الأمم المتحدة A/AC.291/9/Add.3

الجمعية العامة

Distr.: General
16 May 2022
Arabic
Original: English

اللجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية

الدورة الثانية

فيينا، 30 أيار/مايو – 10 حزيران/يونيه 2022

تجميع للمقترحات والمساهمات المقدمة من الدول الأعضاء بشأن الأحكام المتعلقة بالتجريم والأحكام العامة والأحكام المتعلقة بالتدابير الإجرائية وإنفاذ القانون لاتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية

إضافة

المحتويات

الصفحة

250522 250522 V.22-03009 (A)

خامسا- مساهمات إضافية

مقدمة

تتضمن هذه الإضافة مساهمات مقدمة من الدول الأعضاء من أجل الدورة الثانية للجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية وردت بعد 14 نيسان/أبريل 2022؛ وهي غير مرتبة في فصول مواضيعية.

الهند

[الأصل: بالإنكليزية]
[12 أيار/مايو 2022]

معلومات أساسية

1- يتسم الفضاء السيبراني، باعتباره بيئة معقدة من الأشخاص والبرمجيات والأجهزة والخدمات على الإنترنت، بخصائص متميزة وفريدة مقارنةً بالفضاء المادي. ذلك أن الفضاء السيبراني افتراضي، وبلا حدود، ويتيح حجب الهوية. وفي السنوات الأخيرة، برزت وسائل التواصل الاجتماعي وبيئة الاتصالات الجوالة (أو ما يعرف بالنظام البيئي الجوال (mobile ecosystem)) ضمن قنوات الاتصال العامة المهمة. وفي الآونة الأخيرة، بات العالم يشهد في مختلف أرجائه استعمال العناصر الإجرامية والمعادية للأوطان وسائل التواصل الاجتماعي كأداة رئيسية لارتكاب الجرائم السيبرانية. ومن خلال فضاء سيبراني بلا حدود، إلى جانب إمكانية الاتصال الفوري وحجب الهوية، فإن احتمال ارتكاب الجرائم السيبرانية من خلال استخدام وسائل التواصل الاجتماعي والإنترنت بات أكبر من أي وقت مضى في البلد، كما هو الحال في أي مكان آخر في العالم.

2- كما أصبحت الجريمة السيبرانية قضية رئيسية في وقت يتسم بزيادة هائلة في استخدام الأجهزة القائمة على تكنولوجيا المعلومات والاتصالات على الصعيد العالمي. وقد جعل تقدم التكنولوجيا الإنسان يعتمد على تكنولوجيات المعلومات والاتصالات في جميع احتياجاته. وعلى عكس الجريمة التقليدية، فإن الجريمة السيبرانية ليس لها حدود جغرافية، كما أن مجرمي الإنترنت غير معروفين، بل إنهم مجهولو الهوية، مما يؤثر على جميع أصحاب المصلحة في هذا الشأن، بمن فيهم المواطنون العاديون. ويركز القسم التالي على أنواع الجرائم السيبرانية التي تُرتكب على الصعيد العالمي.

تصنيف الجرائم المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات

3- الجريمة السيبرانية مصطلح واسع يُستخدم لتعريف النشاط الإجرامي الذي تكون فيه أجهزة الحاسوب أو الشبكات الحاسوبية أداة أو هدفا أو مكانا للنشاط الإجرامي، ويشمل كل شيء من التدمير الإلكتروني إلى الهجمات الرامية إلى الحرمان من الخدمة. وبصفة عامة، يمكن تصنيف الجريمة السيبرانية على أنها "جريمة ييسّر الفضاء السيبراني ارتكابها"[(1)] و"جريمة مرتكبة في الفضاء السيبراني[(2)]. وعلاوة على ذلك، يمكن أيضا

(1) مثل أعمال السرقة، والتحرش، واستغلال الأطفال، والغش، والاحتيال التي يمكن ارتكابها بدون حاسوب، ولكن يتيح الحاسوب ارتكابها في ظروف معينة.

(2) القرصنة، وبرمجيات الفدية، والهجمات الموزعة للحرمان من الخدمة (DDoS) والبرمجيات الخبيثة، ونشر الفيروسات، والإرهاب السيبراني.

تصنيفها من حيث الضحايا باعتبارها جرائم سيبرانية ضد الأشخاص، وجرائم سيبرانية ضد الممتلكات، وجرائم سيبرانية ضد الحكومات. ومع ذلك، قد يكون من الأفضل استخدام تعريف "الجرائم المرتكبة من خلال استخدام تكنولوجيات المعلومات والاتصالات" لأنه سيكون شاملا للتكنولوجيات الجديدة والمستجدة أيضا.

التجريم

4- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني تحت بند الجرائم الجنائية وغيره من بنود التجريم المشابهة. (القائمة الواردة أدناه إرشادية ويمكن إضافة المزيد من الجرائم التي تُرتكب باستخدام تكنولوجيات المعلومات والاتصالات).

4 (أ) إتلاف الحواسيب أو النظم الحاسوبية، وما إلى ذلك

تعتمد كل دولة طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني قيام أي شخص بالأفعال التالية بشأن أي حواسيب أو نظم أو شبكات حاسوبية دون إذن من المالك أو أي شخص آخر مسؤول عنها:

(أ) الدخول على حاسـوب أو نظام حاسـوبي أو شـبكة حاسـوبية أو مورد حاسـوبي، أو تأمين إمكانية ذلك الدخول؛

(ب) تنزيل أو نســخ أو اســتخراج أي بيانات أو قاعدة بيانات حاســوبية أو معلومات من ذلك الحاسوب أو النظام الحاسوبي أو الشبكة الحاسوبية، بما في ذلك المعلومات أو البيانات المحفوظة أو المخزَّنة في أي وسيط تخزين قابل للفك والتركيب؛

(ج) إدخال أي ملوثات أو فيروســات حاســوبية في أي حاســوب أو نظام حاســوبي أو شــبكة حاسوبية، أو التسبب في ذلك؛

(د) إتلاف أي حاسوب أو نظام حاسوبي أو شبكة حاسوبية أو بيانات أو قاعدة بيانات حاسوبية أو أي برامج أخرى موجودة في ذلك الحاسوب أو النظام الحاسوبي أو تلك الشبكة الحاسوبية، أو التسبب في ذلك؛

(هـ) تعطيل أي حاسوب أو نظام حاسوبي أو شبكة حاسوبية، أو التسبب في ذلك؛

(و) منع أي شــخص من الدخول على أي حواســيب أو نظم أو شــبكات حاســوبية مأذون له بدخولها أو التسبب في ذلك بأي وسيلة؛

(ز) تقديم المســاعدة لأي شــخص لتســهيل دخوله على حاســوب أو نظام حاســوبي أو شــبكة حاسوبية بما يخالف أحكام هذا القانون أو القواعد أو اللوائح الصادرة بموجبه؛

(ح) قيد الرسوم على الخدمات التي يستفيد منها شخص ما على حساب شخص آخر عن طريق العبث أو التلاعب بأي حاسوب أو نظام حاسوبي أو شبكة حاسوبية؛

(ط) تدمير أو حذف أو تحوير أي معلومات موجودة في مورد حاسوبي أو تقليل قيمتها أو فائدتها أو التأثير فيها على نحو ضار بأي وسيلة؛

(ي) ســرقة أو إخفاء أو تدمير أو تحوير أي شــفرة مصــدرية حاســوبية تُســتخدم من أجل مورد حاسوبي بقصد التسبب في ضرر، أو التسبب في قيام أي شخص بذلك.

4 (ب) عدم حماية البيانات

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني إهمال أي هيئة اعتبارية، تحوز أي بيانات أو معلومات شخصية حساسة في مورد حاسوبي تملكه أو تسيطر عليه أو تشغِّله أو تتعامل مع تلك البيانات أو المعلومات أو تعالجها، في تطبيق وتعهد ممارسات وإجراءات أمنية معقولة، مما يتسبب في خسارة غير مشروعة أو كسب غير مشروع لأي شخص.

4 (ج) العبث بالوثائق المصدرية الحاسوبية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني والمعاقبة عليها: قيام أي شخص، عن علم أو عمد، بإخفاء أو تدمير أو تحوير أي شفرة مصدرية حاسوبية تُستخدم في حاسوب أو برنامج حاسوبي أو نظام حاسوبي أو شبكة حاسوبية، أو التسبب عن علم أو عمد في قيام آخر بذلك، عندما يلزم القانون الساري في ذلك الوقت بالاحتفاظ بالشفرة المصدرية الحاسوبية أو تعهدها.

4 (د) إرسال رسائل مسيئة من خلال خدمة الاتصالات، وما إلى ذلك

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني قيام أي شخص بإرسال ما يلي بواسطة مورد حاسوبي أو جهاز اتصال:

(أ) أي معلومات مسيئة بشكل صارخ أو ذات طابع تهديدي؛ أو

(ب) أي معلومات يعرف أنها كاذبة لغرض التسبب في مضايقة أو إزعاج أو خطر أو عرقلة أو إهانة أو إصابة أو ترهيب إجرامي أو عداوة أو كراهية أو ضغينة، باستمرار عن طريق استخدام ذلك المورد الحاسوبي أو جهاز اتصال؛

(ج) أي بريد إلكتروني أو رسالة بريد إلكتروني بغرض التسبب في مضايقة أو إزعاج أو لخداع أو تضليل المرسل إليه أو المستلم حول منشأ تلك الرسائل.

4 (هـ) تلقي موارد حاسوبية أو أجهزة اتصال مسروقة بطريقة غير شريفة

كل من يتلقى أي مورد حاسوبي أو جهاز اتصال مسروق أو يحتفظ به على نحو غير شريف مع علمه أو وجود سبب لاعتقاده بأنه مسروق.

4 (و) سرقة الهوية (انتحال الشخصية)

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني استخدام أي شخص، على نحو احتيالي أو غير شريف، التوقيع الإلكتروني لشخص آخر أو كلمة المرور الخاصة به أو أي سمة فريدة أخرى من سمات تحديد هويته.

4 (ز) الغش بانتحال الشخصية عن طريق استخدام مورد حاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني قيام أي شخص بالغش بانتحال الشخصية عن طريق استخدام جهاز اتصال أو مورد حاسوبي.

4 (ح) انتهاك الخصوصية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني قيام أي شـخص، عمدا أو عن علم، بالتقاط صـورة لمنطقة خاصـة لأي شـخص أو بنشـرها أو بثها دون موافقته، في ظروف تنتهك خصوصية ذلك الشخص:

(أ) "البث" يعني إرسال صورة مرئية إلكترونيا بقصد أن يشاهدها شخص أو أشخاص؛

(ب) "الالتقاط"، فيما يتعلق بصـورة، يعني التصـوير الفيديوي أو الفوتوغرافي أو السـينمائي أو التسجيل بأي وسيلة؛

(ج) "المنطقة الخاصـة" تعني الأعضاء التناسلية العارية أو المكسوة بالملابس الداخلية أو منطقة العانة أو الأرداف أو الثدي الأنثوي:

(د) "النشر" يعني الاستنساخ في شكل مطبوع أو إلكتروني والإتاحة للجمهور؛

(هـ) "في ظروف تنتهك الخصـوصـية" يعني الظروف التي يمكن فيها للشـخص أن يتوقع بشـكل معقول ما يلي:

'1' إمكانية خلع الملابس في خلوة، دون القلق من التقاط صورة للمنطقة الخاصة؛ أو

'2' اسـتعصـاء رؤية الجمهور لأي جزء من المنطقة الخاصـة، بغض النظر عن وجود ذلك الشخص في مكان عام أو خاص.

