً من الإجراءات التي تشهدها قاعات المحاكم. بيد أنَّ تزايد أهمية الأدلة الإثباتية الإلكترونية في الإجراءات الجنائية يطرح تحديات لم تكن معروفة من قبل، ومن ثمَّ كانت الدراسة عن الجريمة السيبرانية بمثابة "عملية رسم خريطة" لتجسيد النُّهُج القانونية الوطنية فيما يتعلق بمقبولية تلك الأدلة الإثباتية في المحاكم الجنائية.

١٨- وفي هذا السياق، أفادت نسبة ٨٥ في المائة من البلدان المجيبة بأنَّ الأدلة الإثباتية الإلكترونية مقبولة في الإجراءات الجنائية. وأفاد العدد الأكبر من البلدان التي تقبل الأدلة الإثباتية الإلكترونية بأنَّ تلك الأدلة الإثباتية تحظى بنفس معاملة الأدلة الإثباتية المادية. وأفادت نسبة تقلّ عن ٤٠ في المائة من البلدان بوجود تمييز قانوني بين الأدلة الإثباتية الإلكترونية والأدلة الإثباتية المادية. وأبلغ عدد قليل جدًّا من البلدان عن وجود قوانين إثباتية خاصة تحكم الأدلة الإثباتية الإلكترونية. وفيما يخص البلدان المبلِّغة بذلك، تشمل القوانين مجالات مثل الافتراضات القانونية المتعلقة بملكية البيانات والوثائق الإلكترونية أو تأليفها، إلى جانب الظروف التي يجوز فيها اعتبار الأدلة الإثباتية الإلكترونية ذات حجية.[١٢]

٢- التعاون الدولي

١٩- تطرح الجرائم التي تنطوي على أدلة إثباتية رقمية تحديات فريدة أمام التعاون الدولي. ونظراً للطابع غير المستقر للأدلة الإثباتية الإلكترونية، يقتضي التعاون الدولي بشأن مسائل الجريمة السيبرانية استجابةً سريعة وقدرةً على طلب إجراءات تحقيقية متخصصة، بما في ذلك

(١٢) Cybercrime Study, Chapter 6, pp. 165-167.

حفظ البيانات وتوفيرها من قِبل مقدمي الخدمات من القطاع الخاص. وتشمل التحديات الشائعة لدى طلب تلك البيانات من ولاية قضائية أخرى حالات التأخير في الاستجابة للطلبات، وعدم الالتزام والمرونة من جانب السلطة التي تُطلب منها الأدلة الإثباتية، والشكل الذي تُقدَّم به الأدلة الإثباتية إلى الولاية القضائية الطالبة وما إذا كان يمكن أن تُستخدم في الإجراءات الجنائية، واختلاف تعاريف الجرائم الجنائية بين الولايات القضائية.(١٣)

٢٠- وفي حين يوجد عدد من أنماط التعاون غير الرسمية في مجال إنفاذ القانون، بما في ذلك الشبكات العاملة على مدار الساعة طوال أيام الأسبوع، ما زالت البلدان تعتمد بشدة على الوسائل القضائية الرسمية التقليدية، وخصوصاً الصكوك الثنائية المعنية بالمساعدة القانونية المتبادلة، لغرض الحصول على الأدلة الإثباتية التي تتجاوز الحدود الإقليمية، حيث يستخدم أكثر من ٧٠ في المائة من البلدان طلبات المساعدة القانونية المتبادلة الرسمية.(١٤) وتبلغ المدة الزمنية التي تستغرقها الاستجابة لطلبات المساعدة القانونية بشأن التحقيق في جريمة سيبرانية نحو ١٥٠ يوماً عادة. وفي كثير من الأحيان قد تتجاوز هذه المدد الزمنية مدة احتفاظ مقدم الخدمات للبيانات، أو قد يتمكّن مرتكبو الجريمة خلالها من إتلاف الأدلة الإثباتية الرقمية الرئيسية تلفاً نهائيًّا.

٢١- لذا فإنَّ التعاون الدولي الفعَّال في القضايا التي تنطوي على أدلة إثباتية رقمية يقتضي وجود آليات لحفظ البيانات بسرعة ريثما يُنظر في المزيد من تدابير التحرّي. ويمكن أيضاً تحسين التعاون الدولي في القضايا التي تنطوي على أدلة إثباتية رقمية باتّباع نُهُج مشتركة في صياغة طلبات الحصول على أنواع محدَّدة من الأدلة الإثباتية، بما في ذلك الأدلة الإثباتية الخاصة بشبكة الإنترنت وسجلات الوصلات والصور طبق الأصل لأغراض الاستدلال الجنائي.

٢٢- وتُنشئ بعض الصكوك المتعدِّدة الأطراف الموجودة آليات تهدف إلى تيسير وصول أجهزة إنفاذ القانون إلى البيانات، مثل نقاط الاتصال المتاحة على مدار الساعة فيما يتعلق بالتحرِّيات عن الجرائم السيبرانية، والوصول عبر الحدود إلى البيانات الحاسوبية المخزَّنة بموجب تصريح أو حيثما تكون متاحةً لعامة الناس، والطلبات العاجلة للمساعدة المتبادلة.

(١٣) مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، دراسة مقارنة حول الممارسات الراهنة في مجال المراقبة الإلكترونية في سياق التحقيق في الجرائم الخطيرة والمنظَّمة، UNODC Comparative study on current practices in electronic surveillance in the investigation of serious and organized crime, p. 9 (www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf).

