

Distr.: General
7 November 2022
Arabic
Original: English

الجمعية العامة



اللجنة المخصصة لوضع اتفاقية دولية شاملة
بشأن مكافحة استخدام تكنولوجيات المعلومات
والاتصالات للأغراض الإجرامية
الدورة الرابعة
فيينا، 9-20 كانون الثاني/يناير 2023

وثيقة التفاوض الموحدة بشأن الأحكام العامة والأحكام المتعلقة بالتجريم
وبالتدابير الإجرائية وإنفاذ القانون لاتفاقية دولية شاملة بشأن مكافحة
استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية

تقرير من الرئيسة

- 1- تحضيرا للدورة الرابعة للجنة المخصصة لوضع اتفاقية دولية شاملة لمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، وتماشيا مع خريطة الطريق وأسلوب العمل للجنة المخصصة، المعتمدين في دورتها الأولى، أعدت رئيسة اللجنة، بدعم من الأمانة، وثيقة تفاوض موحدة وضعت على أساس نتائج القراءة الأولى للأحكام العامة والأحكام المتعلقة بالتجريم وبالتدابير الإجرائية وإنفاذ القانون في مشروع الاتفاقية (انظر المرفق).
- 2- وبشكل أكثر تحديدا، تستند وثيقة التفاوض الموحدة إلى عناصر المقترحات المقدمة من الدول الأعضاء المجمعة في الوثائق [A/AC.291/9](#) و [A/AC.291/9/Add.1](#) و [A/AC.291/9/Add.2](#) و [A/AC.291/9/Add.3](#)، وكذلك إلى البيانات والآراء التي أعربت عنها الدول الأعضاء خلال الدورة الثانية. وبذل جهد لاقتراح خيار واحد لكل حكم بإدراج عناصر مأخوذة من مقترحات أو بيانات مختلفة. وقد استخدمت معقوفتان لبعض المصطلحات لتجسيد الآراء المتباينة بشأن استخدامها على النحو الذي أعربت عنه بعض الدول الأعضاء في دورات اللجنة المخصصة.
- 3- وستعد وثيقة تفاوض موحدة ثانية على أساس نتائج القراءة الأولى للديباجة، والأحكام المتعلقة بالتعاون الدولي، والمساعدة التقنية، والتدابير الوقائية، وآلية التنفيذ، والأحكام الختامية للاتفاقية، التي اضطلعت بها اللجنة المخصصة في دورتها الثالثة، وستتاح لتنظر فيها اللجنة قبل دورتها الخامسة.



المرفق

وثيقة التفاوض الموحدة بشأن الأحكام العامة والأحكام المتعلقة بالتجريم
وبالتدابير الإجرائية وإنفاذ القانون لاتفاقية دولية شاملة بشأن مكافحة
استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية

الفصل الأول

أحكام عامة

المادة 1- بيان الغرض

أغراض هذه الاتفاقية هي:

- (أ) تشجيع وتعزيز التدابير الرامية إلى منع ومكافحة [استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية] [الجريمة السيبرانية]، مع حماية مستخدمي تكنولوجيات المعلومات والاتصالات من تلك الجريمة؛
- (ب) تشجيع وتيسير وتعزيز التعاون الدولي في مجال منع ومكافحة [استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية] [الجريمة السيبرانية]؛
- (ج) توفير تدابير عملية لتعزيز المساعدة التقنية فيما بين الدول الأطراف وبناء قدرات السلطات الوطنية على منع ومكافحة [استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية] [الجريمة السيبرانية]، وخصوصا لمصلحة البلدان النامية، وتعزيز وتشجيع تبادل المعلومات والمعارف المتخصصة والخبرات والممارسات الجيدة.

المادة 2- استخدام المصطلحات

[استنادا إلى البيانات التي أدلى بها العديد من الدول الأعضاء خلال الدورة الثانية للجنة المختصة، ينبغي تناول هذا الحكم بعد تعريف المواد الموضوعية الرئيسية للاتفاقية.]