4 (ط) الإرهاب السيبراني

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى كي تُجرَّم في قانونها الوطني الفعلين التاليين باعتبارهما جريمتين من جرائم الإرهاب السيبراني:

(أ) قيام أي شـخص، بقصـد تهديد وحدة الدولة أو سـلامتها أو أمنها أو سـيادتها أو بث الرعب في صفوف الناس أو أي شريحة من منهم، بالتسبب الفعلي أو المرجح، عن طريق:

'1' حرمان أي شخص من الدخول على مورد حاسوبي له حق الدخول عليه، أو التسبب في ذلك؛ أو

'2' محاولة اختراق مورد حاسـوبي أو الدخول عليه دون إذن أو تجاوز حدود الدخول المأذون به؛ أو

'3' إدخال أي ملوث حاسوبي أو التسبب في إدخاله،

في وفاة أو إصـابة أشـخاص أو في إتلاف أو تدمير ممتلكات أو تعطيل إمدادات أو خدمات أسـاسـية لحياة المجتمع مع علمه بأن من المرجح أن تتسبب أفعاله في إلحاق الضرر بتلك الإمدادات أو الخدمات أو تعطيلها أو التأثير السلبي في البنى التحتية الأساسية للمعلومات؛ أو

(ب) قيام أي شخص باختراق مورد حاسوبي أو النفاذ إليه، عن علم أو عن قصد، دون ترخيص أو بما يتجاوز حدود النفاذ المرخص به، والدخول من خلال هذا السـلوك على معلومات أو بيانات أو قاعدة بيانات حاسـوبية مقيد الاطلاع عليها لأسـباب تتعلق بأمن الدولة أو علاقاتها الخارجية؛ أو الدخول على أي معلومات أو بيانات أو قاعدة بيانات حاسـوبية مقيد الاطلاع عليها لأسـباب تدعو إلى الاعتقاد بأن الحصـول

على هذه المعلومات أو البيانات أو قواعد البيانات الحاسوبية على هذا النحو يمكن أو يرجح أن يُستخدم لإلحاق الضرر بالمصالح المتعلقة بسيادة الدولة وسلامتها، أو أمن الدولة أو علاقات الصداقة مع الدول الأجنبية، أو النظام العام، أو الآداب أو الأخلاق، أو لازدراء (أوامر) المحاكم، أو للتشهير أو التحريض على ارتكاب جريمة، أو لفائدة أي دولة أجنبية أو مجموعة من الأفراد أو لأغراض أخرى.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني ارتكاب هذين الفعلين أو التآمر على ارتكابهما على النحو المبين في الفقرة 1 (أ) و(ب).

4 (ي) نشر أو بث مواد فاحشة في شكل خطابات إلكترونية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني قيام أي شخص بنشر أو بث، أو بالتسبب في نشر أو بث، في شكل إلكتروني، أي مادة تدعو للفسق أو تثير الشهوات أو من شأنها إغواء وإفساد الأشخاص الذين يُحتمل أن يقرأوا أو يشاهدوا أو يسمعوا المحتوى الوارد أو المجسد فيها، مع مراعاة جميع الظروف ذات الصلة.

4 (ك) نشر أو بث مواد تتضمن فعلا جنسيا صريحا، وما إلى ذلك، في شكل إلكتروني

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني قيام أي شخص بنشر أو بث، أو بالتسبب في نشر أو بث، أي مادة تتضمن فعلا أو سلوكا جنسيا صريحا في شكل إلكتروني.

4 (ل) نشر أو بث مواد تصور الأطفال أثناء ممارسة فعل جنسي صريح، وما إلى ذلك، في شكل إلكتروني

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم في قانونها الوطني قيام أي شخص بالأفعال التالية:

(أ) نشر أو بث مواد في أي شكل إلكتروني تصور أطفالا منخرطين في فعل أو سلوك جنسي صريح، أو التسبب في ذلك؛

(ب) نشر نصوص أو صور رقمية أو جمع مواد تصور بأي شكل إلكتروني الأطفال بطريقة فاحشة أو غير لائقة أو جنسية صريحة أو التماس تلك المواد أو تصفحها أو تنزيلها أو الإعلان عنها أو ترويجها أو تبادلها أو توزيعها؛

(ج) تشجيع الأطفال على إقامة علاقة عبر الإنترنت مع طفل واحد أو أكثر من أجل ممارسة فعل جنسي صريح أو بطريقة قد تخدش حياء شخص بالغ حصيف أو إغراؤهم أو حثهم على ذلك عبر مورد حاسوبي؛

(د) تيسير الاعتداء على الأطفال عبر الإنترنت؛

(هـ) تسجيل اعتداء جنسي صريح على الأطفال يرتكبه الشخص هو نفسه أو آخرون بأي شكل إلكتروني؛

على ألا ينسحب هذا الحكم على أي كتاب أو كتيب أو ورقة أو نص مكتوب أو رسم أو لوحة فنية أو صورة في شكل إلكتروني في الحالتين التاليتين:

'1' أن يثبت أن نشر هذا العمل له ما يبرره باعتباره من أجل الصالح العام على أساس أنه يخدم مصلحة العلم أو الأدب أو الفن أو التعلم أو غير ذلك من المجالات ذات الاهتمام العام؛ أو

'2' أن يُحتفظ به أو يُستخدم لأغراض تراثية أو دينية حسنة النية.

ويحدد سن "الطفولة" وفقا للتشريعات الوطنية لتلك الدولة.

4 (م) الكشف عن المعلومات بالمخالفة لعقد قانوني

قيام أي شخص، بما في ذلك الوسطاء، يحصل من خلال تقديمه لخدمات بموجب شروط عقد قانوني على إمكانية الوصول إلى أي مواد تحتوي على معلومات شخصية عن شخص آخر، بكشف تلك المواد للغير دون موافقة الشخص المعني أو في انتهاك للعقد القانوني، بقصد التسبب في خسارة غير مشروعة أو مكاسب غير مشروعة أو مع علمه باحتمال التسبب في هذا، ما لم تنص الاتفاقية على خلاف ذلك.

5- الأفعال غير المشروعة الأخرى المرتكبة باستخدام تكنولوجيات المعلومات والاتصالات

دون الإخلال بأحكام (المادة المتعلقة بحماية السيادة)، تتفق الأطراف المتعاقدة فيما بينها على تحديد أي أفعال غير مشروعة أخرى تُرتكب باستخدام تكنولوجيات المعلومات والاتصالات لأغراض التعاون المقررة بموجب هذه الاتفاقية. (ينبغي أن يكون هناك حكم في هذه الاتفاقية بعنوان "الأفعال غير المشروعة الأخرى" بالنظر إلى التقدم المحرز في تكنولوجيات المعلومات والاتصالات). وإضافة إلى ذلك، يمكن من خلال هذه الاتفاقية توسيع نطاق الجرائم السيبرانية التالية في ضوء مناقشة التجريم الواردة ضمن الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدرات والجريمة عن الجرائم السيبرانية[3]:

- الوصول (الدخول) غير المشروع
- الاعتراض غير المشروع: الاعتراض بغير وجه حق، باستخدام وسائل تقنية، لعمليات إرسال غير عمومية لبيانات حاسوبية إلى نظام حاسوبي أو منه أو خلاله، بما في ذلك التدخل الكهرومغناطيسي غير المشروع
- أدوات إساءة استخدام الحاسوب
- جرائم الهوية
- الضرر الشخصي
- العنصرية وكره الأجانب
- جرائم دعم الإرهاب
- برمجيات الفدية

(3) المصدر: United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, draft of February 2013. p 22.

13- المصطلحات المستخدمة

(أ) "جهاز الاتصال" يعني الهواتف المحمولة أو وسائل المساعدة الرقمية الشخصية أو مزيج من كليهما أو أي جهاز آخر يُستخدم لإيصال أو إرسال أو بث أي نص أو فيديو أو صوت أو صورة؛

(ب) "الحاسوب" يعني أي جهاز أو نظام إلكتروني أو مغناطيسي أو بصري أو أي جهاز أو نظام عالي السرعة آخر لمعالجة البيانات يؤدي وظائف منطقية وحسابية ووظائف لحفظ الذاكرة عن طريق التلاعب بالنبضات الإلكترونية أو المغناطيسية أو البصرية، ويشمل جميع مرافق الإدخال أو الإخراج أو المعالجة أو التخزين أو البرمجيات الحاسوبية أو مرافق الاتصال المربوطة أو المتصلة بالحاسوب في نظام حاسوبي أو شبكة حاسوبية؛

(ج) "الشبكة الحاسوبية" تعني الربط البيني لحاسوب أو أكثر أو نظم حاسوبية أو جهاز اتصال من خلال:

'1' استعمال وسائط الاتصال السلكية أو باستخدام الموجات الدقيقة أو الخطوط الأرضية أو وسائط الاتصال السلكي أو اللاسلكي أو وسائط الاتصال الأخرى؛

'2' المحطات الطرفية أو مجمع يتكون من اثنين أو أكثر من أجهزة الحاسوب المترابطة أو جهاز اتصال سواء حوفظ على التوصيل البيني بشكل مستمر أم لا؛

(د) "مورد حاسوبي" يعني حاسوبا أو نظاما حاسوبيا أو شبكة حاسوبية أو بيانات أو قاعدة بيانات أو برمجيات حاسوبية؛

(هـ) "نظام حاسوبي" يعني جهازا أو مجموعة من الأجهزة، بما في ذلك أجهزة دعم الإدخال والإخراج، باستثناء الآلات الحاسبة غير القابلة للبرمجة والاستخدام بالاقتران بملفات خارجية، وتحتوي تلك الأجهزة على برامج حاسوبية وتعليمات إلكترونية وبيانات إدخال وإخراج، تؤدي وظائف منطقية وحسابية ووظائف لتخزين البيانات واسترجاعها والتحكم في الاتصالات وغيرها من الوظائف؛

(و) "الملوثات الحاسوبية" تعني أي مجموعة من التعليمات الحاسوبية المصممة من أجل

'1' تعديل البيانات أو البرامج الموجودة داخل حاسوب أو نظام حاسوبي أو شبكة حاسوبية أو تدميرها أو تسجيلها أو بثها؛ أو

'2' القيام بأي وسيلة بسلب التشغيل العادي للحاسوب أو النظام الحاسوبي أو الشبكة الحاسوبية؛

(ز) "قاعدة البيانات الحاسوبية" تعني تمثيلا لمعلومات أو معارف أو حقائق أو مفاهيم أو تعليمات نصية أو تصويرية أو صوتية أو مرئية معدة أو يجري إعدادها بطريقة تشكيلية أو أنتجها حاسوب أو نظام حاسوبي أو شبكة حاسوبية ويُقصد بها الاستخدام في حاسوب أو نظام حاسوبي أو شبكة حاسوبية؛

(ح) "الفيروس الحاسوبي" يعني أي تعليمات أو معلومات أو بيانات أو برامج حاسوبية تؤدي إلى تدمير مورد حاسوبي أو إتلافه أو إضعافه أو التأثير سلبا على أدائه أو ترتبط بمورد حاسوبي آخر وتعمل عند تشغيل برنامج أو بيانات أو تنفيذ تعليمات أو عندما يقع حدث آخر في ذلك المورد الحاسوبي؛

(ط) "الإتلاف" يعني تدمير أي مورد حاسوبي أو إجراء تحوير أو حذف أو إضافة أو تعديل أو إعادة ترتيب في بياناته بأي وسيلة؛

(ي) "الشفرة المصدرية الحاسوبية" تعني قائمة البرامج والأوامر الحاسوبية والتصميم والتخطيط وتحليل البرامج للمورد الحاسوبي بأي شكل من الأشكال؛

(ك) "الأمن السيبراني" يعني حماية المعلومات والمعدات والأجهزة والحواسيب والموارد الحاسوبية وأجهزة الاتصال والمعلومات المخزنة فيها من الوصول إليها أو استخدامها أو كشفها أو تعطيلها أو تعديلها أو تدميرها على نحو غير مصرح به؛

(ل) "البيانات" تعني تمثيلا لمعلومات أو معارف أو حقائق أو مفاهيم أو تعليمات معدة أو يجري إعدادها بطريقة تشكيلية بقصد معالجتها أو تجري معالجتها أو عولجت بالفعل في نظام حاسوبي أو شبكة أو سحابة حاسوبية، وقد تكون في أي شكل (بما في ذلك المطبوعات الحاسوبية، ووسائط التخزين المغناطيسية أو البصرية، والبطاقات المثقوبة، والأشرطة المثقوبة) أو تخزن داخليا في ذاكرة الحاسوب؛

(م) "المعلومات" تشمل البيانات والرسائل والنصوص والصور والأصوات والرموز والبرامج الحاسوبية والبرمجيات وقواعد البيانات والأفلام الدقيقة (الميكروفيلم) والبطاقات الدقيقة (الميكروفيشات) المنشأة بواسطة الحاسوب؛

(ن) "الهيئة (ذات الشخصية) الاعتبارية" تعني شركة من أي نوع تمارس أنشطة تجارية أو مهنية، بما يشمل الشركات الأحادية الملاك والشركات المتعددة المساهمين؛

