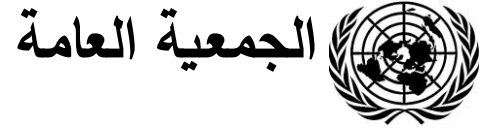


Distr.: General
21 April 2022
Arabic
Original: Arabic/English/French/
Russian/Spanish



اللجنة المخصصة لوضع اتفاقية دولية شاملة
بشأن مكافحة استخدام تكنولوجيا المعلومات
والاتصالات للأغراض الإجرامية
الدورة الثانية
فيينا، 30 أيار/مايو-10 حزيران/يونيه 2022

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

ملخص

تحضيراً للدورة الثانية للجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، أعدت رئيسة اللجنة هذه الوثيقة بدعم من الأمانة. وهي تتألف من المقترحات الواردة من الدول الأعضاء بشأن أحكام التجريم (A/AC.291/9)، والأحكام العامة (A/AC.291/9/Add.1)، وكذلك الأحكام المتعلقة بالتدابير الإجرائية وإنفاذ القانون (A/AC.291/9/Add.2).



المحتويات

الصفحة

3		أولاً - مقدمة
3		ثانياً - التجريم
3		أنغولا
4		أستراليا
7		البرازيل
12		بوروندي
16		كندا
19		كولومبيا
20		مصر
26		السلفادور
30		الاتحاد الأوروبي ودوله الأعضاء
32		غانا
39		إيران (جمهورية - الإسلامية)
40		اليابان
43		الأردن
44		المكسيك
45		نيوزيلندا
50		النرويج
51		الاتحاد الروسي، المقترح مقدم أيضا باسم بيلاروس وبوروندي والصين وطاجيكستان ونيكاراغوا
58		جنوب أفريقيا
63		سويسرا
66		المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية
72		جمهورية تنزانيا المتحدة
73		الولايات المتحدة الأمريكية
78		فنزويلا (جمهورية - البوليفارية)
80		فييت نام

أولاً - مقدمة

- 1- تحضيراً للدورة الثانية للجنة المخصصة لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وتماشياً مع خريطة الطريق وأسلوب عمل اللجنة المخصصة المعتمدين في دورتها الأولى، وخصوصاً الفقرتين 3 و4 منهما، دُعيت الدول الأعضاء إلى أن تقدم إلى الأمانة مشاريع نصوص لفصول أو أحكام تتعلق بالتجريم (A/AC.291/9) وبالأحكام العامة (A/AC.291/9/Add.1) وبالتدابير الإجرائية وإنفاذ القانون (A/AC.291/9/Add.2) حتى يُنظر فيها أثناء الدورة الثانية.
- 2- وعلى هذا الأساس، أعدت رئاسة اللجنة، بدعم من الأمانة، وثيقة التفاوض هذه التي تتضمن جميعاً للمقترحات والمساهمات المقدمة من الدول الأعضاء، مع التركيز على الفصول المحددة التي سيُنظر فيها خلال الدورة الثانية. ولذلك، لا تتضمن هذه الوثيقة سوى اقتراحات صياغية محددة أو تعليقات عامة بشأن الفصول المتعلقة بالتجريم والأحكام العامة والتدابير الإجرائية وإنفاذ القانون، وهي مجمعة على أساس الفصول، بصيغتها الواردة من الدول الأعضاء ومترجمة إلى اللغات الرسمية الست للأمم المتحدة. وما لم يُنكر خلاف ذلك، تتضمن الحواشي نصوصاً وردت من الدول الأعضاء.
- 3- وكما ذكر أعلاه، لا تتضمن هذه الوثيقة تعليقات على مواضيع أخرى أو توضيحات لاقتراحات صياغية محددة، حيث يمكن الاطلاع على تلك التعليقات والتوضيحات في التقارير الأصلية، وهي متاحة على الموقع الشبكي للجنة المخصصة بالشكل الذي وردت به وفي صيغتها الأصلية وقت الاستلام.
- 4- وحتى 14 نيسان/أبريل 2022، تلقت الأمانة 24 تقريراً، تمثل آراء 54 دولة عضواً والاتحاد الأوروبي.

ثانياً - التجريم

أنغولا

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

- ينبغي للاتفاقية أن تصنّف وتجَرّم أخطر سلوكيات الجرائم السيبرانية، ولا سيما عندما تؤثر على البنى التحتية الحيوية، وأن تعتبرها بمثابة إرهاب سيبراني أو جرائم ضد الإنسانية، وأن تحدد قواعد الأولوية والتعجيل في مجال التعاون الدولي على التحقيق مع مرتكبي الجرائم السيبرانية وملاحقتهم قضائياً.
- ينبغي للاتفاقية أن تصنّف وتجَرّم السلوكيات الإجرامية السيبرانية التي تنطوي على استخدام العملات المشفرة والموجودات المشفرة من أجل تمويل الإرهاب وغسل الأموال.

/التجريم

الجرائم المرتكبة في الفضاء السيبراني (الجرائم التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها): الدخول غير المشروع، والاعتراض غير القانوني، وإتلاف البيانات الحاسوبية، وتخريب الحواسيب، والزيف الحاسوبي، والاستتساخ غير القانوني للبرامج الحاسوبية.

الجرائم السيبرانية الأدوات (الجرائم التقليدية المرتكبة باستخدام تكنولوجيا المعلومات والاتصالات): عمليات الاحتيال عبر الإنترنت، والتصيد الاحتيالي، والجرائم الاقتصادية والمالية عبر الإنترنت، وسرقة

الهوية عبر الإنترنت، والاعتداء الجنسي على الأطفال واستغلالهم جنسيا عبر الإنترنت، والتتبع السيبراني، والمطاردة السيبرانية، واستخدام المواد الإباحية لأغراض انتقامية (الإباحية الانتقامية)، والإرهاب السيبراني. ومن أجل بناء مفاهيم هذه الأنواع القانونية من الجرائم، يمكن اللجوء إلى الصكوك القانونية الإقليمية والدولية المذكورة أعلاه⁽¹⁾.

أستراليا

[الأصل: بالإنكليزية]

[13 نيسان/أبريل 2022]

التجريم

تتيح الاتفاقية الجديدة الفرصة لتحسين التعاون الدولي فيما يتعلق بالجرائم السيبرانية، وفي الوقت نفسه ضمان الاتساق مع الاتفاقيات الدولية القائمة المتعلقة بالجريمة وغيرها من الصكوك ذات الصلة وتجنب الازدواجية غير الضرورية. وينبغي أن تكون مواد التجريم متسقة مع الصكوك الدولية القائمة وأن تتجنب التنازع بين تلك الصكوك. وينبغي أيضا موازنة مواد التجريم على النحو المناسب مع احترام سيادة القانون وحقوق الإنسان والحريات الأساسية.

وترى أستراليا أن الاتفاقية الجديدة تتيح فرصة لزيادة المناسبة العالمية للجرائم السيبرانية. وهذا بدوره سيققل من الملاذات الآمنة لمرتكبي الجرائم السيبرانية ويعزز قدرة أجهزة إنفاذ القانون على مكافحة نشاط مرتكبي الجرائم السيبرانية عبر الإنترنت.

وينبغي أن تكون أحكام القانون الجنائي الموضوعية للاتفاقيات الجديدة محددة، وأن تبين بوضوح السلوك الإجرامي الأساسي. وينبغي للاتفاقية أيضا أن تولي الاعتبار الواجب للجرائم الأصلية والمسؤولية الإضافية عن الجرائم المرتكبة في الفضاء السيبراني والجرائم التي ييسرها الفضاء السيبراني. وينبغي أن يشمل ذلك التمديدات المعتمدة لنطاقات المسؤولية الجنائية المنصوص عليها في صكوك مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد.

الجرائم المرتكبة في الفضاء السيبراني

ترى أستراليا أن الاتفاقية الجديدة ينبغي أن تتضمن معايير لتجريم الأفعال الموجهة إلى النظم الحاسوبية ("الجرائم المرتكبة في الفضاء السيبراني"). وتقترح أستراليا إدراج الجرائم التالية المرتكبة في الفضاء السيبراني في الاتفاقية الجديدة:

- الدخول غير المشروع إلى أي جزء من نظام حاسوبي (بما في ذلك البيانات الحاسوبية) دون وجه حق
- الاعتراض غير المشروع لعمليات نقل البيانات الحاسوبية دون وجه حق
- التدخل غير المشروع في البيانات الحاسوبية (بما في ذلك محو البيانات الحاسوبية أو إفسادها أو تحويلها أو طمسها) دون وجه حق

(1) ملحوظة من الأمانة: تحيل هذه الإشارة إلى الصكوك المدرجة تحت العنوان الفرعي "الديباجة" للقرير المقدم من أنغولا، وهي: "اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالاو)، واتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست)، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، واتفاقية الأمم المتحدة لمكافحة الفساد".

- التدخل غير المشروع في عمل نظام حاسوبي أو شبكة حاسوبية
- إنتاج البرمجيات الضارة أو توزيعها أو الحصول عليها لأغراض ارتكاب جريمة سيبرانية أخرى

الجرائم التي يبيّن الفضاء السيبراني ارتكابها

تُعتبر القوانين الجنائية الداخلية القائمة لدى جميع الدول تقريباً كافية لمعاقبة الجرائم المألوفة، بما في ذلك التعدي على ممتلكات الغير والتخريب والسرقة والجرائم المتصلة بالمخدرات وغير ذلك من جرائم العنف.

ولا تحتاج الاتفاقية إلى إعادة تعريف هذه الجرائم لمجرد أنها ارتُكبت بواسطة نظام حاسوبي أو تكنولوجيا رقمية، إذا لم يغير استخدام النظام الحاسوبي في ارتكاب الجريمة طابع السلوك الإجرامي أو مدى خطورته.

بيد أن أستراليا ترى أنّ هناك بعض الجرائم "التقليدية" التي زاد نطاقها وحجمها وسهولة ارتكابها زيادة كبيرة من جراء ما توفره شبكات المعلومات والاتصالات من سرعة وإمكانية إخفاء الهوية وانتشار واسع النطاق. وهذه الجرائم يمكن وصفها بأنها جرائم "يبيّن الفضاء السيبراني ارتكابها". وينبغي للاتفاقية أن تعالج هذه الجرائم بحكمة من خلال وضع إطار واضح لتحديد سبب تغيير بعض الجرائم تغييراً كبيراً من جراء تضمّنها "عنصراً سيبرانياً" بحيث صارت تتطلب معياراً دولياً منسّقاً جديداً يجعل هذا السلوك يتجاوز نطاق الجرائم "التقليدية". وليس لزاماً أن تنشئ الاتفاقية فئات جديدة من الأفعال الإجرامية لكل جريمة قائمة قد تتضمن "عنصراً سيبرانياً"، لا سيما عندما لا يؤثر هذا العنصر تأثيراً كبيراً في شدة السلوك المجرّم أو حجمه أو نطاقه أو سهولة ارتكابه.

وفي حين أن أستراليا تعتقد أن الاتفاقية ينبغي أن تعتمد نهجاً متحفظاً في إدراج أي فئة جديدة من فئات الجرائم، فإنها مستعدة لسماع حجج تؤيد توسيع نطاق الاتفاقية إلى ما هو أبعد من الجرائم المرتكبة في الفضاء السيبراني وبما يشمل "الجرائم التي يبيّن الفضاء السيبراني ارتكابها".

وتحقيقاً لهذه الغاية، لاحظت أستراليا مع التقدير النداءات العديدة التي وُجّهت للتصدي للتهديد الشديد الذي يشكّله الاستغلال الجنسي للأطفال والاعتداء عليهم جنسياً عبر الإنترنت خلال الدورة الأولى للجنة المخصصة. وترى أستراليا أن هذه مسألة يمكن للبلدان أن تتوصل بشأنها بصورة بناءة إلى توافق في الآراء. واعترافاً بخطورة هذا الضرب من الإجماع، قدمت أستراليا بشكل منفصل اقتراحاً بشأن الجرائم التي تشمل الاعتداء على الأطفال عبر الإنترنت، بما في ذلك استمالتهم عبر الإنترنت والبلث المباشر.

وترى أستراليا أيضاً أن الزيادة الكبيرة في معدلات ارتكاب جرائم الاحتيال والسرقة بالاستعانة بالفضاء السيبراني، بما في ذلك جرائم الابتزاز المتصلة باستخدام برمجيات طلب الفدية (الابتزاز ببرمجيات الفدية)، ظاهرة واسعة الانتشار قد تتوصل الدول بشأنها إلى توافق في الآراء لتجريم هذا السلوك لأغراض الاتفاقية.

تجريم أفعال الاعتداء على الأطفال عبر الإنترنت

المادة [ألف] - مواد الاعتداء على الأطفال من خلال نظام حاسوبي

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم السلوكيات التالية في إطار قانونها الوطني في حال ارتكابها عمداً [دون عذر قانوني]⁽²⁾:

(2) أدرج هذا التحفظ لضمان ألا تشمل الجريمة عن غير قصد بعض الحالات المشروعة - على سبيل المثال، عندما تكون هناك ضرورة طبية للاطلاع على مواد أو إنتاج مواد يمكن أن تقع تحت طائلة هذا الحكم في غير هذه الحالة.

(أ) الوصول إلى مواد الاعتداء على الأطفال أو التحكم فيها أو بثها أو توزيعها أو عرضها أو شراؤها أو إنتاجها أو إتاحتها من خلال نظام حاسوبي⁽³⁾؛ أو

(ب) حيازة مواد للاعتداء على الأطفال ناتجة عن السلوك الوارد في الفقرة الفرعية 1 (أ).

2- لأغراض المادة [ألف]، يشمل مصطلح "مواد الاعتداء على الأطفال" المواد التي تصور أو تصف طفلاً، أو تمثيلاً لطفل، على نحو يُفهم منه ضمناً أو يبدو من خلاله أنه يمارس أنشطة جنسية أو يوجد في مكان يمارس فيه شخص أنشطة جنسية، أو أي تصوير للأعضاء الجنسية لطفل⁽⁴⁾ لأغراض جنسية في المقام الأول، أو ضحية للتعذيب أو المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة.

المادة [باء] - تيسير مواد الاعتداء على الأطفال من خلال نظام حاسوبي

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في إطار قانونها الوطني في حال ارتكابها عمداً [دون عنر قانوني]⁽⁵⁾: إنشاء نظام حاسوبي لأغراض تيسير مواد الاعتداء على الأطفال على النحو المحدد في المادة [ألف] أو تطوير نظام حاسوبي أو تحويله أو تعهده أو التحكم فيه أو الإشراف عليه أو مساعدته⁽⁶⁾ أو إتاحتها أو الإعلان عنه أو ترويجه لمثل تلك الأغراض.

2- لأغراض الفقرة 1، يشمل مصطلح "تيسير الاعتداء على الأطفال" ارتكاب أي من السلوكيات المبينة في الفقرة 1 بهدف السماح للأشخاص بالوصول إلى "مواد الاعتداء على الأطفال" أو بثها أو توزيعها أو عرضها أو إتاحتها أو إنتاجها للنفس أو للغير.

المادة [جيم] - استمالة الأطفال أو جلبهم لأغراض جنسية من خلال نظام حاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في إطار قانونها الوطني في حال ارتكابها عمداً عن طريق [نظام حاسوبي]: استمالة طفل كي يلتقي بأشخاص يمارسون أنشطة جنسية أو كي يشهد تلك الأنشطة أو يشارك فيها أو عرض ذلك عليه أو جلب طفل أو التسبب في جلبه من أجل ذلك.

(3) يُعرّف "النظام الحاسوبي" بأنه جهاز يعالج البيانات أوتوماتياً وفقاً لبرنامج ما أو مجموعة من الأجهزة المترابطة أو المتصلة يقوم واحد أو أكثر منها بمعالجة البيانات أوتوماتياً وفقاً لبرنامج ما. وقد يشمل النظام مرافق للإدخال والإخراج والتخزين، كما قد يكون مستقلاً أو متصلاً عبر شبكة بأجهزة أخرى. ويلاحظ أن هذا المصطلح (أو تعريفه) يمكن تغييره لضمان الاتساق مع الأحكام الأخرى من مشروع الاتفاقية.

وقد تشمل المواد المولدة ذاتياً مواد مولدة ذاتياً بصفة بحتة، وكذلك مواد مولدة ذاتياً بالإكراه أو الابتزاز. وفي هذه السياقات، يهدف الحكم إلى توفير موقف عام يتوخى المزيد من الحذر في التجريم مع ترك الأمر للنظم القانونية الداخلية لاتخاذ قرارات متناسبة ومعقولة في هذا الشأن.

(4) المصطلحات مستقاة من البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية.

(5) وفقاً للحاشية 21.

(6) يمكن استيعاب شق "المساعدة" في نهاية المطاف من خلال تمديد نطاق الأحكام العامة للمسؤولية الجنائية. ويبقى الأمر على ذلك إلى أن يُنظر في تلك الأحكام.

المادة [س] - أحكام عامة تتعلق بالمقترح

- 1- لأغراض المواد [ألف وباء وجيم]، يشمل مصطلح "الطفل" جميع الأشخاص الذين تقل أعمارهم عن 18 عاما. وإضافةً إلى ذلك، يشمل مصطلح "الطفل" أيضا، لأغراض المادة جيم، أي شخص يُعتقد أنه دون الثامنة عشرة⁽⁷⁾. غير أنه يجوز للدولة الطرف، لأغراض المواد [ألف وباء وجيم]، أن تشترط حداً عمرياً أقل، على ألا ينقص عن السادسة عشرة.
- 2- لأغراض المواد [ألف وباء وجيم]، تسري المسؤولية الجنائية على الأشخاص الذين تبلغ أعمارهم 18 عاما فأكثر. ويجوز لكل دولة طرف أن تعلن في أي وقت سريان تلك المسؤولية الجنائية على الأشخاص الذين تقل أعمارهم عن 18 عاما. وإذا أعلنت دولة طرف ذلك، فعليها أن تكفل وجود ضمانات مناسبة في قانونها الوطني لحماية الطفل المتهم، مع ملاحظة ما قد يترتب على إخضاع طفل لإجراءات العدالة الجنائية من آثار.
- 3- حيثما تسعى دولة طرف إلى توجيه تهم جنائية إلى أشخاص تقل أعمارهم عن 18 عاما بموجب المادة ألف، تراعي على النحو الواجب تجنب الإفراط في توجيه التهم الجنائية إلى الأطفال الذين تُضبط بحوزتهم مواد ذاتية الصنع بموجب الفقرة 2 من المادة [ألف]، والحاجة إلى احترام التزاماتها بموجب اتفاقية حقوق الطفل وبروتوكولاتها.

العقوبات المناسبة

نقترح إدراج مادة تنص على التزام الدول الأطراف باعتماد تدابير تشريعية أو تدابير أخرى ضرورية لضمان أن يعاقب على أي أفعال مجرّمة بموجب هذه الاتفاقية بتدابير فعالة ومتناسبة وراذعة، قد تشمل الحرمان من الحرية.

البرازيل

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

الفصل الثاني

التجريم

المادة 4

الدخول غير المشروع⁽⁸⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: النفاذ الكامل أو الجزئي إلى نظام حاسوبي. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة وقوع مخالفة للتدابير الأمنية بقصد الحصول على بيانات حاسوبية أو بنية سيئة أخرى أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

(7) تهدف إضافة صفة الاعتقاد هنا إلى تغطية الحالات التي يتعامل فيها شخص موضع للشبهات أو تُجمع عنه تحريات بسبب ضلوعه في استمالة الأطفال أو جلبهم لأغراض جنسية مع موظف معني بإنفاذ القانون عبر الإنترنت يعمل بصفة سرية.

(8) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست).

المادة 5

التدخل في البيانات⁽⁹⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمدا وبغير وجه حق: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تعديلها أو طمسها. ويجوز للدولة الطرف أن تحتفظ بحقها في اشتراط أن تتسبب الأفعال المشار إليها أعلاه في ضرر جسيم.

المادة 6

التدخل في النظم⁽¹⁰⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتُكبت عمدا وبغير وجه حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

المادة 7

الاعتراض غير المشروع⁽¹¹⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتُكبت عمدا وبغير وجه حق: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 8

الاحتيال الحاسوبي⁽¹²⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُجرّم في قانونها الوطني التسبب عمدا وبغير وجه حق في إلحاق خسائر بممتلكات الغير عن طريق:

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

(ب) أي تدخل في عمل نظام حاسوبي،

بقصد الاحتيال أو بنية سيئة، للحصول، بدون وجه حق، على منفعة اقتصادية للنفس أو للغير.

(9) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

(10) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

(11) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

(12) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

المادة 9

الوصول غير المشروع إلى كلمات المرور وبيانات الاعتماد⁽¹³⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمداً: شراء كلمات المرور أو بيانات الاعتماد للدخول إلى نظام حاسوبي أو الحصول عليهما أو تلقيهما بغير وجه حق.

المادة 10

إساءة استخدام الأجهزة⁽¹⁴⁾

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمداً وبغير وجه حق:

(أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

‘1’ جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملاءمته مبدئياً، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 4 إلى 9؛

‘2’ كلمة سر خاصة بحاسوب، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها الدخول بشكل كامل أو جزئي إلى نظام حاسوبي؛

بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 4 إلى 9؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة 1 (أ) ‘1’ أو ‘2’ أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 4 إلى 9. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية بموجب القانون الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 4 إلى 9 من هذه الاتفاقية، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

3- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقاً بعمليات بيع الأشياء المشار إليها في الفقرة 1 (أ) ‘2’ من هذه المادة أو توزيعها أو إتاحتها بطريقة أخرى.

(13) المصدر: اقتراح البرازيل الأصلي.

(14) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

المادة 11

التزوير الحاسوبي⁽¹⁵⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق: إدخال بيانات حاسوبية أو تغييرها أو حذفها أو إتلافها، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة مشابهة.

المادة 12

الجرائم ذات الصلة بالمواد الإباحية المتعلقة بالأطفال⁽¹⁶⁾

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:

- (أ) إنتاج مواد إباحية متعلقة بالأطفال بغرض توزيعها عبر نظام حاسوبي؛
- (ب) عرض مواد إباحية متعلقة بالأطفال أو إتاحتها عبر نظام حاسوبي؛
- (ج) توزيع مواد إباحية متعلقة بالأطفال أو بثها عبر نظام حاسوبي؛
- (د) اقتناء مواد إباحية متعلقة بالأطفال عبر نظام حاسوبي للنفس أو للغير؛
- (هـ) حيازة مواد إباحية متعلقة بالأطفال داخل نظام حاسوبي أو على وسيط لتخزين البيانات الحاسوبية.

2- لغرض الفقرة 1 أعلاه، يشمل مصطلح "المواد الإباحية متعلقة بالأطفال" المواد الإباحية التي تعرض بشكل مرئي:

- (أ) قاصرا وهو يمارس سلوكا جنسيا صريحا؛
 - (ب) شخصا يبدو قاصرا وهو يمارس سلوكا جنسيا صريحا؛
 - (ج) صورا واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا صريحا.
- 3- لأغراض الفقرة 2 أعلاه، يشمل مصطلح "قاصر" أي شخص دون سن الثامنة عشرة. ويجوز لأي دولة طرف أن تشترط حدا عمريا أدنى لا يقل عن سن السادسة عشرة.
- 4- يجوز لكل دولة طرف أن تحتفظ بالحق في عدم التطبيق، الكلي أو الجزئي، للبندين (د) و(هـ) من الفقرة 1 والبندين (ب) و(ج) من الفقرة 2.

