UNODC/CCPCJ/EG.4/2020/L.1/Add.1

27 July 2020
Arabic
Original: English

فريق الخبراء المعني بإجراء دراسة
شاملة عن الجريمة السيبرانية
فيينا، 27-29 تموز/يوليه 2020

مشروع التقرير

إضافة

ثانيا- قائمة التوصيات والاستنتاجات الأولية *(تابع)*

ألف- التعاون الدولي

1- تماشيا مع خطة عمل فريق الخبراء، تتضمن هذه الفقرة تجميعا للاقتراحات التي قدمتها الدول الأعضاء في الاجتماع في إطار البند 2 من جدول الأعمال المعنون "التعاون الدولي". وهذه الاستنتاجات والتوصيات الأولية مقدمة من الدول الأعضاء، ولا يعني إدراجها أن فريق الخبراء قد أقرها، كما أن ترتيب عرضها لا يعني ضمنا ترتيبا لدرجة أهميتها:

(1) فيما يتعلق بنطاق تعريف الجريمة السيبرانية لأغراض التعاون الدولي، ينبغي للبلدان أن تكفل تجريم الأفعال الإجرامية السيبرانية على نحو كاف، لا يشمل الجرائم التي ترتكب بواسطة الفضاء السيبراني فحسب، وإنما أيضا الجرائم الأخرى التي كثيرا ما ترتكب باستخدام الإنترنت والوسائل الإلكترونية (الجرائم التي تُيسَّر بواسطة الفضاء السيبراني)، مثل الاحتيال السيبراني، والسرقة السيبرانية، والابتزاز، وغسل الأموال، والاتجار بالمخدرات والأسلحة، واستغلال الأطفال في المواد الإباحية، والأنشطة الإرهابية.

(2) فيما يتعلق بآليات التعاون الدولي، تشجع الدول، في حال عدم وجود معاهدة ثنائية للمساعدة القانونية المتبادلة، على الانضمام إلى المعاهدات المتعددة الأطراف القائمة التي توفر أساسا قانونيا للمساعدة القانونية المتبادلة، مثل اتفاقية بودابست واتفاقية الجريمة المنظمة، أو على استخدام تلك المعاهدات المتعددة الأطراف. وفي حال عدم وجود أي معاهدة، يجوز لدولة أن تطلب من دولة أخرى التعاون على أساس مبدأ المعاملة بالمثل؛ وينبغي أيضا استخدام اتفاقية بودابست كمعيار لبناء القدرات والمساعدة التقنية على الصعيد العالمي، مع توجيه الانتباه إلى المفاوضات الجارية بشأن البروتوكول الإضافي الثاني لاتفاقية بودابست الرامي إلى زيادة تعزيز التعاون عبر الحدود. وفي مداخلة أخرى، أعيد التأكيد على أن إمكانية تطبيق اتفاقية بودابست محدودة نظرا لطبيعتها كصك إقليمي وحالة التصديق عليها، فضلا عن افتقارها إلى نهج كلي، وعدم مراعاتها

للاتجاهات الراهنة في مجال الجريمة السيبرانية، وعدم ملاءمتها على نحو كامل بالنسبة للبلدان النامية. ووجه الانتباه إلى قرار الجمعية العامة 247/74 المؤرخ 27 كانون الأول/ديسمبر 2019، الذي قررت فيه الجمعية العامة إنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية، تُمثَّل فيها جميع الأقاليم، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. وأشارت مداخلات أخرى إلى أنه ينبغي للأطر أو الصكوك الجديدة بشأن الجريمة السيبرانية ألا تتعارض مع الأطر أو الصكوك القائمة، وألا تتسبب في أن تتخلى الدول عن المعاهدات الحالية أو الالتزامات التي سبق أن قطعتها على نفسها، وكذلك الاتفاقات القائمة بالفعل، أو تعارض أيا مما سبق.

(3) من الضروري وجود شركاء استراتيجيين في سياق التحقيق في الجرائم السيبرانية، مثل أعضاء المنظمات القائمة، ومنها منظمة الدول الأمريكية أو مجموعة السبع أو الإنتربول.

