23 January 2013
Arabic
Original: English

فريق الخبراء المعني بإجراء دراسة شاملة
عن الجريمة السيبرانية
فيينا، ٢٥-٢٨ شباط/فبراير ٢٠١٣

دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتَّخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدِّي لها

خلاصة وافية

أولاً- مقدّمة

١- طلبت الجمعية العامة، في قرارها ٦٥/٢٣٠، إلى لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقاً للفقرة ٤٢ من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغيّر، فريقَ خبراء حكوميًّا دوليا مفتوح العضوية من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية وأفضل الممارسات والمساعدة التقنية والتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجرائم السيبرانية واقتراح تدابير جديدة في هذا الشأن.[1] وعلاوة على ذلك، أحاطت الجمعية العامة علماً مع التقدير، في قرارها ٦٧/١٨٩، بعمل فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية

(1) مرفق قرار الجمعية العامة ٦٥/٢٣٠.

وشجّعته على تحسين جهوده المبذولة من أجل إنجاز أعماله وعرض نتائج الدراسة في الوقت المناسب على لجنة منع الجريمة والعدالة الجنائية.

٢- وقد عُقدت الدورة الأولى لفريق الخبراء في فيينا في الفترة الممتدة من ١٧ إلى ٢١ كانون الثاني/يناير ٢٠١١، وقام خلالها الفريق باستعراض واعتماد مجموعة من المواضيع ومنهجية للدارسة.[٢] وتقرَّر في إطار منهجية الدراسة توزيع استبيان على الدول الأعضاء والمنظمات الحكومية الدولية وممثلين عن القطاع الخاص والمؤسسات الأكاديمية. وجمع مكتب الأمم المتحدة المعني بالمخدرات والجريمة المعلومات وفقاً للمنهجية المتَّفق عليها في الفترة الممتدة من شهر شباط/فبراير ٢٠١٢ إلى شهر تموز/يوليه ٢٠١٢.[٣] ويتضمن هذا التقرير خلاصة وافية لمشروع الدراسة الشاملة التي أعدّتها الأمانة استناداً إلى المعلومات المجموعة لينظر فيها فريق الخبراء الحكومي الدولي المعني بالجريمة السيبرانية في دورته الثانية.

ثانياً- الموصولية العالمية والجريمة السيبرانية

٣- في عام ٢٠١١، كان عدد الموصولين بالإنترنت لا يقل عن ٢,٣ بليون نسمة، أي ما يعادل أكثر من ثلث مجموع سكان العالم. ويعيش أكثر من ٦٠ في المائة من جميع مستخدمي الإنترنت في البلدان النامية، ولا يتجاوز عمر ٤٥ في المائة من مجموع مستخدمي الإنترنت الـ٢٥ عاماً. وبحلول عام ٢٠١٧، من المتوقع أن تناهز نسبة المشتركين في خدمة الإنترنت النقالة ذات النطاق العريض ٧٠ في المائة من مجموع سكان العالم. وبحلول عام ٢٠٢٠، سيفوق عدد الأجهزة المتصلة بالشبكة ("الأشياء المتصلة بالإنترنت") عدد الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت. ففي عالم الغد المتسم بالموصولية البالغة، سيصعب تصوُّر وقوع "جريمة حاسوبية" وربما أيِّ جريمة أخرى لا تنطوي على أدلة إلكترونية تتعلق بالموصولية بواسطة بروتوكول الإنترنت.

٤- وتتوقف "تعاريف" الجريمة السيبرانية، في المقام الأول، على الغرض من استخدام المصطلح. فالجرائم السيبرانية الأساسية تتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها. أمَّا الأعمال المنفّذة بواسطة الحواسيب

(2) E/CN.15/2011/19.

(3) استُلمت معلومات من ٦٩ دولة عضواً، فيما يلي توزُّعها الإقليمي: أفريقيا (١١) والقارة الأمريكية (١٣) وآسيا (١٩) وأوروبا (٢٤) وأوقيانوسيا (٢). واستُلمت المعلومات من ٤٠ منظّمة من القطاع الخاص و١٧ منظّمة أكاديمية و١١ منظمة حكومية دولية. واستعرضت الأمانة أيضاً أكثر من ٥٠٠ وثيقة من مصادر مفتوحة.

والرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار، بما في ذلك أشكال الجرائم المتصلة بالهوية وبمحتوى الحواسيب (والتي تندرج كلها ضمن نطاق أوسع من معنى "الجريمة السيبرانية")، فلا يمكن تطويعها بسهولة لتنضوي ضمن تعاريف قانونية لمصطلح جامع. ويلزم تعريف الأعمال الأساسية التي تشكِّل جريمة سيبرانية، وإن كان "تعريف" الجريمة السيبرانية لا يتسم بنفس القدر من الأهمية فيما يخص الأغراض الأخرى، كتحديد نطاق صلاحيات الهيئات المختصة بالتحريات والتعاون الدولي، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخص أيِّ جريمة، بدلاً من التركيز على تركيبة واسعة واصطناعية "للجريمة السيبرانية".

ثالثاً- الصورة العالمية للجريمة السيبرانية

٥- شهدت بلدان عديدة زيادة هائلة في الموصولية العالمية في وقت يتَّسم بتحولات اقتصادية وديمغرافية وبتزايد التفاوت في الدخل وتقييد الإنفاق في القطاع الخاص وانخفاض السيولة المالية. وعلى الصعيد العالمي، لاحظ موظّفو إنفاذ القانون المشاركون في الدراسة ارتفاع مستويات الجرائم السيبرانية، حيث يستغل الأفراد والجماعات الإجرامية المنظمة الفرص الجديدة المتاحة لارتكاب الجرائم بغية تحقيق الأرباح والمكاسب الشخصية. وتشير التقديرات إلى أنَّ مصدر أكثر من ٨٠ في المائة من الجرائم السيبرانية هو شكل من أشكال النشاط المنظم، حيث تقوم الأسواق السوداء للجرائم السيبرانية على دورة تتسم بإعداد البرامجيات الخبيثة والفيروسات الحاسوبية والتحكُّم بشبكات حاسوبية ("اعتداءات البوت نت") وتلقُّف البيانات الشخصية والمالية وبيع البيانات والمتاجرة بالمعلومات المالية. ولم يعد مرتكبو الجرائم السيبرانية بحاجة إلى مهارات أو تقنيات معقّدة. ففي البلدان النامية بصورة خاصة، ظهرت شبكات فرعية تضم شباناً يرتكبون أعمال احتيال مالي بالحواسيب، بدأ كثيرون منهم بالتورط في الجرائم السيبرانية في أواخر سنوات المراهقة.

٦- وعلى الصعيد العالمي، تشمل الجرائم السيبرانية طائفة واسعة من الجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوى الحاسوبي، فضلاً عن الأعمال التي تمس بسرية النظم الحاسوبية وسلامتها وقابلية النفاذ إليها. غير أنَّ تصوّرات الخطر والتهديد النسبيَّين تختلف بين الحكومات ومؤسسات القطاع الخاص. وفي الوقت الراهن، لا تمثّل إحصاءات الجرائم المسجّلة لدى الشرطة أساساً سليماً للمقارنات عبر الوطنية، على الرغم من أنَّ هذه الإحصاءات غالباً ما تكون مهمة لوضع السياسات على الصعيد الوطني. ويرى ثلثا البلدان أنَّ نظم إحصاءات الشرطة لديها غير كافية لتسجيل الجرائم السيبرانية. وترتبط معدّلات

الجرائم السيبرانية المسجّلة لدى الشرطة بمستويات التنمية القطرية وقدرة الشرطة المتخصصة أكثر من ارتباطها بمعدّلات الجرائم المرتكبة.

٧- وتمثّل استبيانات الإيذاء الإجرامي أساساً أسلم للمقارنة. وتُظهر هذه الاستبيانات أنَّ حالات التأذي الفردية من الجرائم السيبرانية هي أكثر بكثير من حالات التأذي من أشكال الجرائم "التقليدية". وتتراوح معدّلات التأذي من تزوير بطاقات الائتمان وانتحال الشخصية على الإنترنت والوقوع ضحية لمحاولات تصيُّد احتيالي ومحاولات اطلاع دون إذن على حسابات البريد الإلكتروني بين ١ و١٧ في المائة من نسبة السكان الذين يستخدمون الإنترنت في ٢١ بلداً في جميع أنحاء العالم، مقارنةً بمعدلات التأذّي من السطو والسلب وسرقة السيارات التقليدية التي تقل عن ٥ في المائة من نسبة السكان في هذه البلدان نفسها. وكانت معدلات الإيذاء بسبب الجرائم السيبرانية أعلى في البلدان التي تشهد مستويات نمو منخفضة، مما يُبرز الحاجة إلى تعزيز جهود منع الجرائم في هذه البلدان.