(١٤) Cybercrime Study, Executive Summary, p. xxv.

٢٣- فعلى سبيل المثال، بموجب اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، تتولى نقاط اتصال متاحة على مدار الساعة طوال أيام الأسبوع تسهيل القيام بما يلي أو الاضطلاع به مباشرةً إذا كانت القوانين والممارسات الداخلية تسمح بذلك: '١' تقديم المشورة التقنية؛ و'٢' حفظ البيانات؛ و'٣' جمع الأدلة الإثباتية وتوفير المعلومات القانونية وتحديد موقع المشتبه فيهم.

٢٤- وهناك عدد من الاتفاقات الدولية التي تتناول مجالات ذات صلة بجمع الأدلة الإثباتية الإلكترونية. فعلى سبيل المثال، تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية على أنَّ نطاق الأحكام الإجرائية الواردة في الاتفاقية ينطبق على الصلاحيات والإجراءات لأغراض جمع الأدلة الإثباتية في شكل إلكتروني لفعل إجرامي.

٢٥- ويتضمن مشروع القانون النموذجي بشأن الأمن السيبراني (٢٠١١) للسوق المشتركة لدول شرق أفريقيا والجنوب الأفريقي (كوميسا) أحكاماً تتعلق بمقدِّمي خدمات الإنترنت. وتشمل الأحكام التزامات بالرصد (المادة ١٧)؛ والتزويد الطوعي بالمعلومات (المادة ١٧ (ب))؛ وإشعارات الإزالة (المادة ١٦)؛ ومسؤولية مقدِّمي الخدمات (المادة ١٢)، والتخزين المؤقت (المادة ١٣)، والاستضافة (المادة ١٤)، ومقدِّمي الوصلات التشعبية/محركات البحث (المادة ١٥). وإضافة إلى ذلك، يتضمن توجيه الاتحاد الأوروبي 2000/31/EC و'١' النصوص التشريعية النموذجية بشأن الجريمة السيبرانية/الجرائم الإلكترونية و'٢' الأدلة الإثباتية الإلكترونية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات أحكاماً مشابهة ولكنها أقل عدداً مقارنةً بمشروع القانون النموذجي للكوميسا.

٢٦- وقد يجرى تعاون غير رسمي بين أجهزة إنفاذ القانون لجمع الأدلة الإثباتية الإلكترونية من ولايات قضائية أخرى. ويمكن لذلك التعاون أن ييسِّر مختلف التدابير من أجل الحصول على أدلة إثباتية خارجة عن الحدود الإقليمية، بما في ذلك البحث والمصادرة؛ وحفظ البيانات الحاسوبية؛ وأوامر الحصول على البيانات الحاسوبية؛ وجمع البيانات في الوقت الحقيقي؛ واستخدام أدوات التحليل الجنائي عن بُعد؛ ووصول أجهزة إنفاذ القانون بصورة مباشرة للبيانات الخارجة عن الحدود الإقليمية.[١٥]

٢٧- وقد يتعيَّن على أجهزة إنفاذ القانون، بصورة متزايدة، أن تجد سبلاً ريادية للتعاون في التحرِّيات عبر الوطنية عن الجرائم السيبرانية. وربما كان إشراك كيانات مثل المجمَّع العالمي

(١٥) Cybercrime Study, Chapter 5, pp. 126-133.

للابتكار، التابع للإنتربول،[١٦] والمركز الأوروبي لشؤون الجريمة السيبرانية، التابع لمكتب الشرطة الأوروبي (اليوروبول)،[١٧] في تنسيق التحرِّيات عبر الوطنية ودعمها ذا أهمية بالغة في هذا الشأن. وقد أتاحت محافل ومبادرات أخرى، مثل المؤتمر العالمي المعني بالفضاء السيبراني، أيضاً للبلدان فرصة النظر في تدابير مبتكرة في مجال التعاون الدولي على مكافحة الجريمة السيبرانية.

٢٨- وتطرح الحوسبة السحابية أيضاً تحدياً متزايداً أمام التعاون الدولي بسبب نقل الخدمات الحاسوبية بشكل متزايد إلى خوادم ومراكز بيانات موزَّعة جغرافيا، مما يجعل من الصعب تحديد "موقع" الأدلة الإثباتية الإلكترونية.[١٨] فعلى سبيل المثال، يمكن لمستخدم محرك البحث غوغل الوصول إلى البيانات المخزَّنة أو المعالَجة في أمريكا الشمالية أو جنوب شرق آسيا أو أوروبا الشمالية أو الغربية.[١٩]

باء- تبادل الأدلة الإثباتية الإلكترونية

١- الأطر القانونية الوطنية

٢٩- وضعت بعض الدول تشريعات داخلية تتناول تبادل الأدلة الإثباتية من خلال التعاون الدولي. فعلى سبيل المثال، يوجد لدى العديد من الدول تشريعات داخلية بشأن المساعدة المتبادلة في المسائل الجنائية يمكن أيضا استخدامها لتبادل الأدلة الإثباتية الإلكترونية.

٢- التعاون الدولي

٣٠- لتيسير تبادل الأدلة الإثباتية الإلكترونية بين الولايات القضائية، يمكن للدول إبرام اتفاقات ثنائية وإقليمية ودولية. وقد تتضمن تلك الاتفاقات أحكاماً تتصل بتقديم المساعدة على حفظ البيانات الحاسوبية؛ والمساعدة على ضبط البيانات الحاسوبية والوصول إليها وجمعها والإفصاح عنها؛ والوصول إلى البيانات الحاسوبية عبر الحدود؛ وتقديم المعلومات غير الملتمَسة وتبادل المعلومات؛ وطلبات المساعدة القانونية المتبادلة العامة.[٢٠] وتشكِّل الأحكام

(١٦) www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.

