الأمم المتحدة E/CN.15/2022/6

المجلس الاقتصادي والاجتماعي

Distr.: General
4 March 2022
Arabic
Original: English

لجنة منع الجريمة والعدالة الجنائية

الدورة الحادية والثلاثون

فيينا، 16-20 أيار/مايو 2022

البند 5 من جدول الأعمال المؤقَّت*

المناقشة المواضيعية بشأن تعزيز استخدام الأدلة الرقمية في العدالة الجنائية ومكافحة الجرائم السيبرانية، بما في ذلك الاعتداء على القاصرين واستغلالهم في أنشطة غير مشروعة باستخدام الإنترنت

دليل المناقشة المواضيعية بشأن تعزيز استخدام الأدلة الرقمية في العدالة الجنائية ومكافحة الجرائم السيبرانية، بما في ذلك الاعتداء على القاصرين واستغلالهم في أنشطة غير مشروعة باستخدام الإنترنت

مذكرة من الأمانة

ملخص

أعدت الأمانة هذه المذكرة لتكون دليلا تسترشد به المناقشة المواضيعية التي تجريها لجنة منع الجريمة والعدالة الجنائية في دورتها الحادية والثلاثين، عملا بمقررها 1/18. وكما قررت اللجنة في دورتها الثلاثين المستأنفة، سيكون الموضوع البارز للدورة الحادية والثلاثين هو "تعزيز استخدام الأدلة الرقمية في العدالة الجنائية ومكافحة الجرائم السيبرانية، بما في ذلك الاعتداء على القاصرين واستغلالهم في أنشطة غير مشروعة باستخدام الإنترنت".

وتقدم هذه المذكرة معلومات مستكملة وتصف الاتجاهات والتحديات المتصلة بالجوانب القانونية والسياسية والتشغيلية. كما تحدد ردودا محتملة وتثير أسئلة وقضايا قد تود اللجنة مناقشتها.

* E/CN.15/2022/1.

240322 240322 V.22-01253 (A)

أولا- مقدمة

1- قررت لجنة منع الجريمة والعدالة الجنائية، في دورتها الثلاثين المستأنفة، أن يكون الموضوع المحوري البارز لدورتها الحادية والثلاثين هو "تعزيز استخدام الأدلة الرقمية في العدالة الجنائية ومكافحة الجرائم السيبرانية، بما في ذلك الاعتداء على القاصرين واستغلالهم في أنشطة غير مشروعة باستخدام الإنترنت". وأعدَّت الأمانة هذه المذكِّرة وفقا للمقرر 1/18، الذي قررت فيه اللجنة أن تستند مناقشة الموضوع البارز إلى دليل للمناقشة يتضمن قائمة بالمسائل التي يُراد أن يتناولها المشاركون.

2- ويغطي الموضوع البارز مواضيع مهمة مختلفة تناولها إعلان كيوتو بشأن النهوض بمنع الجريمة والعدالة الجنائية وسيادة القانون: نحو تحقيق خطة التنمية المستدامة لعام 2030، الذي اعتمده مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، المعقود في كيوتو، اليابان في الفترة من 7 إلى 12 آذار/مارس 2021، الذي أعلنت الدول أنها ستسعى إلى اتخاذ إجراءات بشأنه. ولذلك، يؤمل أن تعزز هذه المذكرة مناقشة اللجنة وتثريها وأن تدعم أوجه التقدم المحرز في التنفيذ الفعال لمختلف المعايير الدولية المشار إليها أدناه، فضلا عن إعلان كيوتو.

ثانيا- تعزيز استخدام الأدلة الرقمية في العدالة الجنائية

ألف- الحالة الراهنة والتحديات

السلطات التحقيقية الإجرائية

3- تطرح الجريمة التي تنطوي على أدلة إلكترونية[1] تحديات فريدة للسلطات المكلفة بالتصدي لها. ويكشف فحص الأساس القانوني للصلاحيات التحقيقية المستخدمة في الجرائم التي تنطوي على أدلة إلكترونية عن تنوع كبير في النُّهج المتبعة على الصعيد الوطني من حيث الفوارق في قواعد الإثبات والشروط والضمانات والسلطات التحقيقية المتعلقة بجمع الأدلة الإلكترونية واستخدامها في مسائل العدالة الجنائية، على النحو المنصوص عليه في قوانين الإجراءات الجنائية الوطنية أو غيرها من القوانين المحددة. ومن النتائج الهامة لهذه النُّهج المتنوعة ظهور تجزؤ قانوني[2] على نطاق يتزايد اتساعاً، قد يفضي بدوره إلى تناقضات في ممارسة السلطات الإجرائية ويعرقل جهود التحقيق[3].

4- وتشمل أكثر أنواع التدابير التحقيقية شيوعا في جمع الأدلة الإلكترونية التعجيل بحفظ البيانات الحاسوبية المخزنة والكشف عنها؛ وتوفير البيانات الحاسوبية المخزنة (بما في ذلك في حالات الطوارئ)؛ والتفتيش والمصادرة؛ والمراقبة الإلكترونية؛ واعتراض بيانات المحتوى.

(1) في العديد من السياقات، يستخدم مصطلحا "الأدلة الإلكترونية" و"الأدلة الرقمية" تبادليا. ويستخدم في هذه الوثيقة مصطلح "الأدلة الإلكترونية"، بعد استخدامه في سياقات مماثلة (مثل المناقشة المواضيعية التي أجرتها اللجنة في دورتها السابعة والعشرين) والمبادرات الإقليمية (انظر المبادئ التوجيهية بشأن الأدلة الإلكترونية في الإجراءات المدنية والإدارية التي اعتمدتها لجنة الوزراء التابعة لمجلس أوروبا في 30 كانون الثاني/يناير 2019)، ما لم يُنص على خلاف ذلك (ترد في بعض الحواشي الإشارات إلى عنوان المناقشة المواضيعية في الدورة الحادية والثلاثين للجنة، وكذلك المراجع).

(2) Counter-Terrorism Committee Executive Directorate, "The state of international cooperation for lawful access to digital evidence: research perspectives", CTED Trends Report, January 2022, pp. 23–24.

(3) United Nations Office on Drugs and Crime (UNODC), *Digest of Cyber Organized Crime* (Vienna, 2021), p. 109.

5- وفي حين تبذل جهود كبيرة لإصلاح القوانين على الصعيد المحلي في العديد من الدول الأعضاء (من خلال اعتماد أحكام بشأن الوصول إلى البيانات والتحكم فيها وتبادلها)[4]، فإن عددا كبيرا منها لم يكيف بعد أطره القانونية مع تطور أشكال الجريمة المعاصرة وطابعها الرقمي.

6- وبالتوازي مع ذلك، اتُّخذت مبادرات هامة على الصعيد الدولي، كل منها في مرحلة مختلفة من التطور، بغية صياغة معايير دولية لتنظيم المسائل المتصلة بالوصول المشروع إلى الأدلة الإلكترونية واستخدامها وتبادلها. وأُنشئت اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، التي تُمثَّل فيها جميع الأقاليم، عملا بقرار الجمعية العامة 74/247. وعلى الصعيد الإقليمي، تشمل المبادرات ذات الصلة اعتماد البروتوكول الإضافي الثاني الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية في تشرين الثاني/نوفمبر 2021 (سيفتح باب التوقيع عليه في أيار/مايو 2022) ووضع مشروع لائحة للبرلمان الأوروبي والمجلس الأوروبي بشأن الأوامر الأوروبية المتعلقة بتقديم وحفظ الأدلة الإلكترونية في المسائل الجنائية. وتهدف هذه الصكوك إلى حل الجوانب الرئيسية للمشاكل المرتبطة بالوصول (عبر الحدود) إلى الأدلة الإلكترونية لأغراض إنفاذ القانون والأغراض القضائية.

التعاون عبر الحدود مع مقدمي خدمات الاتصالات

7- يطرح تأمين الأدلة الإلكترونية الموجودة في ولاية قضائية أخرى أو على خوادم سحابية تحديات نظراً للطابع غير المستقر لهذه الأدلة. ويقتضي التعاون الدولي استجابة في الوقت المناسب، بما في ذلك حفظ مقدمي الخدمات للبيانات وتوفيرها، والقدرة على طلب إجراءات تحقيقية متخصصة. وأحد التحديات التي تُطرح عادة عند طلب هذه البيانات من ولاية قضائية أخرى يتمثل في تأخر الاستجابة الذي كثيرا ما يتجاوز مدة الاحتفاظ بالبيانات وقد يمكّن الجناة من إتلاف الأدلة الإلكترونية الرئيسية إتلافاً نهائياً[5]. ولهذا السبب، من الأهمية بمكان إقامة شراكات بين مقدمي خدمات الاتصالات عبر الإنترنت ووكالات إنفاذ القانون.

8- ولا يزال دور مقدمي خدمات الاتصالات في العدالة الجنائية وفي التعاون الدولي في المسائل الجنائية موضوعا حاسما ولكنه لم يستكشف بالكامل. ومقدمو خدمات الاتصالات هم الكيانات الخاصة التي تمتلك البيانات الإلكترونية للمستخدمين، وبصفتهم هذه، يتلقون حجما متزايدا من الطلبات الواردة من سلطات إنفاذ القانون التي تسعى إلى حفظ البيانات الإلكترونية ذات القيمة الإثباتية في تحقيق جنائي و/أو الوصول إليها. وقد يخضع مقدمو خدمات الاتصالات للوائح التنظيمية خاصة بالاتصالات وبالقطاع، حسب موقعهم الجغرافي.