(س) "الممارسات والإجراءات الأمنية المعقولة" تعني الممارسات والإجراءات الأمنية المصممة لحماية المعلومات من هذا القبيل من الوصول إليها أو إتلافها أو استخدامها أو تعديلها أو كشفها أو الإضرار بها، وتحدد في اتفاق مبرم بين الأطراف أو وفق قانون معمول به في ذلك الحين، وفي حالة عدم وجود مثل ذلك الاتفاق أو أي قانون من هذا القبيل، الممارسات والإجراءات الأمنية المعقولة، التي قد تحددها الدول الأطراف بالتشاور مع الهيئات أو الرابطات المهنية التي تراها مناسبة؛

(ع) "البيانات أو المعلومات الشخصية الحساسة" تعني المعلومات الشخصية من هذا القبيل التي قد تحددها الدول الأطراف بالتشاور مع الهيئات أو الرابطات المهنية التي تراها مناسبة؛

(ف) "البريد الإلكتروني" و"رسالة البريد الإلكتروني" يعنيان رسالة أو معلومات منشأة أو مرسلة أو مستلمة في حاسوب أو نظام حاسوبي أو مورد حاسوبي أو جهاز اتصال، بما في ذلك المرفقات المرسلة في شكل نص أو صورة أو مقطع صوتي أو مرئي أو أي سجل إلكتروني آخر قد يشفع بالرسالة؛

(ص) "وسيط وسائل التواصل الاجتماعي" يعني وسيط يتيح بشكل أساسي أو حصري التفاعل عبر الإنترنت بين اثنين أو أكثر من المستخدمين ويسمح للمستخدمين بإنشاء معلومات أو تحميلها أو تبادلها أو نشرها أو تعديلها أو الوصول إليها باستخدام خدماته؛

(ق) "السجل الإلكتروني" يعني بيانات أو قيودا أو بيانات مولدَّة أو صورا أو أصوات مخزنة أو مستلمة أو مرسلة في أشكال إلكترونية أو أفلام أو بطاقات دقيقة يولدها حاسوب؛

(ر) "المنشئ" يعني الشخص الذي يرسل أي رسالة إلكترونية أو يولدها أو يخزنها أو يبثها أو يتسبب في ذلك إلى أي شخص آخر ولكنه لا يشمل الوسيط؛

(ش) "الممتلكات" تعني الأصول من أي نوع، سواء أكانت مادية أم غير مادية، منقولة أم غير منقولة، ملموسة أم غير ملموسة، بما في ذلك الأموال الموجودة في الحسابات المصرفية، والأصول المالية

الرقمية، والعملة الرقمية، بما في ذلك العملات المشـــفرة والوثائق أو الصـــكوك القانونية التي تثبت ملكية تلك الأصول أو أي جزء منها أو مصلحة فيها؛

(ت) "العائدات الإجرامية" تعني أي ممتلكات متأتية أو متحصـل عليها، بصـورة مباشـرة أو غير مباشرة، من خلال ارتكاب جرم أو فعل غير مشروع آخر منصوص عليه في هذه الاتفاقية؛

(ث) "المصـــادرة" تشـــمل، حســـب الاقتضـــاء، إســـقاط حق الملكية، وتعني الحرمان الدائم من الممتلكات بأمر صادر عن محكمة أو سلطة مختصة أخرى؛

(خ) "الجرم الأصـــلي" يعني أي جرم تأتت منه عائدات يمكن أن تصـــبح موضـــوع جرم حســـب التعريف الوارد هذه الاتفاقية؛

(ذ) "اســـتغلال الأطفال في المواد الإباحية" يعني تصـــوير أي طفل، بأي وســـيلة كانت، يمارس ممارسة حقيقية أو بالمحاكاة أنشطة جنسية صريحة أو أي تصوير للأعضاء الجنسية للطفل لأغراض جنسية أساسا.

14- الولاية القضائية المنصبة على البيانات

تعني الولاية القضائية المنصبة على البيانات أن البلد الذي تخزَّن بيانات مواطنيه أو تعالَج أو تُفحص أو تُحفظ مركزيا في أي مكان في العالم يجب أن تخضـــع لولاية قضـــائية أوســـع بغض النظر عن المكان الذي تُخزَّن فيه البيانات أو تعالَج أو تُفحص أو تُحفظ ماديا. وتضـــمن هذه الولاية القضـــائية المنصـــبة على البيانات أولوية ملكية البيانات ومسألة الخصوصية (حق أساسي معترف به للمواطن العالمي) وحقوق الإنسان.

(شـــرح موجز: في الوضـــع الحالي، لا تُعتبر الولاية القضـــائية بمفهومها التقليدي الحالي القائم على نموذج وستفاليا ناجعة في الفضـاء السـيبراني، خاصـة عندما تستخدم الموارد السـحابية التي تجعل من محاولة تحديد الولاية القضـائية كابوسـا مزعجا. ومن الأمثلة النموذجية على ذلك ارتكاب جريمة سـيبرانية تنطوي على صلاحية المعالجة في السحابة في بلد؛ وتجميع المعلومات المخزنة في بلد ثان؛ وتسجُّل مزود الخدمة السحابية في بلد ثالث، وإقامة المستخدم (الضحية والمهاجم) الذي يحتفظ مقدم الخدمة ببياناته في بلد رابع. ومن الواضح أنه في مثل هذه الحالة، من الصعب للغاية تحديد الولاية القضائية استنادا إلى النماذج الإقليمية التقليدية. وفي ضـــوء ما تقدم، تقترح الهند أن تعتمد الاتفاقية مفهوم الولاية القضـــائية المنصـــبة على البيانات بدلا من نموذج الولاية القضائية القائم على أساس إقليمي. وملكية البيانات المرتبطة بالخصوصية هي حق أساسي معترف به للمواطن العالمي. وقد أقرت بذلك محكمة العدل الأوروبية حيث اعترفت بحق الفرد في أن يُنسى. ويرتبط الحق في الخصـــوصـــية أيضـــا بالمســـائل المتعلقة بحقوق الإنســـان التي أثارها عدد كبير من البلدان في لجنة الأمم المتحدة المخصـصـة، وستساعد الولاية القضـائية المنصـبة على البيانات على حماية الحق في الخصـوصـية والحقوق الأساسية وحقوق الإنسان).

15- يمكن تعريف "الولاية القضائية" على النحو التالي:

1- تعتمد كل دولة طرف ما قد يلزم من تدابير لبسط ولايتها القضائية على الأفعال المجرَّمة بمقتضى هذه الاتفاقية في الحالتين التاليتين:

(أ) عندما يُرتكب الجرم في إقليم تلك الدولة الطرف أو تكون له به صلة ؛ أو

(ب) عندما يُرتكب الجرم على متن سفينة ترفع علم تلك الدولة الطرف أو طائرة مسجّلة بمقتضى قوانين تلك الدولة الطرف وقت ارتكاب الجرم.

2- رهنا بأحكام هذه الاتفاقية، يجوز للدولة الطرف أن تُخضِع أيضا أي جرم من هذا القبيل لولايتها القضائية في الحالات التالية:

(أ) أن يُرتكب الجرم ضد أحد مواطني تلك الدولة الطرف وضد أحد أشخاصها الاعتباريين؛ أو

(ب) أن يُرتكب الجرم بواسطة أحد مواطني تلك الدولة الطرف أو أحد أشخاصها الاعتباريين أو شخص عديم الجنسية أو شخص يوجد مكان إقامته المعتاد في إقليمها؛ أو

(ج) أن يُرتكب الجرم خارج إقليمها بهدف ارتكاب فعل مجرم وفقا لهذه الاتفاقية داخل إقليمها؛

(د) أن يُرتكب الجرم ضد الدولة الطرف؛ أو

(هـ) أن يستهدف الجرم موارد حاسوبية موجودة داخل إقليمها؛ أو

(و) أن يتعلق الجرم بالبيانات الرقمية/الإلكترونية لمواطنيها، بصرف النظر عن مكان تخزينها/تجهيزها/فحصها/حفظها المركزي".

3- لأغراض هذه الاتفاقية، تعتمد كل دولة طرف ما قد يلزم من تدابير لإخضاع الأفعال المجرَّمة وفقا لهذه الاتفاقية لولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه لمجرد كونه أحد مواطنيها.

4- يجوز لكل دولة طرف أيضا أن تعتمد ما قد يلزم من تدابير لإخضاع الأفعال المجرَّمة وفقا لهذه الاتفاقية لولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه.

5- إذا أُبلغت الدولة الطرف التي تمارس ولايتها القضائية بمقتضى الفقرة 1 أو 2 من هذه المادة، أو علمت بطريقة أخرى، أن أي دول أطراف أخرى تجري تحقيقا أو ملاحقة أو تتخذ إجراء قضائيا بشأن السلوك ذاته، وجب على السلطات المختصة في تلك الدول الأطراف أن تتشاور فيما بينها، حسب الاقتضاء، بهدف تنسيق ما تتخذه من إجراءات. ولأغراض التشاور بموجب هذه المادة، تأخذ الأطراف المتعاقدة في الاعتبار الولاية القضائية المنصبة على البيانات، أي البيانات التي تخص ضحية الجريمة السيبرانية أو الفعل غير المشروع المرتكب باستخدام تكنولوجيات المعلومات والاتصالات.

6- دون مساس بقواعد القانون الدولي العام، لا تحول هذه الاتفاقية دون ممارسة أي ولاية قضائية جنائية تؤكد الدولة الطرف سريانها وفقا لقانونها الوطني.

17- البحث عن المعلومات المخزنة أو المعالجة إلكترونيا وضبطها

1- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتخويل سلطاته المختصة صلاحية البحث فيما يلي أو الوصول إليه بطريقة مماثلة:

(أ) نظام حاسوبي أو جزء منه والبيانات الحاسوبية المخزنة فيه؛

(ب) وسيط تخزين بيانات حاسوبية يمكن أن تكون بيانات حاسوبية مخزنة فيه في إقليمها.

2- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان أنه في حالة قيام سلطاته بالبحث في نظام حاسوبي معين أو جزء منه أو الوصول إليه بطريقة مماثلة، عملا بالفقرة 1 (أ) وتوافر أسباب

لديها للاعتقاد بأن البيانات المطلوبة مخزنة في نظام حاسوبي آخر أو جزء منه في إقليمها، ويكون من الممكن الوصول إلى هذه البيانات من النظام الأول أو تكون متاحة له بشكل قانوني، تكون السلطات قادرة على توسيع نطاق البحث، أو نطاق الوصول بطريقة مماثلة، ليشمل النظام الآخر على وجه السرعة.

3- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من ضبط البيانات الحاسوبية التي يتم الوصول إليها وفقا للفقرتين 1 أو 2 أو تأمينها بطريقة مماثلة. وتشمل هذه التدابير الصلاحيات التالية:

(أ) ضبط نظام حاسوبي أو جزء منه أو وسيط تخزين بيانات حاسوبية أو تأمين ذلك النظام أو الوسيط بطريقة مماثلة؛

(ب) عمل نسخة من تلك البيانات الحاسوبية والاحتفاظ بها؛

(ج) حفظ/صون سلامة البيانات الحاسوبية

4- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من إصدار الأمر لأي شخص لديه معرفة بعمل النظام الحاسوبي أو التدابير المطبقة لحماية البيانات الحاسوبية الموجودة فيه بأن يقدم، بالقدر المعقول، المعلومات اللازمة للتمكين من اتخاذ التدابير المشار إليها في الفقرتين 1 و2.

18- جمع بيانات الحركة في الوقت الحقيقي

1- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتخويل سلطاته المختصة صلاحية:

(أ) أن تجمع أو تسجل في الوقت الحقيقي، باستخدام الوسائل التقنية في إقليمه، بيانات الحركة المرتبطة باتصالات محددة في ذلك الإقليم مرسلة عن طريق نظام حاسوبي؛

(ب) أن تجبر أي مقدم خدمة، في حدود قدراته التقنية القائمة، على:

'1' أن يجمع أو يسجل هذه البيانات في الوقت الحقيقي باستخدام الوسائل التقنية في إقليم ذلك الطرف؛ أو

'2' أن يتعاون مع السلطات المختصة ويساعدها في جمع أو تسجيل هذه البيانات في الوقت الحقيقي.