(١٧) www.europol.europa.eu/ec3.

(١٨) Cybercrime Study, Chapter 7, p. 216.

(١٩) Cybercrime Study, Chapter 7, pp. 216-217.

(٢٠) Cybercrime Study, Annex 3, pp. 273-274.

المشمولة بتلك الاتفاقات المصادر الأوّلية للقوانين التي تشمل حقوق والتزامات الأطراف في الاتفاقات، بما يُخضِع الأطراف لشروط قانونية ملزِمة. بيد أنَّ وجود معاهدة رسمية لا تقتضيه كل الدول كشرط للتعاون القضائي على تبادل الأدلة الإثباتية الإلكترونية، وقد تقدِّم المساعدة، بدلا من ذلك، على أساس المعاملة بالمثل أو المجاملة.

٣١- ويبيِّن استعراض الاتفاقات الإقليمية والدولية مختلف الأشكال المتاحة للدول لتبادل الأدلة الإثباتية الإلكترونية. وتشمل أشكال التعاون تلك المبادئ العامة للتعاون الدولي؛ والمساعدة القانونية المتبادلة العامة؛ وآليات لتعجيل المساعدة؛ والمساعدة في حفظ البيانات الحاسوبية؛ والمساعدة على ضبط البيانات الحاسوبية/الوصول إليها/جمعها/الإفصاح عنها؛ والوصول إلى البيانات عبر الحدود؛ وتوفير المعلومات غير الملتمَسة/تبادل المعلومات. وتتضمن الاتفاقات التالية طائفة من أشكال التعاون المذكورة أعلاه:

الأمم المتحدة، البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية (٢٠٠٠)؛

كومنولث الدول المستقلة، اتفاق بشأن التعاون على مكافحة الجرائم في مجال المعلومات الحاسوبية (٢٠٠١)؛

مجلس أوروبا، اتفاقية الجريمة السيبرانية والبروتوكول الإضافي لاتفاقية الجريمة السيبرانية المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة بواسطة النظم الحاسوبية (٢٠٠١)؛

اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي (٢٠٠٧)؛

الجماعة الاقتصادية لدول غرب أفريقيا (الإيكواس)، مشروع التوجيه بشأن مكافحة الجريمة السيبرانية داخل إقليم الإيكواس (٢٠٠٩)؛

جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (٢٠١٠)؛

منظمة شنغهاي للتعاون، اتفاق بشأن التعاون في ميدان أمن المعلومات على الصعيد الدولي (٢٠١٠)؛ السوق المشتركة لدول شرق أفريقيا والجنوب الافريقي (كوميسا)؛

مشروع القانون النموذجي بشأن الأمن السيبراني (٢٠١١)؛

الاتحاد الأفريقي، مشروع اتفاقية بشأن وضع إطار عمل قانوني مؤاتٍ للأمن السيبراني في أفريقيا (٢٠١٢)؛

الاتحاد الأوروبي، القرار الإطاري لمجلس الاتحاد الأوروبي 2001/413/JHA بشأن مكافحة

الاحتيال وتزوير وسائط الدفع غير النقدي (٢٠٠١)؛

الاتحاد الأوروبي، القرار الإطاري لمجلس الاتحاد الأوروبي 2005/222/JHA بشأن الهجمات على نُظُم المعلومات (٢٠٠٥)؛

الاتحاد الأوروبي، المقترح COM (2010) 517 final بخصوص توجيه صادر عن البرلمان الأوروبي وعن مجلس الاتحاد الأوروبي بشأن الهجمات على نظم المعلومات ويُلغي المقرَّر الإطاري للمجلس 2005/222/JHA (٢٠١٠).

٣٢- وتتمثل الأساليب الرئيسية المستخدمة في تبادل الأدلة الإثباتية الإلكترونية في التعاون التقليدي، مثل الطلبات الرسمية للمساعدة القانونية المتبادلة. ويوجد عدد من الاتفاقات الثنائية والإقليمية والدولية التي تعالج إجراءات المساعدة القانونية المتبادلة. ويتضمن العديد من الصكوك الإقليمية والدولية بشأن الجرائم السيبرانية المذكورة أعلاه أحكاماً بشأن المساعدة القانونية المتبادلة. وتُحدد الاتفاقات الإقليمية والثنائية بشكل أساسي الإجراءات والطلبات بشأن المساعدة القانونية المتبادلة. وتشمل الأمثلة على الاتفاقات الإقليمية بشأن المساعدة القانونية المتبادلة معاهدة تبادل المساعدة القانونية في المسائل الجنائية لعام ٢٠٠٤ لرابطة أمم جنوب شرق آسيا (آسيان)، والاتفاقية الأوروبية بشأن المساعدة القانونية المتبادلة في المسائل الجنائية بين الدول الأعضاء في الاتحاد الأوروبي لعام ٢٠٠٠ لمجلس أوروبا.