(15) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

(16) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

المادة 13

التشجيع على الانتحار أو الإكراه عليه⁽¹⁷⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني: تشجيع الأشخاص، بمن فيهم القصر، على الانتحار أو إكراههم عليه، من خلال ممارسة الضغط النفسي أو غيره من أنواع الضغط في شبكات المعلومات والاتصالات، بما فيها الإنترنت.

المادة 14

انتهاك حقوق التأليف والنشر والحقوق المجاورة عن طريق تكنولوجيا المعلومات والاتصالات⁽¹⁸⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي تُعتبر السلوكيات التالية جريمة أو فعلاً غير مشروع آخر بموجب قانونها الوطني: انتهاك حقوق التأليف والنشر والحقوق المجاورة وفق تعريفها في تشريعات تلك الدولة الطرف، وذلك إذا ارتُكبت تلك الأفعال عن قصد بواسطة تكنولوجيا المعلومات والاتصالات، بما في ذلك الاستخدام غير المشروع للبرمجيات لاستغلال نظم أو قواعد بيانات حاسوبية محمية بحقوق التأليف والنشر وانتحال مؤلفات الغير.

المادة 15

الشروع والمساعدة والتحريض⁽¹⁹⁾

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمداً: المساعدة في ارتكاب أي من الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية أو التحريض على ذلك.
- 2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتُكبت عمداً: الشروع في ارتكاب أي جريمة من الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية.
- 3- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 2 من هذه المادة كلياً أو جزئياً.

المادة 16

مسؤولية الشركات⁽²⁰⁾

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لضمان مساءلة الأشخاص الاعتباريين عن الجرائم المنصوص عليها في هذه الاتفاقية التي تُرتكب لمصلحتهم من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو باعتباره عضواً في هيئة تابعة للشخص الاعتباري يتبوأ منصبا قياديا داخلها، وذلك بناء على:

(أ) سلطة تمثيل الشخص الاعتباري؛

(17) المصدر: اقتراح مقدم من الاتحاد الروسي والصين.

(18) المصدر: اقتراح مقدم من الاتحاد الروسي والصين.

(19) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مع تغييرات أجرتها البرازيل.

(20) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

(ب) سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛

(ج) سلطة ممارسة الرقابة لدى الشخص الاعتباري.

2- إضافة إلى الحالات المنصوص عليها في الفقرة 1 من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان إمكانية تحميل الشخص الاعتباري المسؤولية في حال ما إذا ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 في ارتكاب جريمة منصوص عليها وفقاً لهذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.

3- رهنا بالمبادئ القانونية للدولة الطرف، يمكن أن تكون المسؤولية القانونية للشخص الاعتباري جنائية أو مدنية أو إدارية.

4- لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

المادة 17

العقوبات والتدابير⁽²¹⁾

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية مُعاقَب عليها بعقوبات فعالة ومتناسبة وراذعة، بما في ذلك العقوبات السالبة للحرية.

2- تضمن كل دولة طرف مساءلة الأشخاص الاعتباريين وفقاً للمادة 16 وإخضاعهم لعقوبات أو تدابير فعالة ومتناسبة وراذعة، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات النقدية.

بوروندي

[الأصل: بالفرنسية]

[8 نيسان/أبريل 2022]

الفصل الثاني - الجرائم التي تمس سرية البيانات والنظم الحاسوبية وسلامتها وتوافرها

المادة 1

الأفعال الموجهة ضد سرية النظم الحاسوبية

المادة 2

الدخول غير المشروع

تجرم الدول الأطراف في هذه الاتفاقية، بمقتضى قوانينها الداخلية، القيام عمداً وبغير وجه حق بالدخول كلياً أو جزئياً إلى النظم الحاسوبية.

(21) المصدر: اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية.

المادة 3

التدخل في نظام حاسوبي

تجرّم الدول الأطراف في هذه الاتفاقية، بمقتضى قوانينها الداخلية، القيام عمدا وبغير وجه حق بإتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.

المادة 4

التدخل في البيانات

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، القيام عمدا وبغير وجه حق بتعويق عمل أي نظام حاسوبي على نحو خطير عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

المادة 5

صنع نظام حاسوبي أو بيعه أو شرائه أو استخدامه أو استيراده أو توزيعه أو حيازته بصورة غير مشروعة والتشجيع على الانتحار

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، القيام بصنع حواسيب أو نظم حاسوبية أو بيعها أو شرائها أو استعمالها أو استيرادها أو توزيعها أو حيازتها أو القيام بتوفير بيانات أو برامج أو نظم حاسوبية بغية استخدامها أو إتاحتها للغير، لغرض ارتكاب جرائم.

المادة 6

الاحتيال الحاسوبي

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، التسبب عمدا وبغير وجه حق في إلحاق خسائر بممتلكات الغير عن طريق: (أ) إدخال بيانات حاسوبية أو تحويلها أو حذفها أو طمسها، أو (ب) أي تدخل في وظيفة نظام حاسوبي، بقصد الاحتيال أو بنوايا إجرامية، للحصول على منفعة مالية غير مستحقة للنفس أو للغير.

(1) الاحتيال في النظم الحاسوبية

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، استخدام مخطط احتيالي، عن طريق الاتصال الإلكتروني، للحصول على أموال أو ممتلكات منقولة أو سندات أو ودائع أو أدوات أو تعهدات أو إيصالات أو إصدارات أو كل ممتلكات شخص آخر أو أي جزء منها، أو الشروع في ذلك.

(2) سرقة الهوية الرقمية

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، انتحال الهوية الرقمية لشخص آخر أو استخدام عنصر أو أكثر من عناصر البيانات من أي نوع بما يحدد هوية ذلك الشخص بقصد إزعاجه أو المساس بسمعته أو خصوصياته أو ممتلكاته أو سمعة أو خصوصيات أو ممتلكات طرف ثالث بهدف تحقيق مكاسب أو من أجل تضليل أشخاص آخرين.

(3) التصيد الاحتيالي

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، استخدام موقع شبكي أو إرسال رسالة إلكترونية بمساعدة نظام حاسوبي بقصد الحصول على معلومات سرية ممن يزور الموقع الشبكي أو يتلقى الرسالة من أجل استخدام تلك المعلومات لأغراض إجرامية.

(4) خيانة الأمانة فيما يتعلق بالبيانات الحاسوبية

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، قيام شخص باختلاس أو تبديد أي بيانات حاسوبية يعهد بها إليه على سبيل الإعارة على أساس أنه سيعيدها ثانية أو سيستخدمها لغرض محدد.

(5) التلقي غير القانوني لبيانات حاسوبية

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، حيازة أي بيانات حاسوبية يتم الحصول عليها عن طريق ارتكاب جريمة، أيا كانت صفة هذه الحيازة، مع العلم بكيفية الحصول على البيانات.

(6) ابتزاز البيانات الحاسوبية

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، السعي إلى الحصول على بيانات حاسوبية بالقوة أو العنف أو الإكراه.

(7) الابتزاز ونشر الشائعات

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، القيام بتوجيه تهديدات كتابية أو شفوية، أو الإدلاء ببيانات كاشفة أو تشهيرية، أو ابتزاز بيانات حاسوبية أو الشروع في ابتزازها.

(8) الرسائل التطفلية

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، الأفعال التالية:

- 1- إرسال رسائل غير مطلوبة بشكل متكرر أو إلى عدد كبير من الأشخاص باستخدام حاسوب أو نظام حاسوبي؛
- 2- استخدام حاسوب أو نظام حاسوبي لإعادة توجيه رسالة مستلمة إلى عدة أشخاص أو لإعادة إرسالها عدة مرات إلى شخص لا يحتاج إليها.

المادة 7

جرائم المحتوى

1- الجرائم ذات الصلة بالمواد الإباحية المتعلقة بالأطفال

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، القيام عمدا وبغير وجه حق بإنتاج مواد إباحية متعلقة بالأطفال بغرض توزيعها عبر نظام حاسوبي أو عرض مواد إباحية متعلقة بالأطفال أو إتاحتها عبر نظام ما.

المادة 8

نشر النصوص والصور العنصرية أو المعادية للأجانب من خلال نظام حاسوبي

تجرم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، إنشاء أو تنزيل أو نشر أو إتاحة نص أو رسائل أو صور فوتوغرافية أو رسومات أو فيديوهات أو أي تمثيل آخر لأفكار أو نظريات ذات طابع عنصري أو كاره للأجانب بأي شكل من الأشكال بواسطة نظام حاسوبي.

المادة 9

توجيه الإهانات بواسطة نظام حاسوبي

تجرم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، إهانة أي شخص بسبب انتمائه إلى جماعة تتميز بعرق أو لون أو نسب أو أصل قومي أو إثني أو دين ما، إذا استعمل ذلك ذريعة لأي من هذه العوامل، أو مجموعة من الأشخاص الذين يتميزون بأي من هذه الخصائص.

المادة 10

الجرائم المتصلة بالإرهاب أو صنع الأسلحة أو الاتجار بالأشخاص أو المخدرات المرتكبة بمساعدة حاسوب أو نظام حاسوبي

(1) إنشاء أو نشر موقع لجماعات إرهابية

تجرم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، ما يلي:

- 1- إنشاء أو نشر أو استخدام موقع شبكي لجماعة إرهابية بمساعدة الإنترنت أو حاسوب أو نظام حاسوبي من أجل تسهيل اتصالات قيادتها أو أعضائها؛
- 2- جمع الأموال من أجلها أو نشر أفكارها أو التعريف بكيفية إدارتها لعملياتها الإرهابية.

(2) التعريف بأساليب أو وسائل التدمير

تجرم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، القيام بنشر أو إتاحة أي تعليمات بشأن استخدام الأسلحة النارية، من الأنواع التي يمكن أن تلحق الضرر بالأرواح أو الممتلكات أو البيئة، وأجزائها ومكوناتها وذخيرتها، أو بشأن أساليب صنعها، عن طريق نظام حاسوبي لفائدة أشخاص من غير المأذون لهم بالاطلاع عليها.

(3) إنشاء أو نشر موقع لغرض الاتجار بالبشر

تجرم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، إنشاء أو نشر موقع على شبكة معلومات أو معدات حاسوبية أو نظام حاسوبي لغرض الاتجار بالأشخاص أو تيسير تلك المعاملات.

(4) إنشاء أو نشر موقع بغرض الاتجار بالمؤثرات العقلية أو العقاقير المخدرة أو توزيعها

تجرم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، إنشاء أو نشر موقع على شبكة معلومات أو معدات حاسوبية أو نظام حاسوبي لغرض الاتجار بالمؤثرات العقلية أو العقاقير المخدرة أو توزيعها أو تيسير تلك المعاملات.

المادة 11

التواطؤ الجنائي الحاسوبي

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، الاشتراك المتعمد في تشكيل عصابي أو في تأمر بغرض الإعداد لجريمة واحدة أو أكثر أو ارتكابها.

المادة 12

الجرائم المتعلقة بالتعدي على حقوق الملكية الفكرية والحقوق المجاورة

تجرّم الدول الأطراف في هذه الاتفاقية، دون إخلال بقوانينها الداخلية، أي انتهاك لحقوق الملكية الفكرية.

الفصل الثالث - مسؤولية الشخصيات الاعتبارية

تتخذ الدول الأطراف في هذه الاتفاقية ما قد يلزم من ترتيبات لضمان تحميل الأشخاص الاعتباريين المسؤولية عن الأفعال المجرمة بموجب هذه الاتفاقية.

اتخاذ التدابير اللازمة لضمان إمكانية تحميل الشخص الاعتباري المسؤولية عن عدم وجود إشراف أو رقابة من جانب شخص طبيعي يعمل لديه. ويمكن أن تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية.

كندا

[الأصل: بالإنكليزية]

[9 نيسان/أبريل 2022]

الجرائم

الدخول غير المشروع إلى نظام حاسوبي

تجرّم الدخول إلى نظام حاسوبي بالكامل أو جزئياً، عن طريق الاحتيال وبغير وجه حق.

الاعتراض غير القانوني للإرسال غير العمومي لبيانات نظام حاسوبي

تجرّم القيام، عن طريق الاحتيال وبغير وجه حق، باعتراض عمليات الإرسال غير العمومية للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية من نظام حاسوبي يحمل تلك البيانات، بأي وسيلة تقنية.

التدخل في البيانات الحاسوبية

تجرّم الأفعال التالية إذا ما ارتكبت عمداً وبغير وجه حق: إتلاف البيانات الحاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.

التدخل في النظم الحاسوبية

تجرّم القيام عمداً وبغير وجه حق بإعاقة عمل النظم الحاسوبية على نحو خطير عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

إساءة استعمال الأجهزة

1- تجريم الأفعال التالية إذا ما ارتُكبت عمدا وبغير وجه حق:

(أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

'1' جهاز، بما في ذلك برنامج حاسوبي، صُمِمَ أو طُوِّعَ ابتداءً، بغرض ارتكاب أي من الجرائم السيبرانية الواردة في هذه الاتفاقية؛

'2' كلمة سر خاصة بحاسوب، أو رمز الولوح، أو بيانات مماثلة يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو أي جزء منها، بغرض ارتكاب أي من الجرائم السيبرانية الواردة في الاتفاقية؛

(ب) حيازة أحد الأشياء المشار إليها بالفقرة 1 (أ) '1' أو '2'، بغرض ارتكاب أي من الجرائم السيبرانية الواردة في هذه الاتفاقية.

2- لا يجوز تفسير هذه المادة على أنها ترتب مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو التوفير بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم السيبرانية الواردة في هذه الاتفاقية، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

الجرائم المتصلة بالاستغلال الجنسي للأطفال

1- تجريم السلوكيات التالية إذا ما ارتُكبت عمدا وبغير وجه حق:

(أ) إنتاج مواد الاستغلال الجنسي للأطفال بغرض توزيعها عبر نظام حاسوبي؛

(ب) عرض مواد الاستغلال الجنسي للأطفال أو الإعلان عنها أو إتاحتها عبر نظام حاسوبي؛

(ج) توزيع مواد الاستغلال الجنسي للأطفال أو بثها عبر نظام حاسوبي؛

(د) اقتناء مواد الاستغلال الجنسي للأطفال عبر نظام حاسوبي للنفس أو للغير؛

(هـ) الوصول إلى مواد الاستغلال الجنسي للأطفال أو حيازتها داخل نظام حاسوبي أو على وسيط لتخزين البيانات الحاسوبية.

2- لأغراض الفقرة 1، يشمل مصطلح "مواد الاستغلال الجنسي للأطفال" المواد الإباحية المتعلقة بالأطفال وفق تعريفها في البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية، وأيا مما يلي:

(أ) المواد المرئية، بما في ذلك الوسائط الفوتوغرافية والفيديوية ووسائط البث المباشر، التي تصور:

'1' طفلا يمارس نشاطا جنسيا أو يشهده،

'2' شخصا يبدو طفلا وهو يمارس نشاطا جنسيا أو يشهده،

'3' صورا واقعية تُظهر طفلا يمارس نشاطا جنسيا أو يشهده؛

(ب) المواد المكتوبة التي:

- '1' تدعو إلى ممارسة النشاط الجنسي مع طفل،
- '2' تكون مكتوبة لغرض جنسي وتقوم سمتها المهيمنة على وصف النشاط الجنسي مع طفل؛
- (ج) التسجيلات الصوتية التي:
- '1' تدعو إلى ممارسة النشاط الجنسي مع طفل،
- '2' تكون مسجلة لغرض جنسي وتقوم سمتها المهيمنة على وصف النشاط الجنسي مع طفل.

استمالة طفل واستدراجه

- 1- تجريم السلوكيات التالية إذا ما ارتكبت عمدا وبغير وجه حق:
- (أ) بث مواد جنسية صريحة من خلال نظام حاسوبي لطفل أو شخص يُعتقد أنه طفل، أو توزيع تلك المواد أو بيعها أو إتاحتها؛ أو
- (ب) التواصل مع طفل، أو شخص يُعتقد أنه طفل، من خلال نظام حاسوبي؛ أو
- (ج) الاتفاق مع طفل، أو شخص يُعتقد أنه طفل، أو اتخاذ ترتيبات معه من خلال نظام حاسوبي؛
- لغرض تيسير ارتكاب أي من جرائم الاستغلال الجنسي للأطفال المنصوص عليها في هذه الاتفاقية، أو البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية، أو القانون الوطني للدولة الطرف.
- 2- لا تقع أي مسؤولية جنائية على الشخص إذا اتخذ خطوات معقولة للتأكد من أن الشخص ليس طفلا.

النشر غير التوافقي للصور الحميمة ("المواد الإباحية الانتقامية")

- 1- تجريم الأفعال التالية إذا ما ارتكبت عمدا وبغير وجه حق: نشر صورة حميمة لشخص ما بأي وسيلة من وسائل النظم الحاسوبية، أو توزيعها أو بثها أو بيعها أو إتاحتها أو الإعلان عنها، مع العلم بأن الشخص المصور في الصورة لم يعط موافقته على ذلك السلوك، أو دون الالتفات إلى ما إذا كان ذلك الشخص قد أعطى موافقته على ذلك السلوك أم لا.
- 2- لأغراض الفقرة 1، تعني الصورة الحميمة تسجيلاً مرئياً لشخص ما صُنِعَ بأي وسيلة، بما في ذلك تسجيل فوتوغرافي أو سينمائي أو فيديو:
- (أ) يكون فيه الشخص عارياً، أو كاشفاً عن أعضائه التناسلية أو منطقة الشرج أو الثديين، أو يمارس نشاطاً جنسياً صريحاً؛
- (ب) كانت ثمة ظروف بشأنه، وقت التسجيل، تدعو إلى توقع درجة معقولة من الخصوصية؛
- (ج) يتوقع الشخص المصور بشأنه درجة معقولة من الخصوصية وقت ارتكاب الجريمة.
- 3- لا تترتب أي مسؤولية جنائية إذا كان النشر غير التوافقي من أجل الصالح العام أو له غرض مشروع.

كولومبيا

[الأصل: بالإسبانية]

[8 نيسان/أبريل 2022]

3- التجريم

فيما يتعلق بالجرائم المرتكبة في الفضاء السيبراني، ينبغي لكل دولة عضو أن تعتمد ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في نظامها القانوني الداخلي:

- (أ) الدخول غير القانوني: الدخول الكامل أو الجزئي بغير وجه حق إلى نظام حاسوبي⁽²²⁾.
 - (ب) الاعتراض غير القانوني: الاعتراض بغير وجه حق للبيانات الحاسوبية، سواء في مصدرها أو وجهتها أو داخل نظام حاسوبي، أو في الانبعاثات الكهرومغناطيسية من نظام حاسوبي يحمل هذه البيانات⁽²³⁾.
 - (ج) التدخل في البيانات: إتلاف أو تدمير أو حذف أو إفساد أو تحوير أو طمس بيانات حاسوبية أو نظام معالجة معلومات أو مكوناته أو أجزائه المنطقية⁽²⁴⁾.
 - (د) التدخل في النظم: إعاقة عمل نظام حاسوبي أو البيانات الواردة فيه أو شبكة اتصالات أو إعاقة الوصول العادي إلى ذلك النظام أو بياناته أو تلك الشبكة دون وجه حق⁽²⁵⁾.
 - (هـ) إساءة استعمال الأجهزة: إنتاج جهاز، بما في ذلك برنامج حاسوبي أو كلمة مرور حاسوبية أو رمز الولوح أو بيانات مماثلة يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو أي جزء منها، بغرض ارتكاب أي من الجرائم المشار إليها في الفقرات (أ) و(ب) و(ج) و(د) من هذا القسم أو شراؤه أو حيازته أو توزيعه أو الاتجار به⁽²⁶⁾.
 - (و) التزوير الحاسوبي: إدخال بيانات حاسوبية أو تحويرها أو حذفها أو طمسها عن عمد ودون وجه حق بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو استخدامها لأغراض قانونية⁽²⁷⁾.
- وفيما يتعلق بالجرائم التي يبيّن الفضاء السيبراني ارتكابها، ينبغي لكل دولة عضو أن تعتمد ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في نظامها القانوني الداخلي:
- (أ) الجرائم المتعلقة بمواد الاعتداء الجنسي على الأطفال: إنتاج مواد الاعتداء الجنسي على الأطفال أو عرضها أو توزيعها أو بثها أو شراؤها من خلال نظام حاسوبي أو حيازتها فيه⁽²⁸⁾.

(22) المادة 2 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية. تماشيا مع المادة 269 ألف من القانون رقم 1273 لسنة 2009.

(23) المادة 3 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية. تماشيا مع المادة 269 جيم من القانون رقم 1273 لسنة 2009.

(24) المادة 4 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية. تماشيا مع المادة 269 دال من القانون رقم 1273 لسنة 2009.

(25) المادة 5 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية. تماشيا مع المادة 269 باء من القانون رقم 1273 لسنة 2009.

(26) المادة 6 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية.

(27) المادة 7 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية.

(28) المادة 9 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية.

(ب) الاحتيال الحاسوبي: إدخال بيانات حاسوبية أو تحويلها أو حذفها أو طمسها، أو التدخل في عمل نظام حاسوبي، بقصد الاحتيال أو بنية إجرامية للحصول، دون وجه حق، على منفعة اقتصادية للنفس أو للغير على حساب ممتلكات شخص آخر⁽²⁹⁾.

(ج) انتهاك البيانات الشخصية: الحصول غير المصرح به على البيانات الشخصية الواردة في الملفات أو الأرشفات أو قواعد البيانات أو الوسائط المماثلة أو تجميعها أو إزالتها أو عرضها أو بيعها أو تبادلها أو إرسالها أو شراؤها أو اعتراضها أو الكشف عنها أو تعديلها أو استخدامها، لتحقيق مكاسب شخصية أو لمنفعة طرف ثالث⁽³⁰⁾.

الأشخاص الطبيعيون والعقوبات النقدية في حالة الأشخاص الاعتباريين⁽³¹⁾.

مصر

[الأصل: بالعربية]

[8 نيسان/أبريل 2022]

الفصل الثاني:

التجريم والإجراءات الجنائية وإنفاذ القانون

المادة 5

التجريم

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لمنع ارتكاب الجرائم المنصوص عليها في هذه الاتفاقية أو أية جرائم أخرى ترتكب بواسطة تكنولوجيا المعلومات والاتصال، بما في ذلك حجب وإزالة المحتوى المرتبط بهذه الجرائم مع التأكيد على أهمية مبدأ الحيادية التكنولوجية، واكتشافها وملاحقة مرتكبيها ومقاضاتهم وتسليم المجرمين وتسهيل إجراءات التعاون الدولي وجمع الأدلة فيها.
- 2- تعتمد أيضا كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية:

المادة 6

الانتفاع أو تسهيل الانتفاع بدون وجه حق بخدمات الاتصال والمعلومات وتقنياتها

كل من انتفع أو سهل للغير بغير وجه حق الانتفاع بخدمات الاتصالات أو قنوات البث المسموعة أو المرئية، وذلك عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات واتصالات.

(29) المادة 8 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية.

(30) المادة 269 واو من القانون رقم 1773 لسنة 2009.

(31) المادة 13 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية تتسق مع المادة 30 من اتفاقية الأمم المتحدة لمكافحة الفساد والمادة 11 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

المادة 7

الدخول غير المشروع و/أو تجاوز حدود الحق في الدخول

- 1- كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول.
- 2- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
- 3- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:
 - (أ) محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.
 - (ب) الحصول على معلومات حكومية سرية.