(4) يتعين، في سياق التحقيقات والإجراءات القضائية، احترام سيادة الدول وولايتها القضائية. ولا ينبغي تقديم أي طلبات للاسترجاع المباشر للبيانات الموجودة في بلد آخر إلى أي منشأة تجارية أو إلى أفراد دون موافقة مسبقة من ذلك البلد.

(5) ينبغي تحسين كفاءة التعاون الدولي عن طريق إنشاء آليات للاستجابة السريعة للتعاون الدولي وكذلك قنوات للاتصال بين السلطات الوطنية، من خلال موظفي الاتصال ونظم تكنولوجيا المعلومات، لجمع الأدلة عبر الحدود ونقل الأدلة الإلكترونية عبر الإنترنت.

(6) ينبغي للدول أن تواصل تعزيز التعاون لحماية البنى التحتية الحيوية وتعزيز شبكات التعاون بين فرق التصدي للطوارئ الحاسوبية وفرق التصدي للحوادث الحاسوبية.

(7) ينبغي للدول أن تنظر في وضع بروتوكولات مبتكرة لتبادل المعلومات، بما في ذلك المعلومات الاستخبارية والأدلة على الأفعال الإجرامية، من أجل التعجيل بهذه الإجراءات.

(8) هناك حاجة إلى التأكيد مجددا على التزام جميع الدول الأعضاء بضمان سلامة وأمن تكنولوجيا المعلومات والاتصالات من خلال اقتصار استخدامها على الأغراض السلمية وتعزيز الجهود الدولية لمكافحة أي أنشطة خبيثة في الفضاء السيبراني في أوقات الأزمات الكبرى على كل من المستوى العالمي والإقليمي والمحلي.

(9) ينبغي أن تُسيَّر إجراءات التعاون الدولي على النحو الأمثل بحيث يقدم أقصى قدر من المساعدة لطلبات التعاون الدولي المتعلقة بحفظ الأدلة الإلكترونية، والحصول على معلومات السجلات، ومعلومات تسجيل المستخدمين التي لا تتعارض مع حقوق الإنسان والحريات الأساسية أو حقوق الملكية، في حدود الإمكانات المستمدة من الإطار القانوني المحلي.

(10) تدعى البلدان إلى إيلاء اهتمام خاص لضرورة أن تكون تدابير التحقيق متناسبة، مع احترام الحريات الأساسية وأنظمة حماية البيانات الشخصية المرتبطة بالمراسلات الخاصة.

(11) ينبغي للتعاون الدولي في مجال مكافحة الجريمة السيبرانية أن يأخذ في الاعتبار النهوج التي تراعي الاعتبارات المتعلقة بنوع الجنس وعامل السن، واحتياجات الفئات المستضعفة.

(12) فيما يتعلق بنطاق التعاون الدولي، ينبغي أن يكون تقديم المساعدة القانونية من خلال السلطات الوطنية فقط، لكن لا ينبغي أن يقتصر التعاون على الإدارات الحكومية، بل ينبغي أن يشمل أيضا القطاع الخاص، مثل مقدمي خدمات الإنترنت. وفي هذا السياق، أوصي بضرورة اعتماد أحكام تتيح التعاون المباشر مع مقدمي خدمات الإنترنت في ولايات قضائية أخرى فيما يتعلق بطلبات المعلومات عن المشتركين، وطلبات حفظ البيانات، والطلبات الطارئة.

(13) يجب أن تضمن الخيارات المتاحة للتصدي للجريمة السيبرانية وحماية المجتمعات دائما حماية حقوق الإنسان والضمانات الدستورية، وأن تعزز وجود فضاء سيبراني أكثر حرية وانفتاحا وأمنا ومرونة للجميع.

(14) تشجع البلدان على تحسين سبل التعاون مع الأوساط الصناعية، وتعزيز التعاون بين مقدمي الخدمات من القطاعين العام والخاص، ولا سيما بغرض التصدي للتحديات التي تطرحها المواد الإجرامية الضارة على الإنترنت.