٣٣- وفي ضوء طبيعة الأدلة الإثباتية الإلكترونية التي كثيراً ما تكون غير مستقرة وسهلة التلف، قد لا تُقدَّم الاستجابات المطلوبة لتلك الأدلة الإثباتية دائماً بالسرعة المطلوبة من خلال آليات التعاون الرسمية. ولذا يمكن أيضاً استخدام آليات التعاون غير الرسمية، وتنطوي الشبكات العاملة على مدار الساعة طوال أيام الأسبوع بصفة خاصة على إمكانات كبيرة لتبسيط ذلك التعاون غير الرسمي، بل وتيسير التعاون الرسمي في مرحلة لاحقة. بيد أنَّ توافر إجراءات التحقيق الممكنة من خلال التعاون غير الرسمي قد تتفاوت بدرجة كبيرة. وتتمثل إحدى العقبات الرئيسية أمام تبادل الأدلة الإثباتية الإلكترونية من خلال التعاون غير الرسمي في أنَّ العديد من البلدان يحظر استخدام الأدلة الإثباتية التي يُحصل عليها من خلال الآليات غير الرسمية في سياق الإجراءات القضائية.[٢١]

(٢١) دراسة عن آثار تكنولوجيات المعلومات الجديدة على الاعتداء على الأطفال واستغلالهم، الفصل الرابع، الصفحة ٤٧ (انظر أدناه)، متاحة في الرابط: www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.

٣٤- ولاحظت البلدان التي تستخدم التعاون غير الرسمي، لدى تقديم ردودها لأغراض الدراسة عن الجريمة السيبرانية، أنَّ الآليات ذات الصلة تعتمد على وجود جهة نظيرة أجنبية مختصة وجيِّدة التنظيم. ولاحظت البلدان أنَّ ذلك يكون أكثر احتمالاً عندما ينظَّم التعاون غير الرسمي في مجال إنفاذ القانون بموجب اتفاق ذي شكل ما. ولذا، أفاد عدد من البلدان بأنَّ التعاون غير الرسمي يجري على أساس اتفاقات إقليمية وثنائية من خلال استخدام شبكات منشأة من جانب المنظمات والمؤسسات الدولية والإقليمية؛ وبمساعدة السفارات والقنصليات؛ وكذلك من خلال شبكات خاصة بين موظفي إنفاذ القوانين.

٣٥- ولهذا الغرض، تتضمن المادة ٢٧ من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية أحكاماً بشأن التعاون في مجال إنفاذ القانون وتشجِّع الدول على النظر في إبرام اتفاقات أو ترتيبات ثنائية أو متعددة الأطراف تتيح التعاون بين مختلف هيئات إنفاذ القانون. وإضافة إلى ذلك، سنَّت الدول أيضاً قوانين مختلفة بشأن التعاون في مجال إنفاذ القانون، بما في ذلك تبادل المعلومات والتحقيقات المشتركة والمراقبة الإلكترونية وغيرها من أشكال المراقبة، وما إلى ذلك.

٣٦- وبينما تفيد بعض البلدان بوجود تعاون مباشر بين أجهزة الشرطة، تركِّز بلدان أخرى أساساً على التعاون غير الرسمي من خلال قنوات المنظمة الدولية للشرطة الجنائية (الإنتربول). وللإنتربول مكاتب في ١٩٠ بلداً كثيراً ما تكون مرتبطة بالأجهزة الوطنية لإنفاذ القانون.[٢٢] ونتيجة لذلك، قد تدعم المكاتب العلاقات غير الرسمية، مما يعزز من احتمال وجود بدائل ناجحة لإجراءات التعاون الدولي الرسمية.

٣٧- ويُمكن لعدد من التحديات التي تعترض إجراءات التعاون الرسمي وغير الرسمي على السواء فيما يتعلق بالأدلة الإثباتية الإلكترونية في المسائل الجنائية أن يعرقل جمع تلك الأدلة الإثباتية وتبادلها على السواء. وتشمل الأمثلة على ذلك التباين في نطاق الأحكام المتعلقة بالتعاون في الصكوك المتعددة الأطراف والثنائية، وعدم فرض أجل ملزِم للاستجابة للطلبات، وتعدُّد شبكات سلطات إنفاذ القانون غير الرسمية، والتباين في ضمانات التعاون.[٢٣]

(٢٢) Cybercrime Study, Chapter 7, p. 187.

(٢٣) Cybercrime Study, Chapter 7, pp. 197-215.

ثالثاً- الأدوات التي استحدثها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة

٣٨- خلال السنوات الماضية، استحدث المكتب عدداً من الأدوات التي تعالج موضوع الأدلة الإثباتية الإلكترونية من وجهات نظر واختصاصات وولايات مختلفة. وفي هذا الصدد، تشمل أدوات المكتب طائفة من المعارف المتداعمة التي كثيراً ما يتم جمعها من خلال مشاورات مكثفة مع الدول الأعضاء والجهات صاحبة المصلحة ذات الصلة. وتوفِّر أدوات المكتب، التي تتراوح بين التحليل القائم على البحوث بشأن أشكال محدَّدة من الجرائم والمنصات الإلكترونية التي تتيح الوصول المباشر إلى الموارد القانونية، توليفةً من الأدوات المعرفية المتعددة الأوجه فيما يتعلق بجمع الأدلة الإثباتية الإلكترونية وتبادلها.

٣٩- وبالرغم من عدم تخصيص أيٍّ من أدوات المكتب للأدلة الإثباتية الإلكترونية حصراً، فيما يلي لمحة عامة عن الأدوات/المواد التوجيهية/البحثية للمكتب ذات الأهمية بالنسبة للموضوع قيد المناقشة.