٨- وأبلغت مؤسسات القطاع الخاص في أوروبا عن معدلات تأذي مماثلة — تراوحت بين ٢ و١٦ في المائة — وكانت تتعلق بانتهاك البيانات بسبب الاقتحام أو التصيد الاحتيالي. والساحة التي تُستخدَم فيها هذه الأدوات المختارة لارتكاب الجرائم، مثل "اعتداءات البوت نت"، هي ساحة عالمية. فقد كان أكثر من مليون عنوان فريد من عناوين بروتوكول الإنترنت يعمل على الصعيد العالمي كخادوم "بوت نت" للتحكُّم في شبكات الحواسيب ومراقبتها في عام ٢٠١١. ومثّل محتوى الإنترنت أيضاً مصدر قلق كبير للحكومات، فمن المواد المُراد حذفها منه المواد الإباحية المتعلقة بالأطفال، والخطابات المفعمة بالكراهية، ومواد التشهير، وانتقاد الحكومات، الأمر الذي أثار شواغل متعلقة بقانون حقوق الإنسان في بعض الحالات. ويُقدَّر أنَّ حوالي ٢٤ في المائة من إجمالي حركة الإنترنت العالمية تنتهك حقوق المؤلف، إذ تشمل تنزيل كثير من المواد من مواقع تبادل الملفات بين النظراء من مستخدمي الإنترنت (P2P)، ولا سيّما في بلدان في أفريقيا وأمريكا الجنوبية وغرب آسيا وجنوبها.

رابعاً- التشريعات الخاصة بالجريمة السيبرانية

٩- تؤدي التدابير القانونية دوراً رئيسياً في منع ومكافحة الجريمة السيبرانية. وهذه التدابير ضرورية في جميع المجالات، بما في ذلك التجريم والصلاحيات الإجرائية والولاية القضائية والتعاون الدولي ومسؤولية مقدّمي خدمات الإنترنت. وعلى الصعيد الوطني، كثيراً ما تتعلق قوانين الجريمة السيبرانية، القائمة والجديدة (أو المخطط لها) على حدٍّ سواء، بالتجريم، مما يدّل على التركيز بصفة رئيسية على تجريم أفعال "متخصّصة" تغطي الجرائم السيبرانية الأساسية. غير أنَّ البلدان

تُسلِّم أكثر فأكثر بالحاجة إلى تشريعات في مجالات أخرى. ومقارنةً بالقوانين القائمة، تعالج القوانين الجديدة أو المخطط لها الخاصة بالجريمة السيبرانية إجراءات التحقيق والولاية القضائية والأدلّة الإلكترونية والتعاون الدولي. وعلى الصعيد العالمي، رأى أقلّ من نصف البلدان المجيبة عن الاستبيان أنَّ أطر القوانين الجنائية والإجرائية الخاصة بها كافية، وإن كانت تنطوي على تباينات إقليمية كبيرة. ففي حين أبلغ أكثر من ثلثي البلدان في أوروبا عن وجود تشريعات كافية، كانت الصورة معكوسة في أفريقيا والقارة الأمريكية وآسيا وأوقيانوسيا، حيث رأى أكثر من ثلثي البلدان أنَّ قوانينها كافية جزئياً فقط، أو غير كافية البتة. وأشار نصف البلدان التي أبلغت أنَّ قوانينها غير كافية أيضاً إلى قوانين جديدة أو مخطط لها، مما يسلّط الضوء على الحاجة الملحَّة إلى تعزيز التشريعات في هذه المناطق.

١٠- وشهد العقد الأخير تطورات مهمة على صعيد إصدار الصكوك الدولية والإقليمية الملزمة وغير الملزمة الرامية إلى التصدّي للجرائم السيبرانية. ويمكن تحديد خمس مجموعات من الصكوك، أُعدَّت في إطار هيئات أو استُقيت من هيئات هي: '١' مجلس أوروبا أو الاتحاد الأوروبي، و'٢' كومنولث الدول المستقلة أو منظمة شنغهاي للتعاون، و'٣' المنظمات الأفريقية الحكومية الدولية، و'٤' جامعة الدول العربية، و'٥' الأمم المتحدة. ويثري كل من هذه الصكوك الصكوك الأخرى إثراءً كبيراً، في مجالات منها على وجه الخصوص المفاهيم والنهج التي وُضعت في اتفاقية المجلس الأوروبي المتعلقة بالجريمة السيبرانية. ويظهر تحليل لمواد ١٩ صكاً متعدد الأطراف متصلاً بالجريمة السيبرانية وجود أحكام أساسية مشتركة من جهة، وتبايناً كبيراً في المجالات الموضوعية المتناولة من جهة أخرى.

١١- وعلى الصعيد العالمي، وقَّع أو صدَّق ٨٢ بلداً على صك ملزم بشأن الجريمة السيبرانية.[٤] ولهذه الصكوك المتعددة الأطراف المتعلقة بالجريمة السيبرانية تأثير مباشر يتمثل في العضوية فيها وتنفيذها رسمياً، وتأثير غير مباشر على القوانين الوطنية، من خلال استخدامها كنموذج من جانب الدول غير الأطراف فيها، أو من خلال تأثير تشريعات الدول الأطراف فيها على البلدان الأخرى. وتتناسب العضوية في الصكوك المتعددة الأطراف المتعلقة بالجريمة السيبرانية مع الزيادة المتصورة في مدى كفاية القانون الجنائي والإجرائي الوطني، مما يدل على أنَّ الأحكام الحالية المتعددة الأطراف في هذه المجالات تُعتبر فعّالة

(4) صك واحد أو أكثر من الصكوك التالية: اتفاقية المجلس الأوروبي المتعلقة بالجريمة السيبرانية، أو الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أو الاتفاقية المتعلقة بالتعاون بين بلدان كومنولث الدول المستقلة لمكافحة الجرائم في مجال المعلومات الحاسوبية، أو اتفاق منظمة شنغهاي للتعاون في ميدان أمن المعلومات على الصعيد الدولي.

عموماً. وفيما يخص البلدان التي يفوق عددها الأربعين والتي قدّمت المعلومات، كانت اتفاقية المجلس الأوروبي المتعلقة بالجريمة السيبرانية هي الصك المتعدد الأطراف الذي استندت إليه بصفة رئيسية لوضع التشريعات الخاصة بالجرائم السيبرانية. وإجمالاً، استخدم حوالي نصف هذه البلدان صكوكاً متعددة الأطراف مندرجة في "المجموعات" الأخرى.

١٢- وأفاد ثلث البلدان المجيبة عن الاستبيان عموماً بأنَّ تشريعاتها تتناسق إلى حد كبير، أو إلى حد كبير جداً، مع تشريعات البلدان التي تُعتبر علاقاتها بها مهمة لأغراض التعاون الدولي. غير أنَّ الوضع يتباين على الصعيد الإقليمي، إذ ترتفع مستويات التنسيق المبلّغ عنها في القارة الأمريكية وأوروبا. وقد يكون ذلك نتيجة لاستخدام بعض المناطق لصكوك متعددة الأطراف مصممة بطبيعتها لأداء دور في تنسيق التشريعات. وقد يعزى عدم الاتساق على المستوى الدولي وتنوّع القوانين الوطنية، من حيث تجريم الأعمال التي تعتبر جرائم سيبرانية والقواعد التي تحدّد الولاية القضائية وآليات التعاون، إلى وجود صكوك متعددة بشأن الجريمة السيبرانية لها نطاق موضوعي وجغرافي مختلف. والحال أنَّ التباين يعتري الصكوك والمناطق بسبب الاختلافات القانونية والدستورية فيها، بما في ذلك ما يسود فيها من مفاهيم مختلفة بشأن الحقوق والخصوصية.

خامساً- التجريم

١٣- جُمعت المعلومات بشأن القوانين الجنائية المتعلقة بالجرائم السيبرانية من خلال الاستبيان الخاص بالدراسة، ومن خلال تحليل المصادر الرئيسية للتشريعات المتوافرة التي جمعتها الأمانة.[٥] وأشار الاستبيان إلى ١٤ فعلاً يندرج عادةً ضمن مفاهيم الجرائم السيبرانية.[٦] وتبيَّن من إجابات البلدان على الاستبيان أنَّ هذه الأفعال الـ١٤ مجرَّمة على نطاق واسع، باستثناء الجرائم

(5) لقد حُلِّل المصدر الرئيسي لتشريعات ٩٧ دولة عضواً، بما في ذلك ٥٦ دولة أجابت عن الاستبيان، وكان توزعها الإقليمي على النحو التالي: أفريقيا (١٥) والقارة الأمريكية (٢٢) وآسيا (٢٤) وأوروبا (٣٠) وأوقيانوسيا (٦).