المادة 8

الاعتداء على تصميم موقع

كل من أتلف أو عطل أو أبطأ أو شوّه أو أخفى أو غير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق.

المادة 9

الاعتراض غير المشروع

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

المادة 10

الاعتداء على سلامة البيانات

تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصداً وبدون وجه حق.

المادة 11

إساءة استخدام وسائل تقنية المعلومات

إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير أو حيازة أية أدوات أو برامج مصممة أو مكيفة أو كلمة سر أو معلومات مشابهة يتم بواسطتها دخول نظام المعلومات بقصد استخدامها لارتكاب إحدى الجرائم المنصوص عليها بموجب تلك الاتفاقية، أو إنشاء البرمجيات الخبيثة التي يقصد بها تدمير أو حجب أو تعديل أو نسخ أو نشر المعلومات الرقمية أو تحييد سماتها الأمنية، باستثناء البحوث المشروعة.

المادة 12

التزوير

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

المادة 13

الاحتيال

التسبب في إلحاق الضرر بالمستفيدين والمستخدمين - عن قصد وبدون وجه حق - بنية الاحتيال لتحقيق مصالح ومنافع بطريقة غير مشروعة، للفاعل أو للغير، بما في ذلك من خلال جرائم احتيالية إلكترونية متعلقة بالعملات الافتراضية (الرقمية أو المشفرة).

المادة 14

التهديد والابتزاز

استخدام تكنولوجيا المعلومات والاتصالات أو أية وسيلة تقنية أخرى في التهديد أو الابتزاز لحمل شخص على ارتكاب فعل أو الامتناع عنه.

المادة 15

الإباحية

- 1- إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية بغرض الدعاية واستغلال السيدات والقصر من خلال تقنيات الاتصالات والمعلومات وفقا للقانون الداخلي لكل دولة.
- 2- إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية عن الأطفال والقُصر، بما في ذلك حيازة مواد إباحية أو مخلة بالحياء عن الأطفال والقصر، باستخدام تقنيات الاتصالات والمعلومات أو وسيط تخزين تلك التقنيات.

المادة 16

الجرائم الأخرى المرتبطة بالإباحية

ضروب الاستغلال الجنسي أو التحرش، لاسيما المتعلقة بالنساء والأطفال والقُصر.

المادة 17

التشجيع على الانتحار أو الإكراه عليه

تشجيع الانتحار أو الإكراه عليه، بما في ذلك انتحار الأطفال، عن طريق الضغط النفسي أو غيره من الضغوط على شبكات المعلومات والاتصالات، بما فيها شبكة الإنترنت، سواء كان ذلك عن طريق التعامل المباشر أو عن طريق التقنيات الحديثة والألعاب الإلكترونية.

المادة 18

تورط الأطفال في ارتكاب أعمال غير مشروعة

تورط القُصر، عن طريق تكنولوجيا المعلومات والاتصالات، في ارتكاب أفعال غير مشروعة تعرض حياتهم أو صحتهم الجسدية والنفسية للخطر.

المادة 19

الاعتداء على حرمة الحياة الخاصة

وذلك بواسطة تكنولوجيا المعلومات والاتصالات، بما في ذلك تجريم كل من اصطنع بريدا إلكترونيا أو موقعا أو حسابا خاصا ونسبه زورا إلى شخص طبيعي أو اعتباري.

المادة 20

الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات

- 1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها أو تبريرها.
- 2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، وتوفير الدعم اللوجستي لمرتكبيها.
- 3- نشر طرائق صناعة المتفجرات التي تستخدم خاصة في عمليات إرهابية.
- 4- إثارة النعرات ونشر الفتن والكراهية والعنصرية.
- 5- تتخذ الدول التدابير اللازمة لمنع نشر هذا المحتوى على وسائل تكنولوجيا المعلومات والاتصال، بما في ذلك حجب وإزالة المحتوى المرتبط بهذه الجرائم.

المادة 21

الجرائم المالية بما في ذلك الجرائم المتعلقة بغسل الأموال

- 1- استخدام تكنولوجيا المعلومات والاتصالات لارتكاب أية جرائم مالية وإساءة استخدام العملات الافتراضية (الرقمية والمشفرة).
- 2- القيام بعمليات غسل أموال، أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

المادة 22

الاستخدام غير المشروع لأدوات الدفع الإلكترونية

- 1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت.
- 2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.
- 3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.
- 4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

المادة 23

الجرائم المتعلقة بالجريمة المنظمة أو ذات الطابع عبر الوطني والمرتكبة بواسطة تقنية المعلومات

- 1- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.
- 2- التوزيع غير المشروع للأدوية والمنتجات الطبية المقلدة.

- 3- تهريب المهاجرين.
- 4- الاتجار غير المشروع بالأشخاص والاتجار بالأعضاء البشرية.
- 5- الاتجار غير المشروع بالأسلحة.
- 6- الاتجار غير المشروع في الممتلكات الثقافية.

المادة 24

الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة

انتهاك حق المؤلف والحقوق المجاورة ذات الصلة كما هي مُعرّفة في قانون الدولة الطرف ووفقاً له، وذلك إذا ارتكب الفعل عن قصد.

المادة 25

الدخول غير المصرح به في البنية التحتية للمعلومات الحيوية

1- إنشاء وتوزيع واستخدام برامج أو معلومات رقمية أخرى مصممة للدخول غير المشروع في البنية التحتية للمعلومات الحيوية، بما في ذلك تدمير أو حظر أو تعديل أو نسخ المعلومات الواردة فيها أو تحييد ميزات الأمان.

2- انتهاك قواعد تشغيل الوسائط المصممة لتخزين ومعالجة ونقل البيانات الرقمية المحمية في البنية التحتية للمعلومات أو نظم المعلومات الهامة، بموجب القانون الداخلي للدولة الطرف، وشبكات المعلومات والاتصالات التي تنتمي إلى البنية التحتية الحيوية للمعلومات، أو وسائل الوصول إليها إذا كان هذا الانتهاك يضر بالبنية التحتية الحيوية للمعلومات.

المادة 26

التحريض على الأنشطة التخريبية أو المسلحة أو الجرائم الجنائية الأخرى

الدعوات الصادرة عن طريق تكنولوجيا المعلومات والاتصالات من أجل الترويج للأنشطة التخريبية أو المسلحة الموجهة ضد نظام دولة أخرى مما من شأنه زعزعة الأمن العام والاستقرار، أو ارتكاب الجرائم الجنائية المعاقب عليها بالحبس مدة لا تقل عن سنة.

المادة 27

الجرائم المتعلقة بالتطرف

توزيع المواد التي تدعو إلى ارتكاب أفعال غير مشروعة بدافع سياسي أو إيديولوجي أو اجتماعي أو عرقي، عن طريق تكنولوجيا المعلومات والاتصالات، أو أي فعل غير قانوني آخر يدعو لكرهية عرقية أو دينية أو العداء بصفة عامة، وتجريم الدعوة إلى مثل هذه الأعمال أو تبريرها أو توفير سبل النفاذ إليها.

المادة 28

الشروع أو المشاركة في ارتكاب جريمة

الشروع في ارتكاب أحد الأفعال المجرمة المنصوص عليها في الاتفاقية، و/أو المساهمة كشريك في أحد الأفعال المجرمة المنصوص عليها في الاتفاقية، و/أو تنظيم أو توجيه أشخاص آخرين لارتكاب أحد الأفعال المجرمة المنصوص عليها في الاتفاقية.

المادة 29

الأفعال الأخرى غير القانونية

لا تمنع هذه الاتفاقية الدولة الطرف من تجريم أي فعل غير قانوني آخر يُرتكب عمداً عن طريق تكنولوجيا المعلومات والاتصالات.

المادة 30

مسؤولية الشخصيات الاعتبارية

1- تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجنائية للأشخاص الاعتباريين عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها، دون الإخلال بفرض العقوبة على الشخص الطبيعي - بما في ذلك مدير الموقع - الذي يرتكب الجريمة.

2- مع عدم الإخلال بالأحكام الواردة بهذه الاتفاقية، يلتزم مقدمو الخدمات/ مديرو المواقع والتابعون لهم بما يلي، مع تجريم مخالفة أي من تلك الالتزامات:

(أ) حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة (يتم تحديدها). وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي:

- البيانات التي تمكن من التعرف على مستخدم الخدمة.
- البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل متى كانت تحت سيطرة مقدم الخدمة.
- البيانات المتعلقة بحركة الاتصال.
- البيانات المتعلقة بالأجهزة الطرفية للاتصال.
- أي بيانات أخرى تحددها الدولة لأغراض تنفيذ هذه الاتفاقية.

(ب) المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات المختصة، ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها

(ج) تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها.

(د) يجب على مقدم الخدمة/ مدير الموقع أن يوفر لمستخدمي خدماته ولأي جهة مختصة البيانات والمعلومات التالية بأشكال وطرائق تتيح الوصول إليها بصورة ميسرة ومباشرة ومستمرة:

- اسم مقدم الخدمة وعنوانه.
- معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني.
- بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها.
- (هـ) يوفر مقدم الخدمة/ مدير الموقع - حال طلب السلطات المختصة التي تم تحديدها من قبل الدولة - كافة الإمكانيات الفنية التي تتيح لتلك السلطات ممارسة اختصاصاتها.

السلفادور

[الأصل: بالإسبانية]

[12 نيسان/أبريل 2022]

أحكام التجريم

ينبغي للدول أن تعتمد تدابير تشريعية وتدابير أخرى مناسبة لتجريم الأفعال التالية بموجب قوانينها الوطنية وأن تفرض بشأنها عقوبات جنائية وغيرها من العقوبات، بما في ذلك السجن، مع مراعاة عدد الضحايا ومدى الضرر الناجم:

الدخول غير المشروع

الدخول إلى كامل نظام حاسوبي أو أي جزء منه عندما يُرتكب ذلك عمدا ودون إذن مناسب. ولا ينطبق ذلك على الاختبارات المأذون بها أو أنشطة التحقيق المشروعة والتي يمكن التحقق منها، شريطة ألا تسبب أضرارا جسيمة غير مباشرة.

الاعتراض غير القانوني

القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات عندما يُرتكب ذلك عمدا ودون حق ودون إذن مناسب.

التدخل في البيانات

إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها عندما يُرتكب ذلك عمدا ودون وجه حق ودون إذن مناسب.

التدخل في النظم الحاسوبية

الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها، عندما يُرتكب ذلك عمدا ودون وجه حق.

إساءة استعمال الأجهزة

الأفعال التالية عندما تُرتكب عمدا ودون وجه حق: عمليات الإنتاج أو البيع أو الاحتياز بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة المتعلقة بأي أجهزة، بما في ذلك البرامج الحاسوبية، تكون مصممة أو مكيفة أساسا لغرض ارتكاب أي من الجرائم المنصوص عليها في هذه الاتفاقية؛ أو المتعلقة بكلمات المرور أو رموز الولوج أو البيانات المماثلة التي يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو جزء منها، بغرض ارتكاب أي من الأفعال المجرمة في هذه الاتفاقية. ولا ينطبق ذلك على الاختبارات المأذون بها أو أنشطة التحقيق المشروعة والتي يمكن التحقق منها، شريطة ألا تسبب أضرارا جسيمة غير مباشرة.

التزوير الحاسوبي

إدخال بيانات حاسوبية أو تحويلها أو حذفها أو طمسها عندما يُرتكب ذلك عمدا ودون وجه حق، مما يؤدي إلى بيانات غير أصلية، بغض النظر عما إذا كانت البيانات قابلة للقراءة والفهم مباشرة. ويجوز أن يشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة مماثلة.

الاحتيال المرتكب بواسطة تكنولوجيات المعلومات والاتصالات

الأفعال التي تتسبب في إلحاق ضرر بممتلكات شخص آخر من خلال أي إدخال أو تحويل أو حذف أو طمس لبيانات حاسوبية، أو أي تدخل في عمل نظام حاسوبي بنية الاحتيال أو نية سيئة للحصول على منفعة اقتصادية للنفس أو للغير، عندما تُرتكب عمدا ودون وجه حق.

الجرائم المتعلقة بالمواد ذات المحتوى المسيء للأطفال

القيام عمدا ودون وجه حق بإنتاج محتوى من هذا القبيل أو إعادة إنتاجه أو توزيعه أو نشره أو استيراده أو تصديره أو عرضه أو تمويله أو بيعه أو تسويقه أو تعميمه أو حيازته في أي نوع من الأجهزة أو الوسائط التكنولوجية.

انتهاك حقوق التأليف والنشر والحقوق المجاورة

التعدي على الملكية الفكرية والحقوق المجاورة، على النحو المعرف في تشريعات الدولة الطرف عندما يكون متعمدا ويرتكب من خلال استخدام تكنولوجيات المعلومات والاتصالات، بما في ذلك الاستخدام غير المشروع للبرمجيات لاستغلال النظم الحاسوبية وقواعد البيانات المحمية بحقوق التأليف والنشر وانتحال مؤلفات الغير.

المساعدة أو التحريض والشروع

الضلوع في ارتكاب أي فعل مجرم وفقا لهذه الاتفاقية كشريك أو مساعد أو محرض أو بأي دور آخر، أو الشروع في ارتكاب هذا الفعل أو الإعداد له.

المسؤولية

تعتمد كل دولة طرف ما قد يلزم من تدابير، تتسق مع مبادئها القانونية، لتقرير مسؤولية الأشخاص الاعتباريين عن المشاركة في الأفعال المجرمة في هذه الاتفاقية حيثما تُرتكب تلك الجرائم لمصلحتهم من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو باعتباره عضوا في هيئة تابعة للشخص الاعتباري يتبوأ منصبا قياديا داخلها، وذلك بناء على ما يلي: سلطة تمثيل الشخص الاعتباري؛ سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛ سلطة ممارسة الرقابة لدى الشخص الاعتباري.

وإضافة إلى الحالات المنصوص عليها في الفقرة السابقة، تتخذ كل دولة طرف التدابير اللازمة لضمان إمكانية تحميل الشخص الاعتباري المسؤولية حيثما يتيح غياب الإشراف أو المراقبة من قبل الشخص الطبيعي المشار إليه في الفقرة السابقة ارتكاب فعل مجرم وفقا لهذه الاتفاقية لصالح ذلك الشخص الاعتباري من جانب شخص طبيعي يتصرف بمقتضى سلطته.

ورهنًا بالمبادئ القانونية للدولة الطرف، يجوز أن تكون مسؤولية الشخصيات الاعتبارية جنائية أو مدنية أو إدارية. ولا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم. وتكفل كل دولة طرف، على وجه الخصوص، إخضاع الشخصيات الاعتبارية التي تلقى عليها المسؤولية وفقا لهذه الاتفاقية لعقوبات جنائية أو غير جنائية فعالة ومتناسبة وراعية، بما فيها العقوبات النقدية.

الملاحقة والمقاضاة والجزاءات

تجعل كل دولة طرف ارتكاب أي فعل مجرم وفقا لمواد هذه الاتفاقية خاضعا لعقوبات تُراعى فيها جسامة ذلك الجرم.

وتسعى كل دولة طرف إلى ضمان أن أية صلاحيات قانونية تقديرية يتيحها قانونها الداخلي فيما يتعلق بملاحقة الأشخاص لارتكابهم جرائم مشمولة بهذه الاتفاقية تُمارَس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القانون التي تُتخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة ردع ارتكابها.

وفي حالة الأفعال المجرّمة وفقا لمواد هذه الاتفاقية، تتخذ كل دولة طرف تدابير مناسبة، وفقا لقانونها الداخلي ومع إيلاء الاعتبار الواجب لحقوق الدفاع، لضمان أن تراعي الشروط المفروضة بخصوص قرارات الإفراج إلى حين المحاكمة أو الاستئناف ضرورة حضور المدعى عليه في الإجراءات الجنائية اللاحقة.

وتكفل كل دولة طرف مراعاة محاكمها أو سلطاتها المختصة الأخرى خطورة الجرائم المشمولة بهذه الاتفاقية لدى النظر في إمكانية الإفراج المبكر أو المشروط عن الأشخاص المدانين بارتكاب تلك الجرائم.

وتحدّد كل دولة طرف في قانونها الداخلي، عند الاقتضاء، مدة تقادم طويلة تستهل أثناءها الإجراءات الخاصة بأيّ جرم مشمول بهذه الاتفاقية، ومدة أطول عندما يكون الجاني المزعوم قد فرّ من وجه العدالة.

وليس في هذه الاتفاقية ما يمس بالمبدأ القاضي بأن يكون الحق في توصيف الأفعال المجرّمة وفقا لهذه الاتفاقية وتوصيف الاستثناءات القانونية أو المبادئ القانونية الأخرى التي تحكم مشروعية السلوك محفوزا حصرا للقانون الداخلي للدولة الطرف، وبوجوب الملاحقة القضائية لمرتكبي تلك الجرائم ومعاقبتهم وفقا لذلك القانون.

غسل عائدات الجرائم المرتكبة باستخدام تكنولوجيات المعلومات والاتصالات

تعتمد كل دولة طرف، وفقا للمبادئ الأساسية لقانونها الداخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، عندما تُرتكب عمدا:

(أ) تحويل الممتلكات أو نقلها، مع العلم بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات، أو مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي الذي تأتت منه على الإفلات من العواقب القانونية لأفعاله؛

(ب) إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأن تلك الممتلكات هي عائدات إجرامية؛

(ج) اقتناء ممتلكات أو حيازتها أو استخدامها مع العلم، وقت استلامها، بأنها عائدات إجرامية؛

(د) المشاركة في ارتكاب أي فعل مجرم وفقا لهذه الاتفاقية، أو التواطؤ أو التآمر على ارتكابه، والشروع في ارتكابه والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.

ولأغراض تنفيذ أو تطبيق أحكام هذه الفقرة، تسعى كل دولة طرف إلى:

- (أ) تطبيق أحكام هذه الفقرة على أوسع طائفة من الجرائم الأصلية؛
- (ب) إدراج الأفعال المجرمة وفقا لمواد هذه الاتفاقية في عداد الجرائم الأصلية. أما الدول الأطراف التي تحدد تشريعاتها قائمة جرائم أصلية معينة، فتدرج في تلك القائمة، كحد أدنى، مجموعة شاملة من الجرائم المرتبطة بالجماعات الإجرامية المنظمة؛
- (ج) لأغراض الفقرة الفرعية (ب)، تشمل الجرائم الأصلية الجرائم المرتكبة داخل وخارج الولاية القضائية للدولة الطرف المعنية. غير أن الجرائم المرتكبة خارج الولاية القضائية للدولة الطرف لا تمثل جرائم أصلية إلا إذا كان السلوك ذو الصلة يُعتبر فعلا إجراميا بمقتضى القانون الداخلي للدولة التي ارتُكبت فيها وكان من شأنه أن يُعتبر فعلا إجراميا بمقتضى القانون الداخلي للدولة الطرف التي تُنفَّذ أو تُطَبَّق هذه المادة لو كان قد ارتُكبت هناك؛
- (د) تزود كل دولة طرف الأمين العام للأمم المتحدة بنسخ من قوانينها المُنفَّذة لهذه المادة وبنسخ من أي تغييرات تُدخَل على تلك القوانين لاحقا أو بوصف لها.

إعاقة سير العدالة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتُكبت عمدا:

- (أ) استخدام القوة البدنية أو التهديد أو الترهيب أو الوعد بمزية غير مستحقة أو عرضها أو منحها للتحريض على الإدلاء بشهادة زور أو للتدخل في الإدلاء بالشهادة أو تقديم الأدلة في إجراءات تتعلق بارتكاب جرائم مشمولة بهذه الاتفاقية؛
- (ب) استخدام القوة البدنية أو التهديد أو الترهيب للتدخل في ممارسة أي موظف قضائي أو موظف معني بإنفاذ القانون مهامه الرسمية في إجراءات تتعلق بارتكاب جرائم مشمولة بهذه الاتفاقية. وليس في هذه الفقرة الفرعية ما يمسّ حقوق الدول الأطراف في أن تكون لديها تشريعات تحمي فئات أخرى من الموظفين العموميين.

الولاية القضائية

تعتمد كل دولة طرف ما قد يلزم من تدابير لبسط ولايتها القضائية على الأفعال المجرمة وفقا لهذه الاتفاقية في الحالتين التاليتين:

- (أ) عندما يُرتكب الجرم في إقليم تلك الدولة الطرف؛
- (ب) عندما يُرتكب الجرم على متن سفينة ترفع علم تلك الدولة الطرف أو طائرة مسجلة بمقتضى قوانين تلك الدولة الطرف وقت ارتكاب الجرم.
- يجوز أيضا للدولة الطرف أن تبسط ولايتها القضائية على أي جريمة من هذا القبيل عندما:
- (أ) يُرتكب الجرم ضد أحد مواطني تلك الدولة الطرف؛
- (ب) يُرتكب الجرم ضد أحد مواطني تلك الدولة الطرف أو شخص عديم الجنسية يوجد مكان إقامته المعتاد في إقليمها؛
- (ج) يُرتكب الجرم ضد الدولة الطرف.

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

إذا أبلغت الدولة الطرف التي تمارس ولايتها القضائية وفقا للفقرات السابقة، أو علمت بطريقة أخرى، أن دولة طرفا 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.

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

الاتحاد الأوروبي ودوله الأعضاء

[الأصل: بالإنكليزية]

[6 نيسان/أبريل 2022]

الفصل الثاني

التجريم وإنفاذ القانون

المادة 5

الدخول غير المشروع

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم القيام عمدا وبغير وجه حق بالدخول الكامل أو الجزئي إلى نظام حاسوبي عن طريق خرق تدبير أمني.
- 2- يجوز للدولة الطرف أن تشترط لتحقيق الجريمة أن تُرتكب بقصد الحصول على بيانات حاسوبية أو بنية سيئة أخرى، أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 6

الاعتراض غير المشروع

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي، إذا ما ارتكب عمدا وبغير وجه حق: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات.
- 2- يجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 7

التدخل غير المشروع في البيانات

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم القيام عمدا وبغير وجه حق بإتلاف البيانات الحاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.
- 2- يجوز للدولة الطرف أن تشترط تسبب السلوك المشار إليه في الفقرة 1 في ضرر جسيم.

المادة 8

التدخل غير المشروع في النظم

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي، إذا ما ارتكب عمدا وبغير حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

المادة 9

إساءة استخدام الأجهزة

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتكبت عمدا وبغير وجه حق:

(أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

‘1’ جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 8 من هذه الاتفاقية؛

‘2’ كلمة سر خاصة بحاسوب، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام حاسوبي،

بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 8 من هذه الاتفاقية؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة 1 (أ) ‘1’ أو ‘2’ أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 8 من هذه الاتفاقية. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 5 إلى 8 من هذه الاتفاقية، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

3- يجوز لكل دولة طرف عدم تطبيق الفقرة 1 من هذه المادة، شريطة ألا يكون ذلك متعلقا بعمليات بيع الأشياء المشار إليها في الفقرة 1 (أ) ‘2’ من هذه المادة أو توزيعها أو إتاحتها بطريقة أخرى.

المادة 10

الشروع والمساعدة والتحريض

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم القيام عمدا بالمساعدة في ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 9 من هذه الاتفاقية أو التحريض على ارتكابها.

2- يجوز لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الشروع عمدا في ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 9 من هذه الاتفاقية.