ألف- الدراسات التي اضطلع بها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة عملاً بقرارات الأمم المتحدة

٤٠- عملاً بولايات المجلس الاقتصادي والاجتماعي ذات الصلة، دشَّن مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة على مدى السنوات الأخيرة الدراسات التالية التي تمس، في جملة أمور، جمع وتبادل الأدلة الإثباتية الإلكترونية في سياق أنواع معينة من الجرائم: (أ) كتيب الجرائم المتصلة بالهوية،[٢٤] و(ب) الدراسة بشأن آثار تكنولوجيات المعلومات الجديدة على الاعتداء على الأطفال واستغلالهم[٢٥] (المشار إليها فيما يلي بعبارة "الدراسة بشأن الاعتداء على الأطفال واستغلالهم").

٤١- وبالمثل، عملاً بقراري الجمعية العامة ٦٥/٢٣٠ و٦٧/١٨٩، قدَّم المكتب خدمات السكرتارية والدعم التقني لاجتماعات فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة لمشكلة الجريمة السيبرانية. وفي هذا السياق، أعد المكتب، استناداً إلى المعلومات المقدَّمة من الدول الأعضاء، مشروع دراسة شاملة عن الجريمة السيبرانية، وهي دراسة أشير إليها كمادة مرجعية في أجزاء مختلفة من ورقة المعلومات الأساسية هذه.

(٢٤) www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

(٢٥) انظر الحاشية ٢١.

١- كتيِّب الجرائم المتصلة بالهوية

٤٢- يركِّز الكتيِّب، الذي أصدره المكتب في عام ٢٠١١، عملاً بقراري المجلس الاقتصادي والاجتماعي ٢٠/٢٠٠٧ و٢٢/٢٠٠٩ بشأن التعاون الدولي على منع جرائم الاحتيال الاقتصادي والجرائم ذات الصلة بالهوية والتحرِّي عنها وملاحقة مرتكبيها قضائيًّا ومعاقبتهم، على مسائل قانونية وسياساتية معينة تتعلق بالجريمة ذات الصلة بالهوية، بما في ذلك جمع واستخدام البيانات والمعلومات الإلكترونية. ويتمثل هدفه الرئيسي في عرض طائفة من الخيارات والاعتبارات التي يتعيَّن أن تؤخذ في الحسبان في معرض تناول شؤون العدالة الجنائية الداخلية (توصيف الجرائم/نُهُج التجريم/حماية الضحايا)، والتحديات المحدّدة في مجال التعاون الدولي في المسائل الجنائية، وإمكانية إقامة علاقات تآزر وشراكات بين القطاعين العام والخاص، لا سيما فيما يتعلق بمنع الجرائم المتصلة بالهوية. ويساعد الجمع بين الورقات البحثية والمواد ذات المنحى العملي في أقسام الدليل على توضيح مختلف جوانب وبارامترات المشاكل المعقدة التي يثيرها هذا الشكل من الجريمة.

٤٣- ونظراً لتنوع المسائل المشمولة، فقد أُعِدَّ الكتيّب لكي يستخدمه المشرِّعون ومقررو السياسات والنيابة العامة وسلطات وممارسو إنفاذ القانون، وكذلك أصحاب مصلحة آخرون (ممثلو المنظمات الدولية والمنظمات الحكومية الدولية الناشطة في هذا المجال وممثلو القطاع الخاص والخبراء من الأوساط الأكاديمية).

٤٤- ويُمكن أن يُستخدم الكتيب أيضاً كمادة مرجعية يستعان بها في برامج المساعدة التقنية وأنشطة بناء القدرات بغية زيادة المعارف المتخصصة لمعالجة المسائل القانونية والمؤسسية والتشغيلية التي تكتنف الجرائم المتصلة بالهوية كشكل ناشئ من أشكال الجريمة.

٤٥- وإضافة إلى ذلك، يقدِّم الدليل العملي بشأن التعاون الدولي على مكافحة الجرائم المتصلة بالهوية، الذي يَرِدُ في كتيّب الجرائم ذات الصلة بالهوية، لمحة عامة عن الجوانب الخاصة بالبعد عبر الوطني للجريمة ذات الصلة بالهوية ويركّز على المعلومات الأساسية والمبادئ التوجيهية كيفية معالجة طلبات التعاون الدولي في ذلك المجال على أفضل نحو، بما في ذلك من خلال استخدام أمثلة عن القضايا ذات الصلة.

٢- دراسة عن آثار تكنولوجيات المعلومات الجديدة على الاعتداء على الأطفال واستغلالهم

٤٦- استجابة لقرار المجلس الاقتصادي والاجتماعي ٣٣/٢٠١١، المعنون "المنع والحماية والتعاون الدولي في مجال مكافحة استعمال تكنولوجيات المعلومات الجديدة بغرض الاعتداء

على الأطفال و/أو استغلالهم"، أصدر المكتب، في عام ٢٠١٥، دراسة عن آثار تكنولوجيات المعلومات الجديدة على الاعتداء على الأطفال واستغلالهم (عُرضت في بادئ الأمر في الدورة الثالثة والعشرين للجنة منع الجريمة والعدالة الجنائية في أيار/مايو ٢٠١٤). واستندت دراسة المكتب إلى بحوث مفتوحة المصدر عن هذه المسألة إلى جانب عمل اجتماع غير رسمي لفريق خبراء تابع للمكتب بشأن هذا الموضوع، عُقد في فيينا في الفترة من ٢٣ إلى ٢٥ أيلول/سبتمبر ٢٠١٣ وضمَّ خبراء من منظمات دولية وأجهزة إنفاذ القانون وممارسين آخرين من ذوي الصلة وأعضاء في الدوائر الأكاديمية. وتقدِّم الدراسة معلومات أساسية ذات صلة بشأن المسائل التالية:

(أ) التعاريف والمصطلحات الناشئة؛

(ب) أنواع الجرائم؛

(ج) أكثر أنواع وأشكال السلوكيات ذات الصلة شيوعاً؛

(د) الأشكال الرئيسية لتكنولوجيات المعلومات والاتصالات التي تيسِّر أنواعاً معينة من الجريمة، مثل الاعتداء على الأطفال واستغلالهم؛

(هـ) ملامح المجرم ومدى تقدم معارفه التكنولوجية؛

(و) عوامل الخطر المرتبطة بالإيذاء؛

(ز) طبيعة المواد، مثل الصور الفوتوغرافية والصور السالبة والشرائح والمجلات والكتب والرسوم والأفلام وأشرطة الفيديو والأقراص أو الملفات الحاسوبية؛

(ح) نوع الأجهزة والبرامج المستخدمة للأغراض الإجرامية، مثل: الهواتف المحمولة وخدمات التخزين عن بُعد التي تتضمن تكنولوجيا الترميز المدمجة والحوسبة السحابية والتطبيقات الجديدة مثل سناب شات وويكر التي تمكِّن المستخدمين من توزيع صور مؤقتة تختفي في غضون ثوان عقب تلقِّيها.

٤٧- وإضافة إلى ذلك، كُرِّسَ الفصل الثالث من الدراسة للتحقيق في الاعتداء على الأطفال واستغلالهم بمساعدة تكنولوجيا المعلومات والاتصالات.

٤٨- وتتوسَّع الدراسة في عرض إمكانية الحصول على البرامجيات والتكنولوجيات المتصلة بالصور وتطبيقاتها العملية التي تمكِّن أجهزة إنفاذ القانون من تحديد هوية الضحايا المجهولي الهوية الذين يظهرون في المواد المعروضة على شبكة الإنترنت وإنقاذهم، وكذلك تحديد أولويات التحقيقات التي تجريها هذه الأجهزة في مجال التحليل الجنائي من خلال مقارنة المواد

الرقمية الخاصة بالمشتبه فيهم بالصور الموجودة في قواعد البيانات. وتوفِّر الدراسة معلومات مفيدة عن التكنولوجيات المبتكرة المستخدمة للحد من الازدواجية في جهود التحقيق مع حماية مصالح الضحايا في الوقت نفسه. وهي تشمل، على سبيل المثال، ما يلي:

تقنية "PhotoDNA" لشركة مايكروسوفت: برامجية مجانية تُستخدم لإنشاء توقيع فريد لصورة رقمية، على غرار بصمة الإصبع، يمكن مقارنتها بتوقيعات صور أخرى للعثور على نسخ من تلك الصورة.

قواعد بيانات تضم صوراً للاعتداء وتشمل معلومات عن الضحايا المعلومين والمجهولين.[٢٦]

قاعدة البيانات الدولية لصور الاستغلال الجنسي للأطفال التابعة للإنتربول: قاعدة بيانات تُستخدم لتحديد وإنقاذ ضحايا كانوا مجهولي الهوية من قبل باستخدام برامجيات متطورة لمقارنة الصور وإقامة روابط بين الضحايا والأماكن.

٤٩- ويستخدم مقدِّمو خدمات الإنترنت الابتكارات التقنية المذكورة أعلاه أيضاً للعثور بواسطة خوارزميات على مواد الاعتداء الجنسي على الأطفال وإزالتها من خوادمهم.

٥٠- وعلاوة على ذلك، تصف الدراسة التحليل الجنائي الرقمي باعتباره فرعاً من علم الأدلة الجنائية يُعنى باسترجاع الآثار الرقمية الحاسوبية والتحقيق فيها. وفي هذا الصدد، تلقي الدراسة الضوء على البيانات الحاسوبية والاتصالات الإلكترونية من النوع الذي يمكن أن يكون ذا صلة بعمل إجرامي، والمجموعة المنوَّعة من الصيغ والنظم الممكنة المستخدمة لحفظها في الملفات وكذلك الأدوات المستخدمة في فحص البيانات.

٥١- وتتناول الدراسة أيضاً استخدام برامجيات "البحث الآلي" من أجل تحقيقات التحليل الجنائي. وهي تؤكد على استخدام هذه الأداة للعثور بسهولة وسرعة على المواقع والمحتويات المعلَّمة بكلمات رئيسية شائعة الاستخدام.

٥٢- وتنظر الدراسة إضافة إلى ذلك في التقدم المحرز خلال العقد الماضي بشأن استحداث واستخدام أدوات وبرامجيات تكنولوجية تسمح بالبحث سريعاً عن بيانات معيّنة في الآلاف من مختلف قواعد البيانات والسجلات المالية وعيّنات الحمض الخلوي الصبغي والعينات الصوتية ولقطات الفيديو والخرائط ومخططات الطوابق والتقارير الاستخبارية البشرية

(٢٦) مثل قواعد البيانات التي استحدثتها المنظمة الدولية للشرطة الجنائية والمركز الوطني للأطفال المفقودين والمستغلَّين الذي يقع مقره في الولايات المتحدة.

وشبكات التواصل الاجتماعي. وتُجمِّع هذه الأدوات البيانات المعنية في مسار دقيق ومتسق ومفيد، بما يتيح تحليلاً مفاهيميًّا للروابط.

٥٣- وعلاوة على ذلك، تتناول الدراسة مدى ملاءمة التحقيقات السرّية وخصائصها فيما يتعلق بالجريمة الإلكترونية.