(6) النفاذ غير المشروع إلى نظام حاسوبي؛ والنفاذ غير المشروع إلى بيانات الحواسيب أو اعتراض هذه البيانات أو احتيازها؛ والتدخل غير المشروع في البيانات أو النظم؛ وإنتاج أو توزيع أو حيازة أدوات لإساءة استعمال الحواسيب؛ وانتهاك تدابير حماية الخصوصية أو البيانات؛ والاحتيال أو التزوير بواسطة الحواسيب؛ وجرائم الهوية المرتكبة بواسطة الحواسيب؛ وجرائم حقوق المؤلف والعلامات التجارية المرتكبة بواسطة الحواسيب؛ والأعمال المرتكبة بواسطة الحواسيب والتي تتسبب بضرر شخصي؛ والأعمال المرتكبة بواسطة الحواسيب والتي تنطوي على عنصرية أو كراهية للأجانب؛ وإنتاج أو توزيع أو حيازة المواد الإباحية المتعلقة بالأطفال بواسطة الحواسيب؛ وإغواء أو "مراودة" الأطفال بواسطة الحواسيب؛ وأعمال دعم الجرائم الإرهابية بواسطة الحواسيب.

المتعلقة بالرسائل الإلكترونية الاقتحامية بصفة رئيسية، وكذلك إلى حد ما الجرائم المتعلقة بأدوات إساءة استعمال الحواسيب والعنصرية وكراهية الأجانب وإغواء أو "مراودة" الأطفال على الإنترنت. ويجسِّد هذا الأمر نوعاً من توافق الآراء الأساسي على ما يُعاقب عليه من السلوكيات الإجرامية السيبرانية. وأبلغت بلدان عن بعض الجرائم الإضافية غير المذكورة في الاستبيان، والمتعلقة بصفة رئيسية بمحتوى الحواسيب، بما في ذلك تجريم المواد الفاحشة ولعب القمار على الإنترنت والأسواق غير المشروعة على الإنترنت من قبيل أسواق الاتجار بالمخدرات والبشر. وفيما يخص الأعمال الـ١٤ المذكورة، أبلغت بلدان بأنها تستند إلى الجرائم الخاصة بالفضاء السيبراني لتحديد الجرائم السيبرانية الأساسية التي تمس بسرية النظم الحاسوبية وسلامتها وقواعد النفاذ إليها. وفيما يخص الأشكال الأخرى من الجرائم السيبرانية، استُخدمت الجرائم العامة (غير السيبرانية) في أغلب الأحيان. غير أنه أُبلغ عن الأخذ بالنهجين فيما يخص الأفعال المرتكبة بواسطة الحواسيب والتي تشتمل على خرق السرية أو الاحتيال أو التزوير أو ارتكاب جرائم متصلة بالهوية.

١٤- ولئن كان هناك توافق رفيع المستوى في الآراء بشأن مجالات التجريم الواسعة، فإنَّ التحليل المفصّل للأحكام الواردة في التشريعات المرجعية يكشف عن نُهُج متباينة. ذلك أنَّ الجرائم التي تنطوي على نفاذ غير مشروع إلى النظم الحاسوبية والبيانات تختلف باختلاف موضوع الجريمة (بيانات أو نظم أو معلومات) ومستوى التجريم، أي تجريم النفاذ بحد ذاته أو اقتضاء وجود نية أخرى من وراء النفاذ مثل التسبُّب بخسائر أو أضرار. وتختلف النية المطلوب وجودها ليكون الفعل المرتكب جريمة باختلاف نهج تجريم التدخُّل في النظم الحاسوبية أو البيانات الحاسوبية. فمعظم البلدان تقضي بأن يكون التدخُّل في النظم أو البيانات متعمداً ليعتبر جريمة، في حين تجرِّم بلدان أخرى التدخُّل المستهتر فيها. وفيما يتعلق بالتدخُّل في البيانات الحاسوبية، يتراوح السلوك الذي يشكّل تدخلاً فيها بين إتلافها أو حذفها وصولاً إلى تغييرها أو قمعها أو إدخالها أو نقلها. ويختلف تجريم التدخُّل غير المشروع تبعاً لما إذا كان الجرم محصوراً بنقل البيانات غير العمومية، وما إذا كان محصوراً بالتدخُّل "بواسطة الوسائل التقنية". ولا تجرِّم جميع البلدان أدوات إساءة استعمال الحواسيب. أمَّا في البلدان التي تجرِّمها، فتبرز الاختلافات تبعاً لما إذا كان الجرم يشمل حيازة أو توزيع أو استعمال البرامجيات (كالبرامجيات الخبيثة) و/أو رموز النفاذ إلى الحواسيب (ككلمات سر الضحية). ومن منظور التعاون الدولي، قد يكون لهذه الاختلافات تأثير على الاستنتاجات المتعلقة بازدواجية التجريم بين البلدان.

١٥- واعتمدت بلدان عديدة مصطلح جرائم الفضاء السيبراني فيما يتعلق بجرائم الاحتيال والتزوير والجرائم المتصلة بالهوية المرتكبة بواسطة الحاسوب، في حين قامت بلدان أخرى بتوسيع نطاق الأحكام العامة المتعلقة بالاحتيال أو السرقة، أو اعتمدت على الجرائم التي تشمل العناصر المكونة ذات الصلة — كالنفاذ غير المشروع والتدخُّل في البيانات والتزوير، في حالة الجرائم المتعلقة بالهوية. وقد جُرِّم على نطاق واسع عدد من الجرائم المتصلة بالمحتوى، لا سيّما الجرائم المنطوية على مواد إباحية متعلقة بالأطفال. غير أنَّ الاختلافات تبرز بشأن تعريف مصطلح "الطفل"، والقيود المتعلقة بالمواد "البصرية" أو استبعاد المواد المحاكية، والأفعال المشمولة. وعلى الرغم من أنَّ الغالبية العظمى من البلدان تجرِّم، على سبيل المثال، إنتاج وتوزيع المواد الإباحية المتعلقة بالأطفال، يظهر تباين أكبر في تجريم حيازة هذه المواد والاطلاع عليها. وفيما يتعلق بانتهاك حقوق المؤلف والعلامات التجارية بواسطة الحواسيب، أبلغ أكثر البلدان عن تطبيق الجرائم الجنائية العامة على الأفعال المرتكبة عمداً وعلى نطاق تجاري.

١٦- ودفع الاستخدام المتزايد لوسائل التواصل الاجتماعي ومحتوى الإنترنت الذي ينتجه المستخدمون الحكومات إلى اتخاذ تدابير تنظيمية، ومن ذلك اللجوء إلى القانون الجنائي، والدعوة إلى احترام الحق في حرية التعبير. وأبلغت البلدان المجيبة عن الاستبيان عن قيود مختلفة على التعبير، ومن ذلك القيود المفروضة على التشهير والإهانة والتهديد والتحريض على الكراهية وإهانة المشاعر الدينية والمواد الفاحشة وتقويض الدولة. ويُجسَّد العنصر الاجتماعي والثقافي لبعض القيود ليس فقط في القانون الوطني وإنما أيضاً في الصكوك المتعددة الأطراف. فبعض الصكوك الإقليمية المتعلقة بالجريمة السيبرانية تشمل على سبيل المثال جرائم واسعة النطاق بشأن انتهاك الآداب العامة والمواد الإباحية والمبادئ أو القيم الدينية أو العائلية.

١٧- ويعمل القانون الدولي لحقوق الإنسان بمثابة سيف ودرع على حد سواء، إذ إنه يقضي بتجريم أشكال تعبير متطرفة (محدودة)، ويحمي أشكال تعبير أخرى. ومن ثم يتعيّن على الدول الأطراف في الصكوك الدولية لحقوق الإنسان فرض بعض القيود على حرية التعبير، بما في ذلك التحريض على الإبادة الجماعية والكراهية التي تشكّل تحريضاً على التمييز أو العداء أو العنف وتحريضاً على الإرهاب ودعايةً للحرب. ومن جهة أخرى، ثمة "هامش تقدير" يتيح للبلدان المجال لوضع حدود للتعبير المقبول بما يتماشى مع ثقافاتها وتقاليدها القانونية. ومع ذلك، يكون للقانون الدولي لحقوق الإنسان دور عند نقطة معينة. فتطبيق القوانين الجنائية المتعلقة بالتشهير وعدم احترام السلطة والإهانة مثلاً على التعبير على الإنترنت، سيواجه صعوبات كبيرة لإثبات تناسب التدابير وملاءمتها واتِّسامها بأقل قدر من التدخُّل. وعندما يكون المحتوى غير قانوني في بلد ما، ويكون إنتاجه ونشره قانونياً في بلد

آخر، سيتعين على الدول التركيز في تدابير العدالة الجنائية التي ستتخذها على الأشخاص الذين يطّلعون على المحتوى الذي يعدّ غير قانوني ضمن ولايتها القضائية الوطنية، بدلاً من التركيز على المحتوى المنتج خارج البلد.