(15) تكون للشركات الخاصة، ولا سيما مقدمي خدمات الإنترنت، مسؤولية مشتركة في منع الجرائم السيبرانية والتحقيق فيها؛ وينبغي لهذه الشركات أن تعجل استجاباتها لطلبات المساعدة القانونية وأن توسع من نطاقها، وأن تقدمها في البلدان التي توجد فيها، وأن تضمن أن يكون لديها قنوات مناسبة للتواصل مع السلطات المحلية.

(16) يجب تعزيز الشراكات بين القطاعين العام والخاص؛ ويجب إنشاؤها حيثما لا توجد تلك الشراكات، وينبغي للشركات الخاصة أن تشارك في الأفرقة العاملة (المنتديات المتعددة الأطراف) وأن تكون جزءا من الحوار بشأن تعزيز النهج المتبع إزاء الجرائم السيبرانية.

(17) يجب أيضا أن تشكل المنظمات غير الحكومية والأوساط الأكاديمية جزءا من الجهود الرامية إلى منع الجريمة السيبرانية والتصدي لها، نظرا إلى أنها تقدم منظورا شاملا تعدديا يستوعب الجميع، لتحقيق عدة أهداف منها ضمان حماية حقوق الإنسان، ولا سيما حرية التعبير والحق في الخصوصية.

(18) تدعى البلدان إلى الانضمام إلى شبكات الممارسين المعتمدة والتوسع في استخدامها وتعزيزها بغرض حفظ الأدلة الإلكترونية المقبولة وتبادلها، ومنها الشبكات العاملة على مدار الساعة (7/24) والشبكات المتخصصة في مجال الجريمة السيبرانية وقنوات الإنتربول من أجل التعاون الفوري المباشر بين أجهزة الشرطة، وكذلك إلى بناء شبكات مع الشركاء المتوائمين استراتيجيا بهدف تبادل البيانات المتعلقة بمسائل الجريمة السيبرانية والتمكين من الاستجابة السريعة والتقليل إلى أدنى حد من فقدان الأدلة الدامغة. وأوصت التدخلات أيضا باستخدام التعاون المباشر بين أجهزة الشرطة وغير ذلك من أساليب التعاون غير الرسمي قبل استخدام قنوات المساعدة القانونية المتبادلة.

(19) تقوم كل دولة بإنشاء نقطة اتصال فعلية تعمل على مدار الساعة (7/24)، مصحوبة بتوفير موارد مناسبة لتيسير حفظ البيانات الرقمية إلى جانب المساعدة الدولية المتبادلة التقليدية في المسائل الجنائية، وذلك بالاعتماد على النموذج الناجح لتجميد البيانات في إطار اتفاقية مجلس أوروبا.

(20) ينبغي للبلدان أن تعزز التعاون فيما بين المؤسسات، وأن تحسن قابلية التشغيل المتبادل من خلال توحيد طلبات الحصول على المعلومات وإجراءات التوثيق، ومشاركة أصحاب المصلحة المتعددين.

(21) ينبغي للبلدان أن تحسن تنفيذ القوانين الوطنية وأن تعزز تحسين التنسيق والتآزر على الصعيد المحلي من أجل جمع المعلومات والأدلة وتبادلها لأغراض الملاحقة القضائية.

(22) ينبغي للدول أن تعزز تدابير تبادل المعلومات المالية أو النقدية، وتجميد الحسابات، ومصادرة الموجودات لضمان عدم تمتع المجرمين بفوائد الأنشطة الإجرامية.

(23) تشجع الدول على إنشاء أفرقة تحقيق مشتركة مع بلدان أخرى على المستوى الثنائي أو الإقليمي أو الدولي لتعزيز قدرات الإنفاذ.

(24) ينبغي للدول أيضا أن تتيح إمكانية التعامل الفعال مع الأدلة الإلكترونية ومقبولية تلك الأدلة أمام المحكمة، بما في ذلك عندما تكون مرسلة إلى ولاية قضائية أجنبية أو واردة منها. وفي هذا الصدد، تشجع

البلدان على مواصلة جهود الإصلاح في مجال التشريعات المتعلقة بالجريمة السيبرانية والأدلة الإلكترونية، أو الشروع في تلك الجهود، باتباع الأمثلة والإصلاحات الإيجابية من جميع أنحاء العالم.