المادة 11

مسؤولية الشخصيات الاعتبارية

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، بما يتماشى مع مبادئها القانونية، لضمان إمكانية مساءلة الأشخاص الاعتباريين عن الأفعال المجرّمة وفقاً للمواد 5 إلى 10 من هذه الاتفاقية.
- 2- رهنا بالمبادئ القانونية للدولة الطرف، يمكن أن تكون المسؤولية القانونية للشخص الاعتباري جنائية أو مدنية أو إدارية.
- 3- لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم.

المادة 12

الملاحقة والمقاضاة والجزاءات

- 1- تكفل كل دولة طرف إخضاع أيّ فعل مجرّم وفقاً للمواد 5 إلى 10 من هذه الاتفاقية لجزاءات فعالة ومتناسبة ورادعة بالنسبة للأشخاص الطبيعيين والاعتباريين على السواء.
- 2- تسعى كل دولة طرف إلى ضمان أن أية صلاحيات قانونية تقديرية يتيحها قانونها الداخلي فيما يتعلق بملاحقة الأشخاص لارتكابهم جرائم مشمولة بهذه الاتفاقية تُمارَس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القانون التي تتخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة ردع ارتكابها.
- 3- تتولى كل دولة طرف إنشاء وتعهد نظام وطني للعدالة الجنائية يتسم بالفعالية ويقوم على سيادة القانون يكون بوسعه أن يكفل تقديم أي شخص يلاحق بسبب جرائم مشمولة بهذه الاتفاقية إلى العدالة مع ضمان الحماية الكاملة لحقوق الإنسان والحريات الأساسية، بما في ذلك الحق في محاكمة عادلة وحقوق الدفاع.

غانا

[الأصل: بالإنكليزية]

[12 نيسان/أبريل 2022]

الفصل الثاني - أحكام التجريم⁽³²⁾

الجرائم المرتكبة في الفضاء السيبراني: الجرائم التي تمس سرية النظم والبيانات الحاسوبية وسلامتها وتوافرها

المادة 5

الدخول غير المأذون به إلى نظام حاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي، إذا ما ارتُكب عمداً: الدخول الكامل أو الجزئي إلى نظام حاسوبي دون إذن أو بما يتجاوز حدود الدخول المأذون به. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة وقوع مخالفة للتدابير الأمنية بقصد الحصول على بيانات حاسوبية أو بنية سيئة أخرى أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

(32) يستند النص الخاص بهذا القسم أساساً إلى اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، واتفاقية الاتحاد الأفريقي بشأن أمن الفضاء السيبراني وحماية البيانات ذات الطابع الشخصي، وقانون المعاملات الإلكترونية لسنة 2008 (القانون 772)، وقانون الأمن السيبراني لسنة 2020 (القانون 1038). وتشكل هذه الصكوك الإطار التشريعي للجرائم السيبرانية في غانا.

المادة 6

الدخول غير المأذون به إلى بنية تحتية حيوية للمعلومات

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي، إذا ما ارتكب عمدا: الدخول الكامل أو الجزئي إلى بنية تحتية حيوية للمعلومات دون إذن.

المادة 7

الاعتراض غير المأذون به

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير إذن: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات.

ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 8

التدخل في البيانات

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبدون إذن: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو نسخها أو طمسها.

2- يجوز للدولة الطرف أن تحتفظ بحقوقها في اشتراط أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم.

المادة 9

التدخل في النظم

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبدون إذن: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

المادة 10

إساءة استخدام الأجهزة

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:

(أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

1' جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملائمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 9؛

'2' كلمة سر خاصة بحاسوب، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو أي جزء منها، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 9؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة (أ) '1' أو '2' أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 9. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية بموجب القانون الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 5 إلى 9 من هذه الاتفاقية، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

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

الجرائم التي يبيّن الفضاء السيبراني ارتكابها: الجرائم التي ازداد نطاقها وسرعتها وأثرها نتيجة لظهور النظم الحاسوبية⁽³³⁾

المادة 11

التزوير الحاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق: إدخال بيانات حاسوبية أو تحويلها أو حذفها أو طمسها، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة مشابهة.

المادة 12

الاحتيال الحاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُجرّم في قانونها الوطني التسبب عمدا وبغير وجه حق في إلحاق خسائر بممتلكات الغير عن طريق:

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

(ب) أي تدخل في وظيفة نظام حاسوبي؛

بقصد الاحتيال أو نية سيئة، للحصول، بدون وجه حق، على منفعة اقتصادية للنفس أو للغير.

(33) يتسق توصيف جرائم الاحتيال والتزوير وغيرها من الجرائم المرتكبة بواسطة الحاسوب لاستهداف الأطفال مع أحكام اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، واتفاقية الاتحاد الأفريقي بشأن أمن الفضاء السيبراني وحماية البيانات ذات الطابع الشخصي، وقانون الأمن السيبراني لعام 2020 (القانون 1038).

الجرائم المرتكبة ضد الأطفال

المادة 13

الجرائم المتصلة بالاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا عبر الإنترنت

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:

(أ) إنتاج مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا بغرض نشرها وتوزيعها عبر نظام حاسوبي؛

(ب) اقتناء مواد للاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا للنفس أو للغير؛

(ج) عرض أو إتاحة مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا من خلال نظام حاسوبي أو جهاز إلكتروني؛

(د) نشر وتوزيع وبث (بما في ذلك البث المباشر) ونقل مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا من خلال حاسوب أو جهاز إلكتروني؛

(هـ) حيازة مواد للاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا داخل نظام حاسوبي أو حاسوب أو وسيط لتخزين التسجيلات الإلكترونية.

2- لأغراض الفقرة (ج) من المادة الفرعية (1)، كل من يقوم بما يلي يعتبر أنه ينشر مواد للاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا:

(أ) منح شخص آخر حيازة مواد للاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا؛ أو

(ب) كشف مواد للاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا لشخص آخر أو عرض حيازتها عليه.

3- لأغراض هذا القسم، تتضمن مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا الصور المادية والتسجيلات المرئية والفيديوهات والتسجيلات الصوتية ومواد البث المباشر والرسومات أو النصوص التي تصور أو تصف ما يلي:

(أ) طفلا وهو يمارس سلوكا جنسيا صريحا أو سلوكا يوحى بذلك؛

(ب) شخصا يبدو طفلا وهو يمارس سلوكا جنسيا صريحا أو سلوكا يوحى بذلك؛

(ج) صورا تُظهر طفلا وهو يمارس سلوكا جنسيا صريحا أو سلوكا يوحى بذلك؛

(د) صورا جنسية صريحة للأطفال؛

(هـ) عمليات أو مواد معدة لمشاهدة الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا في الوقت الحقيقي يتولى الجاني في الكثير منها توجيه عملية الاعتداء؛

(و) أي مواد مكتوبة أو تمثيلات مرئية أو تسجيلات صوتية تدعو إلى ممارسة نشاط جنسي غير قانوني مع الأطفال أو تنصح به؛

(ز) أي مواد مكتوبة تتمثل خصائصها السائدة في وصف للأنشطة الجنسية غير القانونية مع الأطفال لغرض جنسي؛

(ح) أي تسجيلات صوتية تتمثل خصائصها السائدة في وصف للأنشطة الجنسية غير القانونية مع الأطفال لغرض جنسي.

المادة 14

التعامل مع الطفل لأغراض الاعتداء الجنسي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير للنص في قوانينها الوطنية على تجريم القيام عمدا باستخدام:

- (أ) خدمة حاسوبية عبر الإنترنت؛ أو
- (ب) خدمة إنترنت؛ أو
- (ج) خدمة لوحة إعلانات محلية؛ أو
- (د) أي جهاز آخر قادر على تخزين البيانات أو بثها إلكترونياً؛

لإغواء طفل أو شخص آخر يعتقد الشخص أنه طفل أو إغرائه أو استدراجه أو استمالته أو استهوائه أو الشروع في ذلك لغرض تيسير ممارسة أي طفل آخر سلوكاً جنسياً غير قانوني أو معه أو التصوير المرئي لذلك السلوك، أو تشجيع ذلك أو عرضه أو طلبه.

المادة 15

المطاردة السيبرانية لطفل

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: استخدام خدمة حاسوبية عبر الإنترنت، أو خدمة إنترنت، أو خدمة محلية للوحة إعلانات عبر الإنترنت، أو أي جهاز إلكتروني آخر للحصول على اسم طفل أو رقم هاتفه أو عنوان بريده الإلكتروني أو عنوانه السكني أو صورته أو وصفه البدني أو خصائصه أو أي معلومات تعريفية أخرى عنه أو إرسال تلك المعلومات أو نشرها أو استنساخها أو شرائها أو بيعها أو تلقّيها أو تبادلها أو تعميمها للمساعدة على ترتيب لقاء مع الطفل لغرض الانخراط في اتصال جنسي أو سلوك جنسي صريح أو نشاط جنسي غير قانوني.

الجرائم الجنسية الأخرى عبر الإنترنت⁽³⁴⁾

المادة 16

الابتزاز الجنسي

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكبت عمداً: التهديد بتوزيع صور خاصة أو صور متحركة لشخص آخر يمارس سلوكاً جنسياً صريحاً عن طريق البريد أو من خلال البريد الإلكتروني أو الرسائل النصية أو بوسائل إلكترونية أو غير ذلك، بنية محددة هي:

(34) بما يتسق مع أحكام قانون الأمن السيبراني.

(أ) مضايقة ذلك الشخص أو تهديده أو إكراهه أو تخويفه أو ممارسة أي تأثير غير مبرر عليه، لا سيما لابتزاز المال أو أي مقابل آخر أو لإجبار الضحية على الانخراط في نشاط جنسي غير مرغوب فيه؛ أو

(ب) ابتزاز المال أو أي مقابل آخر فعليا أو إجبار الضحية على الانخراط في نشاط جنسي غير مرغوب فيه.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا: التهديد بتوزيع صور خاصة أو صور متحركة لطفل يمارس سلوكا جنسيا صريحا عن طريق البريد أو البريد الإلكتروني أو الرسائل النصية أو بوسائل إلكترونية أو غير ذلك، بنية محددة هي:

(أ) مضايقة الطفل أو تهديده أو إكراهه أو تخويفه أو ممارسة أي تأثير غير مبرر عليه، لا سيما لابتزاز المال أو أي مقابل آخر أو لإجباره على الانخراط في نشاط جنسي غير مرغوب فيه؛ أو

(ب) ابتزاز المال أو أي مقابل آخر فعليا أو إجبار الضحية على الانخراط في نشاط جنسي غير مرغوب فيه.

3- ولأغراض الفقرتين 1 و2، يجوز النص على أن الصور الحميمة يمكن أن تشمل تصوير المناطق التناسلية أو الشرجية عارية أو مغطاة فقط بالملابس الداخلية؛ أو إظهار الثديين أسفل قمة الهالة، التي تكون إما مكشوفة أو مرئية بوضوح من خلال الملابس.

المادة 17

نشر الصور الحميمة دون رضا أصحابها

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني: التوزيع المتعمد لصورة حميمة أو تسجيل مرئي محظور لشخص يمكن التعرف عليه أو التسبب عمدا في قيام شخص آخر بتوزيع تلك الصورة أو ذلك التسجيل دون موافقة الشخص المصور فيهما بقصد إحداث اضطراب عاطفي خطير مع وجود أسباب في هذا الشأن كانت تدعو إلى توقع درجة معقولة من الخصوصية إما وقت التقاط الصورة أو عمل التسجيل المرئي و/أو وقت ارتكاب الجريمة.

2- لأغراض هذا القسم، يشمل "الاضطراب العاطفي الخطير" أي سلوك متعمد يؤدي إلى ردود فعل نفسية مثل الخوف والعصبية والحزن والقلق والهم والدهشة والصدمة والإذلال والهوان وكذلك الألم الجسدي.

المادة 18

التهديد بتوزيع صور أو تسجيلات مرئية حميمة محظورة

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا: التهديد بتوزيع صور أو تسجيلات مرئية حميمة محظورة لشخص آخر بطريقة من شأنها أن تسبب له إحساسا بالكرب ينشأ بصورة معقولة في جميع الظروف، ويكون التهديد قد صدر بطريقة من شأنها أن تجعل ذلك الشخص الآخر ينتابه خوف ينشأ بصورة معقولة في جميع الظروف، من التهديد الممارس ضده.

المادة 19

الجرائم المتعلقة بانتهاكات حقوق التأليف والنشر والحقوق المجاورة⁽³⁵⁾

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق التأليف والنشر، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعا لالتزاماتها بموجب وثيقة باريس المؤرخة في 24 تموز/يوليه 1971 فيما يتعلق باتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما يُرتكب هذا الفعل عمداً على نطاق تجاري وبواسطة نظام حاسوبي.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق المجاورة، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعا لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما يُرتكب هذا الفعل عمداً على نطاق تجاري وبواسطة نظام حاسوبي.

3- يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و2 من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين 1 و2 من هذه المادة.

المادة 20

الشروع والمساعدة والتحريض

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمداً: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 19 من هذه الاتفاقية مع توفر النية على ارتكابها.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتُكبت عمداً: الشروع في ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من 7 إلى 9؛ و11؛ و12؛ و13، الفقرة (1) (أ) و(ب) و(هـ)؛ و14؛ و15؛ و16؛ و17.

المادة 21

مسؤولية الشركات

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لضمان مساءلة الأشخاص الاعتباريين عن الجرائم المنصوص عليها في هذه الاتفاقية التي تُرتكب لمصلحتهم من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو باعتباره عضواً في هيئة تابعة للشخص الاعتباري يتبوأ منصبا قياديا داخلها، وذلك بناء على:

(35) بما يتفق مع اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية واتفاقية الاتحاد الأفريقي بشأن أمن الفضاء السيبراني وحماية البيانات ذات الطابع الشخصي.

- (أ) سلطة تمثيل الشخص الاعتباري؛
- (ب) سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛
- (ج) سلطة ممارسة الرقابة لدى الشخص الاعتباري.
- 2- إضافة إلى الحالات المنصوص عليها مسبقاً في الفقرة 1 من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان إمكانية تحميل الشخص الاعتباري المسؤولية في حال ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 في ارتكاب جريمة منصوص عليها وفقاً لهذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.
- 3- رهنا بالمبادئ القانونية للدولة الطرف، يمكن أن تكون المسؤولية القانونية للشخص الاعتباري جنائية أو مدنية أو إدارية.
- 4- لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

المادة 22

العقوبات والتدابير

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في المواد من 5 إلى 20 معاقب عليها بعقوبات فعالة ومتناسبة وراعية، بما في ذلك العقوبات السالبة للحرية.
- 2- تضمن كل دولة طرف مساءلة الأشخاص الاعتباريين وفقاً للمادة 21 وإخضاعهم لعقوبات أو تدابير فعالة ومتناسبة وراعية، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات النقدية.

إيران (جمهورية - الإسلامية)

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

2- التجريم

هناك زيادة في الحالات التي ينظم فيها الجناة وينفذون أنشطة غير مشروعة، ليس فقط ضد أجهزة تكنولوجيا المعلومات والاتصالات، ولكن من خلالها أيضاً. وعلى الرغم من إمكانية تجريم مثل تلك الأفعال بغض النظر عن إساءة استخدام تكنولوجيا المعلومات والاتصالات أو العكس، فإن خطورة الجريمة والعوامل الأخرى المحيطة بها تتطلب في بعض الحالات تجريم الفعل غير المشروع عندما يُرتكب عن طريق استخدام تكنولوجيا المعلومات والاتصالات. وينطبق هذا بصفة خاصة عندما يكتف استخدام تكنولوجيا المعلومات والاتصالات من خطورة الجرائم من حيث جملة أمور منها مدى الضرر الذي يلحقه بالضحايا. ولذلك، فإضافة إلى الجرائم التي تعتمد على تكنولوجيا المعلومات والاتصالات، ينبغي تجريم الأفعال الإجرامية التي تتيح هذه التكنولوجيات ارتكابها في إطار الاتفاقية. غير أن هذا قد يتطلب من وجهة نظر قانونية اتباع نهج يتناول كل حالة على حدة لأن هناك أشكالاً مختلفة للجريمة يمكن أن تعكس عناصر مختلفة إلى جانب الركن المادي والركن المعنوي للجريمة. ولدى اعتماد تدابير لتحديد الجرائم، ينبغي إيلاء الاعتبار الواجب للمبادئ الأساسية للنظم القانونية الوطنية.

وينبغي أيضا تحديد مسؤولية الأشخاص الاعتباريين لضمان التصدي الشامل للأنشطة الإجرامية وحرمان الجناة من حرية العمل تحت ستار الكيانات الاعتبارية. وينبغي أن يحمل هذا التدبير الأشخاص الاعتباريين المسؤولية عن تورطهم المتعمد أو الواعي بطريقة أخرى في ارتكاب الأفعال المجرمة وفقا للاتفاقية.

اليابان

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

1- التجريم

1-1- الجرائم المرتكبة في الفضاء السيبراني

1-1-1- تسلّم اليابان بوجود توافق عام في الآراء في اللجنة المخصصة بشأن تجريم الأعمال الإجرامية المرتكبة في الفضاء السيبراني، التي تتألف أساسا من أعمال تنتهك سرية البيانات والنظم الحاسوبية وسلامتها وتوافرها. واستنادا إلى هذا الاعتراف، تؤيد اليابان تجريم الأعمال الإجرامية المرتكبة في الفضاء السيبراني.

1-1-2- نعتقد أن العديد من الأفعال، التي يلزم تجريمها للتصدي لتحديات اليوم التي توليها كل دولة عضو أهمية، مثل هجمات برمجيات الفدية والهجمات على نظم الحواسيب في البنى التحتية الحيوية، تدرج ضمن الجرائم المرتكبة في الفضاء السيبراني. ويمكن أن تشمل تلك الجرائم المرتكبة في الفضاء السيبراني الدخول غير القانوني، والاعتراض غير القانوني، والتدخل في البيانات أو النظم الحاسوبية، وإساءة استخدام الأجهزة.

1-1-3- تسلّم اليابان بأهمية اتخاذ تدابير مضادة للهجمات على النظم الحاسوبية للبنى التحتية والمرافق الخاصة بالمعلومات. ومع ذلك، وبما أن الهجمات من قبيل سرقة البيانات أو تغييرها عن طريق القرصنة يمكن اعتبارها مندرجة ضمن نطاق الجرائم المرتكبة في الفضاء السيبراني، فليست هناك حاجة إلى التعامل مع هذه الجرائم باعتبارها مسائل خاصة بالبنى التحتية والمرافق الخاصة بالمعلومات. ولما كان من المهم أيضا جعل الاتفاقية المقبلة قابلة للتطبيق على المدى البعيد، تجدر الإشارة إلى أن الأحكام المتعلقة بالتجريم ستفقد مرونتها إذا ما ركزت تركيزا مفرطا على فرادى أساليب العمل. وعلاوة على ذلك، من المهم أن تنص هذه الاتفاقية الجديدة على أحكام أساسية وضرورية يمكن أن يمثل لها وينفذها أكبر عدد ممكن من الدول الأعضاء. وفي ضوء ذلك، ينبغي أن تبدأ المناقشة بالجرائم السيبرانية الشائعة مثل الدخول غير المشروع. وينبغي النظر بعناية فيما إذا كان من الضروري وضع حكم محدد بشأن الهجمات على النظم الحاسوبية للبنى التحتية والمرافق الخاصة بالمعلومات إضافة إلى الأحكام بشأن الجرائم السيبرانية العادية بغية تجنب الازدواجية بين الأحكام المتعلقة بالتجريم.

1-1-4- إضافة إلى ذلك، من الضروري تجنب خطر حدوث أثر مثبط على العمليات والأنشطة المشروعة، مثل تطوير التكنولوجيا، أو إساءة استخدام السلطة من جانب أجهزة إنفاذ القانون بسبب نطاق التجريم الواسع للغاية. فعلى سبيل المثال، عند تجريم الدخول غير المشروع، يمكن أن يُشترط عدم وجود سبب مشروع للدخول والوعي بذلك من أجل تجنب فرض مسؤولية مطلقة في هذا الشأن.

1-1-5- علاوة على ذلك، فإن فرض عقوبة موحدة على الشروع في ارتكاب الجرائم أو على المساعدة على ارتكاب الجرائم والتحريض عليها، أو فرض عقوبة على الأفعال في مرحلة الإعداد أو التآمر التي لا تكفي لتشكيل شروع في ارتكاب جريمة، سيكون تدخلا مفرطا في التشريعات الجنائية الداخلية لفرادى الدول. وينبغي ترك تجريم هذه الأفعال للتشريعات الوطنية لكل دولة عضو. وفيما يتعلق بالتدابير المضادة للجرائم

السيبرانية ذات الطابع العابر للحدود الوطنية، من المهم جدا عدم إنشاء ملاذ آمن للجرائم السيبرانية. ولذلك، من الضروري تجنب النص على الأحكام التي تحد من عدد الدول الأعضاء التي يمكنها الانضمام إلى الاتفاقية الجديدة بسبب الاختلافات في المفاهيم القانونية الأساسية الموجودة حتما بين الدول الأعضاء.

2-1- حرية التعبير

1-2-1- عند النظر في تجريم الأنشطة المضطّعة بها في الفضاء السيبراني، لا بد من الإشارة إلى المعاهدات الدولية لحقوق الإنسان. ولدى تحديد الأفعال التي يمكن تجريمها بوصفها جرائم يبيّر الفضاء السيبراني ارتكابها في إطار الاتفاقية الجديدة، ولا سيما فيما يتعلق بتجريم الأفعال المتصلة بالمحتوى الضار على الإنترنت، يجب ألا تنسى الدول الأعضاء أهمية حماية حرية التعبير.

1-2-2- على سبيل المثال، تنص الفقرة 2 من المادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية على أن يكون "لكل إنسان حق في حرية التعبير يوليه حرية في طلب جميع أنواع المعلومات والأفكار وتلقيها وإذاعتها، دون أي اعتبار للحدود، بالقول أو الكتابة أو الطباعة أو الفن أو بأية وسيلة أخرى يختارها." ومع مراعاة أن الفقرة 3 من المادة 19 تنص على بعض القيود المفروضة على هذا الحق، يجب أن نكفل وجود مجال لوضع قوانين وطنية تراعي الحالة الفعلية في كل دولة عضو حتى لا تُنتهك الحقوق والحريات المتصلة بالبحث الأكاديمي والنشاط الثقافي والفني والصحافة انتهاكا غير عادل.

1-2-3- من أجل حماية حرية التعبير، من الضروري تجنب التسبب في تأثير ميثبط على الأنشطة التعبيرية. ولذلك، فإن تجريم الأفعال المتصلة بالمحتوى الضار على شبكة الإنترنت ينبغي ألا يتم إلا بقدر ما يمكن لجميع الدول الأعضاء أن تتفق على تعريف تلك الأفعال، وأن تكون هناك أسباب يمكن إثباتها للحاجة إلى العقاب.

1-2-4- بغية جعل هذه الاتفاقية معاهدة يمكن لأكثر عدد ممكن من الدول الأعضاء الانضمام إليها، وانتظارا لأن تبلغ المناقشات مرحلة النضج على الصعيدين الدولي والوطني، نعتقد أن أحد أكثر الخيارات الواعدة هو ترك تجريم الأفعال المتعلقة بالمحتوى الضار لبروتوكول إضافي في المستقبل.