9- وقد أصدر عدد متزايد من مقدمي خدمات الاتصالات مبادئ توجيهية لسلطات إنفاذ القانون والسلطات القضائية تهدف إلى توضيح متطلبات وعمليات تقديم الطلبات التي تنطوي على أدلة إلكترونية، ويشمل ذلك أنواع الأدلة التي يمكن طلبها، والحفاظ على الأدلة الإلكترونية، والكشف في حالات الطوارئ، والطلبات المباشرة للكشف الطوعي والاحتفاظ بالبيانات. ولا يزال نشر هذه المبادئ التوجيهية في أوساط إنفاذ القانون والأوساط القضائية في جميع أنحاء العالم يشكل تحديا لمقدمي خدمات الاتصالات، في حين ازداد حجم طلبات كشف البيانات المقدمة من السلطات. وبالنسبة لسلطات إنفاذ القانون، تطرح الإجراءات الفردية المصممة خصيصا (وإن كانت مفيدة) تحديا مزدوجا يتمثل في الاضطرار إلى إعادة تقييم أساليبها وممارساتها التحقيقية وفحص مصادر المعلومات المختلفة، مما يعني أن إعداد الطلبات والتحقيق نفسَه سيتطلبان وقتا أطول[6].

---

(4) Counter-Terrorism Committee Executive Directorate, “The state of international cooperation for lawful access to digital evidence”.

(5) ورقة معلومات أساسية من إعداد الأمانة بشأن جمع وتبادل الأدلة الإثباتية الإلكترونية (CTOC/COP/WG.3/2015/2)، الفقرة 19.

(6) European Union Agency for Law Enforcement Cooperation (Europol), *SIRIUS EU Digital Evidence Situation Report: 3rd Annual Report* (2021), pp. 49–50.

10- ولا تزال قدرة سلطات إنفاذ القانون والسلطات القضائية على التعاون مع مقدمي خدمات الاتصالات في المقرات الأجنبية وفقا للقوانين السارية ولمتطلباتهم تمثل التحدي الرئيسي، ولا سيما في التحقيقات العابرة للحدود، حيث قد تتداخل أطر قانونية مختلفة أو تنطوي على نهج مختلفة.

مقبولية الأدلة الإلكترونية في المحكمة

11- يشير الباحثون إلى أن مقبولية الأدلة في شكل رقمي قد تحققت إلى حد كبير من خلال إعادة تعريف المفاهيم القانونية في قواعد الإثبات المرنة[7]. وكثيرا ما تطبق قواعد الإثبات العامة على مقبولية الأدلة الإلكترونية في المحكمة، ولا سيما في البلدان التي لا ينظم فيها القانون هذه الأدلة ولا يحددها. وخلصت بيانات من تقرير شمل بلدانا في جميع أنحاء الاتحاد الأوروبي إلى أن الغالبية العظمى من البلدان التي شملتها الدراسة (82,4 في المائة)، يمكن فيها قبول البيانات التي تجمعها السلطات من خلال طلب كشف طوعي توجهه لكيان خاص مقره في الخارج كدليل في المحكمة[8]. وعلى الرغم من اختلاف الأطر القانونية بين البلدان، يبدو أن غياب التنظيم القانوني لهذه السلطة بالذات لا يمنع السلطات من إرسال طلبات الكشف الطوعي إلى مقدمي خدمات الاتصالات، وتطبيق قواعد الإثبات العامة المحلية.

12- وعلى هذا الأساس، من المسلم به على نطاق واسع أن النهج المحايد إزاء التكنولوجيا يجب أن يسود في تعامل المحاكم مع الأدلة الإلكترونية. وينبغي لا أن تميز المحاكم ضد الأدلة الإلكترونية ولا أن تعطيها أفضلية على أنواع أخرى من الأدلة، وينبغي أن تسترشد بمبدأ المساواة بين الأطراف في الإجراءات ذات الصلة[9].

13- وعلى الرغم من بروز هذه المبادئ، يبدو أنه لا توجد ممارسة موحدة عندما يتعلق الأمر بمقبولية الأدلة الإلكترونية في المحكمة، ولا سيما إذا جُمعت من مقدمي خدمات اتصالات في مقرات أجنبية. ففي حين أن بعض الولايات القضائية تعتبر فئات معينة من البيانات (مثل المعلومات الأساسية للمشتركين) مقبولة في ظل ظروف معينة (عندما تجمع مباشرة من مقدمي خدمات الاتصالات في مقرات أجنبية من خلال التعاون الطوعي)، فإن ولايات قضائية أخرى تشترط طلبا قضائيا رسميا لاستخدام الأدلة الإلكترونية التي تم الحصول عليها أمام المحكمة في دعوى جنائية (وإلا، فلا يجوز استخدامها إلا لأغراض استخبارية)[10].

14- وينبغي توضيح مسائل المقبولية لدى جميع الجهات الفاعلة المعنية في مرحلة مبكرة، وعند الضرورة والإمكان، بمشاركة المحاكم المختصة، التي قد يكون لها دور نشط في إدارة الأدلة. وفي التحقيقات عبر الحدود، ينبغي التشديد على منع انتهاك شروط المقبولية (أي تسلسل العهدة من الحجز إلى الحفظ) السارية في الدولة الطالبة.

المسائل المتعلقة بالولاية القضائية

15- تكتسي المسائل المتعلقة بالولاية القضائية أهمية قصوى في استخدام الأدلة الإلكترونية في العدالة الجنائية، لأن معظم التحقيقات التي تكون فيها الأدلة الإلكترونية مهمة تتطلب تقديم طلب إلى مقدم خدمات اتصالات مقره في ولاية قضائية أخرى. وبالمثل، فإن البيانات السحابية في حالة "انتقال" دائم، وقد توجد

(7) Stephen Mason and Daniel Seng, eds., *Electronic Evidence*, 4th ed. (London, University of London, Institute of Advanced Legal Studies, School of Advanced Study, 2017), p. 81.

(8) Europol, *SIRIUS EU Digital Evidence Situation Report*: 2nd Annual Report (2020), p. 17.

(9) Committee of Ministers of the Council of Europe, *Electronic Evidence in Civil and Administrative Proceedings: Guidelines and Explanatory Memorandum* (Strasbourg, France, 2019), p. 7.

(10) Europol, *SIRIUS EU Digital Evidence Situation Report: 3rd Annual Report*, p. 50.

أجزاء مختلفة منها في ولايات قضـــائية مختلفة في نفس الوقت، مما يؤدي إلى صـــعوبات في تأكيد الولاية القضائية ومعرفة مكان إرسال طلبات الأدلة الإلكترونية[11].

16- وقد تصدت جهود بذلت مؤخرا لإصلاح القوانين للتحدي المتمثل في الوصول المشروع إلى الأدلة الإلكترونية التي في حوزة مقدم خدمات اتصـالات في مقر أجنبي أو عهدته أو سـيطرته عن طريق توسـيع نطاق الولاية القضـائية. فعلى سـبيل المثال، في عام 2018، اعتُمد تشـريع في الولايات المتحدة الأمريكية (قانون توضـــيح الاســـتخدام المشـــروع للبيانات في الخارج (قانون CLOUD)) قد يلزم مقدمي خدمات الاتصـــالات في الولايات المتحدة بتوفير البيانات بغض النظر عما إذا كانت هذه البيانات مخزنة أو ســـبق تخزينها في الولايات المتحدة أو في الخارج[12].

المسائل التنفيذية والتحقيقية، بما في ذلك التعاون الدولي

17- مع التزايد السـريع لعدد طلبات المسـاعدة القانونية المتبادلة للحصـول على الأدلة الإلكترونية التي تتجاوز الحدود الإقليمية وحفظها، فإن طرائق التعاون التقليدية التي كثيرا ما تتطلب وقتا طويلا، والتي لا تزال الدول الأعضاء تعتمد عليها في كثير من الأحيان، لا تيسر الوصول السريع إلى الأدلة الإلكترونية الرئيسية، التي تتسم بطبيعة غير مستقرة.

18- وتبذل في جميع أنحاء العالم جهود لتكييف وتسـريع عمليات المسـاعدة القانونية المتبادلة وأطرها القائمة. ومن الأمثلة على ذلك البروتوكول الإضـافي الثاني الملحق باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية الذي اعتمد مؤخرا. وتقتضـي المادة 8 من ذلك البروتوكول أن تعتمد كل دولة طرف ما قد يلزم من التدابير التشريعية والتدابير الأخرى لتمكين سلطاتها المختصة من إصدار أمر يقدم كجزء من طلب إلى طرف آخر بغرض إلزام مقدم خدمات اتصـــالات في إقليم الطرف متلقي الطلب بتقديم معلومات الاشـتراك المحددة والمخزنة (في غضـون 20 يوما) وبيانات حركة المرور (في غضـون 45 يوما) التي يحوزها مقدم خدمة الاتصـــالات هذا أو يتحكم فيها، واللازمة لتحقيقات ذلك الطرف أو إجراءاته الجنائية المحددة. وبهذه الطريقة، ينشـــئ البروتوكول آلية تكمل أحكام المســـاعدة المتبادلة الواردة في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. وهو مصمم ليكون أكثر تبسيطا من عمليات المساعدة المتبادلة الحالية، حيث تكون المعلومات التي يجب على الطرف الطالب تقديمها أكثر محدودية وعملية الحصول على البيانات أكثر سرعة[13]. ومن ميزاته الأخرى وســائل التعاون العاجل في حالات الطوارئ التي تكون فيها أرواح معرضـــة للخطر، وزيادة فعالية تعاون سلطات إنفاذ القانون والقضاء للحصول على بيانات حركة المرور، وأدواتٌ للتحقيقات المشتركة.