(25) يوصى بوضع أطر قانونية تشمل أيضا جوانب تتعلق بالولاية القضائية خارج الحدود الإقليمية على الأفعال التي تعد جرائم حاسوبية.

(26) ينبغي للبلدان أن تنقح الآليات الخاصة بالتخفيف من حدة النزاعات، وأن تتصدى للتحديات المتعلقة بإسناد الفعل إلى الفاعل في قضايا الجرائم السيبرانية والقدرة على التحقيق فيها.

(27) ينبغي للدول أن تعمل على توحيد ونشر الأدوات الإجرائية للتعجيل بإنتاج البيانات وتوسيع نطاق عمليات التفتيش (مثل أوامر توفير البيانات، فضلا عن أوامر التعجيل في حفظها أو الوصول إليها عبر الحدود، إلخ.) وذلك لتيسير عمل سلطات إنفاذ القانون وتعاونها المباشر مع مقدمي خدمات الإنترنت وحل المشاكل المرتبطة بتتبع الأدلة الإلكترونية واستخدامها على النحو المناسب.

(28) ينبغي للدول أن تيسر وضع وتوحيد معايير تقنية قابلة للتشغيل المتبادل في مجال التحليل الجنائي الرقمي واسترجاع الأدلة الإلكترونية عبر الحدود.

(29) يوصى بالاستثمار في سلطة مركزية قوية للتعاون الدولي في المسائل الجنائية لضمان فعالية آليات التعاون التي تنطوي على جرائم سيبرانية أيضا؛ ويوصى بإنشاء وحدات خاصة للتحقيق في الجرائم السيبرانية؛ ويوصى كذلك بمعالجة طلبات الحفظ المقدمة من دولة أخرى من خلال شبكة عاملة على مدار الساعة (7/24) (أو مباشرة مع مقدم الخدمة في بعض الحالات) للحفاظ على البيانات اللازمة في أسرع وقت ممكن. وقد يساعد زيادة فهم المعلومات اللازمة لنجاح طلب المساعدة القانونية المتبادلة في الحصول على البيانات بسرعة أكبر.

(30) يتطلب التعاون الدولي الفعال وجود قوانين وطنية تستحدث إجراءات تمكن من التعاون الدولي. ومن ثم، يجب أن تسمح القوانين الوطنية بالتعاون الدولي بين أجهزة إنفاذ القانون.

(31) إلى جانب القوانين المحلية، يعتمد التعاون الدولي في مجال الجريمة السيبرانية على التعاون الرسمي القائم على المعاهدات وعلى المساعدة التقليدية المباشرة بين أجهزة الشرطة على حد سواء. وعند مناقشة صك جديد بشأن الجريمة السيبرانية، من المهم أن تتذكر البلدان أنه ينبغي للصك الجديد ألا يتعارض مع الصكوك القائمة، التي تمكن بالفعل من التعاون الدولي الآني. وبالتالي، ينبغي للبلدان أن تكفل أن يتفادى أي صك جديد بشأن الجريمة السيبرانية التضارب مع المعاهدات القائمة.

(32) ينبغي إعطاء أولوية لبناء القدرات المستدامة والمساعدة التقنية وزيادتها من أجل زيادة القدرات في جميع المجالات العملياتية وتعزيز قدرة السلطات الوطنية على التصدي للجريمة السيبرانية، بما يشمل بناء الشبكات وعقد الاجتماعات والتدريبات المشتركة، وتبادل أفضل الممارسات والمواد التدريبية ونماذج التعاون. وينبغي أن يشمل بناء القدرات والتدريب تدريبا شديد التخصص للممارسين، يشجع على وجه الخصوص على مشاركة الخبيرات، ويواصل الاستجابة لاحتياجات المشرعين وواضعي السياسات من أجل تحسين معالجة المسائل المتعلقة بالاحتفاظ بالبيانات لأغراض إنفاذ القانون؛ واحتياجات سلطات إنفاذ القانون والمحققين والمحللين من أجل تحسين قدراتهم في مجال التحليل الجنائي واستخدام البيانات المفتوحة المصدر في التحقيقات، وبشأن تسلسل العهدة فيما يتعلق بالأدلة الإلكترونية؛ وفيما يتعلق بجمع وتبادل الأدلة الإلكترونية في الخارج؛ واحتياجات القضاة وأعضاء النيابات العامة والسلطات المركزية والمحامين المتعلقة بالفصل في القضايا ذات الصلة والتعامل معها بفعالية.