سادساً- السلطات المعنية بإنفاذ القانون والتحقيقات

١٨- أشار أكثر من ٩٠ في المائة من البلدان المجيبة عن الاستبيان إلى أنَّ السلطات المسؤولة عن إنفاذ القانون تبلَّغ بمعظم الجرائم السيبرانية من خلال التقارير المقدّمة من الضحايا الأفراد أو الضحايا من الشركات. وقدَّرت البلدان المجيبة عن الاستبيان أنَّ نسبة التأذّي الفعلي من الجرائم السيبرانية المبلّغ عنها إلى الشرطة تبدأ من واحد في المائة. وتشير دراسة استقصائية عالمية للقطاع الخاص إلى أنَّ ٨٠ في المائة من الضحايا الأفراد للجرائم السيبرانية الأساسية لا يبلغون الشرطة عن الجريمة. ويعزى تدني الإبلاغ عن هذه الجرائم إلى عدم الوعي بالإيذاء وآليات الإبلاغ، وإلى شعور الضحايا بالخجل والارتباك، وإلى تخوُّف الشركات من الدعاية السلبية المتصورة التي قد تهدد سمعتها. وأشارت السلطات في جميع مناطق العالم إلى المبادرات الرامية إلى تعزيز الإبلاغ عن تلك الجرائم، بما في ذلك عن طريق نظم الإبلاغ بالاتصال الحاسوبي المباشر وبالخطوط الهاتفية المباشرة وحملات التوعية العامة والتواصل مع القطاع الخاص وتعزيز توعية الشرطة وتبادل المعلومات. غير أنَّ تدابير التصدِّي للجريمة السيبرانية التي تتخذ لمعالجة حوادث معينة يجب أن تقترن بتحقيقات تكتيكية على المدى المتوسط والبعيد، تركز على أسواق الجريمة ومدبري المخططات الإجرامية. وتشارك سلطات إنفاذ القانون في البلدان المتقدمة في هذا المجال، بما في ذلك من خلال الوحدات السرية التي تستهدف المجرمين على مواقع الشبكات الاجتماعية وغرف الدردشة والرسائل الفورية ومواقع تبادل الملفات بين النظراء (P2P). وتنشأ التحديات التي ينطوي عليها التحقيق في الجرائم السيبرانية عن الابتكارات الإجرامية والصعوبات في الحصول على الأدلة الإلكترونية والقيود على الموارد الداخلية والقدرات والقيود اللوجستية. وغالباً ما يلجأ المشتبه بهم إلى تقنيات إخفاء الهوية والتشويش، وتصل التقنيات الجديدة بسرعة إلى جمهور المجرمين الواسع من خلال أسواق الجرائم عبر الإنترنت.

١٩- وتتطلب التحقيقات التي تجريها سلطات إنفاذ القانون في الجرائم السيبرانية مزيجاً من تقنيات عمل الشرطة التقليدية والجديدة. فلئن أمكن تنفيذ بعض إجراءات التحقيق بواسطة التقنيات التقليدية، فإنه يصعب تكييف العديد من الإجراءات التي تستند إلى نهج قائم على مكان الأشياء لجعلها تستند إلى نهج قائم على تخزين البيانات الإلكترونية وتدفق البيانات في

الوقت الحقيقي. وأشار الاستبيان إلى عشرة إجراءات للتحقيق في الجرائم السيبرانية، بدءاً من البحث العام والمصادرة وصولاً إلى الإجراءات المتخصصة، كحفظ البيانات الحاسوبية.[٧] وفي حين أبلغت البلدان في أكثر الأحيان عن وجود صلاحيات عامة (غير خاصة بالمجال السيبراني) في كل مستويات التحريات، أبلغ عدد من البلدان أيضاً عن تشريعات خاصة بالمجال السيبراني، ولا سيما لضمان التعجيل في حفظ البيانات الحاسوبية والحصول على بيانات المشتركين المخزنة. وأبلغت بلدان عديدة عن عدم وجود صلاحيات قانونية لاتخاذ إجراءات متقدّمة، مثل التحاليل الجنائية الحاسوبية عن بُعد. وفي حين أنه يمكن توسيع نطاق الصلاحيات الإجرائية التقليدية لتشمل المجال السيبراني، فقد يؤدي هذا النهج في العديد من الحالات إلى أوجه عدم يقين قانوني وتحديات بشأن مشروعية جمع الأدلة، وبالتالي مقبوليتها. وعموماً، ثمة قواسم مشتركة أساسية في النُهج الوطنية لصلاحيات التحقيق في الجرائم السيبرانية أقل من القواسم المشتركة الأساسية في تجريم العديد من الجرائم السيبرانية.

٢٠- وبصرف النظر عن الشكل القانوني لصلاحيات التحقيق، تستخدم جميع السلطات المجيبة عن الاستبيان البحث والمصادرة للاستحواذ الفعلي على المعدات الحاسوبية والحصول على البيانات الحاسوبية. وتستخدم غالبية البلدان أيضاً أوامر قضائية للحصول على البيانات الحاسوبية المخزنة من مقدّمي خدمات الإنترنت. وخارج أوروبا، أبلغ حوالي ثلث البلدان عن تحديات في إقناع الأطراف الثالثة التي لها علاقة بالتحقيق بتقديم المعلومات. ويستخدم حوالي ثلاثة أرباع البلدان إجراءات تحقيق متخصصة، كجمع البيانات في الوقت الحقيقي أو التعجيل في حفظها. ويتطلب استخدام إجراءات التحقيق عادةً حدًّا أدنى من الأدلة الأولية أو تقريراً عن وقوع جريمة سيبرانية. أمَّا الإجراءات الأكثر تدخلاً، كتلك التي تشتمل على جمع البيانات في الوقت الحقيقي أو النفاذ إلى محتوى البيانات، فتستلزم معايير أكثر صرامة، كوجود دليل على ارتكاب جريمة خطيرة أو دليل على وجود سبب محتمل أو أسس معقولة.

٢١- ويُعدّ التفاعل بين سلطات إنفاذ القانون ومقدّمي خدمات الإنترنت معقّداً بصفة خاصة. ولدى مقدّمي الخدمات المعلومات الخاصة بالمشتركين والفواتير وبعض سجلات الاتصال ومعلومات عن المواقع (كبيانات أبراج الاتصالات اللاسلكية الخاصة بمقدّمي

(7) البحث عن المعدات أو البيانات الحاسوبية ومصادرتها؛ والأمر بالحصول على معلومات المشتركين؛ والأمر بالحصول على بيانات حركة الاتصالات المخزّنة؛ والأمر بالحصول على بيانات المحتوى المخزّنة؛ وجمع بيانات حركة الاتصالات في الوقت الحقيقي؛ وجمع بيانات المحتوى في الوقت الحقيقي؛ والتعجيل في حفظ البيانات الحاسوبية؛ واستخدام أدوات التحاليل الجنائية الحاسوبية عن بُعد؛ والنفاذ عبر الحدود إلى نظم أو بيانات حاسوبية.

خدمات الهواتف النقالة) ومحتوى الاتصالات، وقد تمثّل كل هذه العناصر أدلّة إلكترونية مهمة عن جريمة معيّنة. وتختلف المقتضيات القانونية الوطنية والسياسات المتّبعة في القطاع الخاص بشأن الاحتفاظ بالبيانات وإفشائها اختلافاً كبيراً حسب البلد والقطاع ونوع البيانات. وقد أبلغت البلدان في معظم الأحيان عن اللجوء إلى أوامر قضائية للحصول على أدلة من مقدّمي الخدمات. ولكن سلطات إنفاذ القانون قد تتمكّن في بعض الحالات من الحصول بصورة مباشرة على بيانات المشتركين المخزّنة وبيانات حركة الاتصالات وحتى بيانات المحتوى. وفي هذا الصدد، أبلغ كثير من مؤسسات القطاع الخاص عن أخذها بسياسة أولية تقتضي مراعاة الأصول القانونية للإفشاء عن البيانات، وكذلك بنهج طوعي يتمثل في الاستجابة في بعض الظروف للطلبات المباشرة التي تقدمها سلطات إنفاذ القانون. وتساعد العلاقات غير الرسمية بين سلطات إنفاذ القانون ومقدّمي الخدمات، والتي أُبلغ عن وجودها في أكثر من نصف مجموع البلدان المجيبة عن الاستبيان، في عملية تبادل المعلومات وبناء الثقة. وأشارت الردود إلى أنَّ هناك حاجة إلى تحقيق التوازن بين الخصوصية ومراعاة الأصول القانونية من جهة، وبين إفشاء الأدلة في الوقت المناسب من جهة أخرى لضمان عدم تحوُّل القطاع الخاص إلى "معرقل" للتحقيقات.