المادة 3- نطاق الانطباق

- 1- تنطبق هذه الاتفاقية، وفقا لأحكامها، على منع [استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية] [الجريمة السيبرانية] والكشف عنها والتحقيق فيها وملاحقة مرتكبيها قضائيا، ويشمل ذلك تجميد عائدات الأفعال المجرمة وفقا لهذه الاتفاقية وحجزها ومصادرتها وإعادتها.
- 2- تنطبق هذه الاتفاقية أيضا على جمع الأدلة في شكل إلكتروني على [الجرائم المنصوص عليها في هذه الاتفاقية] [أي فعل إجرامي] [الجرائم الخطيرة] والحصول على تلك الأدلة وحفظها وتبادلها.
- 3- لأغراض تنفيذ هذه الاتفاقية، ليس ضروريا أن تكون الجرائم المبيّنة فيها قد ألحقت ضررا أو أذى بأشخاص، بمن فيهم الشخصيات الاعتبارية، أو بالممتلكات أو بالدولة، باستثناء ما تنص عليه خلافا لذلك.

المادة 4- صون السيادة

- 1- تتفد الدول الأطراف التزاماتها المنصوص عليها بموجب هذه الاتفاقية على نحو يتسق مع مبدأي المساواة في السيادة والسلامة الإقليمية للدول ومع مبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى.
- 2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء المهام التي تقتصر حصراً على سلطات تلك الدولة الأخرى بموجب قوانينها الداخلية.

المادة 5- احترام حقوق الإنسان

- 1- تكفل الدول الأطراف أن يكون تنفيذ التزاماتها بموجب هذه الاتفاقية وفقاً للقانون الدولي لحقوق الإنسان.
- 2- تبذل الدول الأطراف جهوداً لتعميم مراعاة المنظور الجنساني ومراعاة الظروف والاحتياجات الخاصة للفئات الضعيفة، ولا سيما النساء والأطفال والمسنين، في التدابير التي تتخذ لمنع ومكافحة [استخدام تكنولوجيا المعلومات والاتصالات للأغراض إجرامية] [الجريمة السيبرانية].

الفصل الثاني التجريم

المجموعة 1⁽¹⁾

المادة 6- الدخول غير المشروع

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الدخول غير المشروع إلى [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] بأكمله أو إلى أي جزء منه، عندما يرتكب هذا الفعل عمداً.
- 2- يجوز للدولة الطرف أن تشترط أن يرتكب الفعل المجرم بواسطة انتهاك لتدابير أمني، بقصد الحصول على [بيانات حاسوبية] [معلومات إلكترونية/رقمية] أو بأي قصد إجرامي آخر، أو فيما يتعلق بـ [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] متصل بـ [نظام حاسوبي] [نظام/جهاز لتكنولوجيا معلومات واتصالات] آخر.

- 3- يجوز لكل دولة طرف أن تفرض عقوبة مشددة إذا كان هذا الدخول:

- (أ) يؤدي إلى إلحاق الضرر بالمستخدمين والمستفيدين؛
- (ب) يؤدي إلى الحصول على معلومات حكومية سرية؛
- (ج) يتعلق بالبنية التحتية الحيوية أو يؤثر عليها.

المادة 7- الاعتراض غير المشروع

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الاعتراض غير المشروع، الذي يتم بوسائل تقنية، لعمليات إرسال غير عمومية [بيانات حاسوبية] [معلومات إلكترونية/رقمية] إلى [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] أو منه أو خلاله، بما في ذلك الانبعاثات الكهرومغناطيسية

(1) التنظيم إلى مجموعات يراد منه حصراً تنظيم المناقشات التي تجرى أثناء الدورات الرسمية.

من [نظام حاسوبي] [نظام/جهاز تكنولوجيا معلومات واتصالات] يحمل مثل هذه [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية]، عندما يرتكب هذا الفعل عمداً.

2- يجوز للدولة الطرف أن تشترط أن يرتكب الفعل المجرّم بقصد إجرامي، أو فيما يتعلق بـ[نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات] متصل بـ[نظام حاسوبي] [نظام/جهاز تكنولوجيا معلومات واتصالات] آخر.

المادة 8- التدخل في [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية]

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم إدخال [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] أو تنزيلها أو نسخها أو إتلافها أو تعطيلها أو حذفها أو إفسادها أو تحويلها أو طمسها، عندما يرتكب أي من هذه الأفعال عمداً وبصورة غير مشروعة.
- 2- يجوز للدولة الطرف أن تشترط تسبب السلوك المشار إليه في الفقرة 1 في ضرر جسيم.
- 3- يجوز لكل دولة طرف فرض عقوبة مشددة عندما تمس الأفعال الموصوفة في الفقرة 1 بنية تحتية حيوية أو تؤثر فيها.