19- والمعاهدة المتعلقة بإرسال طلبات التعاون الدولي إلكترونياً بين السلطات المركزية هي صك إقليمي آخر سيسهم في تسريع عمليات المساعدة القانونية المتبادلة، بإتاحة نقل الأدلة الإلكترونية بسرعة أكبر عبر الحدود[14].

20- وتمكن أساليب التحري الخاصة، بما في ذلك المراقبة الإلكترونية والعمليات السرية والتسليم المراقب، وكالات إنفاذ القانون من جمع المعلومات في ســـياق التحقيقات في الجرائم الخطيرة دون تنبيه الأشـــخاص

(11) UNODC, Counter-Terrorism Committee Executive Directorate and International Association of Prosecutors, *Practical Guide for Requesting Electronic Evidence across Borders* (Vienna, 2019), p. 78.

(12) Counter-Terrorism Committee Executive Directorate, "The state of international cooperation for lawful access to digital evidence", pp. 17–19.

(13) انظر التقرير التفسيري للبروتوكول الإضافي الثاني الملحق بالاتفاقية المتعلقة بالجريمة السيبرانية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية.

(14) تقرير اجتماع الفريق العامل المعني بالتعاون الدولي المعقود في فيينا يومي 7 و8 تموز/يوليه 2020 (CTOC/COP/WG.3/2020/4)، الفقرة 67.

المستهدفين. وقد تشمل أساليب التحري الخاصة هذه أيضا أساليب لجمع الأدلة الإلكترونية. وتُصادَف عند التحقيق في الجرائم التي تنطوي على أدلة إلكترونية تطورات تكنولوجية جديدة مثل برامجيات إخفاء الهوية، والتشفير العالي الجودة، والعملات الافتراضية، وقد يحتاج المحققون إلى اعتماد استراتيجيات جديدة وإلى النظر في كيفية استخدام أساليب التحري الخاصة وعمليات التحليل الجنائي الرقمي عن بُعد لجمع هذه الأدلة الإلكترونية مع ضمان مقبولية هذه الأدلة وإمكانية استخدامها في المحكمة.

21- وقد تؤدي الاختلافات بين البلدان في قوانين الإجراءات الجنائية وقواعد الإثبات التي تنظم أساليب التحري الخاصة إلى عرقلة التعاون في التحقيقات التي تنطوي على تلك الأساليب[15]. غير أن أحد العناصر الحاسمة هو الامتثال لمبدأ التناسب عند استخدام أساليب التحري الخاصة في التحقيقات في الجرائم السيبرانية، ولا سيما بشأن الشبكة الخفية، أو عندما تصبح الأدلة الإلكترونية ذات صلة بتحقيقات في جرائم "تقليدية". وفي العديد من النظم القانونية المحلية، تختبر هذا المبدأ في المقام الأول السلطةُ القضائية التي تشرف على التحقيقات والمحكمة، حسب الاقتضاء[16].

ضمانات حقوق الإنسان

22- تتطلب شروط وضمانات جمع الأدلة الإلكترونية واستخدامها في الغالب إشرافا قضائيا أو إشرافا مستقلا آخر لبيان حدود الإجراءات والعمليات والأساليب والأدوات المستخدمة لجمع الأدلة الإلكترونية واحتيازها وحفظها وتحليلها[17].

23- ولتجنب استخدام أساليب التحري الخاصة لجمع الأدلة الإلكترونية كما لو كانت "حصان طروادة" في ارتكاب انتهاكات محتملة في مجال حقوق الإنسان الأساسية، مثل الحق في الخصوصية والحق في حرية الرأي والتعبير، لا بد من رصد أساليب التحري الخاصة لجمع الأدلة الإلكترونية وتقييم آثارها على نحو مستمر[18]. وثمة حاجة ملحة أخرى تتمثل في تعزيز تدريب موظفي إنفاذ القانون والعدالة الجنائية على استخدام التكنولوجيات الحديثة المتاحة لهم استخداما فعالا وممتثلا لحقوق الإنسان.

24- وقد سعت المبادرة العالمية للتعامل مع الأدلة الإلكترونية (انظر الفقرتين 25-26 أدناه) منذ إنشائها إلى تعزيز التوازن بين التعامل مع الأدلة الإلكترونية لأغراض إنفاذ القانون والأغراض القضائية وتوخي احترام حقوق الإنسان وحمايتها. وفي هذا الصدد، تعمل المبادرة العالمية على إذكاء وعي موظفي إنفاذ القانون والموظفين القضائيين بحقوق الإنسان والسوابق القضائية ذات الصلة. ويتعرف المسؤولون المدربون في إطار المبادرة العالمية على ضمانات حقوق الإنسان مثل الضمانات المؤسسية، وآليات الرقابة المستقلة المتعلقة بإصدار أذون جمع البيانات وتدابير تبادلها، والضمانات الفعالة لحق الدفاع، والضمانات الإجرائية بإخطار الضحايا الذين انتُهك حقهم في الخصوصية من خلال أنشطة المراقبة التي تأذن بها الدولة، والضمانات ضد التدخل المفرط وغير المبرر في الحق في الخصوصية.

---

(15) UNODC, *Digest of Cyber Organized Crime Cases*, p. 101.

(16) تقرير اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية الذي عُقد في فيينا في الفترة من 27 إلى 29 آذار/مارس 2019 (UNODC/CCPCJ/EG.4/2019/2)، الفقرة 37؛ وورقة معلومات أساسية من إعداد الأمانة عن التعاون الدولي الذي ينطوي على استخدام أساليب التحري الخاصة (CTOC/COP/WG.3/2020/3)، الفقرتان 34 و35.

(17) UNODC, *Digest of Cyber Organized Crime Cases*, p. 109.

(18) انظر أيضا ورقة المعلومات الأساسية التي أعدتها الأمانة العامة لحلقة العمل 4 (الاتجاهات الراهنة للجريمة، والتطورات الأخيرة والحلول المستجدة، لا سيما التكنولوجيات الجديدة بوصفها وسائل لارتكاب الجريمة وأدوات لمكافحتها) لمؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية (A/CONF.234/11)، الفقرة 78.

المساعدة التقنية والتشريعية

25- أطلق مكتب الأمم المتحدة المعني بالمخدرات والجريمة (المكتب) المبادرة العالمية للتعامل مع الأدلة الإلكترونية بالاشتراك مع المديرية التنفيذية للجنة مكافحة الإرهاب والرابطة الدولية للمدعين العامين في عام 2017. وتركز المبادرة على تعزيز قدرة المؤسسات والمسؤولين الوطنيين على مكافحة الجرائم المرتكبة من خلال استخدام تكنولوجيا المعلومات والاتصالات، إضافة إلى الجرائم التي تنطوي على أدلة إلكترونية.

26- وفي إطار المبادرة العالمية، أصدر المكتب تكليفا بوضع *الدليل العملي لطلب الأدلة الإلكترونية عبر الحدود*، وإطار الكشف عن البيانات والأدوات والموارد العملية ذات الصلة، وكلها متاحة على مركز الأدلة الإلكترونية في بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (شيرلوك)[19]. ومن خلال هذه المبادرة، يقود المكتب تعزيز الشراكات بين القطاعين العام والخاص مع الدول الأعضاء والمنظمات الدولية والإقليمية (مثل وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية (يوروجست)، ووكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اليوروبول)، والشبكة القضائية الأوروبية)، فضلا عن مقدمي خدمات الاتصالات.

اعتبارات خاصة بشأن حماية الطفل

27- عند التعامل مع الأدلة الإلكترونية في الإجراءات القضائية المتعلقة بالأطفال، يلزم اتخاذ تدابير خاصة لحماية حقوق الأطفال في الخصوصية والسلامة والرفاه والوصول إلى العدالة. وتكتسي هذه الحقوق أهمية خاصة في وضع حدود لممارسة السلطات التحقيقية وتفعيل الضمانات الإجرائية ضد التدخل الرقمي غير الضروري وغير المتناسب في الخصوصية. ويجب أن يسترشد موظفو العدالة الجنائية بمبدأ مصالح الطفل الفضلى، ويجب أن يتعاملوا مع الأدلة الإلكترونية على نحو يخفف العبء على الأطفال الضحايا باعتبارهم المصدر الوحيد للأدلة.

28- وينبغي أن تتاح للأطفال ضحايا الاعتداء والاستغلال المرتكبين من خلال استخدام الإنترنت أو الشهود عليهما إمكانية الحصول على خدمات الدعم والمساعدة القانونية وتدابير الحماية لمنع معاودة إيذائهم أو إعادة تذكيرهم بما عانوه من صدمة أو وصمهم أو تخويفهم. وينبغي إعادة النظر في سلطات التحري التي تهدف إلى جمع الأدلة الإلكترونية في القضايا التي تنطوي على أطفال ضحايا للاعتداء والاستغلال لضمان ألا تؤدي إلى تفاقم أو زيادة أوجه الضعف لدى الأطفال من الضحايا والشهود[20].

29- ولجمع أي نوع من الأدلة الإلكترونية واستخدامه، بما في ذلك تلقي الأدلة المتعلقة بالأطفال، من الأهمية بمكان حماية أي معلومات تتعلق بهوية الطفل والحفاظ على حق الأطفال في الخصوصية في جميع مراحل الإجراءات. ويستتبع ذلك تأمين المعلومات المتعلقة بمشاركة الطفل في إجراءات العدالة (طوال عملية تسلسل العهدة بأكملها) واتخاذ تدابير لحماية الأطفال من أي افتضاح لا داعي له في جميع مراحل الإجراءات[21].