٣- مشروع الدراسة الشاملة عن الجريمة السيبرانية

٥٤- يتناول الفصل السادس من مشروع الدراسة الشاملة عن الجريمة السيبرانية بإسهاب موضوع الأدلة الإثباتية الإلكترونية والعدالة الجنائية، بدءاً من الحاجة إلى تحديد الأدلة الإثباتية الإلكترونية وجمعها وتحليلها حتى التحليل الجنائي الرقمي. وهو يدرس مقبولية الأدلة الإثباتية الإلكترونية واستخدامها في المحاكمات الجنائية، ويبين كيف يمكن بها لطائفة من التحديات المتعلقة بالملاحقة القضائية أن تؤثّر على أداء نظام العدالة الجنائية. وهو يربط أيضاً بين الاحتياجات فيما يتعلق بقدرات إنفاذ القانون والعدالة الجنائية في ضوء أنشطة المساعدة التقنية المطلوبة والمقدَّمة.

٥٥- وإضافة إلى ذلك، يجري تناول بعض الجوانب المتعلقة بالأدلة الإثباتية الإلكترونية من منظور إنفاذ القانون والتعاون الدولي. وفي هذا الصدد، يتناول الفصل الخامس (إنفاذ القانون والتحقيقات) فحص البيانات الإلكترونية التي يمكن تقديمها كأدلة إثباتية إلكترونية واستخدام تلك البيانات وتخزينها واستبقاءها وحفظها؛ وجمع البيانات آنيًّا؛ واستخدام أدوات التحليل الجنائي عن بُعد؛ وسبل وصول أجهزة إنفاذ القانون بشكل مباشر إلى البيانات الخارجة عن الحدود الإقليمية؛ وحقوق الإنسان والتحقيقات التي تجريها أجهزة إنفاذ القانون والحصول على البيانات من مقدِّمي الخدمات من القطاع الخاص. ومن ناحية أخرى، يتناول الفصل السابع (التعاون الدولي) مسألة الأدلة الإثباتية الخارجة عن الحدود الإقليمية من السُّحُب ومقدِّمي الخدمات ويتناول بإسهاب مجالات مثل موقع البيانات؛ وسبل الحصول على البيانات الخارجة عن الحدود الإقليمية لدى جمع الأدلة الإثباتية؛ والحصول على البيانات من مقدِّمي الخدمات من خارج الحدود الإقليمية.

باء- الأدوات التي استحدثها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة للاستخدام في سياق أنشطة المساعدة التقنية

٥٦- أدت برامج مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة في مجال المساعدة التقنية إلى استحداث أدوات عملية تعالج موضوع الأدلة الإثباتية الرقمية من وجهة نظر الممارسين. وفي هذا الصدد، صاغ المشاركون في الاجتماع الأقاليمي الثاني بشأن تبادل الممارسات الخاصة بطلب وتقديم الأدلة الإثباتية الرقمية في التحقيقات والملاحقات القضائية ذات الصلة بالجريمة المنظَّمة[٢٧] مجموعةً من الإرشادات الأساسية لفائدة المحقِّقين وأعضاء النيابة العامة فيما يتعلق بطلب البيانات/الأدلة الإثباتية الإلكترونية/الرقمية من الولايات القضائية الأجنبية.

٥٧- وتوفِّر مجموعة الإرشادات الأساسية مشورة عملية لطلب الأدلة الإثباتية الإلكترونية من الولايات القضائية الأجنبية، بما في ذلك الحصول على الأدلة الإثباتية الإلكترونية من المصادر المفتوحة أو مباشرة من جهات تقديم خدمات الإنترنت المنشأة أو المسجَّلة في البلد المقدِّم للطلب كشركات منتسبة إلى مقدِّم لخدمات الإنترنت يقع مقره في الخارج؛ وحفظ الأدلة الإثباتية الإلكترونية قبل إرسال طلب الإفصاح عنها؛ وعند الإمكان، إرسال الطلب مباشرة إلى مقدِّم خدمة الإنترنت وإرسال نسخة منه إلى جهة التحقيق أو الملاحقة القضائية التابعة للدولة المتلقية للطلب؛ والتشاور مع الوحدة المعنية بالجريمة السيبرانية بشأن الجوانب التقنية للطلب.

٥٨- وعملاً بالقرار ٤/٧ لمؤتمر الأطراف في اتفاقية الجريمة المنظمة، يواصل المكتب تطوير أدوات من أجل التعاون الدولي، بما في ذلك أداة كتابة طلبات المساعدة القانونية المتبادلة. وفي هذا الصدد، نظَّم المكتب عدداً من الاجتماعات غير الرسمية لفريق خبراء من أجل استعراض ومناقشة إعادة تطوير هذه الأداة والنظر في التوجهات المستقبلية بشأن استخدامها.

٥٩- وخلال الاجتماع غير الرسمي الأخير لفريق الخبراء في أيار/مايو ٢٠١٥، اتفق المشاركون على أن تُدرَج في الأداة المعاد تطويرها نمطية أدلة إثباتية رقمية قد تساعد الدول في طلب المساعدة المتعلقة بهذا النوع من الأدلة الإثباتية. وفي هذا الصدد، تبادل الخبراء الخبرات الوطنية بشأن طلب الأدلة الإثباتية الرقمية والحصول عليها، بما في ذلك مدى توافر نماذج الأدلة الإثباتية الرقمية وما إذا كانت هناك نُهُج موحدة لوصف الأدلة الإثباتية الرقمية.