المادة 9- التدخل في [نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات]

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم القيام عمداً بإعاقة خطيرة وغير مشروعة لعمل [نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات] عن طريق إدخال [بيانات حاسوبية] [معلومات إلكترونية/رقمية] أو إرسالها أو إتلافها أو حذفها أو إفسادها أو تحويلها أو طمسها.
- 2- يجوز لكل دولة طرف فرض عقوبة مشددة عندما تمس الأفعال الموصوفة في الفقرة 1 بنية تحتية حيوية أو تؤثر فيها.

المادة 10- إساءة استخدام الأجهزة والبرامج

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، إذا ما ارتكبت عمداً وعلى نحو غير مشروع:
 - (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 الأفعال المجرّمة وفقاً لهذه الاتفاقية؛
- 2' كلمة مرور أو بيانات اعتماد تسجيل الدخول أو [بيانات] [معلومات] مماثلة يمكن بواسطتها الدخول الكلي أو الجزئي إلى [نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات] قابل للدخول إليه؛

وذلك بقصد استخدام ذلك الجهاز أو كلمة المرور أو بيانات اعتماد الدخول أو [البيانات] [المعلومات] المماثلة لغرض ارتكاب أي من الأفعال المجرّمة [في المادة 6 المتعلقة بالدخول غير المشروع، والمادة 7 المتعلقة بالاعتراض غير المشروع، والمادة 8 المتعلقة بالتدخل في [البيانات الحاسوبية] [المعلومات

الإلكترونية/الرقمية]، والمادة 9 المتعلقة بالتدخل في [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] من هذه الاتفاقية [وفقاً لهذه الاتفاقية]؛

(ب) حيازة أحد الأشياء المشار إليها في الفقرة 1 (أ) '1' أو '2' من هذه المادة، بقصد استخدامها لغرض ارتكاب أي من الأفعال المجرمة [في المادة 6 المتعلقة بالدخول غير المشروع، والمادة 7 المتعلقة بالاعتراض غير المشروع، والمادة 8 المتعلقة بالتدخل في [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية]، والمادة 9 المتعلقة بالتدخل في [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] من هذه الاتفاقية] [وفقاً لهذه الاتفاقية]. ويجوز لدولة طرف أن تشترط الحيازة المسبقة لعدد من هذه الأشياء لإسناد المسؤولية الجنائية بموجب القانون.

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 أحد الأفعال المجرمة وفقاً [للمادة السابقة في] الاتفاقية، بل هو بالأحرى لعمل مرخص به بهدف اختبار أو حماية [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات].

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.

المجموعة 2

المادة 11- التزوير المتعلق بـ[الحاسوب] [تكنولوجيا المعلومات والاتصالات]

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، إذا ما ارتكبت عمداً وبصورة غير مشروعة: إدخال [بيانات حاسوبية] [معلومات إلكترونية/رقمية] أو تحويلها أو حذفها أو طمسها، مما يفضي إلى إنتاج [بيانات] [معلومات] غير أصلية يُبتغى أخذها في الاعتبار أو استخدامها كما لو كانت أصلية لأغراض قانونية، بغض النظر عما إذا كانت تلك [البيانات] [المعلومات] قابلة للقراءة أو الفهم بشكل مباشر أم لا.

2- لأغراض هذه المادة، يجوز للدولة الطرف أن تشترط الوجود المسبق لنية الاحتيال أو نية إجرامية أخرى لإسناد المسؤولية الجنائية.

المادة 12- الاحتيال المتعلق بـ[الحاسوب] [تكنولوجيا المعلومات والاتصالات]

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى من أجل تجريم أعمال الاحتيال التي ترتكب كلياً أو جزئياً عبر الإنترنت، إذا ارتكبت هذه الأفعال عمداً وبصورة غير مشروعة وتسببت في إلحاق خسارة بممتلكات الغير من الأفراد أو الكيانات، عن طريق ما يلي:

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

(ب) أي تدخل في [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]

(ج) أي استخدام لـ[نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] من أجل خداع شخص آخر أو كيان آخر أو حثه على القيام بفعل لم يكن سيقوم به لولا ذلك أو الامتناع عن فعل لم يكن سيمتنع عنه لولا ذلك،