2- حيثما لا يستطيع طرف، بسبب المبادئ الراسخة لنظامه القانوني الوطني، أن يعتمد التدابير المشار إليها في الفقرة 1 (أ)، يجوز له بدلا من ذلك أن يعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان أن يتم في الوقت الحقيقي جمع أو تسجيل بيانات الحركة المرتبطة باتصالات محددة مرسلة في إقليمه، وذلك باستخدام الوسائل التقنية في ذلك الإقليم.

3- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي صلاحية منصوص عليها في هذه المادة وأي معلومات تتعلق بها.

19- جمع المحتوى والبيانات الوصفية

1- يعتمد كل طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لتوفير البيانات الوصـــفية على وجه الســـرعة دون الحاجة إلى معاهدات لتبادل المســـاعدة القانونية. ويوفر مقدم الخدمة، الذي لديه هذه البيانات الوصـفية، تلك المعلومات بناء على طلب مباشـر من أجهزة إنفاذ القانون من خلال جهة التنسـيق المركزية في كل دولة.

2- يعتمد كل طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لتوفير بيانات المحتوى على وجه السرعة. وستوضع آلية من أجل ذلك التبادل السريع للبيانات في إطار هذه الاتفاقية.

20- اعتراض بيانات المحتوى

1- يعتمد كل طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى، فيما يتعلق بمجموعة من الجرائم الخطيرة يحددها القانون الوطني، لتخويل سلطاته المختصة صلاحية:

(أ) أن تجمع أو تسـجل في الوقت الحقيقي، باسـتخدام الوسـائل التقنية في إقليمه، بيانات المحتوى المرتبطة باتصالات محددة في ذلك الإقليم مرسلة عن طريق نظام حاسوبي؛

(ب) أن تجبر أي مقدم خدمة، في حدود قدراته التقنية القائمة، على:

'1' أن يجمع أو يســـجل هذه البيانات في الوقت الحقيقي باســـتخدام الوســـائل التقنية في إقليم ذلك الطرف؛ أو

'2' أن يتعاون مع الســـلطات المختصـــة ويســـاعدها في جمع أو تســـجيل هذه البيانات في الوقت الحقيقي.

2- إذا تعذر على الطرف، بسبب المبادئ الراسخة لنظامه القانوني الوطني، الأخذ بالتدابير المشار إليها في الفقرة 1 (أ)، فيجوز له بدلا من ذلك أن يعتمد ما قد يلزم من تدابير تشـريعية وتدابير أخرى لضـمان الجمع أو التسجيل في الوقت الحقيقي لبيانات المحتوى المرتبطة باتصـالات محددة مرسلة في إقليمه، وذلك باسـتخدام الوسائل التقنية اللازمة في ذلك الإقليم.

3- يعتمد كل طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى لإلزام مقدم الخدمة بالحفاظ على سـرية تنفيذ أي صلاحيات منصوص عليها في هذه المادة وأي معلومات تتعلق بها.

21- التعجيل بالحفاظ على البيانات الحاسوبية المُخزنة

1- يعتمد كل طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى لتمكين سـلطاته المختصـة من الحفاظ على أي بيانات حاسـوبية محددة على وجه السـرعة، إما بأمر مباشـر أو بوسـيلة مماثلة، بما في ذلك بيانات الحركة والمحتوى المخزنة بواسطة نظام حاسوبي، وخاصة في حالة وجود أسس للاعتقاد بأن البيانات الحاسوبية معرَّضة بشكل خاص للفقدان أو التعديل.

2- حيثما ينفذ طرف الفقرة 1 أعلاه عن طريق إصـدار أمر لشـخص ما بالحفاظ على بيانات حاسـوبية محددة توجد بحوزته أو تحت سـيطرته، يعتمد هذا الطرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى لإلزام ذلك الشـخص بالحفاظ على تلك البيانات الحاسـوبية وصـون سـلامتها على النحو اللازم لفترة زمنية بالطول

الضـروري، بحد أقصـى 180 يوما، لتمكين السـلطات المختصـة من السـعي لكشـفها. ويجوز لهذا الطرف أن ينص على تجديد هذا الأمر في وقت لاحق.

3- يعتمد كل طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى لإلزام وديع البيانات الحاسـوبية أو أي شـخص آخر يتعين عليه أن يحافظ عليها بالحفاظ على سـرية تنفيذ هذه الإجراءات خلال الفترة الزمنية المنصوص عليها في قانونه الوطني.

4- ينشئ كل طرف جهة مركزية للتنسيق يمكن من خلالها للدولة الأخرى تنفيذ طلب الحفظ هذا.

جامايكا (باسم الجماعة الكاريبية)

[الأصل: بالإنكليزية]
[12 أيار/مايو 2022]

الفصل الأول- أحكام عامة

المادة- أحكام عامة

أغراض هذه الاتفاقية هي:

1- تشـجيع وتعزيز التدابير الرامية إلى منع ومكافحة الجرائم وغيرها من الأفعال غير المشـروعة الموجهة ضـد سـرية وسـلامة وتوافر نظم تكنولوجيا المعلومات والاتصـالات والبيانات الحاسـوبية بمزيد من الكفاءة والفعالية؛

2- تعزيز وتيسـير ودعم التعاون الدولي والمسـاعدة التقنية لمنع ومكافحة الأفعال الإجرامية وغيرها من الأعمال غير المشـروعة الموجهة ضـد سـرية وسـلامة وتوافر نظم تكنولوجيا المعلومات والاتصـالات والبيانات الحاسوبية.

3- تعزيز وتيسـير ودعم التعاون الدولي والمسـاعدة التقنية في اسـترداد الموجودات الناتجة عن الأفعال الإجرامية وغيرها من الأفعال غير المشروعة المشار إليها في هذه الاتفاقية.

المادة- نطاق الانطباق

1- تنطبق هذه الاتفاقية، وفقا لأحكامها، على منع الأفعال الإجرامية والتحري عنها والتحقيق فيها وملاحقة مرتكبيها، وعلى تعزيز وتيسـير ودعم التعاون الدولي على منع ومكافحة اسـتخدام تكنولوجيات المعلومات والاتصـالات في الأفعال الإجرامية، وعلى تجميد عائدات تلك الأفعال المجرمة وفقا لهذه الاتفاقية وحجزها ومصادرتها وإعادتها.

2- لأغراض تنفيذ هذه الاتفاقية، ليس ضـروريا أن تكون الجرائم المبيّنة فيها قد ألحقت ضـررا أو أذى بالأشخاص أو الممتلكات أو الدولة، ما لم تنص أحكامها على خلاف ذلك.

المادة- صون السيادة

1- تنفذ الدول الأطراف التزاماتها المنصـوص عليها في هذه الاتفاقية على نحو يتفق مع مبادئ السـيادة وتسـاوي الدول في السـيادة والسـلامة الإقليمية ومبدأ عدم التدخل في الشـؤون الداخلية للدول الأطراف أو الدول الأخرى.

2- ليس في هذه الاتفاقية ما يبيح للدولة الطرف أن تقوم في إقليم دولة طرف أخرى أو دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الطرف الأخرى أو الدولة الأخرى بمقتضى قانونها الوطني ووفقا للقانون الدولي والالتزامات الدولية.

الفصل الثاني- التجريم

المادة- الدخول غير القانوني/غير المأذون به على النظم أو البيانات الحاسوبية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يجرَّم الدخول على كامل أي نظام حاسوبي أو جزء منه عندما يُرتكب ذلك عمدا ودون حق. ويجوز للدولة الطرف أن تشترط لتحقق الجريمة وقوع إخلال بتدبير أمني أو خرقه، أو ارتكابها بقصد الحصول على بيانات حاسوبية أو بقصد آخر غير شريف، أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر. (*استنادا إلى المادة 2 من اتفاقية بودابست – النفاذ غير المشروع*)

المادة- الاعتراض غير القانوني/غير المأذون به

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم اعتراض أي نظام حاسوبي أو بيانات حاسوبية عمدا ودون وجه حق أو إذن بوسائل تقنية بهدف اعتراض بيانات الحركة والبيانات التي تعالجها تكنولوجيات المعلومات والاتصالات غير المخصصة للاستخدام العام، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام حاسوبي يحمل مثل هذه البيانات الحاسوبية.

2- يجوز للدولة الطرف أن تشترط لتحقق الجريمة توافر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة- التدخل غير القانوني في البيانات

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، عندما تُرتكب عمدا: إدخال بيانات حاسوبية أو إتلافها أو حذفها أو إفسادها أو تحويرها أو طمسها بدون وجه حق أو إذن.

2- يجوز للدولة الطرف أن تحتفظ بالحق في اشتراط أن يؤدي السلوك الموصوف في الفقرة 1 إلى ضرر جسيم.

المادة- التدخل غير القانوني في النظم

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم القيام عمدا ودون وجه حق أو إذن بإعاقة عمل أي نظام من نظم تكنولوجيا المعلومات والاتصالات عن طريق إدخال بيانات حاسوبية أو إرسالها أو إتلافها أو حذفها أو إفسادها أو تحويرها أو طمسها.

2- يجوز لكل دولة طرف أن تحتفظ بالحق في تشديد العقوبة عندما تمس الأفعال المبينة في الفقرة 1 ببنية تحتية حيوية أو تؤثر فيها.

المادة- إساءة استخدام الأجهزة/البرمجيات الخبيثة/برامج الحاسوب

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لتجريم الأفعال التالية، عندما تُرتكب عمدا وبغير وجه حق:

(أ) إنتاج الأشـياء التالية أو بيعها أو شـراؤها للاسـتخدام أو اسـتيرادها أو توزيعها أو إتاحتها بطريقة أخرى:

'1' جهاز، بما في ذلك برنامج حاسـوب، مصـمم أو مكيَّف في المقام الأول لغرض ارتكاب أي من الجرائم المنصـــوص عليها وفقا للمواد (المتعلقة بالدخول على البيانات والنظم أو التدخل فيها أو اعتراضها بشكل غير قانوني أو غير مأذون به).

'2' كلمة مرور خاصة بحاسوب، أو رمز دخول، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظم المعلومات والاتصالات والتكنولوجيا بقصد استخدامها لغرض ارتكاب أي من الجرائم الجنائية المنصـــوص عليها في المواد (المتعلقة بالدخول على البيانات والنظم أو التدخل فيها أو اعتراضها بشكل غير قانوني أو غير مأذون به)؛

(ب) حيازة إحدى الأشـــياء المشـــار إليها في الفقرتين الفرعيتين (أ) '1' أو '2' أعلاه، بغرض ارتكاب أي من الجرائم المنصـــوص عليها في المواد (المتعلقة بالدخول على البيانات والنظم أو التدخل فيها أو اعتراضـــها بشـــكل غير قانوني أو غير مأذون به). ويجوز للدولة الطرف أن تشـــترط بموجب القانون الحيازة المسبقة لعدد من هذه الأشياء لإسناد المسؤولية الجنائية.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عملية الإنتاج أو البيع أو الشراء بغرض الاسـتخدام أو الاسـتيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشـار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصـــوص عليها في المواد (المتعلقة بالدخول على البيانات والنظم أو التدخل فيها أو اعتراضها بشكل غير قانوني أو غير مأذون به) من هذه الاتفاقية، بل بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لغرض اختبار أو حماية نظام حاسوبي على سبيل المثال.

3- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شـريطة ألا يكون هذا التحفظ متعلقا بعمليات بيع الأشـــياء المشـــار إليها في الفقرة 1 (أ) '2' من هذه المادة أو توزيعها أو إتاحتها بطريقة أخرى.

المادة- جرائم المحتوى

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لتجريم السـلوكيات التالية عندما تُرتكب عمدا وبغير وجه حق:

(أ) إنتاج مواد اسـتغلال الأطفال والاعتداء عليهم جنسـيا من خلال نظام لتكنولوجيا المعلومات والاتصالات؛

(ب) عرض وإتاحة مواد اســـتغلال الأطفال والاعتداء عليهم جنســـيا من خلال نظام لتكنولوجيا المعلومات والاتصالات؛

(ج) توزيع وبث مواد اســـتغلال الأطفال والاعتداء عليهم جنســـيا من خلال نظام لتكنولوجيا المعلومات والاتصالات؛

(د) اقتناء مواد اســـتغلال الأطفال والاعتداء عليهم جنســـيا من خلال نظام حاســـوبي/نظام لتكنولوجيا المعلومات والاتصالات للذات أو لشخص آخر؛

(هـ) حيازة مواد اســتغلال الأطفال والاعتداء عليهم جنســيا في نظام حاســوبي/نظام لتكنولوجيا المعلومات والاتصالات أو على وسيط حاسوبي لتخزين البيانات.