٢٢- وتنطوي التحقيقات في الجرائم السيبرانية دائماً على اعتبارات تتعلق بالخصوصية بموجب القانون الدولي لحقوق الإنسان. وتنصّ معايير حقوق الإنسان على أنَّ القوانين يجب أن تكون واضحة بما فيه الكفاية لتعطي دلالة كافية عن الظروف التي تخوِّل للسلطات استخدام إجراءات التحقيق، وأنَّه يجب أن تكون هناك ضمانات وافية وفعالة لمكافحة إساءة استخدام تلك الإجراءات. وأفادت بلدان بأنَّ قوانينها الوطنية تحمي حقوق الخصوصية، كما أبلغت عن مجموعة من القيود والضمانات في إطار التحقيقات. ولكن عندما تكون التحقيقات عبر وطنية، يستتبع تباين مستويات حماية الخصوصية عدم القدرة على التنبؤ بقدرات سلطات إنفاذ القانون الأجنبية على الحصول على البيانات، وبالثغرات التي قد تنطوي عليها نظم حماية الخصوصية في الولاية القضائية المعنية.

٢٣- وقد بدأ أكثر من ٩٠ في المائة من البلدان التي أجابت عن الاستبيان بإنشاء هياكل متخصصة للتحقيق في الجرائم السيبرانية والجرائم التي تنطوي على أدلّة إلكترونية. لكن هذه الهياكل تفتقر في البلدان النامية إلى ما يكفي من الموارد والقدرات. ولدى البلدان الأقل نمواً عدد أقل بكثير من أفراد الشرطة المتخصصين، بمعدل يبلغ نحو ٠,٢ لكل ١٠٠ ٠٠٠ مستخدم إنترنت ضمن البلد المعني، في حين يكون هذا المعدّل أعلى بمرتين إلى خمس مرات في البلدان التي تفوقها تقدماً. وأُفيد بأنَّ سبعين في المائة من الموظفين المتخصصين المكلفين

بإنفاذ القوانين في البلدان الأقل نمواً يفتقرون إلى المهارات والمعدات الحاسوبية، ولا يتلقى إلا نصفهم تدريباً أكثر من مرة واحدة في السنة. وأفاد أكثر من نصف البلدان المجيبة عن الاستبيان في أفريقيا وثلث البلدان في القارة الأمريكية بأنَّ الموارد المتاحة لسلطات إنفاذ القانون للتحقيق في الجرائم السيبرانية غير كافية. وعلى الصعيد العالمي، يرجّح أن تكون الصورة أسوأ. فلم يرد على الاستبيان على سبيل المثال إلا ٢٠ في المائة من البلدان الخمسين الأقل نمواً في العالم. وأفاد جميع البلدان المجيبة عن الاستبيان في أفريقيا وأكثر من ٨٠ في المائة من البلدان المجيبة في القارة الأمريكية وآسيا وأوقيانوسيا بأنها بحاجة إلى مساعدة تقنية. وكان المجال الذي كثر ذكره باعتباره يستلزم مساعدة تقنية هو أساليب التحرِّي العامة المتعلقة بالجرائم السيبرانية. وقد أشار ٦٠ في المائة من البلدان التي تحتاج إلى المساعدة إلى أنَّ وكالات إنفاذ القانون فيها بحاجة إلى هذا النوع من المساعدة.

سابعاً- الأدلة الإلكترونية والتدابير المتخذة في مجال العدالة الجنائية

٢٤- إنَّ الأدلة هي السبيل إلى تحديد الوقائع ذات الصلة بذنب أو براءة الفرد الجارية محاكمته. والأدلة الإلكترونية هي كل المواد الإثباتية التي توجد بشكل إلكتروني أو رقمي، والتي تكون مخزّنة أو عابرة، وقد تتخذ شكل ملفات حاسوبية أو مواد منقولة أو سجلات أو بيانات فوقية أو بيانات شبكية. وتهتم التحاليل الجنائية الرقمية باستعادة المعلومات – التي كثيراً ما تتسم بسرعة زوالها وسهولة المساس بها – والتي قد تكون قيّمة لأغراض الأدلة. وتتضمن تقنيات التحاليل الجنائية إنشاء نسخ "مطابقة تماماً" من المعلومات المخزنة والمحذوفة، واستخدام برامج "منع الكتابة" من أجل ضمان عدم تحريف المعلومات الأصلية، واستخدام خوارزميات "تجزئة" للملفات المشفّرة، أو استخدام التوقيعات الرقمية، بغية إظهار أي تعديلات تدخل على المعلومات. وأفاد معظم البلدان تقريباً بأنَّ لديها بعض القدرات في مجال التحاليل الجنائية الرقمية. غير أنَّ العديد من البلدان المجيبة عن الاستبيان، من جميع المناطق، أشار إلى عدم كفاية عدد المحققين المختصين في التحاليل الجنائية وإلى تباين القدرات على الصعيد الاتحادي وصعيد الولايات، وإلى الافتقار إلى أدوات التحليل الجنائي، وتراكم الأعمال غير المنجزة بسبب الكميات الهائلة من البيانات اللازم تحليلها. وأفاد نصف البلدان بأنَّ المشتبه بهم يلجأون إلى التشفير، مما يجعل الحصول على هذا النوع من الأدلة بدون رمز التشفير صعباً ويستغرق وقتاً طويلاً. وفي معظم البلدان، تقع مهمة تحليل الأدلة الإلكترونية على عاتق سلطات إنفاذ القانون. غير أنه يتعيّن على المدّعين العامين معاينة وفهم الأدلة الإلكترونية من أجل إقامة الحجة عند المحاكمة. وقد أفاد جميع البلدان في أفريقيا وثلث

البلدان في مناطق أخرى بعدم كفاية الموارد المتاحة للمدّعين العامين للقيام بذلك. وتكون لدى المدّعين العامين مهارات حاسوبية أقل مستوى عادة من المهارات الحاسوبية للمحققين. وعلى الصعيد العالمي، أفاد نحو ٦٥ في المائة من البلدان المجيبة عن الاستبيان بوجود نوع من التخصص في الجرائم السيبرانية لدى المدّعين العامين. ولم يبلغ سوى ١٠ في المائة من البلدان عن وجود دوائر قضائية متخصصة. ويتولّى النظر في الأغلبية العظمى من قضايا الجرائم السيبرانية قضاة غير متخصصين لا يتلقون في ٤٠ في المائة من البلدان المجيبة عن الاستبيان أي نوع من التدريب المتصل بالجرائم السيبرانية. ومن ثم، يعد تدريب القضاة في مجال قانون الجرائم السيبرانية وجمع الأدلة واكتساب المهارات الحاسوبية الأساسية والمتقدمة ذا أولوية خاصة.

٢٥- ولا يميّز أكثر من ٦٠ في المائة من البلدان المجيبة عن الاستبيان تمييزاً قانونياً بين الأدلة الإلكترونية والأدلة المادية. ولئن كانت النُهج المتبعة مختلفة، فإنَّ بلداناً عديدة تعتبر هذه الممارسة جيدة، لأنها تضمن مقبولية الأدلة الإلكترونية على قدم المساواة مع جميع الأنواع الأخرى من الأدلة. ولا يعترف عدد من البلدان خارج أوروبا بالأدلة الإلكترونية على الإطلاق، مما يجعل الملاحقة القضائية لمرتكبي الجرائم السيبرانية وسائر الجرائم المثبتة بواسطة المعلومات الإلكترونية غير مجدية. وليس لدى بعض البلدان عموماً قواعد إثبات منفصلة خاصة بالأدلة الإلكترونية، لكن عدداً من البلدان أشار إلى مبادئ منها القواعد المتعلقة بأفضل دليل وبمدى وجاهة الأدلة وبعدم قبول الإشاعات وبموثوقية الأدلة وسلامتها، وهي مبادئ قد تنطبق جميعها بشكل خاص على الأدلة الإلكترونية. وسلّطت بلدان عديدة الضوء على التحديات التي تقوم في إسناد الأعمال إلى الشخص المعين الذي يرتكبها، وعلّقت بأنَّ هذا الأمر غالباً ما يتوقّف على الأدلة الظرفية.

٢٦- وتدل التحديات التي تواجه المحققين والمدّعين العامين المكلفين بإنفاذ القانون على أنَّ معدّلات "التقديم للعدالة" أدنى بالنسبة لمرتكبي الجرائم السيبرانية. ولوحظ أنَّ عدد المشتبه بارتكابهم جرائم مسجّلة لدى الشرطة في قضايا المواد الإباحية المتعلقة بالأطفال قابل للمقارنة بعدد المشتبه بارتكابهم جرائم جنسية أخرى. ولكنَّ عدد المشتبه بارتكابهم جرائم مسجّلة لدى الشرطة متعلقة بالنفاذ غير المشروع والاحتيال أو التزوير بواسطة الحواسيب لا يتجاوز ٢٥ لكل ١٠٠ جريمة. ولم يتمكّن إلا عدد قليل جداً من البلدان من توفير البيانات بشأن الأشخاص الذين تمت مقاضاتهم أو إدانتهم. لكن إحصاءات الجرائم السيبرانية في بلد واحد أظهرت أنَّ نسبة الأشخاص الذين أُدينوا بارتكاب الجرائم السيبرانية المسجّلة أقل بكثير من نسبة الأشخاص المدانين بارتكاب سائر الجرائم التقليدية.