وذلك بقصد الاحتيال أو بقصد إجرامي للحصول بصورة غير مشروعة للذات أو لشخص آخر على ما يلي:

- '1' منفعة اقتصادية؛ أو
- '2' [بيانات حاسوبية] [معلومات إلكترونية/رقمية] بما يشمل [بيانات] [معلومات] شخصية غير متاحة له بطريقة أخرى.
- 2- تشمل أعمال الاحتيال، على سبيل المثال لا الحصر، النشاط المرتكب داخليا، أو عبر الحدود بواسطة الإنترنت، أو غيرها من الوسائل [السيبرانية] [الرقمية] بالطرائق التالية:
 - (أ) الاحتيال عن طريق تقديم بيانات كاذبة؛
 - (ب) الاحتيال من خلال عدم الكشف عن المعلومات؛
 - (ج) الاحتيال عن طريق إساءة استخدام المنصب، مع نية احتيالية أو إجرامية للتسبب في خسارة لشخص آخر أو تحقيق مكاسب في المال أو الممتلكات الأخرى لشخص آخر.

المادة 1.3- السرقة المتعلقة بـ[الحاسوب] [تكنولوجيا المعلومات والاتصالات]

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم سرقة الممتلكات أو اكتساب الحقوق فيها بصورة غير مشروعة، عن طريق إتلاف [بيانات حاسوبية] [معلومات إلكترونية/رقمية] أو حجبها أو تعديلها أو نسخها أو غير ذلك من أشكال التدخل في عمليات [حاسوبية] [تكنولوجيا المعلومات والاتصالات].
- 2- يجوز لكل دولة طرف أن تعتبر سرقة الممتلكات المتعلقة بـ[الحاسوب] [تكنولوجيا المعلومات والاتصالات]، أو اكتساب الحقوق فيها بصورة غير مشروعة، ظرفا مشددا لعقوبة جريمة السرقة، حسب التعريف الوارد في القانون الداخلي للدولة الطرف.

المادة 14- الاستخدام غير المشروع لأدوات الدفع الإلكترونية

- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية:
- (أ) تزوير أو اصطناع أو تركيب أي أجهزة أو مواد تيسر تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت؛
 - (ب) الاستيلاء على [بيانات] [معلومات] عن أي أداة دفع أو استخدام تلك [البيانات] [المعلومات] أو توفيرها للغير، أو تيسير حصول الآخرين عليها؛
 - (ج) استخدام [شبكة معلومات أو تكنولوجيا معلومات] [نظام حاسوبي] للوصول بدون وجه حق إلى [البيانات] [المعلومات] المتعلقة بأي أداة دفع؛
 - (د) القيام عن علم بقبول أداة دفع مزورة.

المجموعة 3

المادة 1.5- انتهاك المعلومات الشخصية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية إذا ارتكبت عمدا وبصورة غير مشروعة: الحصول على أي مواد تحتوي على معلومات شخصية عن شخص، بما في ذلك المعلومات

المتصلة بالحساب المصرفي للشخص، أو بيع مثل هذه المعلومات أو توفيرها أو إتاحتها على نحو آخر، وذلك بقصد الحصول على منفعة مالية، وكذلك الكشف اللاحق، دون موافقة الشخص المعني، عن هذه المواد لأي شخص آخر.

المادة 16- الجرائم المتعلقة بالهوية

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

- (أ) الحصول على كلمات المرور أو بيانات اعتماد تسجيل الدخول أو تلقيها أو توزيعها للوصول إلى [نظام حاسوبي] [بيانات حاسوبية] دون وجه حق؛
- (ب) الاستخدام الاحتيالي أو غير النزيه للتوقيع الإلكتروني أو كلمة المرور أو أي ميزة تعريف فريدة أخرى يمتلكها شخص آخر.