2- لأغراض الفقرة 1 أعلاه، يشــمل تعبير "مواد اســتغلال الأطفال والاعتداء عليهم جنســيا" المواد التي تصور بصريا:

(أ) طفلا منخرطا في سلوك جنسي صريح؛

(ب) شخصا يظهر أنه طفل منخرطا في سلوك جنسي صريح؛

(ج) صورا واقعية تمثل قاصرا ينخرط في سلوك جنسي صريح.

3- لأغراض الفقرة 2 أعلاه، يعنى "الطفل" كل إنســان لم يتجاوز الثامنة عشــرة، ما لم يكن ســن الرشــد محددا بأقل من ذلك في القانون المنطبق عليه. (اتفاقية حقوق الطفل، المادة 1)

المادة- انتهاك الخصوصية/التوزيع غير التوافقي للصور الجنسية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشــريعية وتدابير أخرى لتجريم الســلوكيات التالية، عندما تُرتكب عمدا وبغير وجه حق:

(أ) تعمُّد نشــر أو توزيع أو بث أو بيع أو إتاحة صــورة حميمة لشــخص أو الإعلان عنها مع العلم بأن الشخص المصور في الصورة لم يعط موافقته على هذا السلوك؛

(ب) نشــر أو توزيع أو بث أو بيع أو إتاحة صــورة حميمة لشــخص أو الإعلان عنها بقصــد التحرش بالشخص المصور في الصورة أو التسبب في ضرر له.

تعريف الصورة الحميمة

2- تعني "الصورة الحميمة" في هذه المادة تسجيلا مرئيا لشخص تم إجراؤه بأي وسيلة، بما في ذلك التقاط صورة فوتوغرافية أو تصوير فيلم أو فيديو؛

(أ) يكون فيه الشــخص عاريا، أو كاشــفا عن أعضــائه التناســلية أو منطقة الشــرج أو الثديين، أو منخرطا في نشاط جنسي صريح؛

(ب) كانت هناك ظروف وقت تسجيله أدت إلى توقع معقول للخصوصية؛

(ج) ظل الشخص المصور يتوقع بشأنه قدرا معقولا من الخصوصية وقت ارتكاب الجريمة.

المادة- الملكية الفكرية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم التعدي على حقوق التأليف والنشــر والحقوق المجاورة، وفق تعريفها في تشــريعاتها، عندما تُرتكب تلك الأفعال عمدا عن طريق تكنولوجيا المعلومات والاتصالات، وعلى نطاق تجاري.

الجرائم الحاسوبية

المادة- التزوير الحاسوبي

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لتجريم إدخال بيانات حاســـوبية أو تحويرها أو حذفها أو طمسها عن عمد ودون وجه حق بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو اســـتخدامها لأغراض قانونية بغض النظر عما إذا كانت البيانات قابلة للقراءة مباشـــرة ومفهومة أم لا.

2- يجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة أخرى.

المادة- الاحتيال الحاسوبي

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى كي يُجرَّم، إذا ما ارتُكب عمدا وبغير وجه حق أو صلاحية قانونية، التسبب في إلحاق خسارة بممتلكات الغير عن طريق:

(أ) أي إدخال أو تحوير أو محو أو طمس لبيانات حاسوبية؛

(ب) أي تدخل في عمل نظام حاسوبي؛

بقصد الاحتيال أو بقصد غير شريف للحصول على منفعة اقتصادية للذات أو لشخص آخر.

المادة- الجرائم غير التامة

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم المشاركة بأي صفة، مثل الشريك أو المساعد أو المحفز أو المحرض أو المتآمر، في أي فعل مجرّم وفقا لهذه الاتفاقية.

2- يجوز لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشـريعية وتدابير أخرى لكي تجرّم الشـروع في ارتكاب أي فعل مجرّم وفقا لهذه الاتفاقية.

3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لكي تجرّم الإعداد لارتكاب أي فعل مجرّم وفقا لهذه الاتفاقية.

المادة- مسؤولية الشخصيات الاعتبارية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير، وفقا لمبادئها القانونية، لتقرير مسؤولية الأشخاص الاعتباريين عن المشـــاركة في ارتكاب أي فعل مجرم وفقا لهذه الاتفاقية يقوم به لصـــالحهم أي شـــخص طبيعي، يتصـــرف إما بمفرده أو باعتباره عضوا في هيئة تابعة للشخص الاعتباري يتبوأ منصبا قياديا داخلها، وذلك بناء على:

(أ) سلطة تمثيل الشخص الاعتباري؛

(ب) سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛

(ج) سلطة ممارسة الإشراف أو الرقابة داخل الشخص الاعتباري.

2- إضـــافةً إلى الحالات المنصـــوص عليها في الفقرة 1 من هذه المادة، تعتمد كل دولة طرف التدابير الضـرورية لضـمان إمكانية تحميل الشـخص الاعتباري المسـؤولية إذا أتاح عدم الإشـراف أو الرقابة من قبل

الشخص الطبيعي المشار إليه في الفقرة 1 ارتكاب فعل مجرم وفقا لهذه الاتفاقية لفائدة ذلك الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته الصريحة أو الضمنية:

3- رهنا بالقانون الوطني للدولة الطرف، يجوز أن تكون مسؤولية الشخصيات الاعتبارية جنائية أو مدنية أو إدارية.

4- لا تخلُّ هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم.

5- تكفل كل دولة طرف، على وجه الخصوص، إخضاع الشخصيات الاعتبارية التي تلقى عليها المسؤولية وفقا لهذه المادة لعقوبات جنائية أو غير جنائية فعّالة ومتناسبة ورادعة، بما فيها العقوبات النقدية.

المادة- الجزاءات والتدابير

1- تُخضِع كل دولة طرف ارتكاب أي فعل مجرم وفقا لهذه الاتفاقية لجزاءات تتناسب مع جسامة ذلك الفعل، وتكون فعالة ومتناسبة ورادعة، بما في ذلك الحرمان من الحرية.

2- تكفل كل دولة طرف إخضاع الشخصيات الاعتبارية التي تلقى عليها المسؤولية وفقا لهذه المادة (مسؤولية الشخصيات الاعتبارية) لعقوبات جنائية أو غير جنائية فعالة ومتناسبة ورادعة، بما فيها العقوبات النقدية.

الفصل الثالث- القانون الإجرائي وإنفاذ القانون

المادة- نطاق الأحكام الإجرائية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار الصلاحيات والإجراءات المنصوص عليها في هذا الفصل لأغراض التحقيقات أو الإجراءات الجنائية.

2- تطبق كل دولة طرف، ما لم يُنص على خلاف ذلك في المادة (اعتراض الاتصالات)، الصلاحيات والإجراءات المشار إليها في الفقرة 1 من هذه المادة على:

(أ) الأفعال المجرَّمة وفقا للمواد (أحكام التجريم) من هذه الاتفاقية؛

(ب) الجرائم الجنائية الأخرى المرتكبة عن طريق نظام للمعلومات والاتصالات والتكنولوجيا؛

(ج) جمع الأدلة على الجرائم في شكل إلكتروني.

3- يجوز لكل دولة طرف أن تحتفظ بالحق في قصر تطبيق التدابير المشار إليها في المادة (جمع البيانات في الوقت الحقيقي) على الأفعال الإجرامية أو فئاتها المحددة في التحفظ، شريطة ألا يكون نطاق تلك الجرائم أضيق من نطاق الأفعال الإجرامية التي تطبق عليها الدولة الطرف التدابير المشار إليها في المادة (اعتراض بيانات المحتوى).

4- عندما لا تستطيع دولة طرف، بسبب قيود في تشريعاتها السارية وقت اعتماد هذه الاتفاقية، أن تطبق التدابير المشار إليها في المادة (جمع البيانات في الوقت الحقيقي) والمادة (اعتراض بيانات المحتوى) على الاتصالات المرسَلة داخل أي نظام حاسوبي تابع لمقدم الخدمة:

'1' يجري تشغيله لصالح مجموعة مغلقة من المستخدمين،

'2' لا يستخدم شبكات اتصالات عامة ولا يتصل بنظام حاسوبي آخر، سواء كان عاما أو خاصا،

يجوز لتلك الدولة الطرف أن تحتفظ بالحق في عدم تطبيق تلك التدابير على تلك الاتصالات.

5- تنظر كل دولة طرف في تقييد هذا التحفظ حتى تتمكن من تطبيق التدابير المشار إليها في المادتين (جمع البيانات في الوقت الحقيقي واعتراض بيانات المحتوى) على أوسع نطاق.

المادة- الشروط والضمانات

1- تكفل كل دولة طرف خضوع إنشاء الصلاحيات والإجراءات المنصوص عليها في هذه المادة وتنفيذها وتطبيقها للشروط والضمانات المنصوص عليها في قانونها الوطني الذي ينص على حماية حقوق الإنسان وحرياته، بما في ذلك الحقوق الناشئة عملا بالالتزامات التي تعهدت بها بموجب العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، وغيره من الصكوك الدولية لحقوق الإنسان المنطبقة.

2- تشمل هذه الشروط والضمانات، حسب الاقتضاء في ضوء طبيعة الإجراءات أو الصلاحيات ذات الصلة، الإشراف القضائي أو غيره من أشكال الإشراف المستقل، والأسباب التي تبرر التطبيق، وحدود ومدة تلك الصلاحية أو ذلك الإجراء.

3- تأخذ كل دولة طرف في الاعتبار أثر هذه الصلاحيات والإجراءات الواردة في هذه المادة على حقوق الأطراف الثالثة ومسؤولياتها ومصالحها المشروعة من حيث مدى اتساقه مع المصلحة العامة، وخاصة إقامة العدل على نحو سليم.

المادة- التعجيل بالحفاظ على البيانات الحاسوبية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من أن تصدر أوامر من أجل الحصول على بيانات حاسوبية معينة، بما في ذلك بيانات الحركة، وجمعها والحفاظ عليها أو أن تتوصل إلى ذلك بطريقة مماثلة على وجه السرعة، خاصة في حالة وجود أسس للاعتقاد بأن البيانات معرضة بشكل خاص للحذف أو التعديل أو الفقدان.

2- حيثما تُفعِّل دولة طرف الفقرة 1 أعلاه عن طريق إصدار أمر إلى شخص، طبيعي أو اعتباري، بالمحافظة على بيانات حاسوبية محددة ومخزنة توجد بحوزته أو تحت سيطرته، تعتمد الدولة الطرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام ذلك الشخص بالحفاظ على تلك البيانات الحاسوبية وصون سلامتها للمدة اللازمة، بما لا يتعدى الفترة التي يحددها القانون الوطني لتلك الدولة الطرف، لتمكين السلطات المختصة من السعي لكشفها. ويجوز للدولة الطرف أن تنص على تجديد هذا الأمر في وقت لاحق.

3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الشخص المكلف بحفظ المعلومات بالحفاظ على سرية هذه الإجراءات طيلة الفترة الزمنية المنصوص عليها في قانونها الوطني.

4- تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين (نطاق الأحكام الإجرائية والشروط والضمانات).

المادة- التعجيل بالحفاظ على بيانات الحركة والكشف الجزئي عنها

1- تعتمد كل دولة طرف، بشأن بيانات الحركة التي يتعين الحفاظ عليها بمقتضى المادة (التعجيل بالحفاظ على البيانات الحاسوبية)، ما قد يلزم من تدابير تشريعية وتدابير أخرى من أجل:

(أ) ضمان إمكانية التعجيل بالحفاظ على بيانات الحركة بغض النظر عن مشاركة مقدم خدمة واحد أو أكثر في بث تلك الاتصالات؛

(ب) ضمان سرعة الكشف للسلطة المختصة في الدولة الطرف، أو لشخص تعينه تلك السلطة، عن كمية كافية من بيانات الحركة لتمكين الدولة الطرف من تحديد مقدمي الخدمات والمسار الذي بُث الاتصال من خلاله.

2- تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين (نطاق الأحكام الإجرائية والشروط والضمانات).