ثامناً- التعاون الدولي

٢٧- أفادت البلدان التي أجابت عن الاستبيان بأنَّ ٣٠ إلى ٧٠ في المائة من الجرائم السيبرانية تشتمل على بعد عبر وطني، وتنطوي من ثم على مسائل متعلقة بالتحقيقات عبر الوطنية والسيادة والولاية القضائية والأدلة الواقعة خارج نطاق الولاية القضائية ومتطلبات التعاون الدولي. وينشأ البعد عبر الوطني للجريمة السيبرانية عندما يكون للجريمة المعنية عنصر أو أثر مهم في إقليم آخر، أو عندما يكون أحد جوانب تنفيذ الجريمة قد تم في إقليم آخر. وينصّ القانون الدولي على عدد من الأسس المتعلقة بالولاية القضائية بشأن الأفعال المعنية، بما في ذلك أشكال الولايات القضائية المستندة إلى الإقليم والمستندة إلى الجنسية. وتوجد بعض هذه الأسس أيضاً في الصكوك المتعددة الأطراف المتعلقة بالجرائم السيبرانية. وفي حين ترى كل البلدان الأوروبية أنَّ قوانينها الوطنية توفّر إطاراً كافياً لتجريم الأفعال التي تندرج في عداد الجرائم السيبرانية والمرتكبة خارج نطاق الولاية القضائية ولملاحقة مرتكبيها قضائياً، فقد أبلغ نحو ثلث إلى أكثر من نصف البلدان في مناطق أخرى من العالم عن عدم كفاية الأطر القائمة في هذا المجال. وفي بلدان عديدة، تجسد الأحكام فكرة أنَّه ليس من الضروري أن تقع "كل عناصر" الجريمة داخل البلد من أجل تأكيد ولايته القضائية الإقليمية. ويمكن تحديد الروابط الإقليمية بالإشارة إلى عناصر الفعل المعني أو آثاره، أو موقع النظم أو البيانات الحاسوبية المستخدمة في ارتكابه. وتجري عادةً تسوية تنازع الولايات القضائية من خلال المشاورات الرسمية وغير الرسمية بين البلدان. ولا تكشف إجابات البلدان حالياً عن أي حاجة إلى أشكال إضافية من الولاية القضائية على بعد "فضاء سيبراني" مفترض، فغالباً ما تكون أشكال الولاية القضائية المستندة إلى الإقليم والمستندة إلى الجنسية قادرة دائماً على ربط الجريمة السيبرانية المرتكبة ربطاً كافياً بدولة واحدة على الأقل.

٢٨- وتشمل أشكال التعاون الدولي تسليم المطلوبين وتبادل المساعدة القانونية والاعتراف المتبادل بالأحكام الأجنبية والتعاون غير الرسمي بين أجهزة الشرطة. ونظراً لطبيعة الأدلة الإلكترونية التي تتسم بسهولة زوالها وتغيّرها، يتطلّب التعاون الدولي في المسائل الجنائية المتعلقة بالجرائم السيبرانية اتخاذ الإجراءات في الوقت المناسب والتمكن من طلب تنفيذ إجراءات تحقيق متخصصة، مثل حفظ البيانات الحاسوبية. ويعد استخدام الأشكال التقليدية للتعاون الأسلوب الأكثر شيوعاً للحصول على الأدلة خارج نطاق الولاية الإقليمية في قضايا الجرائم السيبرانية، حيث أبلغ أكثر من ٧٠ في المائة من البلدان عن استخدام طلبات المساعدة القانونية المتبادلة الرسمية لهذا الغرض. وفي إطار هذا النوع من التعاون الرسمي، يستخدم حوالي ٦٠ في المائة من الطلبات الصكوك الثنائية باعتبارها الأساس القانوني للتعاون.

وتُستخدم الصكوك المتعددة الأطراف في ٢٠ في المائة من الحالات. وأُفيد بأنَّ الاستجابة للطلبات المعنية تستغرق أشهراً لكل من طلبات تسليم المطلوبين والمساعدة القانونية المتبادلة، وتطرح هذه الفترة الزمنية تحديات على صعيد جمع الأدلة الإلكترونية السريعة الزوال والتغيُّر. وأفاد ٦٠ في المائة من البلدان في أفريقيا والقارة الأمريكية وأوروبا و٢٠ في المائة من البلدان في آسيا وأوقيانوسيا عن وجود قنوات للطلبات العاجلة، غير أنَّ تأثيرها على زمن الاستجابة غير واضح. وأفاد ثلثا البلدان المجيبة تقريباً بأنَّ أساليب التعاون غير الرسمي ممكنة، لكن عدداً قليلاً من البلدان كان لديه سياسة لاستخدام مثل هذه الآليات. وتوفِّر المبادرات المتعلقة بالتعاون غير الرسمي وبتسهيله، كالشبكات العاملة على الدوام، إمكانيات مهمة لتسريع الاستجابة، لكنها غير مستخدمة بشكل كافٍ، إذ اقتصر استخدامها على نحو ثلاثة في المائة من العدد الإجمالي لقضايا الجرائم السيبرانية التي تناولتها سلطات إنفاذ القانون في مجموعة البلدان المبلغة.

٢٩- وقد صُمِّمت أساليب التعاون الرسمية وغير الرسمية لإدارة عملية موافقة الدولة على إجراء سلطات إنفاذ القانون الأجنبية تحقيقات تؤثّر على سيادتها. غير أنَّ المحققين يطلعون باطراد، عن علم أو غير علم، على بيانات تندرج خارج إطار الولاية القضائية لبلدهم خلال عملية جمع الأدلة، دون الحصول على موافقة الدولة التي تقع فيها البيانات فعلياً. وتحدث هذه الحالة، بصورة خاصة، بسبب تقنيات الحوسبة السحابية التي تنطوي على تخزين البيانات في مراكز بيانات متعددة في مواقع جغرافية مختلفة. ويصبح "موقع" البيانات، وإن أمكنت معرفته من الناحية التقنية، اصطناعياً أكثر فأكثر، إلى حد أنه كثيراً ما توجّه طلبات المساعدة القانونية المتبادلة التقليدية إلى البلد الذي يوجد فيه مقدّم الخدمات، بدلاً من البلد الذي يقع فيه مركز البيانات فعلياً. وقد تحصل سلطات إنفاذ القانون الأجنبية مباشرة على البيانات التي تتجاوز حدود ولايتها الإقليمية عندما يستخدم المحققون رابطاً مباشراً قائماً انطلاقاً من جهاز المشتبه به، أو عندما يستخدم المحققون وثائق تفويض قانونية بالحصول على البيانات. وقد يحصل المحققون المكلفون بإنفاذ القوانين، في بعض الأحيان، على البيانات من مقدمي الخدمات خارج الولاية الإقليمية من خلال تقديم طلب مباشر غير رسمي، على الرغم من أنّ مقدّمي الخدمات يطلبون عادةً مراعاة الأصول القانونية. ولكن هذه الحالات غير مشمولة على النحو المناسب في الأحكام القائمة بالنفاذ إلى البيانات "عبر الحدود"، المنصوص عليها في اتفاقية المجلس الأوروبي المتعلقة بالجريمة السيبرانية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك بسبب التركيز على "موافقة" الشخص الذي يتمتع بالسلطة القانونية لإفشاء البيانات، والمعرفة المفترضة لموقع البيانات وقت النفاذ إليها أو استلامها.

٣٠- وقد يفضي هذا الوضع على صعيد التعاون الدولي إلى ظهور مجموعات من البلدان لديها الصلاحيات والإجراءات اللازمة لتتعاون فيما بينها، في حين تبقى هذه الصلاحيات والإجراءات محصورة، بالنسبة لجميع البلدان الأخرى، بالوسائل "التقليدية" للتعاون الدولي التي لا تأخذ في الاعتبار خصوصيات الأدلة الإلكترونية والطابع العالمي للجرائم السيبرانية. وهذا هو الحال بصفة خاصة فيما يتعلق بالتعاون في إجراءات التحقيق. ويعني عدم وجود نهج مشترك، بما في ذلك في إطار الصكوك الحالية المتعددة الأطراف بشأن الجرائم السيبرانية، أنَّ طلبات اتخاذ الإجراءات، مثل الحفظ العاجل للبيانات خارج البلدان الملزَمة دولياً بضمان مثل هذه الخدمة وتوفيرها عند الطلب، قد لا تُنفّذ بسهولة. ومن شأن إدراج هذه الصلاحية في مشروع اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني أن يحقّق بعض التقدُّم في سدّ هذه الثغرة. أمَّا على الصعيد العالمي، فإنَّ التباين في نطاق الأحكام المتعلقة بالتعاون في الصكوك المتعددة الأطراف والثنائية، وعدم فرض أجل ملزم للاستجابة للطلبات، وعدم الاتفاق على إتاحة النفاذ المباشر إلى البيانات التي توجد خارج الولاية القضائية، وتعدُّد شبكات سلطات إنفاذ القانون غير الرسمية، والتباين في ضمانات التعاون، أمور تمثل تحديات كبيرة في وجه التعاون الدولي الفعال فيما يتعلق بالأدلة الإلكترونية في المسائل الجنائية.