30- ويمكن اتخاذ مجموعة متنوعة من التدابير للمساعدة في تقديم الأطفال للأدلة وتلقي الأدلة منهم، بما في ذلك الأدلة الإلكترونية. وتتعلق هذه التدابير، على سبيل المثال، بمقبولية الأدلة، مثل الأقوال المسجلة بالفيديو وجلسات الاستماع أو الإجراءات المغلقة، التي قد تشمل استخدام مرافق تسمح للطفل بالإدلاء بشهادته، دون الحاجة إلى رؤية المتهم، من غرفة مقابلات خاصة عن طريق دائرة تلفزيونية مغلقة[22]. ومن

(19) https://sherloc.unodc.org/cld/en/st/evidence/electronic-evidence-hub.html.

(20) اتفاقية حقوق الطفل، المادتان 16 و40، الفقرة 2 (ب) ’7‘.

(21) المبادئ التوجيهية بشأن العدالة في الأمور المتعلقة بالأطفال ضحايا الجريمة والشهود عليها. القسم العاشر.

(22) UNODC, Justice in Matters involving Child Victims and Witnesses of Crime: Model Law and Related Commentary (Vienna, 2009), part two, chap. III, sect. C, art. 28, para. 3. (*العدالة في الأمور المتعلقة بالأطفال ضحايا الجريمة والشهود عليها: القانون النموذجي والتعليق*).

الضروري أيضا وضع آليات وإجراءات ومبادئ توجيهية لتعزيز تعاون مقدمي خدمات الاتصالات (بما في ذلك الجهات في المقرات الأجنبية) في التحقيقات والإجراءات الجنائية المتعلقة بالأطفال ضحايا الاعتداء والاستغلال.

باء- التدابير الممكنة

31- يمكن للمكتب، من خلال مبادرته العالمية للتعامل مع الأدلة الإلكترونية، أن يواصل بناء قدرات: (أ) موظفي إنفاذ القانون من أجل تحديد البيانات الإلكترونية اللازمة للتحقيق في الجرائم وجمعها واحتيازها وحفظها؛ و(ب) سلطات الادعاء والسلطات القضائية من أجل استخدام تلك البيانات كأدلة في المحكمة؛ و(ج) السلطات المركزية والمختصة من أجل التعامل مع تلك البيانات وتبادلها عبر الحدود والولايات القضائية، دون المساس بمقبوليتها وقيمتها الإثباتية في المحكمة.

32- وفي سياق الشراكات بين القطاعين العام والخاص، يمكن للمكتب المعني بالمخدرات والجريمة أن يوفر بناء القدرات، بما في ذلك بشأن مقبولية الأدلة الإلكترونية التي يتم الحصول عليها من مقدمي خدمات الاتصالات في المقرات الأجنبية، بهدف زيادة معارف سلطات العدالة الجنائية وخبراتها ومهاراتها.

33- ووفقا للقرار 4/10 الصادر عن مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، نظمت الأمانة اجتماعين غير رسميين لفريق خبراء من أجل تنقيح القانون النموذجي بشأن المساعدة المتبادلة في المسائل الجنائية بحيث يتضمن أحكاما بشأن جمع الأدلة الإلكترونية واستخدام أساليب التحري الخاصة. ويوجه انتباه اللجنة إلى التوجيه النموذجي، بصيغته المنقحة، من أجل اطلاع الدول الأعضاء وأيضا باعتباره، إلى جانب القوائم المرجعية النموذجية المتاحة لطلبات المساعدة القانونية المتبادلة، أداة للبلدان التي تلتمس الدعم في تحديث تشريعاتها وتبسيط عملياتها المتعلقة بالمساعدة القانونية المتبادلة في مجال الأدلة الإلكترونية.

جيم- مسائل مطروحة للنظر فيها

34- لعل اللجنة تود أن تنظر في النقاط التالية لتناولها بمزيد من المناقشة:

(أ) ما هي التحديات التي تواجهها السلطات المختصة عند استخدام أساليب التحري الخاصة لجمع الأدلة الإلكترونية في سياق التحقيقات الجنائية، وما هي الممارسات الجيدة في مجال الاستجابة؟ وكيف يمكن أن تؤخذ ضمانات حقوق الإنسان في الاعتبار على أفضل وجه في هذا الصدد؟

(ب) ما هي الخبرة المتراكمة في مجال مقبولية الأدلة الإلكترونية في المحكمة؟ وما هي الدروس المستفادة من تطبيق المبادئ العامة للقوانين الإجرائية المحلية وقواعد الإثبات المخصصة، فضلا عن تطوير الفقه القضائي الوطني، في هذا الصدد؟

(ج) ما هي الدروس المستفادة من الجهود المبذولة لتعزيز التعاون بين سلطات إنفاذ القانون ومقدمي خدمات الاتصالات لتأمين الأدلة الإلكترونية من أجل الكشف عن الجرائم الخطيرة والتحقيق فيها ومقاضاة مرتكبيها، وما الآثار التي يمكن أن تترتب عن المبادرات الجديدة في هذا الميدان وما هي إمكاناتها؟

(د) كيف يمكن السعي إلى تحقيق أوجه التآزر والشراكات على أفضل وجه بين المنظمات الدولية التي تقدم المساعدة التقنية في مسائل الأدلة الإلكترونية من أجل تزويد الدول الأعضاء بخدمات ملموسة ومستدامة في مجال بناء القدرات؟

ثالثا- مكافحة الجريمة السيبرانية

ألف- الحالة الراهنة والتحديات

35- في عام 2018، كان الموضوع الرئيسي للدورة السابعة والعشرين للجنة هو "تدابير العدالة الجنائية لمنع الجريمة السيبرانية بجميع أشكالها والتصدِّي لها، بوسائل منها تعزيز التعاون على الصعيدين الوطني والدولي". وأعدت الأمانة للمناقشة المواضيعية دليل مناقشة شاملا يدرس مختلف جوانب سياسات مكافحة الجريمة السيبرانية واستراتيجياتها، من التجريم والصلاحيات الإجرائية إلى التنسيق بين الوكالات والتعاون الدولي والمنع[23].

36- وعلاوة على ذلك، عرض الأمين العام في تقريره بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، الذي أُعد وفقاً لقرار الجمعية العامة 187/73، آراء 61 دولة عضوا بشأن التحديات التي تعترضها في مجال مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية[24].

37- وأُبلغت اللجنة أيضاً في دورتيها التاسعة والعشرين والثلاثين بالتقدم الذي أحرزه المكتب في عامي 2019 و2020 في تعزيز وتقديم المساعدة التقنية وبناء القدرات في مجال مكافحة الجريمة السيبرانية[25].

38- وبناء على ما سبق، يهدف دليل المناقشة هذا إلى تقديم معلومات محدثة مركزة بشأن بعض التطورات الأخيرة في مجال الجريمة السيبرانية، بما في ذلك تأثير جائحة مرض فيروس كورونا (كوفيد-19).

التطورات السياساتية والعمليات الحكومية الدولية

39- أنشأت الجمعية، في قرارها 274/74، لجنة الخبراء المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، مع المراعاة الكاملة للصكوك الدولية القائمة وللجهود المبذولة حالياً على كل من الصعيد الوطني والإقليمي والدولي لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، ولا سيما أعمال ونتائج فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي أنشأته الجمعية بموجب قرارها 230/65، والذي عقد سبع دورات، من عام 2011 إلى عام 2021، بما في ذلك اجتماع تقييمي[26].

40- وفي أعقاب الدورة التنظيمية للجنة المخصصة المعقودة في أيار/مايو 2021، بتت الجمعية العامة، في قرارها 282/75، في جملة أمور منها طرائق اتخاذ القرارات في اللجنة والمسائل المتصلة بالمشاركة، وقررت عقد ست دورات على الأقل مدة كل منها 10 أيام ودورة ختامية، من أجل تقديم مشروع اتفاقية إلى الجمعية العامة في دورتها الثامنة والسبعين. وبسبب أثر جائحة كوفيد-19، أجلت الجمعية العامة بموجب مقررها 552/76 الدورة التفاوضية الأولى للجنة المخصصة التي كان مقررا أصلاً عقدها في كانون الثاني/يناير 2022. وبناء على ذلك، عقدت اللجنة المخصصة دورة بشأن المسائل التنظيمية في 24 شباط/فبراير وعقدت دورتها الأولى في الفترة من 28 شباط/فبراير إلى 11 آذار/مارس 2022.

41- وناقشت اللجنة المخصصة، في دورتها الأولى، أسلوب عملها خلال الدورات اللاحقة وفترات ما بين الدورات، وأهداف الاتفاقية ونطاقها وهيكلها، وبدأت تبادلا أوليا للآراء بشأن العناصر الرئيسية للاتفاقية.

---

(23) E/CN.15/2018/6.

(24) A/74/130.

(25) E/CN.15/2020/12 و E/CN.15/2021/13.

(26) انظر UNODC/CCPCJ/EG.4/2021/2.

المنع

42- تطرح الجريمة السيبرانية تحديات خاصة في مجال منع الجريمة. ويشمل ذلك زيادة انتشار الأجهزة المتصلة بالإنترنت في كل مكان وميسورية تكلفتها، مما يوجِد أعدادا كبيرة من الضحايا المحتملين؛ والزيادة النسبية في استعداد الأشخاص لاتباع سلوك "محفوف بالمخاطر" عبر الإنترنت؛ وإمكانية إخفاء الهوية واتباع أساليب التعتيم من جانب الجناة؛ والطبيعة العابرة للحدود الوطنية للعديد من أعمال الجريمة السيبرانية؛ والوتيرة السريعة للابتكار الإجرامي. وتترتب على كل من هذه التحديات آثار على التنظيم والأساليب والنُهج المعتمدة لمنع الجريمة السيبرانية.