المادة- الأمر بتقديم المعلومات

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة، حيثما تكون هناك أسباب معقولة تدعو للاعتقاد بأن فعلا إجراميا قد ارتُكب أو يجري ارتكابه، من اتخاذ الإجراءات التالية:

(أ) أن تأمر شخصا، طبيعيا أو اعتباريا، في إقليمها بأن يقدم إليها ما بحوزته أو تحت سيطرته من بيانات حاسوبية مخزنة في نظام حاسوبي أو في وسيط لتخزين البيانات الحاسوبية؛

(ب) أن تأمر مقدم خدمة في إقليمها بأن يقدم إليها ما بحوزته أو تحت سيطرته من معلومات عن المشتركين في خدماته.

2- تحدد الصلاحيات والإجراءات المشار إليها في هذه المادة وفقا للمادتين (نطاق الأحكام الإجرائية والشروط والضمانات).

3- لأغراض هذه المادة، يعني مصطلح "معلومات المشتركين" أي معلومات يحتفظ بها مقدم الخدمة عن المشتركين في خدماته، بخلاف بيانات الحركة أو بيانات المحتوى، يمكن على أساسها تحديد ما يلي:

(أ) نوع خدمة المعلومات والاتصالات المستخدمة، والتدابير التقنية المتخذة ومدة الخدمة؛

(ب) هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه والأرقام الأخرى التي يمكن بها الوصول إليه، بما في ذلك عناوين بروتوكول الإنترنت والمعلومات الخاصة بالفواتير والسداد، المتاحة في اتفاق أو ترتيب الخدمة؛

(ج) المعلومات المتعلقة بموقع معدات المعلومات والاتصالات التي لها صلة باتفاق أو ترتيب الخدمة.

المادة- البحث عن المعلومات المخزنة أو المعالجة إلكترونيا وضبطها

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتخويل سلطاتها المختصة، حيثما تكون هناك أسباب معقولة تدعو للاعتقاد بأن فعلا إجراميا قد ارتُكب أو يجري ارتكابه، صلاحية البحث فيما يلي أو الوصول إليه بطريقة مماثلة:

(أ) نظام لتكنولوجيا المعلومات والاتصالات أو جزء منه والبيانات الحاسوبية المخزنة فيه.

(ب) وسيط تخزين بيانات حاسوبية يمكن أن تكون بيانات حاسوبية مخزنة فيه في إقليمها.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان أنه في حالة قيام سلطاتها بالبحث في نظام حاسوبي معين أو جزء منه أو الوصول إليه بطريقة مماثلة عملا بالفقرة 1 (أ)، وتكون لديها أسباب معقولة للاعتقاد بأن البيانات الملتمسة مخزنة في نظام حاسوبي آخر أو في جزء منه في إقليمها، ويكون

من الممكن الوصول إلى هذه البيانات من النظام الأول أو تكون متاحة له بشكل قانوني، تكون السلطات قادرة على توسيع نطاق البحث، أو نطاق الوصول بطريقة مماثلة، ليشمل النظام الآخر على وجه السرعة.

3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من ضبط البيانات الحاسوبية التي يتم الوصول إليها وفقا للفقرتين 1 أو 2 أو تأمينها بطريقة مشابهة. وتشمل هذه التدابير صلاحية:

(أ) ضبط نظام حاسوبي أو جزء منه أو وسيط تخزين بيانات حاسوبية أو تأمين ذلك النظام أو الوسيط على نحو مماثل؛

(ب) عمل نسخة من تلك البيانات الحاسوبية والاحتفاظ بها؛

(ج) الحفاظ على سلامة البيانات الحاسوبية المخزنة ذات الصلة؛

(د) جعل الوصول إلى تلك البيانات الحاسوبية متعذرا في النظام الحاسوبي الذي تم الوصول إليه أو إزالتها منه.

4- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من أن إصدار الأمر لأي شخص لديه معرفة بعمل النظام الحاسوبي أو التدابير المطبقة لحماية البيانات الحاسوبية الموجودة فيه بأن يقدم، بالقدر المعقول، المعلومات اللازمة للتمكين من اتخاذ التدابير المشار إليها في الفقرات 1 و2 و3.

5- تخضع الصلاحيات والإجراءات المشار إليها في هذه المادة للمادتين (نطاق الأحكام الإجرائية والشروط والضمانات).

المادة- جمع بيانات الحركة في الوقت الحقيقي

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتخويل سلطاتها المختصة الصلاحيات التالية، حيثما تكون هناك أسباب معقولة تدعو للاعتقاد بأن فعلا إجراميا قد ارتُكب أو يجري ارتكابه:

(أ) أن تجمع أو تسجل في الوقت الحقيقي، باستخدام الوسائل التقنية في إقليمها، بيانات الحركة المرتبطة باتصالات محددة في ذلك الإقليم مرسلة عن طريق نظام حاسوبي؛

(ب) أن تجبر أي مقدم خدمة، في حدود قدراته التقنية القائمة، على:

'1' أن يجمع أو يسجل هذه البيانات في الوقت الحقيقي باستخدام الوسائل التقنية في إقليم تلك الدولة الطرف؛ أو

'2' أن يتعاون مع السلطات المختصة ويساعدها في جمع أو تسجيل هذه البيانات في الوقت الحقيقي.

2- إذا تعذر على الدولة الطرف، بسبب المبادئ الراسخة لنظامها القانوني الوطني، الأخذ بالتدابير المشار إليها في الفقرة 1 (أ)، فيجوز لها بدلا من ذلك أن تعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات الحركة المرتبطة باتصالات محددة مرسلة في إقليمها، وذلك باستخدام الوسائل التقنية اللازمة في ذلك الإقليم.

3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي صلاحيات منصوص عليها في هذه المادة وأي معلومات تتعلق بها.

4- تخضـــع الصـــلاحيات والإجراءات المشـــار إليها في هذه المادة للمادتين (نطاق الأحكام الإجرائية والشروط والضمانات).

المادة- اعتراض بيانات المحتوى

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها قانونها الوطني، لتخويل سلطاتها المختصـة الصـلاحيات التالية، حيثما تكون هناك أسـباب معقولة للاعتقاد بأن فعلا إجراميا قد ارتُكب أو يجري ارتكابه:

(أ) أن تجمع أو تسـجل أو تخزن في الوقت الحقيقي، باسـتخدام الوسـائل التقنية في إقليمها، بيانات المحتوى المرتبطة باتصالات محددة في ذلك الإقليم مرسلة عن طريق نظام حاسوبي؛

(ب) أن تجبر أي مقدم خدمة، في حدود قدراته التقنية القائمة، على:

'1' أن يجمع أو يسـجل أو يخزن هذه البيانات في الوقت الحقيقي باسـتخدام الوسـائل التقنية في إقليم تلك الدولة الطرف؛ أو

'2' أن يتعاون مع السـلطات المختصـة ويسـاعدها في جمع أو تسـجيل هذه البيانات في الوقت الحقيقي.

2- إذا تعذر على الدولة الطرف، بســبب أحكام قانونها الوطني، الأخذ بالتدابير المشـــار إليها في الفقرة 1 (أ)، فيجوز لها بدلا من ذلك أن تعتمد ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لضـــمان الجمع أو التسجيل في الوقت الحقيقي لبيانات المحتوى المرتبطة باتصـالات محددة مرسلة في إقليمها، وذلك باستخدام الوسائل التقنية اللازمة في ذلك الإقليم.

3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـــريعية وتدابير أخرى لإلزام مقدم الخدمة بالحفاظ على سرية تنفيذ أي صلاحيات منصوص عليها في هذه المادة وأي معلومات تتعلق بها.

4- تخضـــع الصـــلاحيات والإجراءات المشـــار إليها في هذه المادة للمادتين (نطاق الأحكام الإجرائية والشروط والضمانات).

ماليزيا

[الأصل: بالإنكليزية]
[20 نيسان/أبريل 2022]

الفصل الأول- أحكام عامة

المادة 1- بيان الغرض

أغراض هذه الاتفاقية هي:

(أ) تعزيز وتدعيم التدابير الرامية إلى منع ومكافحة الجرائم السـيبرانية/التصـدي لها على نحو أكفأ وأنجع؛

(ب) تشجيع وتيسير التعاون الدولي؛

(ج) دعم العمل على بناء القدرات وتوفير المساعدة التقنية لتمكين الدول الأعضاء من تدعيم قدراتها على التصدي للجرائم السيبرانية؛

(د) ضمان التوازن السليم بين المصالح المتعلقة بإنفاذ القانون واحترام حقوق الإنسان الأساسية.

المادة 2- استخدام المصطلحات

لأغراض هذه الاتفاقية:

(أ) "الطفل" يعني أي فرد يقل عمره عن 18 عاما؛

(ب) "السلطة المختصة" تعني سلطة قضائية أو إدارية أو سلطة أخرى لإنفاذ القانون مخولة بموجب القانون الوطني بأن تأمر بتنفيذ تدابير بمقتضى هذه الاتفاقية فيما يتعلق بالتحقيقات أو الإجراءات الجنائية أو تأذن بها أو تضطلع بتنفيذها؛

(ج) "الحاسوب" يعني جهازا إلكترونيا أو مغناطيسيا أو بصريا أو كهروكيميائيا أو أي جهاز آخر لمعالجة البيانات، أو مجموعة من هذه الأجهزة المترابطة أو المتصلة، يؤدي وظائف منطقية وحسابية ووظائف للتخزين والعرض، ويشمل أي مرفق لتخزين البيانات أو مرفق اتصالات مرتبط مباشرة بذلك الجهاز أو تلك المجموعة من الأجهزة المترابطة أو المتصلة أو يعمل بالاقتران بذلك الجهاز أو تلك المجموعة، ولكنه لا يشمل الآلة الكاتبة أو منضِّد الحروف المؤتمتين، أو الآلة الحاسبة المحمولة باليد أو أي جهاز آخر مماثل غير قابل للبرمجة أو لا يحتوي على أي مرفق لتخزين البيانات؛

(د) "الجرائم السيبرانية" تعني الأفعال المجرمة وفقا لهذه الاتفاقية؛

(هـ) "البيانات" تعني تمثيلات لمعلومات أو مفاهيم معدة أو يجري إعدادها في شكل مناسب للاستخدام في حاسوب؛

(و) "الوظيفة" تشمل المنطق أو عمليات التحكم أو الحساب أو الحذف أو التخزين أو الاسترجاع أو الاتصالات بالحاسوب أو منه أو داخله؛

(ز) "البرنامج" يعني بيانات تمثل تعليمات أو مقولات تؤدي، عند تنفيذها في الحاسوب، إلى أداء الحاسوب لوظيفة.

المادة 3- نطاق الانطباق

1- تنطبق هذه الاتفاقية على منع الأفعال المجرَّمة فيها والتحري عنها والتحقيق فيها وملاحقة مرتكبيها، ما لم تنص أحكامها على خلاف ذلك.

2- يجوز أن تنطبق هذه الاتفاقية أيضا على جمع الأدلة على الجرائم في شكل إلكتروني حيثما نصت أحكامها على ذلك.

3- توفير المساعدة التقنية والعمل على بناء القدرات بشأن المسائل التي تغطيها هذه الاتفاقية.

المادة 4- صون السيادة

1- تؤدي الدول الأطراف التزاماتها بمقتضى هذه الاتفاقية على نحو يتسق مع مبدأيْ تساوي الدول في السيادة وسلامة أراضيها، ومع مبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى.

2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية أو أداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الوطني.

الفصل الثاني- التجريم وإنفاذ القانون

المادة 5- الدخول غير المأذون به

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم الدخول غير المأذون به من أي نوع لأي شخص على أي برامج أو بيانات يُحتفظ بها داخل حاسوب في حال ارتكاب ذلك عن عمد.

المادة 6- الاعتراض غير المأذون به

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم قيام أي شخص باعتراض برامج أو اتصالات بأي شكل دون إذن في حال ارتكاب ذلك عن عمد.

المادة 7- التدخل في البيانات

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي تُجرَّم في قانونها الوطني الأفعال التالية، عندما ترتكب عمدا وبغير وجه حق: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويرها.

2- يجوز للدولة الطرف أن تحتفظ بالحق في اشتراط أن يؤدي السلوك الموصوف في الفقرة 1 إلى ضرر جسيم.

المادة 8- إعاقة حاسوب أو برنامج أو بيانات

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إعاقة عمل الحواسيب أو البرامج أو تدفق البيانات على نحو خطير من خلال التدخل فيه أو اعتراضه أو الإضرار به أو عرقلته أو منع الاستفادة منه أو تعطيله في حال ارتكاب ذلك عن عمد.