المجموعة 4

المادة 17- انتهاك حق المؤلف

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم التعدي على حق المؤلف، حسبما تعرفه تشريعات تلك الدولة الطرف، عندما يرتكب هذا الفعل عمداً، عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]، بما في ذلك الاستخدام غير المشروع لبرامج حاسوبية وقواعد بيانات محمية بحق المؤلف، وانتحال مؤلفات الغير، عملاً بالالتزامات التي تعهدت بها بموجب الاتفاقيات ذات الصلة والمنطقة، باستثناء أي حقوق معنوية تمنحها تلك الاتفاقيات، عندما ترتكب هذه الأفعال عمداً وعلى نطاق تجاري.
- 2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم انتهاك الحق المتعلق بالتأليف، وفقاً لتعريفه في تشريعات تلك الدولة الطرف، عند ارتكابه عمداً، بواسطة [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]، وذلك عملاً بما ترتبط به من التزامات بموجب الاتفاقيات المنطبقة وذات الصلة، باستثناء أي حقوق معنوية تمنحها تلك الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات].
- 3- يجوز للدولة الطرف الاحتفاظ بالحق في عدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و 2 في ظروف محدودة شريطة توافر سبل فعالة أخرى للانتصاف، وشريطة ألا ينتقص هذا التحفظ من الالتزامات الدولية للدولة الطرف.

المجموعة 5

المادة 18- الجرائم المتعلقة بالمواد المتاحة عبر الإنترنت عن الاعتداء

على الأطفال أو استغلالهم جنسياً

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، إذا ما ارتُكبت عمداً وعلى نحو غير مشروع:
- (أ) إنتاج أو إعادة إنتاج مواد الاعتداء على الأطفال أو استغلالهم جنسياً لغرض توزيعها عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]؛

- (ب) تمويل مواد الاعتداء على الأطفال أو استغلالهم جنسيا أو تيسيرها بأي طريقة أخرى عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]؛
- (ج) إدارة مواد الاعتداء على الأطفال أو استغلالهم جنسيا أو الترويج لها أو عرضها أو الإعلان عنها أو إظهارها علانية أو إتاحتها بواسطة [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]؛
- (د) توزيع مواد الاعتداء على الأطفال أو استغلالهم جنسيا أو بثها عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]؛
- (هـ) الحصول على مواد الاعتداء على الأطفال أو استغلالهم جنسيا عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]؛
- (و) الحصول عن علم على إمكانية وصول إلى مواد الاعتداء الجنسي على الأطفال أو استغلالهم جنسيا أو حيازتها في [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] أو على [واسطة حاسوبية لتخزين البيانات] [جهاز إلكتروني/رقمي لتخزين البيانات]، أو مشاهدة طفل يشارك في سلوك جنسي صريح عن طريق البث المباشر؛
- (ز) المشاركة في أي عمل تجاري أو تلقي أرباح منه إذا كان الشخص يعلم أو لديه أسباب للاعتقاد بأن ذلك العمل التجاري يتعلق بمواد للاعتداء على الأطفال أو استغلالهم جنسيا عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات].
- 2- لأغراض الفقرة 1، يشمل مصطلح "مواد الاعتداء على الأطفال أو استغلالهم جنسيا" المواد المرئية، بما في ذلك وسائل التصوير الفوتوغرافي ووسائل الفيديو والبث المباشر، فضلا عن الرسومات والمواد المكتوبة والتسجيلات السمعية التي تصور ما يلي:
- (أ) طفلا يمارس سلوكا جنسيا صريحا حقيقيا أو تمثليا؛
- (ب) شخصا يبدو أنه طفل يمارس سلوكا جنسيا صريحا حقيقيا أو تمثليا؛
- (ج) صورة واقعية تظهر طفلا يمارس سلوكا جنسيا صريحا حقيقيا أو تمثليا؛
- (د) أي تصوير لأعضاء الطفل الجنسية لأغراض جنسية في المقام الأول؛
- (هـ) ضحية من ضحايا التعذيب أو المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة.
- 3- لأغراض الفقرة 2، يشمل مصطلح "طفل" أي شخص دون سن الثامنة عشرة.
- 4- تراعي الدول الأطراف على النحو الواجب تجنب الإفراط في توجيه التهم الجنائية إلى الأطفال الذين يمتلكون مواد منتجة ذاتيا على النحو الموصوف في الفقرة 2، والحاجة إلى احترام التزاماتها بموجب اتفاقية حقوق الطفل وبروتوكولاتها.
- 5- يجوز لكل دولة طرف أن تحتفظ بالحق في عدم التطبيق، الكلي أو الجزئي، للبندين (هـ) و(و) من الفقرة 1 والبندين (ب) و(ج) من الفقرة 2.