(٢٧) تبليسي، جورجيا، ٩-١١ كانون الأول/ديسمبر ٢٠١٤. استُحدثت هذه الأداة كجزء من مبادرة المكتب الرامية إلى إنشاء وتعزيز شبكة المدّعين العامّين والسلطات المركزية من بلدان المصدر والعبور والمقصد للتصدي للجريمة المنظمة عبر الوطنية في آسيا الوسطى وجنوب القوقاز.

وقَدَّم الاجتماع إرشادات بشأن الصيغة والهيكل الممكنين لنميطة الأدلة الإثباتية الرقمية، مع التركيز على الأنواع المختلفة من الأدلة الإثباتية الرقمية، مثل بيانات الأجهزة وبيانات الشبكات ومعلومات المشتركين وبيانات المحتوى. ومن المقرَّر وضع أداة كتابة طلبات المساعدة القانونية المتبادلة، المعاد تطويرها، في صيغتها النهائية كنتيجة للاجتماع غير الرسمي لفريق الخبراء الجديد الذي سيُعقَد من ٢٢ إلى ٢٣ تشرين الأول/أكتوبر ٢٠١٥ في فيينا.

جيم- برامج إدارة المعارف التابعة لمكتب الأمم المتحدة المعني بالمخدِّرات والجريمة

١- بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (بوابة "شيرلوك")

٦٠- واصل المكتب العمل على تطوير بوابة "شيرلوك"، وهي بوابة لإدارة المعارف تهدف إلى تبادل الموارد القانونية الخاصة بالجريمة. وتركِّز البوابة على جمع الموارد بشأن مختلف أنواع الجريمة والمواضيع ذات الصلة، بما فيها الأدلة الإثباتية الإلكترونية. وحتى ١٨ آب/أغسطس ٢٠١٥، كانت البوابة تتضمن ٤٤ تشريعاً ذا صلة تضع المعايير بشأن مسألة الأدلة الإثباتية الإلكترونية.

٢- مستودع الجريمة السيبرانية

٦١- إضافة إلى بوابة "شيرلوك"، استحدث المكتب مستودع الجريمة السيبرانية، وهو قاعدة بيانات مركزية للقوانين والدروس المستفادة لأغراض تيسير التقييم المتواصل للاحتياجات وقدرات العدالة الجنائية وتقديم المساعدة التقنية وتنسيقها.

٦٢- والمستودع، الذي دُشّن في عام ٢٠١٥، هو أول أداة عالمية متاحة تتضمن القوانين والحالات والدروس المستفادة بشأن الجريمة السيبرانية والأدلة الإثباتية الإلكترونية، استناداً إلى المعلومات التي تقدِّمها وتحدِّثها الدول الأعضاء. ويرمي المستودع إلى تحقيق أهداف متعددة الجوانب، منها: تمكين المشرِّعين من الاعتماد على قاعدة بيانات التشريعات لدى صياغة قوانين بشأن الجريمة السيبرانية أو الأدلة الإثباتية الإلكترونية؛ وتيسير التعاون الدولي من خلال مساعدة موظفي إنفاذ القانون وأعضاء النيابة العامة على تحديد الأحكام التشريعية ذات الصلة بالجريمة السيبرانية المنطبقة في الدول الأعضاء الأخرى؛ وتزويد المستخدمين بأمثلة على الممارسات الجيِّدة في مجال منع الجريمة السيبرانية والتحقيق فيها وملاحقة مرتكبيها. ولا تُشير كل التشريعات الوطنية المتعلقة بالمساعدة القانونية المتبادلة إلى سلطة مركزية أو تحدِّد وظائفها. وحيثما يحدث ذلك، فقد تُسمِّي التشريعات الوطنية مؤسسةً حكومية كسلطة

مركزية وتتيح قائمةً بوظائف تلك السلطة وتتيح، في بعض الحالات، بنداً تَحوُّطِيًّا يؤكِّد أنَّ القانون لا يحدُّ من صلاحية تلك السلطة في توجيه الطلبات أو تلقِّيها أو في التعاون مع دولة أجنبية عبر قنوات أو وسائل أخرى. وعلى سبيل المثال، ينصُّ قانون المساعدة القانونية في أحد البلدان الأوروبية على أن تتولَّى السلطة المركزية "(١) تلقِّي طلبات المساعدة ...؛ و(٢) تنفيذ الطلبات، إمَّا مباشرة وإمَّا من خلال سلطات أخرى ...؛ و(٣) توجيه طلبات للمساعدة؛ و(٤) الاضطلاع بترجمة الوثائق".

رابعاً- الاستنتاجات والتوصيات

٦٣- لعلَّ الفريق العامل المعني بالتعاون الدولي يودُّ أن يوصي مؤتمر الأطراف بما يلي:

(أ) أن يطلب إلى الأمانة أن تُعِدَّ، بالتعاون مع المنظمات الحكومية الدولية ذات الصلة، ورهناً بتوافر الأموال من خارج الميزانية، دليلاً بشأن جمع الأدلة الإثباتية الإلكترونية وتبادلها؛

(ب) أن يطلب إلى الأمانة، كجزء من جهودها الرامية إلى تحسين الأدوات في مجال التعاون الدولي، تعميم موضوع الأدلة الإثباتية الإلكترونية؛

(ج) أن يطلب إلى الدول الأعضاء أن تخطر الأمانة بوجود وحدات أو هياكل متخصصة في مجال الجريمة السيبرانية لإدراجها في دليل السلطات الوطنية المركزية.