المادة 9- إساءة استخدام البيانات أو البرامج أو الحواسيب

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إنتاج أي بيانات أو برامج أو حواسيب أو تكييفها أو بيعها أو اشترائها لأغراض الاستخدام أو استيرادها أو عرضها أو توزيعها أو توريدها أو إتاحتها بأي شكل آخر، عندما يُرتكب ذلك عمدا وبغير وجه حق.

المادة 10- الجرائم المتصلة باستغلال الأطفال في المواد الإباحية

1- تجريم الأفعال التالية في حال ارتكابها عمدا وبغير وجه حق:

(أ) صـــنع أي مواد إباحية عن الأطفال أو إنتاجها أو توجيه العمل في إنتاجها لغرض توزيعها من خلال نظام حاسوبي؛

(ب) اسـتخدام طفل أو التسـبب في اسـتخدامه في التحضـير لصـنع مواد إباحية عن الأطفال أو لإنتاجها، أو في التحضـير لتوجيه العمل في صـنع تلك المواد أو إنتاجها، أو اسـتخدامه أو التسـبب في استخدامه في صنع تلك المواد أو إنتاجها، أو في توجيه العمل في صنع تلك المواد أو إنتاجها لغرض توزيعها من خلال نظام حاسوبي؛

(ج) تبادل أي مواد إباحية عن الأطفال أو نشـرها أو طبعها أو اسـتنسـاخها أو بيعها أو تأجيرها أو توزيعها أو عرضـها أو الإعلان عنها أو بثها أو ترويجها أو اسـتيرادها أو تصـديرها أو إيصـالها أو عرضـها أو إتاحتها من خلال نظام حاسوبي؛

(د) الحصول على أي مواد إباحية عن الأطفال أو جمعها أو التماسها من خلال نظام حاسوبي؛ أو

(هـ) المشـــاركة في أي أعمال مرتبطة بأي مواد إباحية عن الأطفال من خلال نظام حاســـوبي أو تلقّي أرباح منها إذا كان المشارك يعرف ذلك أو لديه من الأسباب ما يجعله يعرف ذلك؛

(و) الوصـول إلى أي مواد إباحية عن الأطفال أو حيازتها بصـورة شـخصـية أو التحكم فيها من خلال نظام حاسوبي.

2- لأغراض الفقرة 1، يسـتخدم مصـطلح "اسـتغلال الأطفال في المواد الإباحية" وفق تعريفه الوارد في البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشـأن بيع الأطفال واسـتغلال الأطفال في البغاء وفي المواد الإباحية.

المادة 11- الشروع والمساعدة والتحريض

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشـريعية وتدابير أخرى لكي تجرّم، وفقا لقانونها الوطني، التشجيع على ارتكاب فعل مجرّم وفقا لهذه الاتفاقية أو الضلوع في ارتكابه بأي صفة، مثل الشريك أو المساعد أو المحرض.

2- يجوز لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشـريعية وتدابير أخرى لكي تجرّم، وفقا لقانونها الوطني، أي شروع في ارتكاب فعل مجرّم وفقا لهذه الاتفاقية.

3- يمكن لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشـريعية وتدابير أخرى لكي تجرّم، وفقا لقانونها الوطني، الإعداد لارتكاب فعل مجرّم وفقا لهذه الاتفاقية.

المادة 12- مسؤولية الشخصيات الاعتبارية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير، تتسق مع مبادئها القانونية، لتقرير مسؤولية الشـخصـيات الاعتبارية عن المشاركة في الأفعال المجرّمة وفقا لهذه الاتفاقية.

2- رهنا بالمبادئ القانونية للدولة الطرف، يجوز أن تكون مسؤولية الشخصيات الاعتبارية جنائية أو مدنية أو إدارية.

3- لا تخلُّ هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم.

4- تكفل كل دولة طرف، على وجه الخصوص، إخضاع الشخصيات الاعتبارية التي تلقى عليها المسؤولية وفقا لهذه المادة لعقوبات جنائية أو غير جنائية فعّالة ومتناسبة ورادعة، بما فيها العقوبات النقدية.

المادة 13- الملاحقة والمقاضاة والجزاءات

1- تكفل كل دولة طرف إخضاع الأفعال المجرمة وفقا لهذه الاتفاقية لعقوبات تُراعى فيها جسامة الجرم المرتكب.

2- تسعى كل دولة طرف إلى ضمان أن أية صلاحيات قانونية تقديرية يتيحها قانونها الوطني لملاحقة مرتكبي الجرائم المشمولة بهذه الاتفاقية تُمارس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القوانين التي تتخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة ردعها.

3- في حالة الأفعال المجرّمة وفقا لهذه الاتفاقية، تتخذ كل دولة طرف تدابير مناسبة، وفقا لقانونها الوطني ومع إيلاء الاعتبار الواجب لحقوق الدفاع، لضمان أن تراعي شروط قرارات الإفراج إلى حين المحاكمة أو الاستئناف ضرورة ضمان حضور المدعى عليه في الإجراءات الجنائية اللاحقة.

4- تكفل كل دولة طرف أن تراعي محاكمها أو سلطاتها المختصة الأخرى خطورة الجرائم المشمولة بهذه الاتفاقية لدى النظر في إمكانية الإفراج المبكر أو المشروط عن الأشخاص المدانين بارتكابها.

5- ليس في هذه الاتفاقية ما يمس بالمبدأ القاضي بأن يكون الحق في توصيف الأفعال المجرّمة وفقا لها وتوصيف الدفوع القانونية المنطبقة أو المبادئ القانونية الأخرى التي تحكم مشروعية السلوك محفوظا حصرا للقانون الوطني للدولة الطرف، وبوجوب الملاحقة والمعاقبة على تلك الجرائم وفقا لذلك القانون.

الفصل الثالث- الإجراءات الجنائية وإنفاذ القانون

المادة 14- نطاق التدابير الإجرائية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقرار السلطات والإجراءات المنصوص عليها في هذا الفصل لأغراض التحقيقات أو الإجراءات الجنائية.

2- تطبق كل دولة طرف، ما لم يُنص على خلاف ذلك، الصلاحيات والإجراءات المشار إليها في الفقرة 1 من هذه المادة على:

(أ) الأفعال المجرمة وفقا لهذه الاتفاقية؛

(ب) الجرائم الجنائية الأخرى المرتكبة عن طريق نظام حاسوبي؛

(ج) جمع الأدلة على الجرائم في شكل إلكتروني.

المادة 15- الأمر بتقديم المعلومات

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من أن تأمر شخصا في إقليمها بتقديم بيانات حاسوبية محددة في حوزته أو تحت سيطرته ومخزنة في نظام حاسوبي أو في وسيط حاسوبي لتخزين البيانات.

المادة 16- البحث عن البيانات الحاسوبية المُخزنة وضبطها

تعتمد كل دولة طرف ما قد يلزم من تدابير لتمكين سلطاتها المختصة من البحث عن أي دليل من هذا القبيل وضبطه وتحريزه ويكون من حق السلطات المختصة الاطلاع على أي برامج أو بيانات محفوظة في أي حاسوب أو الدخول على أي حواسيب أو أجهزة أو مواد مرتبطة بها أو تفتيشها أو التحقق من تشغيلها إذا كانت هناك أسباب معقولة تدعو للاشتباه في أنها مستخدمة أو استخدمت بالفعل لارتكاب جرائم مشمولة بالاتفاقية.

المادة 17- الولاية القضائية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير لبسط ولايتها القضائية على الأفعال المجرَّمة بمقتضى هذه الاتفاقية في الحالتين التاليتين:

(أ) عندما يُرتكب الجرم في إقليم تلك الدولة الطرف؛ أو

(ب) عندما يُرتكب الجرم على متن سفينة ترفع علم تلك الدولة الطرف أو طائرة مسجّلة بمقتضى قوانين تلك الدولة الطرف وقت ارتكاب الجرم.

2- رهنا بأحكام المادة المتعلقة بالسيادة من هذه الاتفاقية، يجوز للدولة الطرف أن تُخضِع أيضا أي جرم من هذا القبيل لولايتها القضائية في الحالات التالية:

(أ) عندما يُرتكب الجرم ضد أحد رعايا تلك الدولة الطرف؛ أو

(ب) عندما يرتكب الجرم أحد رعايا تلك الدولة الطرف؛ أو

(ج) عندما يُرتكب الجرم ضد الدولة الطرف.

3- لأغراض المادة المتعلقة بتسليم المطلوبين من هذه الاتفاقية، تعتمد كل دولة طرف ما قد يلزم من تدابير لإخضاع الأفعال المجرَّمة وفقا لهذه الاتفاقية لولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه لمجرد كونه أحد رعاياها.

4- يجوز لكل دولة طرف أيضا أن تعتمد ما قد يلزم من تدابير لإخضاع الأفعال المجرَّمة وفقا لهذه الاتفاقية لولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه.

5- إذا أُبلغت الدولة الطرف التي تمارس ولايتها القضائية بمقتضى الفقرة 1 أو 2 من هذه المادة، أو علمت بطريقة أخرى، أن أي دول أطراف أخرى تجري تحقيقا أو ملاحقة أو تتخذ إجراء قضائيا بشأن السلوك ذاته، وجب على السلطات المعنية في تلك الدول الأطراف أن تتشاور فيما بينها، حسب الاقتضاء، بهدف تنسيق ما تتخذه من إجراءات.

6- دون مساس بقواعد القانون الدولي العام، لا تحول هذه الاتفاقية دون ممارسة أي ولاية قضائية جنائية تؤكد الدولة الطرف سريانها وفقا لقانونها الوطني.

المادة 18- حقوق الضحايا

1- تضع كل دولة طرف قواعد إجرائية ملائمة توفر لضحايا الجرائم المشمولة بهذه الاتفاقية سبل الحصول على التعويض.

2- تتيح كل دولة طرف، رهنا بقانونها الوطني، إمكانية عرض آراء وشواغل الضحايا وأخذها بعين الاعتبار في المراحل المناسبة من الإجراءات الجنائية المتخذة ضد الجناة، على نحو لا يمس بحقوق الدفاع.

سنغافورة

[الأصل: بالإنكليزية]
[28 نيسان/أبريل 2022]

أحكام عامة

المصطلحات والتعاريف

2- ينبغي توضيح تعاريف المصطلحات التي ستُستخدم في الاتفاقية منذ البداية. وعلى وجه الخصوص، هناك تعبيران رئيسيان اقتُرحا لوصف موضوع الاتفاقية، وهما "الجريمة السيبرانية" و"استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية". ويجدر بالذكر أن تعبير "الجريمة السيبرانية" مقبول على نطاق واسع كتعبير يشمل الجرائم التي تُرتكَب وتُيسَّر من خلال الفضاء السيبراني. ومن شأن التعبير الثاني ("استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية") أن يغطي طائفة واسعة من المسائل المتصلة بتكنولوجيا الاتصالات خارج نطاق "الجريمة السيبرانية".

3- وترى سنغافورة أن الاتفاقية ينبغي أن تستند إلى تعبير "الجريمة السيبرانية"، لأنه تعبير مقبول على نطاق واسع يغطي التهديدات الحالية والمستجدة للجرائم السيبرانية التي تواجهها الدول الأعضاء. ومن شأن ذلك أن يزيد من تركيز الاتفاقية على الجرائم الخاصة بالفضاء السيبراني أو التي يمكِّن ذلك الفضاء من ارتكابها، وأن يمكِّن من اتباع نهج أكثر واقعية في التعامل مع هذه التهديدات.

4- وجرت أيضا مداولات في الدورة الأولى بشأن ما إذا كان ينبغي استخدام "منع ومكافحة" أو "التصدي" في الاتفاقية. وتفضل سنغافورة استخدام عبارة "منع ومكافحة"، التي استُخدمت في صكوك سابقة، بما في ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

خصوصية البيانات

5- ينبغي تحقيق التوازن بين اعتبارات خصوصية البيانات والحاجة إلى ضمان السلامة العامة، بما في ذلك مكافحة الجرائم السيبرانية لضمان السلامة على الإنترنت، والسماح لأجهزة إنفاذ القانون باتخاذ الإجراءات اللازمة لمكافحة الجريمة السيبرانية بسرعة وفعالية.