المادة 19- تيسير مواد الاعتداء على الأطفال أو استغلالهم جنسيا عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في إطار قانونها الوطني في حال ارتكابها عمدا وبدون عذر قانوني: استحداث [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات

والاتصالات] لأغراض تيسير مواد الاعتداء على الأطفال أو استغلالهم جنسيا المعرفة في المادة 18 من هذه الاتفاقية، أو إنشاء ذلك [النظام الحاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات] أو تطويره أو تحويله أو تعهده أو التحكم فيه أو الإشراف عليه أو مساعدته أو إتاحتها أو الإعلان عنه أو ترويجه لمثل تلك الأغراض.

2- لأغراض الفقرة 1، يشمل مصطلح "تيسير مواد الاعتداء على الأطفال أو استغلالهم جنسيا" أيًا من السلوكيات المبينة في الفقرة 1 التي ترتكب لأغراض السماح للأشخاص بالوصول إلى مواد الاعتداء على الأطفال أو استغلالهم جنسيا أو للسماح لهم بإنتاجها أو بثها أو توزيعها أو عرضها أو إتاحتها للنفس أو للغير.

المادة 20- استمالة طفل أو جلبه لأغراض جنسية بواسطة [نظام حاسوبي]

[نظام/جهاز تكنولوجيا المعلومات والاتصالات]

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية إذا ارتكبت عمداً: استمالة طفل أو الاتفاق معه أو وضع ترتيبات معه أو مرادته عن نفسه أو جلبه أو طلبه أو إرغامه أو [إغوائه] [إغرائه] لغرض تيسير ممارسة طفل أو شخص آخر يُعتقد أنه طفل سلوكاً جنسياً غير مشروع أو ممارسة ذلك السلوك معه أو التسبب في أن يشهد أو يمارس بطريقة أخرى أنشطة جنسية عن طريق [نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات].

2- لأغراض الفقرة 1، تنطبق المادة 2 [(x)] [بشأن تعريف "الطفل" والمسؤولية الجنائية للأطفال]. وإضافةً إلى ذلك، يشمل مصطلح "الطفل" أيضاً أي شخص يُعتقد أنه دون الثامنة عشرة.

3- لا تقع أي مسؤولية جنائية على الشخص إذا اتخذ خطوات معقولة للتأكد من أن الشخص ليس طفلاً.

المادة 21- المطاردة السيبرانية لطفل

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية إذا ما ارتكبت عمداً: استخدام [نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات] لجمع معلومات 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 ممارسة اتصال جنسي أو سلوك جنسي صريح أو نشاط جنسي غير مشروع.

المجموعة 6

المادة 22- إشراك القصر في ارتكاب أعمال غير مشروعة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم استخدام [نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات] لإشراك القصر في ارتكاب أفعال غير مشروعة تعرض حياتهم أو صحتهم البدنية أو العقلية للخطر، باستثناء الأفعال المنصوص عليها في المادة [23]، المتعلقة بالتشجيع على الانتحار أو الإكراه عليه من هذه الاتفاقية.

المادة 23- التشجيع على الانتحار أو الإكراه عليه

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم التشجيع على الانتحار أو الإكراه عليه، بما في ذلك بالنسبة للأطفال، عن طريق الضغط النفسي أو غيره من أشكال الضغط الذي يمارس بواسطة [نظام حاسوبي] [نظام/جهاز تكنولوجيا المعلومات والاتصالات].

المجموعة 7

المادة 24- الابتزاز الجنسي

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى من أجل تجريم التهديد بتوزيع صورة حميمة لشخص آخر أو إرسالها بوسائل إلكترونية، إذا ارتكب هذا الفعل عمدا وبقصد محدد هو:
 - (أ) مضايقة ذلك الشخص أو تهديده أو إكراهه أو تخويفه أو ممارسة أي تأثير غير مبرر عليه، لا سيما من أجل الحصول على منفعة مالية أو منفعة مادية أخرى، ويشمل ذلك إجبار الضحية على الانخراط في نشاط جنسي غير مرغوب فيه؛ أو
 - (ب) الحصول على منفعة مالية أو مادية أخرى، بما في ذلك إجبار الضحية على الانخراط في نشاط جنسي غير مرغوب فيه.
- 2- لأغراض الفقرة 1، تعني "الصورة الحميمة" تسجيلاً مرئياً لشخص ما صنع 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) ظل الشخص المصور يتوقع بشأنه قدراً معقولاً من الخصوصية في الوقت الذي ارتكب فيه الفعل.