3-1- الجرائم التقليدية التي تستغل الفضاء السيبراني

1-3-1- فيما يتعلق بالجرائم المتصلة بالإرهاب والجرائم المتصلة بالأسلحة النارية والجرائم المتصلة بالمخدرات، فإنها قد تشكل جرائم مشمولة بالاتفاقية حتى عندما تُرتكب عن طريق استخدام الإنترنت، ويمكن أيضا تطبيق المعاهدات القائمة مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

1-3-2- ينبغي النظر بعناية في تجريم هذه الأفعال حتى لا تتكرر الجهود القائمة المذكورة أعلاه. وينبغي الرجوع أيضا إلى المناقشات التي دارت أثناء عملية صوغ المعاهدات القائمة، حتى لا يُكتفى بإدراج الأحكام، التي لم تُدرج في تلك المعاهدات عمدا، في هذه الاتفاقية في شكل مختلف فحسب.

4-1- الأفعال الإجرامية التي يمكن النظر في اعتبارها جرائم يبيّر الفضاء السيبراني ارتكابها

فيما يتعلق بالجرائم التي يبيّر الفضاء السيبراني ارتكابها، بخلاف الجرائم المتعلقة بالمحتوى الضار (انظر 1-2 أعلاه)، فإن بعض الأفعال الإجرامية التي يبيّر الفضاء السيبراني ارتكابها والتي يُعترف بأهمية اعتبارها جرائم سيبرانية بموجب هذه الاتفاقية يمكن أن تخضع للمناقشة من أجل تجريمها على أساس أن من الممكن لجميع الدول الأعضاء أن تتفق على تعريف لها وأن هناك أسبابا يمكن إثبات وجاهاتها تدعو إلى

المعاقبة عليها. ومن بينها الجرائم التي يؤدي استخدام الحواسيب فيها إلى زيادة نطاقها وسرعتها وحجمها. ويمكن أن يشمل ذلك الجرائم التالية.

1-4-1 التزوير الحاسوبي

إن من الصعب اكتشاف تزوير البيانات الحاسوبية بالحواسيب البشرية. وعلاوة على ذلك، تنفذ في عالم اليوم العديد من العمليات التجارية بواسطة الحاسوب، ومن ثم، فإن التأثير الاجتماعي لتدني الثقة في البيانات الحاسوبية كبير. ولذلك، يمكن لليابان أن تؤيد تجريم القيام بإدخال بيانات حاسوبية أو تحويلها أو حذفها أو طمسها عمدا وبغير وجه حق على نحو يفضي إلى بيانات زائفة.

2-4-1 الاحتيال الحاسوبي

من السهل ارتكاب جرائم احتيال باستخدام البيانات الحاسوبية عن طريق تزويرها أو عن طريق التدخل في عمل النظم الحاسوبية من أجل تحقيق طائفة واسعة من الأهداف ويمكن أن تسبب هذه الجرائم أضرارا جسيمة للممتلكات في العديد من الدول الأعضاء. لذلك، يمكننا تأييد الدعوة إلى تجريم التسبب في إلحاق خسائر بممتلكات الغير عن طريق أي إدخال أو تحويل أو حذف أو طمس للبيانات الحاسوبية، أو أي تدخل في وظيفة النظام الحاسوبي بقصد الاحتيال أو بنية سيئة للحصول على منفعة اقتصادية.

3-4-1 انتهاكات حقوق التأليف والنشر

يمكن بسهولة نسخ البيانات وإعادة إنتاج المحتوى على الإنترنت، وينتشر ذلك المحتوى بسرعة، مما قد يزيد من درجة انتهاك حقوق التأليف والنشر. ونعتقد أنه سيكون من المفيد تجريم التعدي على حقوق التأليف والنشر والحقوق المجاورة عندما تُرتكب تلك الأفعال عمدا وعلى نطاق تجاري وعن طريق نظام حاسوبي، مع الإشارة إلى الاتفاقات الدولية القائمة المتعلقة بحقوق التأليف والنشر.

4-4-1 الاعتداء الجنسي على الأطفال واستغلالهم جنسيا

يُعتبر إنتاج مواد الاعتداء الجنسي على الأطفال وتوزيعها من الأعمال الخبيثة للغاية وذات التأثير الضار على الصحة العقلية والبدنية للأطفال المصوّرين، كما أنها تنتهك بشكل خطير حقوق الإنسان الخاصة بهم. ومن الصعب حذف مواد الاعتداء الجنسي على الأطفال بمجرد نشرها عبر الإنترنت، وهي ستظل ذات تأثير خطير على التنشئة السليمة للأطفال. ومن منظور حماية حقوق الإنسان للأطفال، نؤيد تجريم إنتاج وتوزيع المواد التي تعرض بشكل مرئي طفلا وهو يمارس سلوكا جنسيا صريحا.

ومع ذلك، نعتقد أنه ينبغي النظر بعناية في معاملة الصور الواقعية التي تمثل شخصا يبدو أنه قاصر أو طفل غير موجود وهو يمارس سلوكا جنسيا صريحا كمواد اعتداء جنسي على الأطفال وتجريم الأفعال المتعلقة بهذه الصور، مع مراعاة عدم تعرض قاصر حقيقي للإساءة المباشرة وكذلك أهمية حرية التعبير.

5-1 مسؤولية الشخصيات الاعتبارية

إننا نؤيد النص على مسؤولية الأشخاص الاعتباريين إلى حد ما في الحالات التي يرتكبون فيها جرائم سيبرانية على نطاق واسع فيما يتعلق بأعمالهم التجارية بشرط إمكانية اعتبار المسؤولية جنائية أو مدنية أو إدارية رهنا بالمبادئ القانونية لكل دولة عضو. ويُعتبر تقسيم الأدوار بين المسائل الجنائية والمدنية

والإدارية وضرورة فرض العقوبات مسألتين ينبغي أن يُتركَا للتشريعات المحلية لكل دولة عضو، حيث يجب النظر فيهما في ضوء الهيكل الوطني لكل دولة عضو والتكافؤ مع الحوكمة خارج قطاع الإنترنت في كل دولة عضو.

الأردن

[الأصل: بالعربية]

[7 نيسان/أبريل 2022]

تقترح المملكة الأردنية الهاشمية تجريم الأفعال التالية في مشروع الاتفاقية:

- تجريم الدخول غير المشروع إلى الشبكة المعلوماتية أو نظام معلومات أو أي جزء منها بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، على أن يتم تشديد العقوبة في حال تبعية الشبكة المعلوماتية أو نظام المعلومات أو أي جزء منهما للمؤسسات الرسمية أو العامة أو الأمنية أو المالية أو المصرفية أو البنى التحتية الحرجة والاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني.
- تجريم الاعتراض غير القانوني لخط سير البيانات.
- تجريم الاعتداء على بيانات أو معلومات تتعلق بوسائل الدفع الإلكتروني أو في تنفيذ المعاملات المالية أو المصرفية الإلكترونية أو تحويل الأموال عن طريق الشبكة المعلوماتية أو نظام المعلومات.
- تجريم الاحتيال الإلكتروني.
- تجريم التحايل على العنوان البروتوكولي.
- تجريم الاستغلال الجنسي من خلال أنظمة وشبكات المعلومات والمواقع الإلكترونية.
- تجريم نشر الإشاعات والأخبار الكاذبة بواسطة أنظمة وشبكات المعلومات والمواقع الإلكترونية.
- تجريم خطاب الكراهية والأفعال المتعلقة بالإساءة للأديان والدول باستخدام شبكات المعلومات والمواقع الإلكترونية.
- تجريم التدخل غير المشروع في أنظمة المعلومات وشبكات المعلومات من خلال زرع أو إدخال برمجيات خبيثة.
- تجريم إنشاء موقع إلكتروني شبيه بموقع إلكتروني حقيقي بهدف تضليل وخداع المستخدمين لغايات سرقة بيانات الدخول أو معلومات شخصية أو لغايات جمع التبرعات غير المشروعة.
- تجريم إرسال رسائل بريد إلكترونية أو رسائل نصية بهدف التصيد الإلكتروني لغايات سرقة بيانات أو نشر برمجيات خبيثة أو محاولة الدخول إلى شبكات أو أنظمة معلومات غير مسموح له بدخولها.
- تجريم إنشاء صفحات أو مجموعات أو حسابات مزيفة على مواقع التواصل الاجتماعي بهدف تضليل وخداع المستخدمين أو لغايات جمع التبرعات غير المشروعة والتسول الإلكتروني.
- تجريم استهداف أجهزة المستخدمين لإنشاء شبكة معلومات بغير علمهم لغايات استخدامها في هجمات حجب الثقة أو أمور غير شرعية.

- تجريم استغلال أو محاولة استغلال الثغرات الأمنية في شبكات أو أنظمة المعلومات بهدف اختراقها أو سرقة البيانات أو تدميرها أو تعديلها.
- تجريم مسح أو محاولات مسح بروتوكولات الانترنت أو منافذ الدخول للشبكات بدون تصريح بهدف جمع المعلومات أو إيجاد ثغرات أمنية.
- تجريم استخدام الأجهزة أو البرمجيات التي تؤدي إلى تخمين أسماء المستخدمين أو كلمات المرور بدون تصريح.
- تجريم استخدام تكنولوجيا الذكاء الاصطناعي لغيات القيام بأفعال غير مشروعة.
- تجريم الأفعال المتعلقة بانتحال الشخصية.
- تجريم الأفعال المتعلقة بانتهاك الخصوصية.
- تجريم الأفعال المتعلقة بالملكية الفكرية وقرصنة البرمجيات.
- تجريم الأفعال التي تشكل اعتداء على سلاسل الإمداد.
- تجريم الأفعال المتعلقة بالاستخدام غير المصرح به للبيانات لدى مزودي الخدمات.
- تجريم الأفعال المتعلقة بنشر الفكر الإرهابي أو دعمه أو الترويج له.
- الجرائم المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات للأغراض الإرهابية.
- تجريم الأفعال المتعلقة بالتزوير الإلكتروني.
- تجريم الأفعال المتعلقة بالترويج للمخدرات أو الاتجار بها بوسائل إلكترونية.
- تجريم الأفعال المتعلقة بغسل الأموال بوسائل إلكترونية.

المكسيك

[الأصل: بالإنكليزية]

[13 نيسان/أبريل 2022]

التجريم

سكنون الولاية القضائية الوطنية عنصرا أساسيا لتحديد التزامات التجريم. وفي هذا الصدد، ترى المكسيك أن اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية الأمم المتحدة لمكافحة الفساد تقدمان أمثلة على الأحكام المنطبقة أيضا على مكافحة الجرائم المتصلة باستخدام تكنولوجيا المعلومات والاتصالات، باستثناء الحالات المرتبطة بالمعلومات الموجودة على منصات الموارد السحابية والتي تتطلب مزيدا من التحليل والمناقشة استنادا إلى التجارب الأخيرة المستمدة من تحقيقات محددة في هذا الشأن.

وينبغي أن تكون نقطة الانطلاق بالنسبة إلى التجريم تضمين الاتفاقية السلوكيات التي يعترف بها القانون الدولي بوصفها جرائم - ولا سيما في إطار الشروط المنصوص عليها في المعاهدات الأخرى المعتمدة في إطار الأمم المتحدة - والتي ترتكب بواسطة تكنولوجيا المعلومات والاتصالات والوسائل الإلكترونية والرقمية. وعليه، يُوصى بإدراج المادة التالية:

"تجرّم الدول الأطراف لأغراض هذه الاتفاقية جميع الأفعال الجنائية المعترف بها في أحكام القانون الدولي القائمة التي ترتكب بواسطة تكنولوجيا المعلومات والوسائل الإلكترونية".

ومن بين الأفعال الجنائية الأخرى، سيكون من الأهمية بمكان بالنسبة لحكومة المكسيك إدراج الجرائم المتعلقة بالاستغلال الجنسي للأطفال وكذلك الجرائم المتعلقة بالعنف الجنساني بواسطة تكنولوجيات المعلومات والاتصالات.

ويوصى بإدراج عناصر عملياتية لتعزيز التحقيق والملاحقة؛ ومن ثمّ سيكون من المناسب النظر في إدراج مرفقات مع تلك النماذج تحدد البيانات اللازمة لمعالجة طلبات الحصول على المعلومات.

وبما أنه من غير المتوقع إدراج جميع أنواع الأفعال الجنائية وإنما إدراج الجرائم المرتكبة في الفضاء السيبراني في المقام الأول، ومن أجل منع التعارض أو الازدواجية مع القوانين الوطنية، يوصى بإدراج التزام عام على الدول الأطراف بمواءمة تشريعاتها، عند الاقتضاء. ويقترح في هذا الشأن النصان التاليان:

"ليس في هذه الاتفاقية ما يمس الحقوق والالتزامات والمسؤوليات الأخرى للدول والأفراد بموجب القانون الدولي القائم التي تهدف إلى منع ومكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية."

"في جميع الإجراءات الرامية إلى تنفيذ هذه الاتفاقية، يولى الاعتبار الأول للمصالح الفضلى لضحايا الجرائم المشمولة بهذه الاتفاقية - من أفراد ومؤسسات ومنظمات".

نيوزيلندا

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

أحكام التجريم

1- خلال الجلسة الأولى، استمعنا إلى تأييد واسع النطاق لإدراج أحكام تستهدف الجرائم السيبرانية في هذه الاتفاقية، ولا سيما الجرائم المرتكبة في الفضاء السيبراني ومجموعة محدودة من الجرائم التي يبيّن الفضاء السيبراني ارتكابها، ولا توجد معارضة لذلك.

2- ونقترح في المرفق 1 من هذه الوثيقة قائمة بأحكام التجريم التي تعتقد نيوزيلندا أنها الأكثر احتمالاً بأن تحظى بتوافق في الآراء وينبغي من ثمّ أن تكون محور اهتمام اللجنة المخصصة نظراً لمحدودية الموارد وضيق الوقت. كما نقدم بعض الاقتراحات النصية للمساعدة في الصياغة، وهي مستمدة أساساً من صكوك دولية أخرى ذات صلة مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، واتفاقية الأمم المتحدة لمكافحة الفساد، واتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست).

3- وتؤيد نيوزيلندا إدراج حكم بشأن الولاية القضائية يحاكي، عند الاقتضاء، الصكوك القائمة، مثل المادة 42 من اتفاقية الأمم المتحدة لمكافحة الفساد، مع عناصر إضافية تشترط على الدول أن تمارس ولايتها القضائية حيثما تُرتكب الجريمة أو أي جزء من الجريمة في إقليم الدولة الطرف، لتجسيد حقيقة أن الجرائم السيبرانية يمكن أن تُرتكب في الفضاء السيبراني، مع إمكانية أن يكون الجاني والضحية والبيانات والنظام الحاسوبي المستخدم في ولايات قضائية مختلفة.

المرفق 1- أحكام التجريم

الدخول غير المشروع إلى النظم الحاسوبية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: الدخول الكامل أو الجزئي إلى نظام حاسوبي. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة وقوع مخالفة للتدابير الأمنية بقصد الحصول على بيانات حاسوبية أو بأي نية سيئة أخرى أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

اعتراض البيانات الحاسوبية بصورة غير مشروعة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

التدخل في البيانات الحاسوبية

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.
- 2- يجوز للدولة الطرف أن تحتفظ بحقها في اشتراط أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم.

التدخل في عمل حاسوب

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

إساءة استخدام الأجهزة أو البرامج الحاسوبية

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:
 - (أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:
 - '1' جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في [المواد ذات الصلة]؛

‘2’ كلمة سر خاصة بحاسوب، أو رمز الولوح، أو بيانات مماثلة يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو أي جزء منها، بغرض ارتكاب أي من الجرائم المنصوص عليها في [المواد ذات الصلة]؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرتين (أ) ‘1’ أو ‘2’ أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في [المواد ذات الصلة]. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية بموجب القانون الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في [المواد ذات الصلة]، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

3- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقاً بعمليات بيع الأشياء المشار إليها في الفقرة 1 (أ) ‘2’ من هذه المادة أو توزيعها أو إتاحتها بطريقة أخرى.

تجريم الابتزاز السيبراني

1- تؤيد نيوزيلندا إدراج حكم يجرم ما يلي:

(أ) ابتزاز مستخدم نظام حاسوبي لفتح البيانات؛

(ب) ابتزاز مستخدم نظام حاسوبي من خلال التهديد بالكشف عن بيانات أو معلومات شخصية دون إذن.

2- وتتطلع نيوزيلندا إلى العمل مع الزملاء لوضع صيغة دقيقة فيما يتعلق بهذه الجريمة.

الاحتياال الحاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُجرّم في قانونها الوطني التسبب عمدا وبغير وجه حق في إلحاق خسائر بممتلكات الغير عن طريق ما يلي:

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

(ب) أي تدخل في عمل نظام حاسوبي،

بقصد الاحتيال أو بنية سيئة، للحصول، بدون وجه حق، على منفعة اقتصادية للنفس أو للغير.

التزوير الحاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق: إدخال بيانات حاسوبية أو تحويلها أو حذفها أو طمسها، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة مشابهة.

الاستغلال الجنسي للأطفال باستخدام النظم الحاسوبية

- 1- نتطلع إلى العمل مع الزملاء لوضع أحكام تجريم فعالة وشاملة تتعلق بالاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا عبر الإنترنت.
- 2- وكحد أدنى، ينبغي أن تشمل هذه المخالفات الجرائم المتصلة باستخدام نظام حاسوبي من أجل:
 - (أ) إنتاج مواد الاستغلال الجنسي للأطفال؛
 - (ب) عرض مواد الاستغلال الجنسي للأطفال أو إتاحتها؛
 - (ج) توزيع مواد الاستغلال الجنسي للأطفال أو بثها؛
 - (د) اقتناء مواد الاستغلال الجنسي للأطفال للنفس أو للغير؛
 - (هـ) حيازة مواد الاستغلال الجنسي للأطفال؛
 - (و) استمالة الأطفال لأغراض الاستغلال الجنسي.

نشر أو توزيع تسجيل مرئي حميم دون موافقة

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني: نقل تسجيل مرئي حميم للضحية أو إرساله أو نشره أو تعميمه أو توصيله بطريقة أخرى، بواسطة نظام حاسوبي، دون عذر معقول
 - (أ) مع العلم أن الضحية لم توافق على النشر؛ أو
 - (ب) مع التغاضي عما إذا كانت الضحية قد وافقت على النشر.
- 2- للتوضيح، لا يجوز الاعتداد بموافقة أي طفل أو شاب يقل عمره عن 16 عاما على نشر تسجيل مرئي حميم يكون هو موضوعه.

المشاركة والشرع

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرم، وفقا لقانونها الداخلي، المشاركة بأي صفة، كطرف متواطئ أو مساعد أو محرض مثلا، في فعل مجرم وفقا لهذه الاتفاقية.
- 2- يجوز لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرم، وفقا لقانونها الداخلي، أي شروع في ارتكاب فعل مجرم وفقا لهذه الاتفاقية.
- 3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرم، وفقا لقانونها الداخلي، الإعداد لارتكاب فعل مجرم وفقا لهذه الاتفاقية.

مسؤولية الشخصيات الاعتبارية

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير، تتسق مع مبادئها القانونية، لتقرير مسؤولية الشخصيات الاعتبارية عن المشاركة في الأفعال المجرمة وفقا لهذه الاتفاقية.
- 2- رهنا بالمبادئ القانونية للدولة الطرف، يجوز أن تكون مسؤولية الشخصيات الاعتبارية جنائية أو مدنية أو إدارية.

- 3- لا تمس تلك 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 فعالة ومتناسبة ورداعة، بما فيها العقوبات النقدية.
- 5- تحظى الشخصيات الاعتبارية بالحماية من المسؤولية عن أي فعل يتم القيام به أو يُمتنع عن القيام به بحسن نية
- (أ) في الأداء الفعلي أو المعترف لواجب مفروض من قبل هذه الاتفاقية أو بمقتضاها؛ أو
- (ب) في الممارسة الفعلية أو المعترضة لوظيفة أو سلطة ممنوحة من قبل هذه الاتفاقية أو بموجبها.

تجريم غسل الأموال

- 1- تعتمد كل دولة طرف، وفقا للمبادئ الأساسية لقانونها الداخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، عندما تُرتكب عمدا:
- (أ) '1' تحويل الممتلكات أو نقلها، مع العلم بأنها عائدات جرائم سيبرانية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي الذي تأتت منه على الإفلات من العواقب القانونية لأفعاله؛
- '2' إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأن تلك الممتلكات هي عائدات جريمة سيبرانية؛
- (ب) رهنا بالمفاهيم الأساسية لنظامها القانوني:
- '1' اقتناء ممتلكات أو حيازتها أو استخدامها مع العلم، وقت استلامها، بأنها عائدات جريمة سيبرانية؛
- '2' المشاركة في ارتكاب أي فعل مجرم وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابه، والشروع في ارتكابه والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.
- 2- لأغراض تنفيذ أو تطبيق الفقرة 1 من هذه المادة:

- (أ) تسعى كل دولة طرف إلى تطبيق الفقرة 1 من هذه المادة على أوسع مجموعة من الجرائم الأصلية؛
- (ب) تدرج كل دولة طرف في عداد الجرائم الأصلية [الجرائم ذات الصلة المنصوص عليها في المادة ذات الصلة من هذه الاتفاقية و] الأفعال المجرمة بموجب [المواد ذات الصلة من] هذه الاتفاقية. أما الدول الأطراف التي تحدد تشريعاتها قائمة جرائم أصلية معينة، فتدرج في تلك القائمة، كحد أدنى، [مجموعة شاملة من الجرائم المرتبطة بالجرائم السيبرانية]؛

- (ج) لأغراض الفقرة الفرعية (ب)، تشمل الجرائم الأصلية الجرائم المرتكبة داخل وخارج الولاية القضائية للدولة الطرف المعنية. غير أن الجرائم المرتكبة خارج الولاية القضائية للدولة الطرف لا تمثل جرائم أصلية إلا إذا كان السلوك ذو الصلة يعتبر فعلا إجراميا بمقتضى القانون الداخلي للدولة التي ارتكب فيها

وكان من شأنه أن يُعتبر فعلاً إجرامياً بمقتضى القانون الداخلي للدولة الطرف التي تُنفذ أو تُطبق هذه المادة لو كان قد ارتكب هناك؛

(د) تزود كل دولة طرف الأمين العام للأمم المتحدة بنسخ من قوانينها المُنفذة لهذه المادة وبنسخ من أي تغييرات تُدخل على تلك القوانين لاحقاً أو بوصف لها؛

(هـ) يجوز النص على أن الجرائم المبينة في الفقرة 1 من هذه المادة لا تنطبق على الأشخاص الذين ارتكبوا الجرم الأصلي إذا كانت المبادئ الأساسية للقانون الداخلي للدولة الطرف تقتضي ذلك؛

(و) يُستدل على عنصر العلم أو القصد أو الغرض، الذي يلزم توافره في أي جرم مبين في الفقرة 1 من هذه المادة، من ملابسات الوقائع الموضوعية.

إعاققة سير العدالة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتكبت عمداً:

(أ) استخدام القوة البدنية أو التهديد أو الترهيب أو الوعد بمزية غير مستحقة أو عرضها أو منحها للتحريض على الإدلاء بشهادة زور أو للتدخل في الإدلاء بالشهادة أو تقديم الأدلة في إجراءات تتعلق بارتكاب جرائم مشمولة بهذه الاتفاقية؛

(ب) استخدام القوة البدنية أو التهديد أو الترهيب للتدخل في ممارسة أي موظف قضائي أو موظف معني بإنفاذ القانون مهامه الرسمية في إجراءات تتعلق بارتكاب جرائم مشمولة بهذه الاتفاقية. وليس في هذه الفقرة الفرعية ما يمسّ حقوق الدول الأطراف في أن تكون لديها تشريعات تحمي فئات أخرى من الموظفين العموميين.