43- وقد أصبح منع الجريمة السيبرانية عنصرا هاما من عناصر السياسات والاستراتيجيات الوطنية الرامية إلى منع ومكافحة الهجمات والتهديدات السيبرانية. وقد أشير إلى ذلك خلال الاجتماع السادس لفريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية الذي ركز، في جملة أمور، على المنع[27].

44- وعلى وجه الخصوص، يمكن للتعاون مع مقدمي خدمات الاتصالات أن يؤدي دورا حاسما في منع الجرائم السيبرانية. ويمكن أن تتراوح مشاركتهم بين الترشيح النشط لما يتداول من الاتصالات والمحتوى عبر الإنترنت بهدف منع أعمال الجريمة السيبرانية قبل ارتكابها أو تعطيلها في مرحلة مبكرة وتخزين بيانات المستخدمين التي يمكن أن يصل إليها موظفو إنفاذ القانون الذين لديهم أمر قضائي لاستخدامها في التحقيقات في الجرائم السيبرانية. وفيما يتعلق بإجراءات تخزين البيانات تلك، يبين أثرها الرادع كيف يمكن لتدابير المنع والتصدي أن تكمل وتعزز بعضها بعضا. وينبغي أن يستند تعاون مقدمي خدمات الاتصالات مع السلطات الوطنية إلى سيادة القانون وحماية حقوق الإنسان.

بناء القدرات والمساعدة التقنية

45- يلزم بذل جهود متواصلة لبناء قدرات الجهات الفاعلة في مجال إنفاذ القانون والعدالة الجنائية على التصدي لأشكال الجريمة السيبرانية السريعة التطور. وقد أصبح تخصص الأجهزة الوطنية لإنفاذ القانون يزداد شيوعاً ويؤدي دورا حاسم الأهمية في تيسير عمليات جمع الأدلة الإلكترونية وتحليلها وتبادلها. ويرتبط هذا التخصص أساساً بالطبيعة الخاصة للجريمة السيبرانية، التي تطرح تحديات محددة فيما يتعلق بتعاريف الجريمة، وإمكانية تطبيق القوانين، وجمع الأدلة الإثباتية وتحليلها. ولذلك سيكون لمهارات أجهزة إنفاذ القانون وقدراتها التقنية أثر مباشر على فعالية التدابير المتخذة في مجال منع الجريمة والعدالة الجنائية لمواجهة الجريمة السيبرانية[28].

باء- التدابير الممكنة

المنع

46- تشكل استراتيجيات أصحاب المصلحة المتعددين فيما يخص الجريمة السيبرانية، التي تستفيد من أدوار مختلف الجهات الفاعلة في القطاعين العام والخاص، وكذلك المجتمع المدني، عنصرا وقائيا حيويا في التصدي للتحديات المتنوعة التي تطرحها الجريمة السيبرانية. ومن الضروري تعزيز وزيادة مشاركة جميع الجهات الفاعلة

(27) UNODC/CCPCJ/EG.4/2020/2، الفقرة 50.

(28) CTOC/COP/WG.3/2015/2، الفقرة 14.

ذات الصلة في منع الجريمة السيبرانية، وفي هذا الصدد، يمكن للمنظمات الإقليمية والقطاع الخاص والأوساط الأكاديمية توفير دعم أساسي، لا سيما للبلدان النامية، من أجل تحقيق ثقافة أمن سيبراني عالمية[29].

47- والشراكات بين القطاعين العام والخاص القائمة على الثقة والاطمئنان المتبادلين للتصدي للتحديات المتعددة الجوانب التي تعترض مكافحة الجريمة السيبرانية لا تقتصر فائدتها على زيادة الوعي، بل تفيد أيضا في منع الجريمة السيبرانية نفسها. فعلى سبيل المثال، يمكن استخدام أدوات الذكاء الاصطناعي للكشف عن المواد التي تنطوي على الاعتداء والاستغلال الجنسيين للأطفال التي توزع عبر الإنترنت. وتوفر الشراكات بين القطاعين العام والخاص آليات الإبلاغ وتقديم المعلومات اللازمة لتحري الجناة وتحديد هويتهم. وعلاوة على ذلك، ومثلما أُفيد في فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، يلزم تحديد مسؤوليات مقدمي خدمات الاتصالات تحديدا واضحا لضمان اتخاذ الاحتياطات الأمنية كتدابير وقائية[30].

48- وتعتبر التدابير الفعالة المتخذة على الصعيدين الوطني والدولي لتيسير ملاحقة الجناة قضائياً ومعاقبتهم والجهود الرامية إلى منع وقوع المزيد من الجرائم بكشف ما يجري من أنشطة إلكترونية غير مشروعة وعرقلتها، بالنظر إلى أثرها الرادع، عنصرا هاما من عناصر سياسات المنع في مكافحة الجريمة السيبرانية. ومما له أهمية في هذا الصدد أيضا ضرورة الاستثمار في بناء القدرات لرفع مستوى مهارات الموظفين العاملين على كامل نطاق نظام العدالة الجنائية، الذين ينبغي إشراكهم على الصعيد الوطني في منع الجرائم السيبرانية والتحقيق فيها.

49- واستنادا إلى مختلف أساليب وتكنولوجيات التحقيق التي تم تطويرها للكشف عن الجريمة السيبرانية، يظل من الضروري مواصلة تطوير رؤى متعمقة لسلوك مرتكبي الجرائم السيبرانية المعاصرين باستخدام تحليل المعلومات الاستخبارية والبحوث الجنائية وتقنيات تحديد السمات النمطية من أجل استغلال الموارد الحالية على نحو أكثر فعالية وتحديد ميزات تكنولوجيات الاتصال المستقبلية المعرضة للاستغلال الإجرامي بصورة استباقية.

بناء القدرات والمساعدة التقنية

50- يساعد البرنامج العالمي المعني بالجريمة السيبرانية الدول الأعضاء على مكافحة الجرائم السيبرانية في أربعة مجالات رئيسية هي: (أ) بناء القدرات؛ و(ب) المنع؛ و(ج) التعاون؛ و(د) الأطر القانونية.

51- وقد أصبحت تقنيات وتكنولوجيات محددة، مثل الذكاء الاصطناعي، ضرورية في التحقيقات في الجرائم السيبرانية. غير أن استخدامها يتطلب تحليلا مسبقا لمشروعية التدابير والتكنولوجيا المختارة وضرورتها وتناسبها، وينبغي النظر في الطريقة الأقل تقييدا من حيث الحقوق الواجب حمايتها.

52- وتواصل الدول الأعضاء تعزيز قدراتها في مجال مكافحة الجرائم السيبرانية من خلال إنشاء مختبرات جنائية ووحدات متخصصة في الشرطة ودوائر النيابة العامة. وقد ساعد المكتب المعني بالمخدرات والجريمة الدول الأعضاء في هذا الصدد بتوفير التدريب والتوجيه والمعدات وبوضع مبادئ توجيهية وإجراءات تشغيل موحدة.

جيم- مسائل مطروحة للنظر فيها

53- لعلَّ اللجنة تودُّ مناقشة الأسئلة التالية:

(أ) ما هي الدروس المستفادة والممارسات الجيدة والتحديات المطروحة في تنفيذ استراتيجيات منع الجريمة السيبرانية؟ وكيف يمكن رصد نتائج هذه الاستراتيجيات وتقييمها وقياسها على أفضل وجه؟

(29) UNODC/CCPCJ/EG.4/2020/2، الفقرة 53.

(30) المرجع نفسه، الفقرة 54.

(ب) كيف يمكن للمؤسسات الأكاديمية والقطاع الخاص والمنظمات غير الحكومية، وكذلك المنظمات الحكومية الدولية، أن تسهم على أفضل وجه في تطوير المعارف والتشريعات والسياسات وتبادلها في مجال الجريمة السيبرانية؟ وكيف يمكنها التعاون مع الدول الأعضاء في الكشف عن الجرائم السيبرانية والتحقيق فيها؟

(ج) ما هي الخبرة المتراكمة للدول الأعضاء فيما يتعلق بالموازنة بين حماية حقوق الإنسان مثل الحق في الخصوصية (حماية البيانات) وحرية الرأي والتعبير من جهة، وفعالية تدابير العدالة الجنائية وإنفاذ القانون ضد الجرائم السيبرانية من جهة أخرى؟

(د) ما هي جوانب التدابير المتصلة بالجريمة السيبرانية التي تحظى بأولوية عالية في المساعدة التقنية وبناء القدرات، ولا سيما بالنظر إلى الطبيعة المتطورة للجريمة السيبرانية وزيادة استخدام التكنولوجيا بسبب جائحة كوفيد-19؟

رابعا- الاعتداء على الأطفال واستغلالهم في أنشطة غير مشروعة باستخدام الإنترنت

ألف- الحالة الراهنة والتحديات

54- يفترض أن ثلثي سكان العالم لديهم الآن إمكانية الوصول إلى الإنترنت. ويعيش 60 في المائة من الأشخاص الموصولين بالإنترنت في البلدان النامية، وتبلغ أعمار 45 في المائة منهم 25 عاما أو أقل. وقد أدى تزايد عدد مستخدمي الإنترنت إلى ارتفاع عالمي في عدد الضحايا والمجرمين المحتملين في الجرائم السيبرانية، على النحو الذي تنبأ به المكتب المعني بالمخدرات والجريمة في بداية الجائحة[31]. وفي هذا السياق، يشكل نوع الجنس والعمر عاملين من عوامل الضعف. ومن الأرجح أن وقوع الأطفال، ولا سيما الفتيات، ضحايا لجرائم سيبرانية، خاصة التحرش عبر الإنترنت والاعتداء الجنسي والاتجار لأغراض مختلفة من الاستغلال باستخدام تكنولوجيات المعلومات والاتصالات.