(33) من الضـــروري وضـــع قواعد وأطر زمنية ملائمة للاحتفاظ بالبيانات/الحفاظ على البيانات، وإن أمكن توحيدها، لكفالة الحفاظ على الأدلة الإلكترونية أو الحصـــول عليها لدعم طلبات المســـاعدة القانونية المتبادلة الأخرى.

(34) تسلم مجموعة الـــ77 والصين بأن للتعاون الدولي أهمية في جمع وتبادل الأدلة الإلكترونية في سياق التحقيقات عبر الحدود، وبضرورة الاستجابة بسرعة وفعالية لطلبات المساعدة القانونية المتبادلة المتعلقة بحفظ الأدلة الإلكترونية والحصول عليها. وتشدد المجموعة أيضا على ضرورة احترام مبدأي السيادة والمعاملة بالمثل في هذه العملية.

(35) تشجع مجموعة الـ77 والصين المكتب المعني بالمخدرات والجريمة على مواصلة تقديم برامج بناء القدرات وبرامج التدريب في مجال مكافحة الجريمة السيبرانية إلى الخبراء الحكوميين الوطنيين من أجل تعزيز القدرات في مجال كشـــف الجرائم الســـيبرانية والتحقيق فيها. وينبغي لعملية بناء القدرات أن تســـعى بوجه خاص إلى تلبية احتياجات البلدان النامية، وأن تركز على أوجه ضعف كل بلد من أجل ضمان تقديم مساعدة تقنية مصممة حسب الحاجة، وأن تشجع على تبادل أحدث المعارف، خدمة لمصلحة الممارسين وأصحاب المصلحة.

(36) اســـتحدث المكتب المعني بالمخدرات والجريمة أداة كتابة طلبات المســـاعدة القانونية المتبادلة عنوانها Mutual Legal Assistance Request Writer Tool، من أجل مســـاعدة الممارســـين في مجال العدالة الجنائية على صـــياغة طلبات المســـاعدة القانونية المتبادلة. كما وضـــع أيضـــا دليلا عمليا لطلب الأدلة الإلكترونية عبر الحدود، عنوانه Practical Guide for Requesting Electronic Evidence Across Borders، وهو متاح عند الطلب للممارسـين الحكوميين في الدول الأعضـاء. ومن ثم، يمكن للبلدان أن تسـتفيد من استخدام هذه الأدوات الأساسية التي استحدثها المكتب.

(37) ينبغي أن تنظر لجنة منع الجريمة والعدالة الجنائية في توســـيع نطاق خطة عمل فريق الخبراء الحكومي الدولي إلى ما بعد عام 2021، باعتباره منتدى للممارسين لتبادل المعلومات بشأن الجريمة السيبرانية.

(38) أوصـــى بعض المتكلمين بأن التفاوض بشـــأن اتفاقية للأمم المتحدة لتعزيز التعاون في مكافحة الجريمة السيبرانية واعتمادها من شأنه أن ييسر تحسين كفاءة التعاون الدولي في مكافحة الجريمة السيبرانية.

(39) أوصـــي بأن يتولى خبراء المكتب المعني بالمخدرات والجريمة في فيينا تناول أي عملية صـــياغة لاتفاقية جديدة.

رابعا- تنظيم الاجتماع *(تابع)*

جيم- الكلمات

2- تكلم خبراء من الدول الأعضاء التالية ودولة غير عضو لها صفة المراقب: الجزائر، الأرجنتين، أرمينيا، البرازيل، كندا، شـــيلي، كولومبيا، إكوادور، مصـــر، الهند، لبنان، المكســـيك، هولندا، النرويج، البرتغال، رومانيا، الاتحاد الروسي، دولة فلسطين، دولة فلسطين نيابة عن مجموعة الـ77 والصين، الولايات المتحدة الأمريكية.