النرويج

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

التجريم

1- نقترح أن تجرم الاتفاقية الأفعال الإجرامية التي ترتكب في الفضاء السيبراني. وعلى الرغم من تطور الجريمة السيبرانية يوماً بعد يوم، فقد تمكنت الأجهزة الوطنية والدولية من تحديد أنواع من السلوك الإجرامي الأساسي المتكرر. وهذه الأفعال مُجرّمة بالفعل في الوقت الراهن في العديد من الدول الأعضاء. وفي هذا الصدد، تود حكومة مملكة النرويج أن توصي بالنظر على الأقل في الجرائم التالية التي تُرتكب في الفضاء السيبراني:

- الوصول غير المشروع إلى البيانات، أي الدخول إلى حاسوب أو نظام حاسوبي دون الحصول على تصريح بذلك؛
- الاعتراض غير المشروع للبيانات، أي الاعتراض غير القانوني في الوقت الحقيقي لمحتوى الاتصالات أو بيانات الحركة المتعلقة بالاتصالات؛

- التدخل في البيانات أو النظم الرقمية، أي البرمجيات الخبيثة وهجمات حجب الخدمات وفيروسات الفدية وحذف البيانات أو تعديلها؛
 - إساءة استخدام الأجهزة، أي استخدام بيانات الائتمان وكلمات المرور والمعلومات الشخصية التي تسمح بالوصول إلى الموارد أو الاتجار بها؛
- 2- ونود أن نُبقي القائمة قصيرة.
- 3- وينبغي للاتفاقية أيضا أن تتجنب تكرار الجرائم التي تتناولها صكوك قانونية أخرى.
- 4- وينبغي أن يكون النص محايدا من الناحية التكنولوجية.
- 5- وإضافة إلى القائمة القصيرة للجرائم المرتكبة في الفضاء السيبراني، ينبغي أن تتضمن الاتفاقية أحكاما بشأن الجرائم المتصلة بمواد الاعتداء الجنسي على الأطفال.

الاتحاد الروسي - المقترح مقدم أيضا باسم بيلاروس وبوروندي والصين وطاجيكستان ونيكاراغوا

[الأصل: بالروسية]

[7 نيسان/أبريل 2022]

الفصل الثاني

التجريم والإجراءات الجنائية وإنفاذ القانون

الباب 1

إرساء المسؤولية

المادة 5

إرساء المسؤولية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي تُجرّم في قانونها الوطني الأفعال المنصوص عليها في المواد 6 و7 و9-12 و14-17 و19 و20 و22-26 و28 من هذه الاتفاقية، كحد أدنى، مع تطبيق العقوبات الجنائية وغيرها من العقوبات، بما فيها السجن، التي تأخذ في الاعتبار مستوى الخطر العام الذي يشكله فعل معين وحجم الضرر الناجم.

المادة 6

الوصول غير المشروع إلى المعلومات الرقمية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني الوصول غير المشروع والمتعمد إلى المعلومات الرقمية بما يؤدي إلى إتلافها أو حجبها أو تعديلها أو نسخها.

المادة 7

الاعتراض غير المشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني الاعتراض المتعمد للمعلومات الرقمية، الذي يتم دون إذن مناسب و/أو ينتهك القواعد المقررة، بما في ذلك

الاعتراض الذي ينطوي على استخدام وسائل تقنية لاعتراض بيانات تنتج المستخدمين والبيانات التي تعالج بواسطة تكنولوجيا المعلومات والاتصالات غير المخصصة للاستخدام العام.

المادة 8

التدخل غير المشروع في المعلومات الرقمية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُعتبر في قانونها الوطني جريمة أو فعلاً غير مشروع آخر التدخل غير المشروع والمتعمد في المعلومات الرقمية عن طريق إتلافها أو حذفها أو تحويلها أو حجبها أو تعديلها أو نسخها.

المادة 9

تعطيل شبكات المعلومات والاتصالات

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني أي فعل متعمد وغير مشروع يهدف إلى تعطيل شبكات المعلومات والاتصالات، ويسبب عواقب وخيمة أو يهدد بالتسبب في ذلك.

المادة 10

إنشاء البرمجيات الضارة واستخدامها وتوزيعها

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني إنشاء المتعمد للبرمجيات الخبيثة، بما في ذلك تكييفها واستخدامها وتوزيعها بقصد إتلاف المعلومات الرقمية أو حجبها أو تعديلها أو نسخها أو نشرها دون إذن، أو تحييد سماتها الأمنية، باستثناء البحوث المشروعة.
- 2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُعتبر في قانونها الوطني جريمة أو فعلاً غير مشروع آخر إنشاء شبكات للسيطرة على الأجهزة الإلكترونية (البوتنتيت) أو استخدامها لغرض ارتكاب أي من الأفعال المنصوص عليها في المواد 6-12 و14 من هذه الاتفاقية.

المادة 11

التدخل غير المشروع في البنى التحتية الحيوية للمعلومات

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني تعمد إنشاء و/أو توزيع و/أو استخدام برمجيات أو معلومات رقمية أخرى مصممة عن علم للتدخل بصورة غير مشروعة في البنى التحتية الحيوية للمعلومات، بما في ذلك البرمجيات أو غيرها من المعلومات الرقمية من أجل إتلاف المعلومات الواردة فيها أو حجبها أو تعديلها أو نسخها، أو لتحديد السمات الأمنية.
- 2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني انتهاك قواعد تشغيل الوسائط المصممة لتخزين ومعالجة ونقل البيانات الرقمية المحمية في البنية التحتية للمعلومات أو نظم المعلومات المهمة أو شبكات المعلومات والاتصالات التي تنتمي إلى البنية التحتية الحيوية للمعلومات، أو انتهاك قواعد الوصول إليها إذا كان ذلك الانتهاك يضر بالبنية التحتية الحيوية للمعلومات.

المادة 12

الوصول غير المصرح به إلى البيانات الشخصية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني الوصول غير المشروع إلى البيانات الشخصية من أجل إتلافها أو تعديلها أو نسخها أو تداولها.

المادة 13

الاتجار غير المشروع بالأجهزة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُعتبر في قانونها الوطني جريمة أو فعلا غير مشروع آخر صنع أجهزة مصممة أو مكيفة أساسا لغرض ارتكاب أي من الأفعال المجرمة بمقتضى المواد من 6 إلى 12 من هذه الاتفاقية أو بيعها أو شراؤها لأغراض استعمالها أو استيرادها أو تصديرها أو نقلها بشكل آخر لأغراض استعمالها بصورة غير مشروعة.

ولا تنطبق أحكام هذه المادة عندما يكون صنع الأجهزة أو بيعها أو شراؤها من أجل الاستخدام استيرادها أو تصديرها أو نقلها بشكل آخر مرتبطا، على سبيل المثال، بتجربة مأذون بها لنظام حاسوبي أو بحمايته.

المادة 14

السراقة المرتبطة بتكنولوجيا المعلومات والاتصالات

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي تُجرّم في قانونها الوطني سرقة الممتلكات أو اكتساب الحقوق فيها بصورة غير مشروعة، بما في ذلك عن طريق الاحتيال عن طريق إتلاف المعلومات الرقمية أو حجبها أو تعديلها أو نسخها أو غير ذلك من أشكال التدخل في عمليات تكنولوجيا المعلومات والاتصالات.

2- يجوز لكل دولة طرف أن تحتفظ بالحق في اعتبار سرقة الممتلكات المتصلة بتكنولوجيا المعلومات والاتصالات أو الاكتساب غير المشروع للحقوق فيها، بما في ذلك عن طريق الاحتيال، ظرفا مشددا للعقوبة عندما تُرتكب تلك السرقة بالأشكال المحددة في قانونها الوطني.

المادة 15

الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات المرتبطة بإنتاج وتوزيع مواد أو أشياء ذات صور إباحية للقصر

1- تعتمد كل دولة طرف أيضا ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، عندما تُرتكب عمدا وبطريقة غير شرعية:

(أ) إنتاج مواد إباحية متعلقة بالأطفال بغرض توزيعها من خلال شبكات المعلومات والاتصالات، بما في ذلك الإنترنت؛

(ب) عرض مواد إباحية متعلقة بالأطفال أو إتاحتها من خلال شبكات المعلومات والاتصالات، بما في ذلك الإنترنت؛

(ج) استخدام شبكات المعلومات والاتصالات، بما في ذلك الإنترنت، لتوزيع مواد إباحية متعلقة بالأطفال أو بثها أو عرضها علنا أو الإعلان عنها؛

(د) استخدام تكنولوجيا المعلومات والاتصالات لاقتناء مواد إباحية متعلقة بالأطفال للنفس أو للغير؛

(هـ) حيازة مواد إباحية متعلقة بالأطفال داخل نظام حاسوبي أو على الأجهزة الإلكترونية لتخزين البيانات الرقمية.

2- لأغراض الفقرة 1 من هذه المادة، يشمل مصطلح "المواد الإباحية المتعلقة بالأطفال" المواد الإباحية التي تعرض بشكل مرئي:

(أ) قاصرا وهو يمارس سلوكا جنسيا صريحا؛

(ب) شخصا يبدو قاصرا وهو يمارس سلوكا جنسيا صريحا؛

(ج) صورا واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا صريحا.

لأغراض الفقرة 2 من هذه المادة، يشمل مصطلح "قاصر" كافة الأشخاص دون سن الثامنة عشر. ويجوز لأي دولة طرف أن تشترط حدا عمريا أدنى لا يقل عن سن السادسة عشرة.

المادة 16

التشجيع على الانتحار أو الإكراه عليه

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُجرّم في قانونها الوطني تشجيع الأشخاص، بمن فيهم القصر، على الانتحار أو إكراههم عليه، من خلال الضغط النفسي أو غيره من أنواع الضغط عبر شبكات المعلومات والاتصالات، بما فيها الإنترنت.

المادة 17

الجرائم المتصلة بإشراك القصر في ارتكاب أعمال غير مشروعة تُعرض حياتهم أو صحتهم للخطر

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني استخدام تكنولوجيا المعلومات والاتصالات لإشراك القصر في ارتكاب أفعال غير مشروعة تهدد حياتهم، باستثناء الأفعال المنصوص عليها في المادة 16 من هذه الاتفاقية.

المادة 18

إنشاء واستخدام المعلومات الرقمية لتضليل المستخدم

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُعتبر في قانونها الوطني جريمة أو فعلا غير مشروع آخر الإنشاء والاستخدام غير المشروعين والمتعمدان للمعلومات الرقمية التي يمكن الخلط بينها وبين المعلومات التي يعرفها المستعمل ويثق بها بالفعل، مما يسبب ضررا جسيما.

2- يجوز لكل دولة طرف أن تحتفظ بالحق في اعتبار تلك الأفعال إجرامية إذا ارتكبت بالاقتران بجرائم أخرى بمقتضى القانون الوطني لتلك الدولة الطرف أو كانت تنطوي على نية متعمدة لارتكاب تلك الجرائم.

المادة 19

التحريض على الأنشطة التخريبية أو المسلحة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي تُجرّم في قانونها الوطني النداءات الصادرة بواسطة تكنولوجيا المعلومات والاتصالات للقيام بأنشطة تخريبية أو مسلحة ترمي إلى الإطاحة بحكومة دولة أخرى بالعنف.

المادة 20

الجرائم المتصلة بالنشاط الإرهابي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي تُجرّم في قانونها الوطني النداءات الصادرة بواسطة تكنولوجيا المعلومات والاتصالات لارتكاب أنشطة إرهابية، أو للتحريض على ارتكاب أنشطة إرهابية أو تجنيد عناصر لارتكابها أو المشاركة فيها بأي شكل آخر، أو للدعوة إلى الإرهاب وتبريره، أو لجمع الأموال أو توفيرها لتمويله.

المادة 21

الجرائم المتصلة بالتطرف

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُعتبر في قانونها الوطني جريمة أو فعلا غير مشروع آخر توزيع المواد التي تدعو إلى ارتكاب أفعال غير مشروعة بدافع الكراهية أو العداوة السياسية أو الأيديولوجية أو الاجتماعية أو العنصرية أو الإثنية أو الدينية، أو الدعوة إلى تلك الأعمال وتبريرها، أو لتوفير إمكانية الحصول على تلك المواد، بواسطة تكنولوجيا المعلومات والاتصالات.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُعتبر في قانونها الوطني جريمة أو فعلا غير مشروع آخر إذلال شخص أو مجموعة من الأشخاص بواسطة تكنولوجيا المعلومات والاتصالات بسبب عرقهم أو خلفيتهم الإثنية أو لغتهم أو أصلهم أو انتمائهم الديني.

المادة 14

الجرائم المتصلة بتوزيع العقاقير المخدرة والمؤثرات العقلية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني الاتجار غير المشروع والمتعمد بالعقاقير المخدرة والمؤثرات العقلية، وكذلك المواد اللازمة لصنعها بواسطة تكنولوجيا المعلومات والاتصالات.

المادة 23

الجرائم المتصلة بالاتجار بالأسلحة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني الاتجار غير المشروع والمتعمد بالأسلحة والذخيرة والأجهزة والمواد المتفجرة بواسطة تكنولوجيا المعلومات والاتصالات.

المادة 24

تحسين صورة النازية أو تبرير الإبادة الجماعية أو الجرائم المرتكبة ضد السلام والإنسانية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني النشر المتعمد بواسطة تكنولوجيا المعلومات والاتصالات للمواد التي تنكر الأعمال التي ترقى إلى مستوى الإبادة الجماعية أو الجرائم المرتكبة ضد السلام والإنسانية، والتي أرساها حكم المحكمة العسكرية الدولية المنشأة بموجب اتفاق لندن المؤرخ 8 آب/أغسطس 1945، وكذلك إقرار تلك الأعمال أو تبريرها.

المادة 25

التوزيع غير المشروع للأدوية والمنتجات الطبية المقلدة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني التوزيع غير المشروع والمتعمد للأدوية والمنتجات الطبية المقلدة بواسطة تكنولوجيا المعلومات والاتصالات.

المادة 26

استخدام تكنولوجيا المعلومات والاتصالات في ارتكاب أفعال مجرمة بموجب القانون الدولي

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الوطني استخدام تكنولوجيا المعلومات والاتصالات لغرض ارتكاب فعل يشكل جرماً بمقتضى أي من الاتفاقات الدولية المدرجة في مرفق⁽³⁶⁾ هذه الاتفاقية.

2- لدى إيداع صك التصديق أو القبول أو الموافقة أو الانضمام، يجوز لأي دولة ليست طرفاً في أي اتفاق مدرج في مرفق هذه الاتفاقية أن تعلن أن ذلك الاتفاق سوف يُعتبر غير مدرج في المرفق المشار إليه أعلاه عند تطبيق هذه الاتفاقية عليها. ويتوقف سريان الإعلان حالما تدخل المعاهدة حيز التنفيذ بالنسبة للدولة الطرف، التي ستقوم بإعلام وديع الاتفاقية بذلك الأمر.

3- إذا لم تُعد الدولة الطرف طرفاً في اتفاق مدرج في مرفق هذه الاتفاقية، يجوز لهذه الدولة أن تصدر إعلاناً بشأن ذلك الاتفاق (تلك الاتفاقات)، على النحو المنصوص عليه في الفقرة 2 أعلاه.

المادة 27

انتهاك حقوق التأليف والنشر والحقوق المجاورة بواسطة تكنولوجيا المعلومات والاتصالات

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُعتبر في قانونها الوطني جريمة أو فعلاً غير مشروع آخر انتهاك حقوق التأليف والنشر والحقوق المجاورة كما تعرّفها تشريعات تلك الدولة الطرف، وذلك إذا ارتكبت تلك الأفعال عن قصد بواسطة تكنولوجيا المعلومات والاتصالات، بما في ذلك الاستخدام غير المشروع للبرمجيات لاستغلال نظم أو قواعد بيانات حاسوبية محمية بحقوق التأليف والنشر وانتحال مؤلفات الغير.

(36) ملحوظة من الأمانة: يرجى الرجوع إلى المرفق الوارد في الوثيقة A/75/980.

المادة 28

المساعدة على ارتكاب جريمة والإعداد لها والشرع في ارتكابها

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني: الإعداد لارتكاب فعل مجرم منصوص عليه في هذه الاتفاقية أو الشرع في ذلك.
- 2- تتنظر كل دولة طرف في اتخاذ ما قد يلزم من تدابير تشريعية وتدابير أخرى للنص في قانونها الوطني على تجريم القيام بصنع أو تهيئة أدوات ووسائل إجرامية أخرى من أجل ارتكاب أي فعل مجرم بمقتضى هذه الاتفاقية أو استدراج شركاء لارتكابه أو التآمر على ارتكابه أو القيام بأي شكل آخر بتهيئة الظروف عن عمد لارتكاب ذلك الفعل في الحالات التي لا تُرتكب فيها الجريمة لأسباب خارجة عن سيطرة من يفعل ذلك.
- 3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي تخضع للمساءلة بموجب قانونها الوطني كل من يشارك في ارتكاب الجرائم المنصوص عليها في الاتفاقية بالتنظيم أو التحريض أو المساعدة، إلى جانب الجناة الفعليين، وكذلك كي تعزز المسؤولية عن الجرائم الجماعية، بما يشمل الجماعات المنظمة والروابط الإجرامية.

المادة 29

الأفعال الأخرى غير المشروعة

لا تمنع هذه الاتفاقية الدولة الطرف من تجريم أي فعل غير مشروع آخر يُرتكب عمداً بواسطة تكنولوجيا المعلومات والاتصالات ويسبب ضرراً جسيماً.

المادة 30

مسؤولية الشخصيات الاعتبارية

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان إمكانية تحميل الأشخاص الاعتباريين المسؤولية عن أي أفعال إجرامية أو غير مشروعة منصوص عليها في هذه الاتفاقية إذا ارتكبها لصالحهم شخص طبيعي، يتصرف إما بمفرده أو كجزء من كيان تابع للشخص الاعتباري المعني، ويشغل منصبا قياديا داخله بموجب:

(أ) توكيل من الشخص الاعتباري؛

(ب) سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛

(ج) سلطة ممارسة الرقابة لدى الشخص الاعتباري.

- 2- إضافة إلى الحالات المنصوص عليها في الفقرة 1 من هذه المادة، تتخذ كل دولة طرف التدابير اللازمة لضمان إمكانية تحميل الشخص الاعتباري المسؤولية في حال ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 في ارتكاب جرم أو فعل غير قانوني آخر منصوص عليه في هذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.

- 3- رهنا بالمبادئ القانونية للدولة الطرف، يجوز أن تكون مسؤولية الشخص الاعتباري جنائية أو مدنية أو إدارية. وتكفل كل دولة طرف إخضاع الشخصيات الاعتبارية التي تلقى عليها المسؤولية لعقوبات فعالة ومتناسبة وراذعة، بما فيها العقوبات النقدية.

4- لا تمسُّ مسؤولية الشخصيات الاعتبارية مسؤولية الأشخاص الطبيعيين الذين ارتكبوا جريمة أو فعلاً آخر غير قانوني.

جنوب أفريقيا

[الأصل: بالإنكليزية]

[14 نيسان/أبريل 2022]

الفصل الثاني - التجريم

المادة 5: الدخول غير المشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبطريقة غير شرعية: الدخول غير المشروع الكامل أو الجزئي إلى نظام حاسوبي. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة وقوع مخالفة للتدابير الأمنية بقصد الحصول بطريقة غير مشروعة على بيانات حاسوبية أو بأي نية سيئة أخرى أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 6: الاعتراض غير المشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبطريقة غير شرعية وبغير وجه حق: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 7: التدخل غير المأذون به في المعلومات الرقمية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبطريقة غير شرعية وبغير وجه حق: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.

2- يجوز للدولة الطرف أن تحتفظ بحقها في اشتراط أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم (يلحق بالأشخاص الطبيعيين أو الأشخاص الاعتباريين أو اقتصاد الدولة الطرف).

المادة 8: التدخل في النظم وتعطّل شبكات المعلومات والاتصالات

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبطريقة غير شرعية وبغير وجه حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

المادة 9: صنع الأجهزة واستخدامها وتوزيعها

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبطريقة غير شرعية وبغير وجه حق:

(أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

‘1’ جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 26؛

‘2’ كلمة سر خاصة بحاسوب، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو أي جزء منها، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 26؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة (أ) ‘1’ أو ‘2’ أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 5 إلى 26. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية بموجب القانون الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 5 إلى 26 من هذه الاتفاقية، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

3- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقا بعمليات بيع الأشياء المشار إليها في الفقرة 1 (أ) ‘2’ من هذه المادة أو بيعها أو إتاحتها بطريقة أخرى.

المادة 10: التزوير الذي يبيسر الفضاء السيبراني ارتكابه

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبطريقة غير شرعية وبغير وجه حق: إدخال بيانات حاسوبية أو تغييرها أو حذفها أو إتلافها، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة مشابهاة.

المادة 11: الاحتيال الذي يبيسر الفضاء السيبراني ارتكابه

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُجرّم في قانونها الوطني التسبب عمدا وبغير وجه حق في إلحاق خسائر بممتلكات الغير عن طريق:

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

(ب) أي تدخل في وظيفة نظام حاسوبي، بقصد الاحتيال أو بنية سيئة، للحصول، بدون وجه حق، على منفعة اقتصادية للنفس أو للغير.

المادة 12: الجرائم المتعلقة بالمواد المرتبطة بالاستغلال الجنسي للأطفال

- 1- تعتمد كل دولة طرف التشريعات والتدابير الأخرى التي تكون ضرورية لتجريم السلوكيات التالية المتعلقة بمواد الاعتداء الجنسي على الأطفال في إطار قانونها الوطني في حال ارتكابها عمدا وبطريقة غير شرعية:
 - (أ) إنتاج مواد الاعتداء الجنسي على الأطفال لغرض توزيعها من خلال نظام حاسوبي أو تكنولوجيات المعلومات والاتصالات؛
 - (ب) عرض أو إتاحة مواد الاعتداء الجنسي على الأطفال من خلال نظام حاسوبي أو تكنولوجيات المعلومات والاتصالات؛
 - (ج) توزيع أو بث مواد الاعتداء الجنسي على الأطفال من خلال نظام حاسوبي أو تكنولوجيات المعلومات والاتصالات؛
 - (د) اقتناء مواد الاعتداء الجنسي على الأطفال من خلال نظام حاسوبي أو تكنولوجيات المعلومات والاتصالات للنفس أو للغير؛
 - (هـ) حيازة مواد الاعتداء الجنسي على الأطفال في نظام حاسوبي أو تكنولوجيات معلومات واتصالات أو على وسيط حاسوبي لتخزين البيانات.
- 2- لغرض الفقرة 1 أعلاه، يشمل مصطلح "مواد الاعتداء الجنسي على الأطفال" المواد التي تعرض بشكل مرئي:

- (أ) قاصرا وهو يمارس سلوكا جنسيا صريحا؛
- (ب) شخصا يبدو قاصرا وهو يمارس سلوكا جنسيا صريحا؛
- (ج) صورا واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا صريحا.