الاعتداء على الأطفال واستغلالهم جنسيا عبر الإنترنت

55- يشمل الاعتداء على الأطفال واستغلالهم جنسيا عبر الإنترنت إنتاج مواد الإيذاء الجنسي للأطفال، بل أيضا "الاستدراج السيبراني" و"الإغواء" و"الاستمالة عبر الإنترنت"، وهي مصطلحات شائعة تستخدم مجتمعة أو تبادليا لوصف الاتصالات التي يجريها البالغون من خلال استخدام تكنولوجيا المعلومات والاتصالات لغرض الاعتداء على الأطفال واستغلالهم جنسيا[32]. وتشمل آثار تكنولوجيا المعلومات والاتصالات على الأشكال الشائعة القائمة للاعتداء على الأطفال واستغلالهم جنسيا تعزيز فرص الوصول إلى الضحايا ومواد الإيذاء الجنسي للأطفال، وزيادة أرباح المشاريع الإجرامية، وتقليل احتمالات الاعتقال للجناة، وتزويدهم بقدر من إثبات الذات اجتماعياً [33]. ومما يثير القلق بوجه خاص الأشكال الجديدة مثل المواد المعدة حسب الطلب التي تصور

(31) UNODC, "Cybercrime and COVID-19: risks and responses" (April 2020).

(32) UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienna, 2015), p. 11.

(33) المرجع نفسه، الصفحات 15-20.

اعتداءات جنسية على الأطفال، والمحتوى الذي ينتجه المستخدمون والمحتوى المُنتج ذاتياً، بما في ذلك تبادل الرسائل الجنسية، والبث المباشر للاعتداء على الأطفال واستغلالهم جنسياً[34].

56- وفي عام 2021، أكدت استطلاعات مستقلة أن حجم وتعقيد الاعتداء على الأطفال واستغلالهم جنسيا عبر الإنترنت آخذان في الازدياد وأن الأطفال يواجهون اليوم تهديدا مستمرا في هذا الصدد[35]. وتؤكد تقارير اليوروبول أيضا أن النشاط المتعلق بتوزيع مواد الاستغلال الجنسي للأطفال عبر الإنترنت يبدو في ازدياد، استنادا إلى عدد من المؤشرات. ويبدو أن جائحة كوفيد-19 والتدابير التقييدية ذات الصلة قد سرعت هذا الاتجاه[36]، وقد يكون الأطفال أكثر ميلا نحو إنتاج المحتوى ذاتياً لتبادله مع أقرانهم أو مع البالغين. وتلقت مؤسسة رصد الإنترنت (Internet Watch Foundation) 000 68 ألف بلاغ عن محتوى جنسي ينتجه الأطفال ذاتياً في عام 2020، وهذا يمثل زيادة بنسبة 77 في المائة مقارنة بعام 2019[37].

الاتجار بالأطفال عن طريق الإنترنت وغيره من أشكال الاعتداء والاستغلال عبر الإنترنت

57- يتزايد استخدام تكنولوجيا المعلومات والاتصالات من جانب مرتكبي الاتجار بالأشخاص في كل شيء من تحديد هوية ضحايا محتملين للمستقبل إلى استغلالهم[38]. وغالبا ما يوفر الأطفال معلوماتهم الشخصية عبر الإنترنت، خاصة على منصات التواصل الاجتماعي ومواقع الألعاب، مما يتيح تحديداً نمطياً يستهدف الضحايا بغرض استمالتهم، مع الحفاظ على سرية هوية الجناة. وقد استفاد المتجرون من التكنولوجيات الجديدة لتحسين أساليبهم في السيطرة على الضحايا، مثلا من خلال التهديد والخداع الذين يحصل المجرمون بواسطتهما على مواد ذات خصوصية حميمة تتعلق بضحاياهم، ثم يستخدمونها لابتزازهم[39].

58- ويشكل الاتجار لأغراض الاستغلال الجنسي غالبية الحالات المكتشفة للاتجار من أجل الاستغلال عبر الإنترنت، ويمثل الأطفال نسبة كبيرة من الضحايا. وفي السنوات الأخيرة، زاد بشكل كبير عدد البلاغات عن المواد المتاحة عبر الإنترنت التي تنطوي على اعتداء جنسي على الأطفال.

59- وتوسع تكنولوجيا المعلومات والاتصالات دائرة الأطفال الذين قد يستغلهم المتجرون جنسيا وعدد عملائهم المحتملين، بسبب عدم وجود قيود مادية أو جغرافية[40]. وبالإضافة إلى ذلك، مكنت هذه التكنولوجيا المتجرين من تحقيق أقصى قدر من الأرباح من خلال وفورات الحجم الكبيرة، وذلك مثلاً عن طريق الانتفاع من الأطفال تجارياً واستغلالهم من خلال البث المباشر على العديد من المواقع الشبكية، والسماح بمشاهدة

(34) Chloe Setter and others, *Global Threat Assessment* 2021 (WeProtect Global Alliance, 2021), p. 54. المرجع نفسه، الصفحتان 21 و22، و.

(35) Setter and others, *Global Threat Assessment 2021*.

(36) United Nations Sustainable Development Group, “Policy brief: the impact of COVID-19 on children” (April 2020), p. 3; Europol, “Catching the virus: cybercrime, disinformation and the COVID-19 pandemic” (April 2020), p. 9.

(37) Setter and others, *Global Threat Assessment 2021*.

(38) في المادة 3 من بروتوكول منع وقمع ومعاقبة الاتجار بالأشخاص، وبخاصة النساء والأطفال، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، يُعرَّف تعبير "الاتجار بالأشخاص" بأنه "تجنيد أشخاص أو نقلهم أو تنقيلهم أو إيواؤهم أو استقبالهم بواسطة التهديد بالقوة أو استعمالها أو غير ذلك من أشكال القسر أو الاختطاف أو الاحتيال أو الخداع أو استغلال السلطة أو استغلال حالة استضعاف، أو بإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص له سيطرة على شخص آخر لغرض الاستغلال".

(39) ورقة معلومات أساسية من إعداد الأمانة بشأن الاستراتيجيات الناجحة للتصدي لاستخدام التكنولوجيا بغرض تيسير الاتجار بالأشخاص، ومنع الاتجار بالأشخاص والتحقيق فيه (CTOC/COP/WG.4/2021/2)، الفقرة 18.

(40) UNODC, *Global Report on Trafficking in Persons 2020* (United Nations publication, 2021), p. 122.

مقاطع الفيديو لمرات غير محدودة، وبيع خدماتهم للعديد من العملاء من خلال نشـــر نفس الإعلان على مجموعة متعددة من المنصـات. وقد أبلغت منظمات مثل المركز الوطني للأطفال المفقودين والمسـتغلين في الولايات المتحدة والمنظمة الدولية للشـــرطة الجنائية (الإنتربول) عن زيادة كبيرة في عدد حالات الاتجار بالأطفال واستغلالهم جنسيا عبر الإنترنت منذ بداية الجائحة[41].

60- ويحدث الاتجار بالأطفال عبر الإنترنت على الشبكة الظاهرة وعلى الشبكات الخفية، التي تُستخدم أيضا لحفظ المواد وإخفائها وتمكن الجناة من إخفاء المواد غير المشروعة عن المحققين بشكل أفضل.

تجنيد الأطفال واستغلالهم من الجماعات الإجرامية المنظمة والمسلحة، بما فيها الجماعات المدرجة في قوائم الجماعات الإرهابية، باستخدام الإنترنت

61- إن تجنيد الأطفال واســـتغلالهم من الجماعات الإجرامية المنظمة والمســـلحة، بما فيها الجماعات المدرجة في قوائم الجماعات الإرهابية، شـكلٌ خطير من أشـكال العنف ضـد الأطفال يحظره القانون الدولي. ويتعين على الدول أن تجرمه وأن تتخذ جميع التدابير المناســـبة[42]، التي تكفل اعتبار هؤلاء الأطفال، عند اتصالهم بالسلطات الوطنية، ضحايا في المقام الأول ومعاملتهم على هذا الأساس[43].

62- ويمثل اسـتخدام تكنولوجيا المعلومات والاتصـالات ودورها في تجنيد الأطفال واسـتغلالهم من قبل هذه الجماعات وسـيلة جديدة نسـبيا لنشـر الدعاية وتوسـيع نطاق رسـائل تلك الجماعات[44]. والأطفال معرضـون للخطر بوجه خاص بسـبب تطورهم ونموهم البدني والنفسـي المسـتمر ولكونهم نشـطين في اسـتخدام الإنترنت. وتعد مواقع وسائل التواصـل الاجتماعي والبريد الإلكتروني وغرف الدردشـة والمجموعات الإلكترونية وتسـجيلات الفيديو من أدوات التجنيد المنتشرة على وجه الخصـوص التي يمكن أن تيسر استمالة الضـحايا. وبالإضـافة إلى ذلك، يمكن أيضـا استخدام "الإعلان الموجه" لتحديد الفئات الضـعيفة مثل الأطفال وتعديل مضمون الروايات بما يناسب الجمهور المستهدف[45].