تاسعاً- منع الجرائم السيبرانية

٣١- ينطوي "منع الجريمة" على استراتيجيات وتدابير تسعى إلى التقليل من احتمالات حدوث جرائم والحد من آثارها الضارة التي قد تلحق بالأفراد والمجتمع. وقد أفاد نحو ٤٠ في المائة من البلدان المجيبة عن الاستبيان بأنَّ لديها قانوناً وطنياً أو سياسة وطنية بشأن منع الجرائم السيبرانية. وهناك حالياً مبادرات قيد الإعداد في بلدان أخرى تبلغ نسبتها ٢٠ في المائة. وأبرزت البلدان أنَّ الممارسات الجيدة في مجال منع الجرائم السيبرانية تتضمن نشر التشريعات، والقيادة الفعّالة، وتنمية القدرات على صعيد العدالة الجنائية وإنفاذ القانون والتعليم والتوعية، وإنشاء قاعدة معرفية قوية، والتعاون بين الحكومة والمجتمعات المحلية والقطاع الخاص وعلى الصعيد الدولي. وأبلغ أكثر من نصف البلدان عن وجود استراتيجيات بشأن الجرائم السيبرانية. وفي حالات عديدة، أُدرجت الاستراتيجيات الخاصة بالجرائم السيبرانية بشكل وثيق ضمن استراتيجيات للأمن السيبراني. وتضمَّن حوالي ٧٠ في المائة من جميع الاستراتيجيات الوطنية المبلّغ عنها مكوّنات بشأن زيادة الوعي والتعاون الدولي والقدرات في مجال إنفاذ القانون. ولأغراض التنسيق، يُبلغ في أغلب الأحيان عن وكالات إنفاذ القانون والملاحقة القضائية باعتبارها مؤسسات رائدة معنية بالجرائم السيبرانية.

٣٢- وتظهر الدراسات الاستقصائية، بما في ذلك في البلدان النامية، أنّ معظم فرادى مستخدمي الإنترنت يتخذون حالياً الاحتياطات الأمنية الأساسية. وقد أشارت الحكومات وهيئات القطاع الخاص والمؤسسات الأكاديمية المجيبة عن الاستبيان إلى أهمية استمرار حملات زيادة الوعي العام، بما في ذلك حملات التوعية بالتهديدات الناشئة، والحملات التي تستهدف جمهوراً محدداً، كالأطفال. ويكون تعليم المستخدمين أكثر فعالية عندما يقترن بنظم تساعدهم على تحقيق أهدافهم بطريقة آمنة. فإذا كانت التكلفة التي يتكبدها المستخدم أعلى من المنفعة المباشرة التي يحصل عليها، لن يتشجّع الأفراد بشكل كبير على اتّباع الإجراءات الأمنية. وأفادت كيانات القطاع الخاص أيضاً بأنه يجب إدراج توعية المستخدمين والموظفين في نهج شامل للأمن. وتتضمن المبادئ الأساسية والممارسة السليمة المُشار إليها المساءلة عن العمل في مجال التوعية وعن سياسات وممارسات تدبُّر المخاطر والقيادة على مستوى مجالس الإدارة وتدريب الموظفين. وقد أجرى ثلثا المجيبين من القطاع الخاص تقييماً لمخاطر الجرائم السيبرانية، وأبلغ معظمهم عن استخدام تكنولوجيا الأمن السيبراني كالجدران النارية وحفظ الأدلة الرقمية واستبانة المحتوى وكشف التسلل والإشراف على النظم ومراقبتها. ولكن أُبديت شواغل لأنَّ الشركات الصغيرة والمتوسطة الحجم إمَّا لا تتخذ خطوات كافية لحماية النظم أو تتصور بشكل خاطئ أنها لن تُستهدف.

٣٣- وتؤدي الأطر التنظيمية دوراً مهماً في منع الجرائم السيبرانية فيما يتعلق بالقطاع الخاص عموماً وبمقدّمي الخدمات خصوصاً. وقد اعتمد حوالي نصف البلدان قوانين لحماية البيانات تحدِّد المتطلبات اللازمة لحماية البيانات الشخصية واستخدامها. وتتضمن بعض هذه القوانين متطلبات محدَّدة خاصة بمقدّمي خدمات الإنترنت وغيرهم من مقدّمي خدمات الاتصالات الإلكترونية. ولئن كانت قوانين حماية البيانات تتطلب حذف البيانات الشخصية عندما لا تعود لازمة، فقد وضع بعض البلدان استثناءات لأغراض التحقيقات الجنائية، تُلزِم مقدّمي خدمات الإنترنت بتخزين أنواع معينة من البيانات لفترة زمنية محدَّدة. ولدى العديد من الدول المتقدمة أيضاً قواعد تلزم المنظمات بإبلاغ الأفراد والجهات التنظيمية عن الانتهاكات المتعلقة بالبيانات. ويتحمّل مقدّمو خدمات الإنترنت عادةً مسؤولية محدودة باعتبارهم "مجرّد قنوات" لمرور البيانات. وتزداد هذه المسؤولية في حال قيامهم بتعديل المحتويات المنقولة وكونهم على علم، بصورة فعلية أو بنَّاءة، بنشاط غير قانوني؛ وتكون المسؤولية محدودة من جهة أخرى في حال مسارعتهم إلى اتخاذ الإجراءات اللازمة إثر إبلاغهم بنشاط غير قانوني. ولئن كانت تتوافر لمقدِّمي خدمات الإنترنت إمكانيات تقنية لفرز محتوى الإنترنت، فإنَّ فرض قيود على النفاذ إلى شبكة الإنترنت يتوقف على القدرة

على التوقع وينبغي أن يكون متناسباً مع مستوى التهديد، وهما شرطان واردان في القانون الدولي لحقوق الإنسان الذي يحمي حقوق التماس المعلومات وتلقيها ونقلها.

٣٤- وتتَّسم الشراكات بين القطاع العام والقطاع الخاص بأهمية أساسية لمنع الجرائم السيبرانية. وقد أفاد أكثر من نصف مجموع البلدان عن وجود هذه الشراكات. وتُقام هذه الشراكات على السواء بموجب اتفاقات غير رسمية وعلى أسس قانونية. وهيئات القطاع الخاص هي أكثر من يدخل في شراكات، تليها المؤسسات الأكاديمية، والمنظمات الدولية والإقليمية. وتُستخدم الشراكات غالباً من أجل تيسير تبادل المعلومات عن التهديدات والاتجاهات، وكذلك من أجل تنفيذ أنشطة وإجراءات وقائية في حالات محددة. وفي سياق بعض الشراكات بين القطاع العام والقطاع الخاص، أخذت كيانات القطاع الخاص بنهج استباقي للتحقيق في الجرائم السيبرانية واتخاذ إجراءات قانونية بشأنها. وتُكمّل هذه الإجراءات تلك التي تتخذها سلطات إنفاذ القانون ويمكن أن تساعد في تخفيف الضرر على الضحايا. وتؤدي المؤسسات الأكاديمية مجموعة متنوعة من الأدوار في منع الجرائم السيبرانية، من خلال أمور منها تثقيف المهنيين وتدريبهم ووضع القوانين والسياسات والعمل على تطوير المعايير والحلول التقنية. وتستضيف الجامعات الخبراء في مجال الجرائم السيبرانية وبعض الأفرقة المعنية بمواجهة الطوارئ الحاسوبية ومراكز البحوث المتخصصة، وتيسّر ما يضطلعون به من أعمال.