المادة 25- النشر غير التوافقي للصور الحميمة

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم نشر أي صورة حميمة لشخص أو توزيعها أو إرسالها أو بيعها أو إتاحتها أو الإعلان عنها عندما يرتكب هذا الفعل عمدا وبصورة غير مشروعة، وذلك عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]، [بقصد التسبب في أذى عاطفي خطير] 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 صنع 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) ظل الشخص المصور يتوقع بشأنه قدراً معقولاً من الخصوصية في الوقت الذي ارتكب فيه الفعل.
- 3- لا تترتب أي مسؤولية جنائية إذا كان النشر غير التوافقي لهدف مشروع.
- 4- لا يجوز للطفل أن يمنح موافقة على نشر صورة حميمة يكون هو موضوعها.

المجموعة 8

المادة 26- التحريض على الأنشطة التخريبية أو المسلحة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الداخلي أي نداء يصدر بواسطة تكنولوجيا المعلومات والاتصالات للقيام بأنشطة تخريبية أو مسلحة ترمي إلى الإطاحة بالحكم في دولة أخرى بالعنف.

المادة 27- الجرائم المتعلقة بالتطرف

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم توزيع المواد التي تدعو إلى ارتكاب أفعال غير مشروعة بدافع الكراهية 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 [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات].

المادة 28- إنكار جرائم الإبادة الجماعية أو الجرائم المرتكبة ضد السلام والإنسانية

أو الموافقة عليها أو تبريرها أو إعادة تأهيلها

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى كي يُجرّم في قانونها الداخلي النشر الدولي المتعمد [بواسطة الحاسوب] [بواسطة تكنولوجيا المعلومات والاتصالات] للمواد التي تنكر الأعمال التي تبلغ 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 لتجريم إقرار تلك الأعمال أو تبريرها.

المجموعة 9

المادة 29- الجرائم المتعلقة بالإرهاب

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم ارتكاب أعمال إرهابية أو التحريض على أنشطة إرهابية أو التجنيد لها أو أي مشاركة أخرى فيها أو الدعوة إلى الإرهاب وتبريره أو جمع الأموال لتمويله أو توفيرها أو القيام بها على نحو آخر، عندما ترتكب بواسطة تكنولوجيات المعلومات والاتصالات، أو التدريب على الأعمال الإرهابية، أو تيسير الاتصال بين المنظمات الإرهابية وأعضائها، بما في ذلك إنشاء موقع على شبكة الإنترنت أو نشره أو استخدامه وتوفير الدعم اللوجستي لمرتكبي الأعمال الإرهابية، ونشر أساليب صنع المتفجرات التي تستخدم بصفة خاصة في الأعمال الإرهابية، ونشر الفتنة أو الكراهية أو العنصرية، عندما يرتكب أي من تلك الأفعال بواسطة تكنولوجيات المعلومات والاتصالات.

المادة 30- الجرائم المتصلة بتوزيع العقاقير المخدرة والمؤثرات العقلية

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الاتجار غير المشروع بالمخدرات والمؤثرات العقلية والمواد اللازمة لصنعها، عند ارتكاب ذلك عمداً، وباستخدام [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] [نظام حاسوبي].

المادة 31- الجرائم المتصلة بالاتجار بالأسلحة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الاتجار بالأسلحة والذخيرة والأجهزة والمواد المتفجرة بواسطة تكنولوجيا المعلومات والاتصالات، عند ارتكاب ذلك عمداً.

المادة 32- التوزيع غير القانوني للأدوية والمنتجات الطبية المقلدة

تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم التوزيع المتعمد وغير القانوني للأدوية والمنتجات الطبية المقلدة بواسطة تكنولوجيا المعلومات والاتصالات.

المجموعة 10

المادة 33- غسل الأموال

1- تعتمد كل دولة طرف، وفقاً للمبادئ الأساسية لقانونها الداخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، إذا ما ارتُكبت عمداً:

(أ) '1' تحويل الممتلكات، بما فيها العملات الافتراضية، 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 تأنت 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 فعل مجرم وفقاً لهذه المادة، أو التعاون أو التواطؤ على ارتكابه، والشروع في ارتكابه والمساعدة والتحريض على ذلك وتيسيره 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 الأفعال ذات الصلة المجرمة وفقاً لهذه الاتفاقية. أما الدول الأطراف التي تحدد تشريعاتها قائمة جرائم أصلية معينة، فتدرج في تلك القائمة، كحد أدنى، مجموعة شاملة من الجرائم المرتبطة بـ [استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية] [الجريمة 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 عندما يكون 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 تُطبَّق هذه المادة لو كان قد ارتُكبت هناك؛

(د) تزود كل دولة طرف الأمين العام للأمم المتحدة بنسخ من قوانينها المنفذة لهذه المادة وينسخ 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.