63- وقد تســـتغل الجماعات الإجرامية المنظمة والمســـلحة، بما فيها الجماعات المدرجة في قوائم الجماعات الإرهابية، ضـعف الأطفال لتجنيدهم واسـتغلالهم المحتملين، ولا سـيما عندما يتفاقم هذا الضـعف، كما حدث أثناء جائحة كوفيد-19. فقد أدت هذه الأزمة إلى تضـخيم المعلومات المضـللة المتاحة عبر وسـائل التواصـــل الاجتماعي وخلقت فرصـــا جديدة لهذه الجماعات، بما في ذلك اســـتغلال نقاط الضـــعف في بيئة وســـائل التواصـــل الاجتماعي للتلاعب بالأفراد ونشـــر نظريات المؤامرة[46]. وقد ركزت اســـتراتيجيات هذه

(41) Patricia Davis, “100,000,000: the race to save children behind the staggering number”, National Center for Missing and Exploited Children, 1 December 2021.

(42) قرار الجمعية العامة 172/69.

(43) قرار مجلس الأمن 2427 (2018)؛ والمبادئ المتعلقة بمركز المؤسسات الوطنية لتعزيز حقوق الإنسان وحمايتها (مبادئ باريس). انظر أيضا: خريطة الطريق بشأن معاملة الأطفال المرتبطين بالجماعات الإرهابية والجماعات المتطرفة العنيفة (UNODC, “Roadmap on the treatment of children associated with terrorist and violent extremist groups” (Vienna, 2019)).

(44) قرار مجلس الأمن 2331 (2016) بشأن إساءة استخدام تكنولوجيا المعلومات والاتصالات لتسهيل الاتجار بالأشخاص من قبل الجماعات الإرهابية.

(45) المكتب المعني بالمخدرات والجريمة، *دليل بشأن الأطفال الذين تجندهم وتستغلهم الجماعات الإرهابية والجماعات المتطرفة العنيفة: دور نظام العدالة* (فيينا، 2017)، الصفحة 13.

(46) United Nations Interregional Crime and Justice Research Institute, “Stop the virus of disinformation: the risk of malicious use of social media during COVID-19 and the technology (منشور لمعهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة).

الجماعات للتجنيد عبر الإنترنت على نشر الروايات البديلة والمضادة، ولهذا السبب يلزم وضع آليات يعاد بواسطتها توجيه الأفراد الذين يبحثون عن محتوى إرهابي ومتطرف عنيف نحو وسائل الإعلام التي تنشر رسائل لمكافحة الدعاية التي تقوم بها هذه الجماعات[47].

التحديات التي تواجه الأطفال ضحايا الاعتداء والاستغلال عبر الإنترنت

64- أدى استخدام الإنترنت بغرض الاعتداء على الأطفال واستغلالهم إلى زيادة مستويات الضرر الذي يلحق بالضحايا، حيث أدت تكنولوجيات مثل تبادل الملفات من نظير إلى نظير إلى تفاقم توزيع مواد تسجل اعتداءات جنسية على الأطفال، ومكنت تكنولوجيا الحوسبة السحابية من وصول أفراد إلى إمكانات تخزين يمكن أن تستضيف كميات كبيرة من المواد بتكلفة منخفضة[48]. وبالإضافة إلى ذلك، غالبا لا يبلغ بقدر كاف عن الاعتداءات التي تحدث عبر الإنترنت، وقد تزايدت التحديات التي تواجه الأطفال في الإبلاغ والوصول إلى العدالة بسبب جائحة كوفيد-19، حيث أدت القيود المفروضة على الحركة إلى تقليل إمكانية وصول الأطفال إلى الأشخاص الذين يوفرون الدعم مثل المعلمين من أجل الإبلاغ عن حوادث تقع في المنزل أو عبر الإنترنت، وفي الوقت نفسه ربما تكون الخدمات المتعلقة بالعمل الاجتماعي والخدمات القانونية والحماية المقدمة للأطفال قد تقلصت أو عُلقت بسبب تدابير التباعد الاجتماعي[49].

65- وتشمل عوامل الخطر التي تعرض الأطفال للوقوع ضحايا للاعتداء والاستغلال عبر الإنترنت نوع الجنس والميل الجنسي، والتعرض لاعتداءات سابقة، والتفكك الأسري، والفقر والهجرة، والسن، والسلوك المستهين بالمخاطر في التعامل مع الإنترنت، وعدم الاهتمام بالسلامة والخصوصية عبر الإنترنت، بالإضافة إلى العزلة الاجتماعية[50]. وقد زادت الجائحة من تلك المخاطر، على النحو المبين أعلاه.

66- وعند الوصول إلى نظام العدالة والإبلاغ عن حوادث الجريمة والعنف، يواجه الأطفال ضحايا الجريمة والعنف عادة العديد من التحديات، مع عدم الاعتراف الكافي بحقوقهم في كثير من الأحيان. ومن الأهمية بمكان الاعتراف بأن الأطفال، وعلى وجه التحديد الأطفال الضحايا، مستضعفون ويحتاجون إلى حماية خاصة تتناسب مع سنهم ومستوى نضجهم واحتياجاتهم الخاصة الفردية[51]. والاعتراف بوضع الأطفال كضحايا للاعتداء والاستغلال عبر الإنترنت شرط مسبق لحصولهم على الحقوق بوصفهم ضحايا للجريمة، ولا سيما بوصفهم مشاركين في الإجراءات القانونية وفيما يتعلق بحقوقهم في جبر الضرر وإعادة التأهيل. والأطفال الضحايا الذين لا يلقون الاعتبار والحماية المناسبين المراعيين للطفولة والاعتبارات الجنسانية قد يتعرضون للإيذاء مرة أخرى أثناء اتصالهم بنظام العدالة، مما قد يجعلهم أكثر عرضة للعنف في المستقبل ويقلل من احتمال إبلاغهم عن جرائم العنف[52].

(47) المكتب المعني بالمخدرات والجريمة، *دليل بشأن الأطفال الذين تجندهم وتستغلهم الجماعات الإرهابية والجماعات المتطرفة العنيفة*. الصفحة 33.

(48) UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, p. 19.

(49) United Nations Sustainable Development Group, "Policy brief: the impact of COVID-19 on children", p. 10.

(50) UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, pp. 23-27.

(51) المبادئ التوجيهية بشأن العدالة في الأمور المتعلقة بالأطفال ضحايا الجريمة والشهود عليها، الفقرة 7.

(52) استراتيجيات الأمم المتحدة وتدابيرها العملية النموذجية للقضاء على العنف ضد الأطفال في مجال منع الجريمة والعدالة الجنائية.

التحديات التي تواجهها الدول الأعضاء في منع الاعتداء على الأطفال واستغلالهم عبر الإنترنت والتصدي لهما

67- الجريمة السيبرانية، بما في ذلك الاعتداء على الأطفال واستغلالهم عبر الإنترنت، هي جريمة معقدة للغاية من حيث التعامل معها. فهي تقع في عالم الفضاء السيبراني الذي لا حدود له، وفيها يمكن أن يكون الضحايا والجناة والأدوات المستخدمة، بل يكونون غالبا، في بلدان مختلفة. وتحدث الجرائم على المنصات المنظمة وغير المنظمة على حد سواء (الشبكة الظاهرة والشبكات الخفية)، مما قد يعوق جمع البيانات والإحصاءات الموثوقة[53]. وتكون غالبية الأدلة في الجرائم السيبرانية إلكترونيةً، وكثيرا ما تتطلب استخدام أساليب خاصة للتحري، بالإضافة إلى إقامة تعاون دولي رسمي وغير رسمي.

68- ولا يزال تجريم أفعال الجريمة السيبرانية غير كاف في العديد من البلدان، وكذلك الكشف الفعال عن الاعتداء على الأطفال واستغلالهم عبر الإنترنت والتحقيق فيهما وملاحقة مرتكبيهما، بما في ذلك توليد أدلة إثبات واضحة من خلال استخدام تحليل الصور وقواعد بيانات الصور، والاستدلال الجنائي الرقمي، والبحث الآلي، وعمليات التنقيب في البيانات وتحليلاتها، والعمليات السرية. وعندما يتعلق الأمر بمقاضاة مرتكبي هذه الجرائم، فإن تحسين آليات التعاون الدولي أمر بالغ الأهمية لأن العديد من الدول الأعضاء قد تكون ما زالت تعتمد على آليات التعاون التقليدية للحصول على أدلة تتجاوز الحدود الإقليمية في هذه الحالات.

69- وأخيرا، قد تواجه الدول الأعضاء تحديات، مثل الافتقار إلى آليات للتنسيق، في حماية الأطفال بفعالية من هذا الشكل الخطير من أشكال العنف. ومعالجة تلك التحديات أمر أساسي لضمان التصدي لهذه الظاهرة على نحو يشجع اتباع نهج يشمل المجتمع بأسره ويعزز الشراكات بين القطاعين العام والخاص والتنسيق والتعاون فيما بين مختلف المؤسسات والجهات الفاعلة (مثل قطاعات العدالة وحماية الطفل والتعليم والصحة والأمن).

أمثلة على المبادرات المستندة إلى الأدلة التي خضعت للتقييم وتهدف إلى التغلب على بعض التحديات

70- التحالف العالمي المعني بتوفير الحماية (We Protect) هو شبكة عالمية تهدف إلى إنهاء استغلال الأطفال والاعتداء عليهم جنسياً عبر الإنترنت. ويضم أعضاؤه 98 حكومة، و52 شركة، و64 من منظمات المجتمع المدني، وتسع منظمات دولية. وهو ينشر وثائق مثل *تقييم التهديد العالمي لعام 2021* والمذكرة التوجيهية بشأن تنفيذ استراتيجية التصدي العالمية للقضاء على استغلال الأطفال والاعتداء عليهم جنسياً عبر الإنترنت.