عاشراً- الاستنتاجات الرئيسية والخيارات

٣٥- فيما يلي الاستنتاجات الرئيسية للدراسة الشاملة عن الجريمة السيبرانية:

(أ) إنَّ عدم اتساق الإجراءات على الصعيد الدولي وتنوّع القوانين المحلية المتعلقة بالجرائم السيبرانية قد يعزيان إلى وجود صكوك متعددة ذات نطاق موضوعي وجغرافي مختلف. ولئن كانت الصكوك تجسِّد شرعياً الاختلافات الاجتماعية والثقافية والإقليمية القائمة، فإنَّ التباين في نطاق الصلاحيات الإجرائية والأحكام المتعلقة بالتعاون الدولي قد يفضي إلى نشوء "مجموعات" متعاونة من البلدان، مما لا يتناسب دائماً مع الطابع العالمي للجرائم السيبرانية؛

(ب) إنَّ الاعتماد على الوسائل التقليدية للتعاون الدولي الرسمي في مسائل الجرائم السيبرانية لا يكفي حالياً للاستجابة في الوقت المناسب لمقتضيات الحصول على أدلّة إلكترونية سريعة الزوال والتغيُّر. وبما أنَّ عدداً متزايداً من الجرائم يشتمل على أدلّة إلكترونية

توجد في أماكن جغرافية متعددة، سيشكّل ذلك مشكلة ليس فقط بشأن الجرائم السيبرانية، وإنما بشأن كل الجرائم عموماً؛

(ج) في عالم الحوسبة السحابية ومراكز البيانات، يجب إعادة تحديد مفهوم دور "موقع" الأدلة، لأهداف منها التوصُّل إلى توافق في الآراء بشأن المسائل المتعلقة بحصول سلطات إنفاذ القانون مباشرة على المعلومات الموجودة خارج نطاق ولايتها القضائية؛

(د) إنَّ تحليل الأطر القانونية الوطنية المتوافرة يشير إلى عدم كفاية التنسيق فيما يتعلق بالجرائم السيبرانية "الأساسية" وصلاحيات التحقيق ومقبولية الأدلة الإلكترونية. ويمثّل القانون الدولي لحقوق الإنسان مرجعاً خارجياً هاماً فيما يتعلق بمسائل التجريم والأحكام الإجرائية؛

(هـ) إنَّ سلطات إنفاذ القانون والمدّعين العامين والسلطات القضائية في البلدان النامية تحتاج إلى دعم ومساعدة تقنيين شاملين على نحو مستدام وعلى المدى البعيد من أجل التحقيق في الجرائم السيبرانية ومكافحتها؛

(و) إنَّ أنشطة منع الجرائم السيبرانية في جميع البلدان تتطلب تعزيز الشراكات بين القطاع العام والقطاع الخاص وإدماج الاستراتيجيات الخاصة بالجرائم السيبرانية ضمن منظور أوسع للأمن السيبراني، وذلك من خلال نهج كلي يشتمل على زيادة الوعي.

٣٦- وقد تتضمن الخيارات المتاحة لتعزيز التدابير القانونية واقتراح تدابير قانونية أو تدابير أخرى جديدة وطنية ودولية للتصدي للجرائم السيبرانية، واحداً أو أكثر مما يلي:

(أ) صوغ أحكام نموذجية دولية بشأن تجريم الأفعال الأساسية التي تمثل جرائم سيبرانية، بغية دعم الدول في القضاء على الملاذات الآمنة من خلال اعتماد عناصر مشتركة للجرائم:

'١' يمكن أن تبقي الأحكام على نهج الصكوك القائمة فيما يتعلق بالجرائم التي تمس بسرية النظم والبيانات الحاسوبية وسلامتها وحقوق النفاذ إليها؛

'٢' يمكن أن تشمل الأحكام أيضاً الجرائم "التقليدية" المرتكبة أو الميسّرة باستخدام النظم الحاسوبية، على أن يقتصر ذلك على الحالات التي تُعتبر فيها نهج التجريم القائمة غير كافية؛

'٣' يمكن أن تعالج الأحكام مجالات غير مشمولة في الصكوك القائمة، كتجريم الرسائل الإلكترونية الاقتحامية؛

‘٤’ يمكن وضع الأحكام على نحو ينسجم مع أحدث المعايير الدولية لحقوق الإنسان بشأن التجريم، بما في ذلك بصورة خاصة، الأحكام التعاهدية التي تحمي الحق في حرية التعبير؛

‘٥’ من شأن استخدام الدول للأحكام أن يقلل إلى أدنى حد التحديات التي تطرحها مشكلة ازدواجية التجريم في التعاون الدولي؛

(ب) صوغ أحكام نموذجية دولية بشأن صلاحيات التحقيق الخاصة بالأدلّة الإلكترونية، بغية دعم الدول في ضمان وجود الأدوات الإجرائية الضرورية للتحقيق في الجرائم التي تشتمل على أدلّة إلكترونية:

‘١’ يمكن أن ترتكز الأحكام على النهج المعتمد في الصكوك القائمة، بما في ذلك أوامر الحفظ العاجل للبيانات وأوامر الحصول على البيانات المخزّنة والآنية؛

‘٢’ يمكن أن توفّر الأحكام إرشادات بشأن توسيع نطاق الصلاحيات التقليدية، مثل التحري بشأن الأدلّة الإلكترونية ومصادرها؛

‘٣’ يمكن أن توفّر الأحكام إرشادات بشأن تطبيق الضمانات المناسبة فيما يخص تقنيات التحقيق التدخلية، مع مراعاة القانون الدولي لحقوق الإنسان، بما في ذلك الأحكام التعاهدية التي تحمي الحق في الخصوصية؛

(ج) صوغ أحكام نموذجية بشأن الولاية القضائية، من أجل توفير أسس فعّالة مشتركة للولاية القضائية في المسائل الجنائية الخاصة بالجرائم السيبرانية:

‘١’ يمكن أن تتضمن الأحكام أسساً كتلك المستمدة من مبدأ الإقليمية الموضوعية ومبدأ الآثار الجوهرية؛

‘٢’ يمكن أن تتضمن الأحكام إرشادات لمعالجة المسائل المتعلقة بالولاية القضائية المشتركة؛

(د) صوغ أحكام نموذجية بشأن التعاون الدولي فيما يتعلق بالأدلّة الإلكترونية، بغية إدراجها في الصكوك الثنائية أو المتعددة الأطراف، بما في ذلك إعداد معاهدة نموذجية منقّحة للأمم المتحدة بشأن المساعدة القانونية المتبادلة، وفقاً للاقتراحات الواردة في دليل المناقشة الخاص بالمؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية:

‘١’ يمكن أن تركّز الأحكام على آليات التعاون العملي التي يمكن إدراجها في الصكوك القائمة من أجل حفظ الأدلّة الإلكترونية في الوقت المناسب وتقديم الأدلّة الإلكترونية في المسائل الجنائية؛

‘٢’ يمكن أن تتضمن الأحكام مقتضيات لتحديد جهات اتصال سريعة الاستجابة فيما يخص الأدلّة الإلكترونية وجداول زمنية متَّفق عليها للاستجابة للطلبات؛

(هـ) صوغ صك متعدد الأطراف بشأن التعاون الدولي فيما يتعلق بالأدلّة الإلكترونية في المسائل الجنائية، بغية توفير آلية دولية للتعاون الجيد التوقيت بغية حفظ الأدلّة الإلكترونية والحصول عليها:

‘١’ يمكن أن يُضاف الصك باعتباره مكمّلاً لمعاهدات التعاون الدولي القائمة، وأن يركّز بشكل أساسي على آلية لطلب الحفظ العاجل للبيانات لفترة زمنية محدَّدة؛

‘٢’ يمكن أن يتضمن الصك أيضاً أحكاماً محدَّدة بشأن التعاون في تنفيذ تدابير تحقيق إضافية، بما في ذلك توفير البيانات المخزّنة وجمع البيانات الآنية؛

‘٣’ يلزم تحديد نطاق تطبيق الصك، غير أنه يجب ألا يقتصر على "الجرائم السيبرانية" أو الجرائم "المتصلة بالحواسيب"؛

‘٤’ يمكن أن يقضي الصك بالاستجابة للطلبات في غضون فترة زمنية محدَّدة، وأن يحدِّد جهة اتصال واضحة لأغراض قنوات تنسيق الاتصالات، انطلاقاً من الآليات القائمة العاملة على مدار الساعة، بدلاً من إنشاء آليات جديدة تفضي إلى ازدواجية الجهود؛

‘٥’ يمكن أن يتضمن الصك ضمانات تعاون دولي تقليدية، واستثناءات مناسبة فيما يتعلق بحقوق الإنسان؛

(و) صوغ صك شامل متعدد الأطراف بشأن الجرائم السيبرانية، يصنع معالم نهج دولي في مجالات التجريم والصلاحيات الإجرائية والولاية القضائية والتعاون الدولي:

‘١’ يمكن أن يتضمن الصك عناصر من جميع الخيارات المُشار إليها أعلاه في شكل ملزم ومتعدد الأطراف؛

‘٢’ يمكن أن يستند الصك إلى القواسم المشتركة الأساسية القائمة في المجموعة الحالية للصكوك الدولية والإقليمية الملزمة وغير الملزمة؛

(ز) تعزيز الشراكات الدولية والإقليمية والوطنية، بما في ذلك الشراكات مع القطاع الخاص والمؤسسات الأكاديمية، من أجل توفير مساعدة تقنية معزّزة لمنع الجرائم السيبرانية ومكافحتها في البلدان النامية:

‘١’ يمكن توفير المساعدة التقنية بالاستناد إلى معايير توضع من خلال أحكام نموذجية على النحو المبيَّن في الخيارات المُشار إليها أعلاه؛

‘٢’ يمكن توفير المساعدة التقنية من خلال أصحاب مصالح متعددين، بما يشمل ممثلين من القطاع الخاص والمؤسسات الأكاديمية.