- 3- لغرض الفقرة 2 أعلاه، يشمل مصطلح "قاصر" كافة الأشخاص دون سن الثامنة عشرة. ويجوز لأي دولة طرف أن تشترط حدا عمريا أدنى لا يقل عن سن السادسة عشرة.

المادة 13: الجرائم المتعلقة بانتهاكات حقوق التأليف والنشر والحقوق المجاورة

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق التأليف والنشر، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعا لالتزاماتها بموجب المعاهدات والاتفاقات الدولية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمدا على نطاق تجاري وبواسطة نظام حاسوبي أو تكنولوجيات المعلومات والاتصالات.
- 2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق المجاورة، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعا لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمدا على نطاق تجاري وبواسطة نظام حاسوبي أو تكنولوجيات المعلومات والاتصالات.

3- يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و2 من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين 1 و2 من هذه المادة.

المادة 14: الجرائم المتصلة بتوزيع العقاقير المخدرة والمؤثرات العقلية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي تجرّم بموجب قانونها الوطني الأفعال التي تنطوي على استخدام تكنولوجيات المعلومات والاتصالات، والتي تعزز الاتجار بالعقاقير المخدرة والمؤثرات العقلية والمواد اللازمة لصنعها.

المادة 15: حماية المبلغين

تنظر كل دولة طرف في أن تُدخل في صلب نظامها القانوني الداخلي تدابير مناسبة لتوفير الحماية من أي معاملة لا مسوّغ لها لأي شخص يقوم، بحسن نية ولأسباب وجيهة، بإبلاغ السلطات المختصة بأي وقائع تتعلق بأفعال مجرّمة وفقا لهذه الاتفاقية وتنطوي على استخدام تكنولوجيات المعلومات والاتصالات.

تنظر كل دولة طرف في أن تدرج في تشريعاتها الداخلية إعفاء من الملاحقة القضائية، رهنا بالوفاء بالمعايير/الشروط التي يعتمدها أحد الأطراف، لأي شخص يبدي تعاوناً كاملاً وبحسن نية عند التعامل مع أجهزة إنفاذ القانون ذات الصلة.

المادة 16: التعاون مع سلطات إنفاذ القانون

1- تتخذ كل دولة طرف تدابير مناسبة لتشجيع الأشخاص الذين يشاركون أو شاركوا في ارتكاب فعل مجرّم وفقا لهذه الاتفاقية وينطوي على استخدام تكنولوجيات المعلومات والاتصالات، على تقديم معلومات مفيدة بحسن نية إلى السلطات المختصة لأغراض التحقيق والإثبات، وعلى توفير مساعدة فعلية محددة للسلطات المختصة يمكن أن تسهم في حرمان الجناة من عائدات الجريمة واسترداد تلك العائدات.

2- تنظر كل دولة طرف في أن تتيح، في الحالات المناسبة، إمكانية تخفيف عقوبة المتهم الذي يقدم عوناً كبيراً بحسن نية في عمليات التحقيق أو الملاحقة بشأن فعل مجرّم وفقا لهذه الاتفاقية وينطوي على استخدام تكنولوجيات المعلومات والاتصالات.

3- تنظر كل دولة طرف في إمكانية منح الحصانة من الملاحقة القضائية، وفقا للمبادئ الأساسية لقانونها الداخلي، لأي شخص يقدم، بحسن نية، عوناً كبيراً في عمليات التحقيق أو الملاحقة بشأن فعل مجرّم وفقا لهذه الاتفاقية ينطوي على استخدام تكنولوجيات المعلومات والاتصالات.

4- تجري حماية أولئك الأشخاص على النحو المنصوص عليه في المادة 22 من هذه الاتفاقية، مع مراعاة ما يقتضيه اختلاف الحال.

5- عندما يكون الشخص المشار إليه في الفقرة 1 من هذه المادة، الموجود في دولة طرف، قادراً على تقديم عون كبير إلى السلطات المختصة لدولة طرف أخرى، يجوز للدولتين الطرفين المعنيتين أن تنظرا في إبرام اتفاقات أو ترتيبات، وفقا لقانونهما الداخلي، بشأن إمكان قيام الدولة الطرف الأخرى بتوفير المعاملة المبيّنة في الفقرتين 2 و3 من هذه المادة.

6- تحتفظ كل دولة طرف بسجل يتضمن معلومات تعريفية لجميع مسجلي أسماء النطاقات وتجار الموجودات المشفرة والموجودات المشفرة داخل ولايتها القضائية، وفقا للمبادئ الأساسية لقانونها الداخلي، وتقدم تلك المعلومات إلى السلطات المختصة لأغراض التحقيق والإثبات.

المادة 17- الولاية القضائية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير لبسط ولايتها القضائية على الأفعال المجرّمة وفقا لهذه الاتفاقية وتتطوي على استخدام تكنولوجيات المعلومات والاتصالات في الحالتين التاليتين:

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

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

2- رهنأ بأحكام المادة 4 من هذه الاتفاقية، يجوز للدولة الطرف أن تبسط أيضا ولايتها القضائية على أي جرم من هذا القبيل وينطوي على استخدام تكنولوجيات المعلومات والاتصالات في الحالات التالية:

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

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

(ج) عندما يكون الجرم واحدا من الأفعال المجرّمة وفقا للفقرة 1 (ب) '2' من المادة 17 من هذه الاتفاقية ويُرتكب خارج إقليمها بهدف ارتكاب فعل مجرم وفقا للمادة 15 من هذه الاتفاقية داخل إقليمها وينطوي على استخدام تكنولوجيات المعلومات والاتصالات؛

(د) يُرتكب الجرم ضد الدولة الطرف، أو يكون له تأثير مباشر على شؤون تلك الدولة الطرف.

3- لأغراض المادة - [يشأن تسليم المطلوبين] من هذه الاتفاقية، تعتمد كل دولة طرف ما قد يلزم من تدابير لإخضاع الأفعال المجرّمة وفقا لهذه الاتفاقية وتتطوي على استخدام تكنولوجيات المعلومات والاتصالات لولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه لمجرد كونه أحد مواطنيها.

4- ويجوز لكل دولة طرف أيضا أن تعتمد ما قد يلزم من تدابير لإخضاع الأفعال المجرّمة وفقا لهذه الاتفاقية التي تنطوي على استخدام تكنولوجيات المعلومات والاتصالات 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 جنائية تؤكد الدولة الطرف سريانها وفقا لقانونها الداخلي.

سويسرا

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

2-2- أحكام التجريم

(أ) الجرائم التي تمس سرية النظم والبيانات الحاسوبية وسلامتها وتوافرها

الدخول غير المشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: الدخول الكامل أو الجزئي إلى نظام حاسوبي. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة وقوع مخالفة للتدابير الأمنية بقصد الحصول على بيانات حاسوبية أو بنية سيئة أخرى أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

الاعتراض غير المشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

التدخل في البيانات

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.
- 2- يجوز للدولة الطرف أن تحتفظ بحقها في اشتراط أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم.

التدخل في النظم

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

إساءة استعمال الأجهزة

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:

(أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

1' جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملاءمته مبدئياً، بغرض ارتكاب أي من الجرائم المنصوص عليها في الأحكام بشأن الدخول غير المشروع والاعتراض غير المشروع، والتدخل في البيانات أو النظم في هذه الاتفاقية؛

2' كلمة سر خاصة بحاسوب، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو أي جزء منها، بغرض ارتكاب أي من الجرائم المنصوص عليها في الأحكام بشأن الدخول غير المشروع والاعتراض غير المشروع، والتدخل في البيانات أو النظم في هذه الاتفاقية؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة (أ) 1' أو 2' أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في الأحكام بشأن الدخول غير المشروع والاعتراض غير المشروع، والتدخل في البيانات أو النظم في هذه الاتفاقية. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في الأحكام بشأن الدخول غير المشروع والاعتراض غير المشروع والتدخل في البيانات أو النظم في هذه الاتفاقية، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

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

(ب) الجرائم الحاسوبية

التزوير الحاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير وجه حق: إدخال بيانات حاسوبية أو تحويلها أو حذفها أو طمسها، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة مشابهة.

الاحتيال الحاسوبي

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُجرّم في قانونها الوطني التسبب عمداً وبغير وجه حق في إلحاق خسائر بممتلكات الغير عن طريق:

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

(ب) أي تدخل في عمل نظام حاسوبي، بقصد الاحتيال أو بنية سيئة، للحصول، بدون وجه حق، على منفعة اقتصادية للنفس أو للغير.

(ج) جرائم المحتوى

الجرائم المتصلة بمواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:

(أ) إنتاج مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا بغرض توزيعها عبر نظام حاسوبي؛

(ب) عرض أو إتاحة مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا من خلال نظام حاسوبي؛

(ج) توزيع مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا أو بثها عبر نظام حاسوبي؛

(د) اقتناء مواد للاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا عبر نظام حاسوبي للنفس أو للغير؛

(هـ) حيازة مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا داخل نظام حاسوبي أو وسيط لتخزين البيانات الحاسوبية.

2- لغرض الفقرة 1 أعلاه، يشمل مصطلح "مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا" المواد التي تعرض بشكل مرئي:

(أ) قاصرا وهو يمارس سلوكا جنسيا صريحا؛

(ب) شخصا يبدو قاصرا وهو يمارس سلوكا جنسيا صريحا؛

(ج) صورا واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا صريحا.

3- لغرض الفقرة 2 أعلاه، يشمل مصطلح "قاصر" كافة الأشخاص دون سن الثامنة عشر. ويجوز لأي دولة طرف أن تشترط حدا عمريا أدنى لا يقل عن سن السادسة عشرة.

4- يجوز لكل دولة طرف أن تحتفظ بالحق في عدم التطبيق، الكلي أو الجزئي، للبندين (د) و(هـ) من الفقرة 1 والبندين (ب) و(ج) من الفقرة 2.

(د) المسؤولية الإضافية والجزاءات

الشروع والمساعدة والتحريض

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في أحكام التجريم من هذه الاتفاقية مع توفر النية على ارتكابها.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا: الشروع في ارتكاب أي جريمة من الجرائم المنصوص عليها في أحكام التجريم من هذه الاتفاقية.

3- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 2 من هذه المادة كليا أو جزئيا.

مسؤولية الشخصيات الاعتبارية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لضمان مساءلة الأشخاص الاعتباريين عن الجرائم المنصوص عليها في أحكام التجريم من هذه الاتفاقية التي تُرتكب لمصلحتهم من قبل أي شخص طبيعي، سواء قام بذلك بمفرده أو باعتباره عضواً 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 الرقابة لدى الشخص الاعتباري.

2- إضافة إلى الحالات المنصوص عليها مسبقاً في الفقرة 1 من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان إمكانية تحميل الشخص الاعتباري المسؤولية في حال ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 في ارتكاب جريمة منصوص عليها وفقاً لهذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.

3- رهنا بالمبادئ القانونية للدولة الطرف، يمكن أن تكون المسؤولية القانونية للشخص الاعتباري جنائية أو مدنية أو إدارية.

4- لا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجريمة.

العقوبات والتدابير

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في أحكام التجريم من هذه الاتفاقية مُعاقب عليها بعقوبات فعالة ومتناسبة وراعية، بما في ذلك العقوبات السالبة للحرية.

2- تضمن كل دولة طرف مساءلة الأشخاص الاعتباريين وفقاً للحكم الخاص بمسؤولية الأشخاص الطبيعيين من هذه الاتفاقية وإخضاعهم لعقوبات أو تدابير فعالة ومتناسبة وراعية، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات النقدية.

المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية

[الأصل: بالإنكليزية]

[12 نيسان/أبريل 2022]

الفصل الخاص بالتجريم

الجرائم المرتكبة في الفضاء السيبراني

تعتقد المملكة المتحدة أن الاتفاقية يجب أن تشمل الجرائم المرتكبة في الفضاء السيبراني مع أوصاف وتعريف مقبولة لجميع الأطراف، ومتسقة مع الاتفاقات الدولية القائمة في هذا المجال.

المادة 5

الدخول غير المشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: الدخول الكامل أو الجزئي إلى نظام حاسوبي. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة وقوع مخالفة للتدابير الأمنية بقصد الحصول على بيانات حاسوبية أو بنية سيئة أخرى أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 6

الاعتراض غير المشروع

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

المادة 7

التدخل في البيانات

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.
- 2- يجوز للدولة الطرف أن تحتفظ بحقها في اشتراط أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم.

المادة 8

التدخل في النظم

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدا وبغير وجه حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

المادة 9

إساءة استخدام الأجهزة

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:
 - (أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

'1' جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملاءمته مبدئياً، بغرض ارتكاب أي من الجرائم المنصوص عليها في أقسام الاتفاقية؛

'2' كلمة سر خاصة بحاسوب، أو رمز الولوح، أو بيانات مماثلة يمكن بواسطتها الدخول على منظومة حاسوبية كاملة أو أي جزء منها، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد الأربع الأخرى من هذا القسم؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة 1 (أ) '1' أو '2'، أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد الأربع الأخرى من هذا القسم. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية بموجب القانون الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد المتعلقة بالدخول غير المشروع والاعتراض غير المشروع، والتدخل في البيانات والنظم، بل هو بالأحرى الاستخدام المرخص للشئ موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

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

الجرائم التي يبيّر الفضاء السيبراني ارتكابها

ترى المملكة المتحدة أيضاً أن الجرائم التي يبيّر الفضاء السيبراني ارتكابها ينبغي إدراجها متى كانت الجريمة تُرتكب بشكل أساسي عبر الإنترنت وكانت الحواسيب تُغير من حجم الجريمة وسرعتها ومتى كانت تعريفات الجريمة مفهومة لدى الجميع.

المادة 10

الاحتتيال

تعتمد كل دولة طرف ما يلزم من تغييرات تشريعية وغيرها من التدابير كي تجرم في قانونها الوطني جريمة الاحتتيال العامة المرتكبة بالكامل أو جزئياً عبر الإنترنت. ويشمل ذلك، على سبيل المثال لا الحصر، النشاط المرتكب داخلياً، وعبر الحدود من خلال الإنترنت، أو غيرها من الوسائل السيبرانية/الرقمية بالطرائق التالية:

(أ) الاحتتيال عن طريق تقديم بيانات كاذبة،

(ب) الاحتتيال من خلال عدم الكشف عن المعلومات،

(ج) الاحتتيال عن طريق إساءة استخدام المنصب، مع نية احتيالية أو غير شريفة للتسبب في خسارة لشخص آخر أو تحقيق مكاسب في المال أو الممتلكات الأخرى لشخص آخر.

المادة 11

الجرائم المتعلقة بالاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا عبر الإنترنت، بما في ذلك مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا واستمالة الأطفال عبر الإنترنت

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم السلوكيات التالية في قانونها الوطني، إذا ما ارتكبت عمدا وبغير وجه حق:

- (أ) إنتاج مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا بغرض توزيعها عبر نظام حاسوبي؛
- (ب) عرض مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا أو إتاحتها عبر نظام حاسوبي؛
- (ج) توزيع مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا أو بثها عبر نظام حاسوبي؛
- (د) اقتناء مواد للاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا عبر نظام حاسوبي للنفس أو للغير؛

(هـ) حيازة مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا داخل نظام حاسوبي أو على وسيط لتخزين البيانات الحاسوبية.

(و) مشاهدة مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا داخل نظام حاسوبي أو على وسيط لتخزين البيانات الحاسوبية.

2- لغرض الفقرة 1 أعلاه، يشمل مصطلح "مواد الاستغلال الجنسي للأطفال والاعتداء عليهم جنسيا" المواد التي تعرض بشكل مرئي:

- (أ) قاصرا وهو يمارس سلوكا جنسيا صريحا حقيقيا أو تمثليا؛
- (ب) شخصا يبدو قاصرا وهو يمارس سلوكا جنسيا صريحا حقيقيا أو تمثليا؛
- (ج) صورا واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا صريحا حقيقيا أو تمثليا.
- (د) أي تصوير للأعضاء الجنسية لقاصر لأغراض جنسية في المقام الأول.

3- لغرض الفقرة 2 أعلاه، يشمل مصطلح "قاصر" كافة الأشخاص دون سن الثامنة عشرة. ويجوز لأي دولة طرف أن تشترط حدا عمريا أدنى لا يقل عن سن السادسة عشرة.

4- يجوز لكل دولة طرف أن تحتفظ بالحق في عدم التطبيق، الكلي أو الجزئي، للبندين (د) و(هـ) من الفقرة 1 والبندين (ب) و(ج) من الفقرة 2.

المادة 12

الجرائم المتعلقة بانتهاكات حقوق التأليف والنشر والحقوق المجاورة

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق التأليف والنشر، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعا لالتزاماتها بموجب وثيقة باريس المؤرخة في 24 تموز/يوليه 1971 فيما يتعلق باتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق

المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام حاسوبي.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق المجاورة، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجاتي الاسطوانيات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام حاسوبي.

3- يجوز للدولة الطرف الاحتفاظ بالحقوق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و 2 من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين 1 و 2 من هذه المادة.

المادة 13

الشروع والمساعدة والتحريض

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمداً: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في [هذه الاتفاقية] مع توفر النية على ارتكابها.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتُكبت عمداً: الشروع في ارتكاب أي جريمة من الجرائم المنصوص عليها في هذه الاتفاقية.

3- يجوز لكل دولة طرف الاحتفاظ بالحقوق في عدم تطبيق الفقرة 2 من هذه المادة كلياً أو جزئياً.

المادة 14

الملاحقة والمقاضاة والجزاءات

1- تجعل كل دولة طرف ارتكاب أي فعل مجرم وفقاً لهذه الاتفاقية خاضعاً لعقوبات تُراعى فيها جسامته ذلك الجرم.

2- تسعى كل دولة طرف إلى ضمان أن أية صلاحيات قانونية تقديرية يتيحها قانونها الداخلي فيما يتعلق بملاحقة الأشخاص لارتكابهم جرائم مشمولة بهذه الاتفاقية تُمارس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القانون التي تتخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة ردع ارتكابها.

3- في حالة الأفعال المجرمة وفقاً لهذه الاتفاقية، تتخذ كل دولة طرف تدابير مناسبة، وفقاً لقانونها الداخلي ومع إيلاء الاعتبار الواجب لحقوق الدفاع، لضمان أن تراعي الشروط المفروضة بخصوص قرارات الإفراج إلى حين المحاكمة أو الاستئناف ضرورة حضور المدعى عليه في الإجراءات الجنائية اللاحقة.

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

5- تحدّد كل دولة طرف في إطار قانونها الداخلي، عند الاقتضاء، مدة تقادم طويلة تستهل أثناءها الإجراءات الخاصة بأيّ جرم مشمول بهذه الاتفاقية، ومدة أطول عندما يكون الجاني المزعوم قد فرّ من وجه العدالة.

6- ليس في هذه الاتفاقية ما يمس بالمبدأ القاضي بأن يكون الحق في توصيف الأفعال المجرّمة وفقا لهذه الاتفاقية وتوصيف الدفوع القانونية المنطبقة أو المبادئ القانونية الأخرى التي تحكم مشروعية السلوك محفوظا حصرا للقانون الداخلي للدولة الطرف، وبوجوب الملاحقة القضائية لمرتكبي تلك الجرائم ومعاقبتهم وفقا لذلك القانون.

المادة 15

الولاية القضائية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير لبسط ولايتها القضائية على الأفعال المجرّمة وفقا لهذه الاتفاقية في الحالات التالية:

- (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 المواد ذات الصلة من هذه الاتفاقية، يجوز للدولة الطرف أن تُخضع أيضا أي جرم من هذا القبيل لولايتها القضائية في الحالات التالية:

- (أ) عندما يُرتكب الجرم ضد أحد مواطني تلك الدولة الطرف؛ أو
- (ب) عندما يُرتكب الجرم أحد مواطني تلك الدولة الطرف أو شخص عديم الجنسية يوجد مكان إقامته المعتاد في إقليمها؛ أو
- (ج) عندما يُرتكب الجرم ضد الدولة الطرف.

3- لأغراض أي مادة من هذه الاتفاقية تتعلق بتسليم المطلوبين، يجوز لكل دولة طرف أن تعتمد ما قد يلزم من تدابير لإخضاع الأفعال المجرّمة 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 المجرّمة وفقا لهذه الاتفاقية لولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه.

5- إذا أبلغت 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 جنائية تؤكد الدولة الطرف سريانها وفقا لقانونها الداخلي.

تعليقات إضافية

تعتقد المملكة المتحدة أن من الواجب تجريم استخدام التكنولوجيا الرقمية للاتصال بقاصر عندما يكون هذا الاتصال جنسيا بطبيعته، أو يتم بقصد تشجيع القاصر على الانخراط في اتصال أو نشاط جنسي، وحيثما يتم هذا الاتصال لغرض الحصول على الإشباع الجنسي، وسنقدم نصا حول هذا الموضوع أثناء المفاوضات. والاتجار بالنساء والفتيات واستغلالهن جنسيا جريمة شديدة الضرر بوجه خاص، ويتعرض الضحايا للعديد من التجاوزات خلال فترة استغلالهن التي تسبب ضررا بدنيا وعاطفيا بالغا. وبما أن الجزء الأكبر من هذا الاستغلال يتم ترتيبه وتسهيله عبر الإنترنت، فإن هذه القضية عالمية، وتعتقد المملكة المتحدة أننا بحاجة إلى نهج موحد إزاء هذا التهديد. وتؤيد المملكة المتحدة إدراج حكم في هذه الاتفاقية لتجريم الرق الحديث والاتجار بالبشر، بما في ذلك الاتجار والاستغلال الجنسي من خلال المواقع الإلكترونية لخدمات البالغين. وتعتقد المملكة المتحدة أن الضرر الذي يشكله النشر غير المصرح به للصور الحميمة يتطلب منا اتباع نهج منسق لمنع مثل تلك الإساءة، بما في ذلك من خلال إزالة تلك الصور وضمان وجود عقوبات فعالة ضد ناشري الصور غير المصرح بها. وتود المملكة المتحدة أن تُدرج أحكام لمعالجة هذا الضرر.

جمهورية تنزانيا المتحدة

[الأصل: بالإنكليزية]

[11 نيسان/أبريل 2022]

4- التجريم

في الآونة الأخيرة، حدثت زيادة هائلة في استخدام الجماعات الإجرامية في جميع أنحاء العالم لتكنولوجيات المعلومات والاتصالات في أغراض إجرامية بسبب التطور التكنولوجي.

1-4 قائمة الجرائم

بسبب هذا التحدي، ترى جمهورية تنزانيا المتحدة ضرورة أن تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير، لتجريم الأفعال التالية، عند ارتكابها عن عمد وقصد، على سبيل المثال لا الحصر:

- (أ) الدخول غير المشروع؛
- (ب) الاعتراض غير المشروع؛
- (ج) التدمير غير القانوني للبيانات الإلكترونية والنظام الحاسوبي؛
- (د) التجسس على البيانات؛
- (هـ) التدخل غير المشروع في النظم؛
- (و) امتلاك أجهزة و/أو برمجيات غير قانونية لأغراض ارتكاب الجرائم؛
- (ز) التزوير والاحتياز الحاسوبي؛
- (ح) المواد الإباحية واستغلال الأطفال في المواد الإباحية؛
- (ط) الجرائم المتعلقة بالهوية؛

- (ي) نشر المعلومات الخاطئة؛
 (ك) المواد العنصرية والمعادية للأجانب؛
 (ل) الإبادة الجماعية والجرائم المرتكبة ضد الإنسانية؛
 (م) التتبع السيبراني؛
 (ن) الشروع والمساعدة والتحريض؛
 (س) المشاركة في جماعة إجرامية منظمة.