التجريم وإنفاذ القانون

6- ينبغي أن تشمل الاتفاقية أيضا عمليات الاحتيال السيبراني (التي تُرتكَب في الفضاء السيبراني أو ييسر الفضاء السيبراني ارتكابها) لأن هذه العمليات تشكل نسبة مفرطة من جميع عمليات الاحتيال في عالم اليوم. وفي سنغافورة وحدها، خسر ضحايا المخططات الاحتيالية ما لا يقل عن 633,3 مليون دولار سنغافوري في عام 2021، مع زيادة حالات الاحتيال بنسبة 52,9 في المائة عن العام السابق وتشكيلها أكثر من نصف جميع الجرائم. وتتمتع عصابات الاحتيال بموارد جيدة وتستفيد من التكنولوجيا لارتكاب عمليات احتيال عبر الحدود الوطنية وحجب مساراتها.

7- وترد اقتراحات سنغافورة بشأن الصياغة أدناه. ونعتقد أن هذه الاقتراحات تشكل نقطة انطلاق واقعية ومعقولة بشأن كيفية استهداف عمليات الاحتيال السيبراني الرئيسية في هذه الاتفاقية.

الوصول غير المشروع

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الوصول إلى كامل نظام حاسوبي أو أي جزء منه عندما يُرتكب ذلك عمدا وبغير وجه حق.

2- يجوز للدولة الطرف أن تشترط لتحقق الجريمة وقوع انتهاك لتدبير أمني، أو ارتكابها بقصد الحصول على بيانات حاسوبية أو بقصد آخر غير شريف، مثل انتحال هوية شخص آخر، أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

الاحتيال الإلكتروني

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرَّم، في حال ارتكابه عمدا وبغير وجه حق، التسبب في إلحاق خسارة بممتلكات الغير عن طريق:

(أ) أي إدخال أو تحوير أو حذف أو طمس لبيانات حاسوبية؛

(ب) أي تدخل في عمل نظام حاسوبي؛

(ج) استخدام نظام حاسوبي لخداع شخص آخر أو كيان آخر أو حثه على القيام بفعل لم يكن سيقوم به لولا ذلك أو الامتناع عن فعل لم يكن سيمتنع عنه لولا ذلك، بقصد الاحتيال عليه أو بقصد آخر غير شريف من أجل أن يحصل الجاني لنفسه أو لشخص آخر، دون وجه حق على:

'1' منفعة اقتصادية؛ و/أو

'2' بيانات حاسوبية أو معلومات شخصية غير متاحة له بطريقة أخرى.

الوصول غير القانوني إلى كلمات المرور وبيانات الاعتماد

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي تُجرَّم في قانونها الوطني الأفعال التالية، عندما تُرتكب عمدا: إحراز كلمات مرور أو بيانات اعتماد للوصول إلى نظام حاسوبي أو بيانات حاسوبية أو الحصول على تلك الكلمات أو البيانات أو تلقيها أو توزيعها بغير وجه حق.

التدابير الإجرائية وإنفاذ القانون

حفظ الأدلة والبيانات الإلكترونية وجمعها والحصول عليها وتشاطرها

8- فيما يتعلق بحفظ الأدلة والبيانات الإلكترونية وجمعها والحصول عليها وتشاطرها، نود أن نوضح ثلاث نقاط:

(أ) مع تخزين المزيد من البيانات في السحابة وتنفيذ المزيد من المعاملات رقميا، فإن التحقيقات الجنائية، خاصة فيما يتعلق بالجرائم السيبرانية، تنطوي في الغالب على أدلة رقمية. وستتعرقل التحقيقات والملاحقات القضائية إذا لم يتم الحفاظ على الأدلة الرقمية وجمعها والحصول عليها في الوقت المناسب؛

(ب) تنطوي الطلبات المقدمة عن طريق القنوات القائمة للحصول على أدلة رقمية، مثل معاهدات المساعدة القانونية المتبادلة، على عمليات مطولة. فإذا لم يتم الحفاظ على الأدلة الرقمية وجمعها والحصول عليها في الوقت المناسب، فهناك احتمال كبير بأن تُمحى هذه الأدلة بحلول الوقت الذي تقرر فيه البلدان الموافقة على طلب المساعدة القانونية المتبادلة. ولذا فإننا نؤيد ضرورة اتخاذ تدابير بشأن الطلبات القانونية المقدمة للتعجيل بحفظ البيانات؛

(ج) الجريمة السيبرانية عابرة للحدود الوطنية بطبيعتها. وتمكِّن التطورات التكنولوجية المجرمين من القيام بأنشطتهم عن بعد وعبر الحدود الوطنية. وستسمح الأحكام المتعلقة بتبادل الأدلة والبيانات الإلكترونية عبر الحدود لأجهزة إنفاذ القانون لدينا بالحصول على أدلة عملية تستند إليها تلك الأجهزة في تحقيقاتها، إلى جانب تيسير القبض على المجرمين بنجاح وملاحقتهم لاحقا واسترداد الموجودات. وينبغي أن تتيح الاتفاقية للأطراف خيار رفض الطلبات إذا كان من المحتمل أن يؤدي تنفيذ الطلب إلى المساس بسيادة الطرف متلقي الطلب أو أمنه أو نظامه العام أو مصالحه الأساسية الأخرى.

9- وإضافة إلى ذلك، نلاحظ أن لدى الدول الأعضاء نظما وظروفا قانونية مختلفة يمكن أن تؤثر في نهاية المطاف على قدرتها على تنفيذ التدابير الإجرائية، ولا سيما تلك المتعلقة بجمع البيانات واعتراضها في الوقت الحقيقي. ونلاحظ في معظم حالات الجرائم السيبرانية أن من شأن إدراج تدابير لحفظ الأدلة والبيانات الإلكترونية وجمعها والحصول عليها وتبادلها أن يفيد بالفعل عمليات التحقيق فائدة كبيرة، ولا سيما في إطار معاهدة متعددة الأطراف تحظى بدعم واسع النطاق من الدول. ولذا، ينبغي أن نتجنب الإفراط في استخدام الصيغ الإلزامية فيما يتعلق بالعمليات التنفيذية بحيث تكون أحكام الاتفاقية قابلة للتطبيق على معظم الدول، مما يسمح بالانضمام إليها والتصديق عليها على نطاق أوسع، الأمر الذي سيسمح لنا بالتصدي للجرائم السيبرانية على نحو أكثر فعالية وبطريقة متضافرة على الصعيد العالمي.

استرداد الموجودات

10- استمعت سنغافورة إلى العديد من آراء الدول الأعضاء بشأن الحاجة إلى آلية لاسترداد الموجودات. ونحن نؤيد ذلك. ونلاحظ أن الجماعات الإجرامية السيبرانية تدير عمليات متطورة عبر وطنية ليس من السهل اكتشافها أو تفكيكها. وهي تحظى بموارد وفيرة وتتفنن في استخدام التكنولوجيا لحجب مساراتها. وعندما تكون العائدات الإجرامية قد حُولت بالفعل إلى خارج بلد ما، كثيرا ما يكون استردادها صعبا للغاية.

11- ولذلك تتيح هذه الاتفاقية الفرصة لتنفيذ تدابير عالمية ملموسة وجيدة التوقيت وفعالة ومتضافرة لاسترداد الموجودات لأن قدرة أي بلد على استرداد العائدات الإجرامية التي نُقلت بالفعل خارج ولايته القضائية تتوقف على تعاون أجهزة إنفاذ القانون في الخارج. ومن المهم أن تعمل البلدان معا على استرداد الموجودات حتى لا تستفيد المنظمات الإجرامية من عائداتها الإجرامية وتزيد من قدراتها ومدى وتطورها.

أوروغواي

[الأصل: بالإنكليزية]
[6 أيار/مايو 2022]

1- تأخذ هذه الاتفاقية في الاعتبار الصكوك والجهود الدولية القائمة على كل من الصعيد الوطني والإقليمي والدولي لمنع ومكافحة استخدام تكنولوجيا المعلومات والاتصالات في الأغراض الإجرامية، تماشيا مع قرار الجمعية العامة 247/74.

وفي هذا السياق، ينبغي للاتفاقية أيضا أن تتضمن حكما ينظم الصلة بينها وبين غيرها من الصكوك الموجودة من قبل، بما في ذلك مسائل من قبيل تطبيق قواعد الأولوية وعدم الاستبعاد.

وترى أوروغواي أن النص ينبغي أن يتضمن دعوة إلى الاتساق داخل منظومة الأمم المتحدة في العمل على منع ومكافحة الاستخدام غير المشروع لتكنولوجيا المعلومات والاتصالات كحكم عام.

2- وينبغي تزويد الاتفاقية بآلية مرنة للمتابعة والمراجعة تأخذ في الاعتبار التقدم المحرز والتغييرات الدائمة القائمة في هذه المسألة.

وينبغي أن تستند الاتفاقية إلى لغة تكنولوجية محايدة، وأن تتجنب استخدام لغة تتصل بنظام تشغيلي محدد أو برمجيات حاسوبية محددة، وأن تهدف إلى توفير نهج أوسع نطاقا يمكن تفسيره في سياق بيئة سريعة التغير.

وترى أوروغواي أن من المهم أن تسمح الاتفاقية بإصدار إعلانات تفسيرية وأن تشمل إجراءات مرنة للتعديل من أجل تيسير تحديثها وإنشاء آليات لتسوية المنازعات.

وينبغي عقد مؤتمر للأطراف دوريا لدراسة التغيرات المهمة في الموضوع، وتجسيدها في محتوى هذه الاتفاقية. وتوفر الفقرة 1 من المادة 69 من اتفاقية الأمم المتحدة لمكافحة الفساد دليلا يسترشد به في هذا الشأن:

"ويبذل مؤتمر الدول الأطراف قصارى جهده للتوصل إلى توافق في الآراء بشأن كل تعديل. وإذا ما استنفدت كل الجهود الرامية إلى تحقيق توافق الآراء دون أن يتسنى التوصل إلى اتفاق، يلزم لاعتماد التعديل، كملجأ أخير، توافر أغلبية ثلثي أصوات الدول الأطراف الحاضرة والمصوتة في اجتماع مؤتمر الدول الأطراف."

3- وينبغي أن يؤخذ في الاعتبار توفير أمثلة للمشاركة والمدخلات من جانب القطاع الخاص والمجتمع المدني والأوساط الأكاديمية.

4- وفيما يتعلق بالولاية القضائية الدولية، ترى أوروغواي أنه ينبغي معالجة مسألة تداخل الولاية القضائية لدولتين أو أكثر مع مراعاة الأولوية الزمنية في التحقيق وتاريخ تقديم الشكوى.

ومع ذلك، إذا أُخطرت دولة طرف أثناء ممارسة ولايتها القضائية على أي فعل مجرم في هذه الاتفاقية، ارتُكب في إقليمها؛ أو على متن سفينة ترفع علمها؛ أو على متن طائرة مسجلة بموجب قوانين تلك الدولة الطرف، أو علمت بطريقة أخرى بأن أي دول أطراف أخرى تجري تحقيقا أو ملاحقة أو تتخذ إجراء قضائيا بشأن الفعل ذاته، وجب على السلطات المختصة في تلك الدول الأطراف أن تتشاور فيما بينها، حسب الاقتضاء، بهدف تنسيق ما تتخذه من إجراءات.

وتتخذ الدولة الطرف أيضا التدابير المقررة في هذه الاتفاقية عندما يكون الجاني موجودا في إقليم بلده ولا يمكن تسليمه استنادا إلى جنسيته. وتحيل الدولة التي يوجد في إقليمها مرتكب الأفعال المجرَّمة في هذه الاتفاقية القضية دون مزيد من الإبطاء إلى سلطاتها المختصة لغرض الملاحقة القانونية وفقا لقانون تلك الدولة.

5- وتمثل مكافحة الجريمة السيبرانية تحديا ملحا حان الوقت لمواجهته، وينبغي التصدي له مع المراعاة التامة لحماية حقوق الإنسان والحريات الأساسية واحترامها وإعمالها.

ويجب أن تُفهم جميع أحكام هذه الاتفاقية وتُستخدم وفقا للالتزامات الدولية ذات الصلة في ميدان حقوق الإنسان. ولذلك، ينبغي أن تكون هناك فقرة استهلالية تؤكد من جديد الإعلان العالمي لحقوق الإنسان، والعهد الدولي الخاص بالحقوق المدنية والسياسية، وغير ذلك من الصكوك ذات الصلة بحقوق الإنسان.