71- وقد سلط الفريق العامل المعني بالاتجار بالأشخاص الضوء على الابتكارات في أساليب التحري التكنولوجية، مثل تقنية PhotoDNA (التي تساعد على إيجاد صور استغلال الأطفال وحذفها) وقواعد البيانات التي تحسن عمليات الاستدلال العلمي الجنائي المستخدمة في التحقيقات في الاتجار بالأطفال والاعتداء الجنسي على الأطفال[54].

التطورات السياساتية والأطر الدولية

72- تحدد اتفاقية حقوق الطفل المعايير الدنيا للحماية التي يحق للأطفال التمتع بها، بما في ذلك الحماية من التأثيرات الضارة والاعتداء والاستغلال. ويركز البروتوكول الاختياري المتعلق ببيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية حصرا على التصدي للاعتداء الجنسي على الأطفال واستغلالهم جنسيا. وتنص اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية على طائفة من الأحكام المتعلقة بالتعاون

(53) Europol, *IOCTA 2016: Internet Organised Crime Threat Assessment* (The Hague, 2016).

(54) انظر CTOC/COP/WG.4/2021/2 لمزيد من الأمثلة.

الدولي على مكافحة الجريمة المنظمة عبر الوطنية، ويُلزم بروتوكولها لمنع وقمع ومعاقبة الاتجار بالأشخاص، وبخاصة النساء والأطفال، الدول الأطراف بتجريم الاتجار بالأشخاص، بمن فيهم الأطفال.

73- وتسليما بالحاجة الملحة إلى معالجة مسألة العنف ضد الأطفال، ولا سيما دور نظام العدالة الجنائية، اعتمدت الجمعية العامة في عام 2014 استراتيجيات الأمم المتحدة وتدابيرها العملية النموذجية للقضاء على العنف ضد الأطفال في مجال منع الجريمة والعدالة الجنائية. وعلاوة على ذلك، تحدد المبادئ التوجيهية بشأن العدالة في الأمور المتعلقة بالأطفال ضحايا الجريمة والشهود عليها، التي اعتمدها المجلس الاقتصادي والاجتماعي في عام 2005، الممارسات الجيدة القائمة على التوافق بين المعارف المعاصرة والقواعد والمعايير والمبادئ الدولية والإقليمية ذات الصلة.

74- وحثت الجمعية العامة، في قرارها 174/74 بشأن مكافحة الاستغلال الجنسي للأطفال وانتهاكهم جنسيًّا على الإنترنت، الدول الأعضاء على تجريم هذه الجرائم وتعزيز جهودها الرامية إلى مكافحة الجرائم السيبرانية المتصلة بالاستغلال الجنسي للأطفال وانتهاكهم جنسيًّا على الإنترنت، بما يشمل ارتكاب هذه الجرائم على الإنترنت.

75- وفي الإعلان السياسي لعام 2021 المتعلق بتنفيذ خطة عمل الأمم المتحدة العالمية لمكافحة الاتجار بالأشخاص، أشارت الدول الأعضاء بقلق إلى تزايد إساءة استخدام تكنولوجيا المعلومات والاتصالات لتسهيل مختلف جوانب الاتجار بالأشخاص ومختلف أشكال الاستغلال، بما في ذلك الاستغلال الجنسي للأطفال عبر الإنترنت، وأكدت أهمية التصدي لإساءة الاستخدام هذه في ظل احترام حقوق الإنسان.

76- وتشمل الصكوك الإقليمية ذات الصلة اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، واتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي، واتفاقية رابطة أمم جنوب شرق آسيا لمكافحة الاتجار بالأشخاص، وبخاصة النساء والأطفال، واتفاقية البلدان الأمريكية بشأن الاتجار الدولي بالقاصرين، والميثاق الأفريقي لحقوق الطفل ورفاهيته.

77- وفي الآونة الأخيرة، اعتمد الاتحاد الأوروبي استراتيجية لزيادة فعالية مكافحة الاعتداء الجنسي على الأطفال.

باء- التدابير الممكنة

78- عندما يتعلق الأمر بمنع الأشكال الخطيرة من العنف ضد الأطفال، بما في ذلك الاعتداء عليهم واستغلالهم عبر الإنترنت، يمكن أن تشمل تدابير الوقاية الأولية ضمان حظر هذا الشكل من أشكال العنف ضد الأطفال بموجب القانون، وتنفيذ استراتيجيات وبرامج وقائية شاملة مصممة خصيصا لهذا الغرض، وتشجيع البحث وجمع البيانات. وقد تركت الدول إلى حد كبير لقطاع التكنولوجيا اتخاذ تدابير تنظيم ذاتي طوعية لمنع جرائم مثل الاتجار بالأشخاص عبر الإنترنت أو الاستغلال الجنسي للأطفال عبر الإنترنت[55]. ولم يثبت ذلك كفايته، وينبغي للدول أن تضع أطرا تنظيمية ورقابية قوية لوقف حالة الإفلات من العقاب السائدة حالياً. ويمكن للدول أن تعتمد تدابير سلامة مثل التحقق من أعمار وموافقة الأشخاص المشاركين في مقاطع الفيديو ذات المحتوى الجنسي الصريح على المنصات الشائعة الاستخدام والتحقق من أعمار مشاهديها، إضافة إلى إجراءات أسهل لإزالة المحتوى عند اكتشاف مواد ضارة وغير مشروعة.

(55) Organisation for Security and Co-operation in Europe, Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, “Policy responses to technology-facilitated trafficking in human beings: analysis of current approaches and considerations for moving forward” (Vienna, 2022), pp. 2–6.

79- ويمكن أن تشمل تدابير الوقاية الثانوية تعزيز قدرة نظام العدالة الجنائية على التصدي للاعتداء على الأطفال واستغلالهم عبر الإنترنت. ويستتبع ذلك إنشاء آليات فعالة للكشف والإبلاغ، وتوفير حماية فعالة للأطفال ضحايا العنف، وضمان التحقيق في حوادث العنف ضد الأطفال ومقاضاة مرتكبيها، وتحسين الإجراءات الجنائية، وتعزيز التعاون بين مختلف القطاعات، وضمان أن تعبّر العقوبات الموقَّعة عما يتسم به العنف ضد الأطفال من طابع خطير، وتعزيز قدرات المهنيين وتدريبهم. ويمكن أن تشمل التدابير المحددة تحديد المحتوى وإزالته عن طريق إشراك كيانات خاصة مثل مقدمي خدمات الاتصالات ووضع بروتوكولات مع شركات التكنولوجيا والمنصات الإلكترونية بحيث لا يحذف مقدمو خدمات الاتصالات المحتوى غير المشروع بل يحيلونه بدلا من ذلك إلى وكالات إنفاذ القانون من أجل التحقيق والمقاضاة[56]. ويلزم تعزيز الشراكات بين القطاعين العام والخاص لضمان مزيد من المساءلة للمنصات التي تستضيف محتوى غير قانوني.

80- ويمكن استكمال هذه الإجراءات بمبادرات الدعوة والتوعية، بما في ذلك أنشطة متخصصة لبناء قدرات جميع الجهات الفاعلة المعنية المشاركة في الكشف عن المحتوى على الإنترنت وإزالته، ومبادرات توعية وتثقيف موجهة إلى الأطفال أنفسهم، بغية تمكينهم من العمل كعوامل للتغيير من أجل حمايتهم.

جيم- مسائل مطروحة للنظر فيها

81- لعلَّ اللجنة تودُّ مناقشة المسائل التالية:

(أ) هل يعالج الإطار القانوني الدولي الحالي بما فيه الكفاية المسائل المتصلة بتكنولوجيا المعلومات والاتصالات والاعتداء على الأطفال واستغلالهم والاتجار بالأشخاص عبر الإنترنت؟

(ب) كيف يمكن للدول الأعضاء تعزيز الدور الرئيسي لنظام العدالة، بوسائل منها التعاون مع أصحاب المصلحة المعنيين الآخرين، في منع الاعتداء على الأطفال واستغلالهم عبر الإنترنت والتصدي لهما؟

(ج) ما هي الأطر والتدابير الرقابية التي ينبغي اعتمادها لتعزيز الكشف عن أعمال الاعتداء على الأطفال أو استغلالهم جنسياً أو الاتجار بهم عبر الإنترنت والإبلاغ عنها، ومعالجة الطلب على محتوى من هذا القبيل، وزيادة مسؤولية شركات التكنولوجيا والمنصات الإلكترونية عن استضافة مواد غير مشروعة وضارة؟

(د) ما هي أنشطة تنمية القدرات اللازمة حاليا لكي تتمكن كيانات إنفاذ القانون من التحقيق بفعالية في الاعتداء على الأطفال واستغلالهم والاتجار بالأشخاص عبر الإنترنت، وجمع الأدلة الإلكترونية ذات الصلة؟

(هـ) كيف يمكن للمنظمات الدولية، مثل المكتب المعني بالمخدرات والجريمة، أن تساعد الدول الأعضاء على تعزيز التعاون الدولي من أجل مقاضاة ومحاسبة مرتكبي الاعتداء على الأطفال واستغلالهم عبر الإنترنت؟

(و) كيف يمكن للمنظمات الدولية، مثل المكتب المعني بالمخدرات والجريمة، أن تساعد الدول الأعضاء على تعزيز الشراكات بين القطاعين العام والخاص من أجل ضمان مساءلة الشركات الخاصة والحصول على الأدلة والبيانات ذات الصلة بالتحقيقات والملاحقات القضائية؟

(ز) ما هي الاستراتيجيات والتدابير المبتكرة القائمة من أجل تعزيز مشاركة الأطفال والشباب في حماية أنفسهم من الاعتداء والاستغلال والاتجار بالأشخاص عبر الإنترنت؟

---

(56) المرجع نفسه، الصفحة 3.