2-4 مسؤولية الشركات

تقترح جمهورية تنزانيا المتحدة أن تشترط الاتفاقية على الدول الأعضاء أن تدرج في تشريعاتها الداخلية أحكاماً تحمل الأشخاص الاعتباريين المسؤولية عما يرتكبونه من أفعال مجرمة بموجب الاتفاقية. وقد تمتد المسؤولية إلى الأشخاص الطبيعيين الذين يتصرفون باسم شركات أو تحت غطاءها.

الولايات المتحدة الأمريكية

[الأصل: بالإنكليزية]

[8 نيسان/أبريل 2022]

التجريم

تجريم الجرائم السيبرانية

"الدخول غير المشروع"

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الدخول الكامل أو الجزئي إلى نظام حاسوبي، إذا ما ارتكب عمداً وبغير وجه حق. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة وقوع مخالفة للتدابير الأمنية بقصد الحصول على بيانات حاسوبية أو بنية سيئة أخرى أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

"الاعتراض غير المشروع"

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي، إذا ما ارتكب عمداً وبغير وجه حق: القيام، من خلال وسائل تقنية، باعتراض الإرسال غير العمومي للبيانات الحاسوبية إلى نظام حاسوبي أو منه أو داخله، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام حاسوبي يحمل هذه البيانات. ويجوز للدولة الطرف أن تشترط لتحقيق الجريمة توفر سوء النية أو وجود علاقة بنظام حاسوبي متصل بنظام حاسوبي آخر.

"التدخل في البيانات"

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتكبت عمداً وبغير وجه حق: إتلاف بيانات حاسوبية أو حذفها أو إفسادها أو تحويلها أو طمسها.

2- يجوز للدولة الطرف أن تحتفظ بحقها في اشتراط أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم.

"التدخل في النظم"

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي، إذا ما ارتكب عمدا وبغير وجه حق: الإعاقة الخطيرة لعمل نظام حاسوبي عن طريق إدخال بيانات حاسوبية أو بثها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.

"إساءة استعمال الأجهزة"

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتكبت عمدا وبغير وجه حق:

(أ) إنتاج الأشياء التالية أو بيعها أو شراؤها بغرض الاستخدام أو استيرادها أو توزيعها أو إتاحتها بأي طريقة أخرى:

'1' جهاز، بما في ذلك برنامج حاسوبي، تم تصميمه أو ملأته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد السابقة من هذا الفصل؛

'2' كلمة سر خاصة بحاسوب، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام حاسوبي؛

بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد السابقة من هذا الفصل؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة 1 (أ) '1' أو '2' أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد السابقة من هذا الفصل. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية القانونية بموجب القانون الحيازة المسبقة لعدد من هذه الأشياء.

2- لا يجوز تفسير هذه المادة على أنها تفرض مسؤولية جنائية، ما دامت عمليات الإنتاج أو البيع أو الشراء بغرض الاستخدام أو الاستيراد أو التوزيع أو الإتاحة بطريقة أخرى أو الحيازة المشار إليها في الفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد السابقة من هذا الفصل، بل هو بالأحرى الاستخدام المرخص للشيء موضوع تلك العمليات لاختبار نظم حاسوبية أو حمايتها على سبيل المثال.

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

"التزوير الحاسوبي"

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتكبت عمدا وبغير وجه حق: إدخال بيانات حاسوبية أو تغييرها أو حذفها أو إتلافها، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد أخذها في الاعتبار أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت

تلك البيانات قابلة للقراءة أو الفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط لإسناد المسؤولية الجنائية الوجود المسبق لنية الاحتيال أو نية سيئة مشابهة.

"الاحتيال الحاسوبي"

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير كي يُجرّم التسبب عمداً وبغير وجه حق في إلحاق خسائر بممتلكات الغير عن طريق:

(أ) أي إدخال أو تغيير أو حذف أو إتلاف لبيانات حاسوبية؛

(ب) أي تدخل في وظيفة نظام حاسوبي؛

بقصد الاحتيال أو بنية سيئة، للحصول، بدون وجه حق، على منفعة اقتصادية للنفس أو للغير.

"الجرائم المتعلقة بالحاسوب التي تنطوي على مواد للاعتداء الجنسي على الأطفال"

1- تتخذ كل دولة طرف ما قد يلزم من تدابير تشريعية أو تدابير أخرى لضمان تجريم السلوك التالي، عندما يُرتكب عن علم ومن خلال نظام حاسوبي:

(أ) إنتاج مواد الاعتداء الجنسي على الأطفال؛

(ب) التسبب في البث المباشر لطفل منخرط في سلوك جنسي صريح؛

(ج) عرض مواد الاعتداء الجنسي على الأطفال أو إتاحتها؛

(د) توزيع مواد الاعتداء الجنسي على الأطفال أو بثها؛

(هـ) اقتناء مواد الاعتداء الجنسي على الأطفال للنفس أو للغير؛

(و) حيازة مواد الاعتداء الجنسي على الأطفال؛

(ز) الحصول عن علم من خلال تكنولوجيا المعلومات والاتصالات على مواد الاعتداء

الجنسي على الأطفال أو مشاهدة البث المباشر لطفل منخرط في سلوك جنسي صريح.

2- تتخذ كل دولة طرف التدابير التشريعية أو غيرها من التدابير اللازمة لتجريم إقناع طفل، أو فرد يُعتقد أنه طفل، عن علم، بممارسة أي نشاط جنسي غير مشروع، أو إغرائه أو استدراجه لذلك أو إكراهه عليه عن طريق تكنولوجيا المعلومات والاتصالات. وتتخذ كل دولة طرف التدابير التشريعية أو غيرها من التدابير اللازمة لضمان ألا يشترط قانونها الوطني وقوع لقاء شخصي بين الفرد والطفل.

"الجرائم الحاسوبية المتعلقة بانتهاكات حقوق التأليف والنشر والحقوق المجاورة"

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي: انتهاك حقوق التأليف والنشر، وفقاً لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعا لالتزاماتها بموجب وثيقة باريس المؤرخة في 24 تموز/يوليه 1971 فيما يتعلق باتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام حاسوبي.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك الحقوق المجاورة، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب الاتفاقية الدولية لحماية الفنانين الأدائيين ومنتجي الاسطوانات وهيئات البث الإذاعي (اتفاقية روما)، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة المنظمة العالمية للملكية الفكرية بشأن الأداء والتسجيلات الصوتية، باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام حاسوبي.

3- يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و 2 من هذه المادة في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وأن يتقيد هذا التحفظ بالالتزامات الدولية للدولة الطرف المنصوص عليها في الصكوك الدولية المشار إليها في الفقرتين 1 و 2 من هذه المادة.

"المشاركة والشروع"⁽³⁷⁾

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرم، وفقاً لقانونها الداخلي، المشاركة بأي صفة، مثل الشريك أو المساعد أو المحرض، في ارتكاب فعل مجرم وفقاً لهذه الاتفاقية.

2- يجوز لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرم، وفقاً لقانونها الداخلي، أي شروع في ارتكاب فعل مجرم وفقاً لهذه الاتفاقية.

3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرم، وفقاً لقانونها الداخلي، الإعداد لارتكاب فعل مجرم وفقاً لهذه الاتفاقية.

مسؤولية الشخصيات الاعتبارية⁽³⁸⁾

1- تعتمد كل دولة طرف ما قد يلزم من تدابير، تتسق مع مبادئها القانونية، لتقرير مسؤولية الشخصيات الاعتبارية بشأن الأفعال المجرمة وفقاً للمواد المتعلقة بالتجريم من هذه الاتفاقية.

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

3- لا تمس تلك المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم.

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

الملاحقة والمقاضاة والجزاءات⁽³⁹⁾

1- تجعل كل دولة طرف ارتكاب أي فعل مجرم وفقاً للمواد المتعلقة بالتجريم من هذه الاتفاقية خاضعاً لعقوبات تُراعى فيها جسامته ذلك الجرم.

(37) المادة 27 من اتفاقية الأمم المتحدة لمكافحة الفساد.

(38) المادة 10 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والمادة 26 من اتفاقية الأمم المتحدة لمكافحة الفساد.

(39) المادة 11 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

- 2- تسعى كل دولة طرف إلى ضمان أنَّ أية صلاحيات قانونية تقديرية يتيحها قانونها الداخلي فيما يتعلق بملاحقة الأشخاص لارتكابهم جرائم مشمولة بهذه الاتفاقية تُمارس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القانون التي تتخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة ردع ارتكابها.
- 3- في حالة الأفعال المجرّمة وفقا للمواد المتعلقة بالتجريم من هذه الاتفاقية، تتخذ كل دولة طرف تدابير مناسبة، وفقا لقانونها الداخلي ومع إيلاء الاعتبار الواجب لحقوق الدفاع، لضمان أن تراعي الشروط المفروضة بخصوص قرارات الإفراج إلى حين المحاكمة أو الاستئناف ضرورة حضور المدعى عليه في الإجراءات الجنائية اللاحقة.
- 4- تكفل كل دولة طرف مراعاة محاكمها أو سلطاتها المختصة الأخرى خطورة الجرائم المشمولة بهذه الاتفاقية لدى النظر في إمكانية الإفراج المبكر أو المشروط عن الأشخاص المدانين بارتكاب تلك الجرائم.
- 5- تحدّد كل دولة طرف في إطار قانونها الداخلي، عند الاقتضاء، مدة تقادم طويلة تستهل أثناءها الإجراءات الخاصة بأيّ جرم مشمول بهذه الاتفاقية، ومدة أطول عندما يكون الجاني المزعوم قد فرّ من وجه العدالة.
- 6- ليس في هذه الاتفاقية ما يمس بالمبدأ القاضي بأن يكون الحق في توصيف الأفعال المجرّمة وفقا لهذه الاتفاقية وتوصيف الدفوع القانونية المنطبقة أو المبادئ القانونية الأخرى التي تحكم مشروعية السلوك محفوظا حصرا للقانون الداخلي للدولة الطرف، وبوجوب الملاحقة القضائية لمرتكبي تلك الجرائم ومعاقبهم وفقا لذلك القانون.

تجريم غسل عائدات الجرائم السيبرانية⁽⁴⁰⁾

- 1- تعتمد كل دولة طرف، وفقا للمبادئ الأساسية لقانونها الداخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، عندما تُرتكب عمدا:
- (أ) '1' تحويل الممتلكات أو نقلها، مع العلم بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات، أو مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي الذي تأتت منه على الإفلات من العواقب القانونية لأفعاله؛
- '2' إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأن تلك الممتلكات هي عائدات إجرامية؛
- (ب) رهنا بالمفاهيم الأساسية لنظامها القانوني:
- '1' اكتساب الممتلكات أو حيازتها أو استخدامها مع العلم، وقت استلامها، بأنها عائدات إجرامية؛
- '2' المشاركة في ارتكاب أي من الجرائم المنصوص عليها في هذه المادة، أو التواطؤ أو التآمر على ارتكابها، والشروع في ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.
- 2- لأغراض تنفيذ أو تطبيق الفقرة 1 من هذه المادة:
- (أ) تدرج كل دولة طرف في عداد الجرائم الأصلية الأفعال المجرّمة وفقا لمواد التجريم من هذه الاتفاقية. أما الدول الأطراف التي تحدد تشريعاتها قائمة جرائم أصلية معينة، فتدرج في تلك القائمة، كحد أدنى، الجرائم الواردة في هذه الاتفاقية؛

(40) مقتبس بتصرف من المادة 6 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

(ب) لأغراض الفقرة الفرعية (ب)، تشمل الجرائم الأصلية الجرائم المرتكبة داخل وخارج الولاية القضائية للدولة الطرف المعنية. غير أن الجرائم المرتكبة خارج الولاية القضائية للدولة الطرف لا تمثل جرائم أصلية إلا إذا كان السلوك ذو الصلة يُعتبر فعلاً إجرامياً بمقتضى القانون الداخلي للدولة التي ارتُكبت فيها وكان من شأنه أن يُعتبر فعلاً إجرامياً بمقتضى القانون الداخلي للدولة الطرف التي تُنفَّذ أو تُطَبَّق هذه المادة لو كان قد ارتُكبت هناك؛

(ج) تزود كل دولة طرف الأمين العام للأمم المتحدة بنسخ من قوانينها المُنفَّذة لهذه المادة وبنسخ من أي تغييرات تُدخَل على تلك القوانين لاحقاً أو بوصف لها؛

(د) يجوز النص على أن الجرائم المبينة في الفقرة 1 من هذه المادة لا تنطبق على الأشخاص الذين ارتكبوا الجرم الأصلي إذا كانت المبادئ الأساسية للقانون الداخلي للدولة الطرف تقتضي ذلك؛

(هـ) يُستدل على عنصر العلم أو القصد أو الغرض، الذي يلزم توافره في أيّ جرم مبين في الفقرة 1 من هذه المادة، من ملابسات الوقائع الموضوعية.

تجريم عرقلة سير العدالة⁽⁴¹⁾

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتُكبت عمداً:

(أ) استخدام القوة البدنية أو التهديد أو الترهيب أو الوعد بمزية غير مستحقة أو عرضها أو منحها للتحريض على الإدلاء بشهادة زور أو للتدخل في الإدلاء بالشهادة أو تقديم الأدلة في إجراءات تتعلق بارتكاب جرائم مشمولة بهذه الاتفاقية؛

(ب) استخدام القوة البدنية أو التهديد أو الترهيب للتدخل في ممارسة أيّ موظف قضائي أو موظف معني بإنفاذ القانون مهامه الرسمية في إجراءات تتعلق بارتكاب جرائم مشمولة بهذه الاتفاقية. وليس في هذه الفقرة الفرعية ما يمسّ حقوق الدول الأطراف في أن تكون لديها تشريعات تحمي فئات أخرى من الموظفين العموميين.

فنزويلا (جمهورية - البوليفارية)

[الأصل: بالإسبانية]

[13 نيسان/أبريل 2022]

5- التجريم

من شأن الاتفاقية أن تلزم الدول الأطراف بتحديد جرائم جنائية وغير جنائية من أجل تغطية طائفة واسعة من الأفعال غير المشروعة المتصلة باستخدام تكنولوجيا المعلومات والاتصالات حيثما كانت الأفعال المحددة في الاتفاقية لا تشكل بالفعل جرائم بموجب القانون الوطني. وفي بعض الحالات، يكون على الدول التزام قانوني بالنص على تجريم تلك الأفعال، بينما تكون ملزمة في حالات أخرى، من أجل مراعاة الاختلافات في التشريعات الوطنية، بوضع تشريعات ذات صلة.

(41) المادة 23 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

وبناءً على ذلك، يجب تحديد الأنشطة الإجرامية التي تُرتكب باستخدام تكنولوجيا المعلومات والاتصالات والمُعترف بها على نطاق واسع في المجتمع الدولي تعريفاً واضحاً. وينبغي أن توفّر الاتفاقية إطاراً يستشرف المستقبل بغية تنسيق التجريم، بما يلبي الاحتياجات في مجال تطوير تكنولوجيا المعلومات والاتصالات حاضراً ومستقبلاً، ويعمل على مكافحة الجريمة.

وفي ضوء ما تقدم، ينبغي لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشريعية وسياساتية وغير ذلك من التدابير لتجريم الأفعال المعنية. ولذلك ينبغي أن تتضمن الاتفاقية أحكاماً تكفل أن يكون لدى الدول التي تحتاج إلى تكييف تشريعاتها وبرامجها الوطنية الوقت الكافي للقيام بذلك وتلقي الدعم اللازم. وينبغي أن تشمل الجرائم الرئيسية التي ستشملها الاتفاقية ما يلي:

- الوصول دون الحصول على الإذن الواجب إلى المعلومات الرقمية عندما يؤدي هذا الوصول إلى إتلاف تلك المعلومات أو حجبها أو تعديلها.
- الاعتراض المتعمد للمعلومات الرقمية دون إذن مناسب و/أو في انتهاك للقواعد المعمول بها، بما في ذلك من خلال استخدام الوسائل التقنية لاعتراض بيانات تتّبع المستخدمين والبيانات غير المخصصة للاستخدام العام التي تُعالج بواسطة تكنولوجيا المعلومات والاتصالات.
- التلاعب غير القانوني بالمعلومات الرقمية عن طريق إتلافها أو حذفها أو تحويلها أو حجبها أو تعديلها.
- الأفعال غير المشروعة المتعمدة التي يُقصد بها التسبب في خلل في شبكات المعلومات والاتصالات تترتب عليه عواقب وخيمة أو يشكل خطراً وخيم العاقبة.
- استخدام وتوزيع برمجيات ضارة تهدف إلى إتلاف المعلومات الرقمية أو حجبها أو تعديلها أو نشرها دون تصريح أو تحييد السمات الأمنية.
- إنشاء برمجيات أو معلومات رقمية أخرى و/أو توزيعها و/أو استخدامها عمداً ومع سبق الإصرار والترصد لغرض التلاعب غير المشروع بالبنى التحتية الحيوية للمعلومات، بما في ذلك إتلاف المعلومات الواردة فيها أو حجبها أو تعديلها أو تحييد السمات الأمنية.
- تعمّد إنشاء و/أو توزيع و/أو استخدام برمجيات أو معلومات رقمية أخرى مصممة عن علم للتدخل بصورة غير مشروعة في البنى التحتية الحيوية للمعلومات، بما في ذلك البرمجيات أو المعلومات الرقمية الأخرى المستخدمة من أجل إتلاف المعلومات الموجودة بتلك المرافق أو حجبها أو تعديلها أو نسخها أو من أجل تحييد السمات الأمنية.
- انتهاك قواعد تشغيل الوسائط المستخدمة لتخزين ومعالجة وبحث البيانات الرقمية المحمية في البنية التحتية الحيوية للمعلومات أو نظم المعلومات وشبكات المعلومات والاتصالات التي تنتمي إلى البنية التحتية الحيوية للمعلومات، أو انتهاك قواعد الوصول إليها إذا كان ذلك الانتهاك يضر بالبنية التحتية الحيوية للمعلومات.
- سرقة الممتلكات أو اكتساب الحقوق في الممتلكات بصورة غير مشروعة، بما في ذلك عن طريق الاحتيال من خلال إتلاف المعلومات الرقمية أو حجبها أو تعديلها أو التدخل بطريقة أخرى في عمليات تكنولوجيا المعلومات والاتصالات.
- النداءات الصادرة بواسطة تكنولوجيا المعلومات والاتصالات للقيام بأنشطة تخريبية أو مسلحة موجهة نحو الإطاحة العنيفة بحكومة دولة أخرى.

- النداءات الصادرة بواسطة تكنولوجيا المعلومات والاتصالات للتحريض على الاضطلاع بأنشطة إرهابية أو تجنيد عناصر لهذا الغرض أو المشاركة فيه بأي شكل آخر، أو للدعوة إلى الإرهاب وتبويره، أو لجمع الأموال أو توفيرها لتمويله.
- الاتجار بالعقاقير المخدرة والمؤثرات العقلية والمواد اللازمة لصنعها، بواسطة تكنولوجيا المعلومات والاتصالات.
- الاتجار بالأسلحة والذخائر والأجهزة والمواد المتفجرة بواسطة تكنولوجيا المعلومات والاتصالات
- الوصول غير المصرح به إلى البيانات الشخصية من أجل إتلافها أو تعديلها أو نسخها أو تداولها.
- الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات المتصلة بإنتاج وتوزيع مواد أو أشياء ذات صور إباحية للقصر.
- الجرائم المتصلة بإشراك القصر في ارتكاب أعمال غير مشروعة تُعرض حياتهم أو صحتهم للخطر.

فبييت نام

[الأصل: بالإنكليزية]

[12 نيسان/أبريل 2022]

الفصل الثاني - التجريم

5- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية، إذا ما ارتكبت عمدا وعلى نحو غير مأذون به:

- (أ) صنع أدوات أو معدات أو برمجيات يُقصد بها مهاجمة شبكة حاسوبية أو شبكة اتصالات أو جهاز إلكتروني أو الاتجار بها أو نقلها لاستخدامها في الاضطلاع بأنشطة إجرامية على النحو الذي تحكمه هذه الاتفاقية؛
- (ب) نشر برمجية حاسوبية ضارة عبر شبكة حاسوبية أو شبكة اتصالات أو جهاز إلكتروني؛
- (ج) حذف برمجيات أو بيانات رقمية أو تخريبها أو تعديلها؛
- (د) عرقلة بث بيانات شبكة حاسوبية أو شبكة اتصالات أو جهاز إلكتروني؛
- (هـ) عرقلة أو تعطيل عمليات شبكة حاسوبية أو شبكة اتصالات أو جهاز إلكتروني؛
- (و) السيطرة على جهاز إلكتروني أو التدخل في تشغيله عن طريق تخطي نظام الأمن أو الحماية، أو إساءة استخدام حقوق الإدارة الخاصة بشخص آخر، أو أي وسيلة أخرى؛
- (ز) سرقة المعلومات أو البيانات أو تعديلها أو تخريبها أو تزيفها؛
- (ح) استخدام شبكة حاسوبية أو شبكة اتصالات أو جهاز إلكتروني للأغراض التالية:
 - '1' استخدام معلومات الحساب المصرفي أو البطاقة المصرفية الخاصة بكيان أو فرد للاستيلاء على الموجودات بشكل غير قانوني؛
 - '2' صنع أو حيازة أو تداول أو استخدام بطاقات مصرفية مزيفة من أجل الاستيلاء على الموجودات بشكل غير قانوني؛

٣' الوصول غير المصرح به إلى حسابات الهيئات الحكومية والمنظمات والأفراد للاستيلاء غير القانوني على الموجودات؛

٤' ارتكاب عمليات احتيال في سياق عمليات التجارة الإلكترونية أو الدفع الإلكتروني أو تداول العملات عبر الإنترنت أو زيادة رأس المال عبر الإنترنت أو التسويق المتعدد المستويات عبر الإنترنت أو تداول الأوراق المالية عبر الإنترنت لغرض الاستيلاء على الممتلكات؛

٥' إنشاء أو توفير خدمة الاتصالات أو الإنترنت دون إذن لغرض الاستيلاء على الممتلكات؛

(ط) جمع معلومات الحسابات المصرفية للأفراد والمنظمات أو حيازتها أو تداولها أو نقلها أو نشرها؛

(ي) تداول المعلومات الخاصة بالهيئات الحكومية أو المنظمات أو الأفراد ونقلها وتعديلها ونشرها دون موافقة أصحابها؛

(ك) استخدام الفضاء السيبراني أو تكنولوجيات المعلومات أو الأجهزة الإلكترونية للقيام بعمل إرهابي أو تمويل الإرهاب.

6- ليس في هذه الاتفاقية ما يمنع الدول الأعضاء من اعتماد ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم أي فعل آخر ينطوي على استعمال تكنولوجيات المعلومات والاتصالات لأغراض إجرامية.

7- ليس في هذه الاتفاقية ما يمس بالمبدأ القاضي بأن يكون الحق في توصيف الأفعال المجرمة وفقا لهذه الاتفاقية وتوصيف الدفوع القانونية المنطبقة أو المبادئ القانونية الأخرى التي تحكم مشروعية السلوك محفوفا حصرا للقانون الداخلي للدولة العضو، وبوجوب الملاحقة القضائية لمرتكبي تلك الجرائم ومعاقتهم وفقا لذلك القانون.