المادة 34- إعاقه سير العدالة

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

(أ) استخدام القوة البدنية أو التهديد أو الترهيب أو الوعد بمزية غير مستحقة أو عرضها أو منحها للتخريض 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.

المجموعة 11

المادة 35- مسؤولية الشخصيات الاعتبارية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، بما يتسق مع مبادئها القانونية، لتقرير مسؤولية الشخصيات الاعتبارية عن فعل إجرامي مجرم في هذه الاتفاقية، يرتكبه لصالحها أي شخص طبيعي، سواء كان يتصرف بمفرده أو باعتباره عضواً في هيئة تابعة للشخصية الاعتبارية، ويتبوأ منصباً قيادياً لديها، وذلك بناء على:

(أ) سلطة تمثيل الشخصية الاعتبارية؛

(ب) سلطة اتخاذ القرارات نيابة عن الشخصية الاعتبارية؛

(ج) سلطة ممارسة السيطرة لدى الشخصية الاعتبارية.

2- إضافة إلى الحالات المنصوص عليها في الفقرة 1 من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان إمكانية تحميل الشخصية الاعتبارية المسؤولية إذا أتاح عدم الإشراف أو السيطرة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 ارتكاب فعل مجرم وفقاً لهذه الاتفاقية لصالح تلك الشخصية الاعتبارية من قبل شخص طبيعي يعمل تحت سلطتها الصريحة أو الضمنية.

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

4- ولا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم.

5- 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.

6- تحظى الشخصيات الاعتبارية بالحماية من المسؤولية عن أي فعل يتم القيام به أو يُمتنع عن القيام به بحسن نية:

- (أ) في الأداء الفعلي أو المعترّم لواجب مفروض من قبل هذه الاتفاقية أو بمقتضاها؛ أو
(ب) في الممارسة الفعلية أو المعترّمة لوظيفة أو سلطة ممنوحة من قبل هذه الاتفاقية أو بموجبها.

المادة 36- المشاركة والشروع

- 1- تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وتدابير أخرى لكي تجرّم، وفقا لقانونها الداخلي، المشاركة بأي صفة، مثل الشريك أو المساعد أو المحفز أو المحرض أو المتآمر، في أي فعل مجرّم وفقا لهذه الاتفاقية، أو تنظيم أو توجيه أي شخص آخر لارتكاب ذلك الفعل المجرّم.
- 2- يجوز لكل دولة طرف أن تعتمد ما يلزم من تدابير تشريعية وتدابير أخرى لكي تجرّم، وفقا لقانونها الداخلي، أي شروع، يرتكب عمدا، في فعل مجرّم وفقا لهذه الاتفاقية.
- 3- يجوز لكل دولة طرف أن تعتمد ما يلزم من تدابير تشريعية وتدابير أخرى لكي تجرّم، وفقا لقانونها الداخلي، الإعداد، الذي يرتكب عمدا، لفعل مجرّم وفقا لهذه الاتفاقية.
- 4- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتعزيز المسؤولية عن الجرائم الجماعية، بما فيها الجرائم التي ترتكبها الجماعات الإجرامية المنظمة.
- 5- يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 2 من هذه المادة كليا أو جزئيا.

المادة 37- العلم والنية والغرض كأركان للفعل الإجرامي

يجوز الاستدلال على عنصر العلم أو النية أو الغرض، الذي يلزم توافره في أي فعل مجرم وفقا لهذه الاتفاقية، من الملاحظات الوقائية الموضوعية.

المادة 38- التقادم

تحدد كل دولة طرف في إطار قانونها الداخلي، عند الاقتضاء، فترة تقادم طويلة تستهل أثناءها الإجراءات القضائية بشأن أي فعل مجرّم وفقا لهذه الاتفاقية، وتحدد فترة تقادم أطول أو تشترط تعليق العمل بالتقادم عندما يكون الجاني المزعوم قد فرّ من وجه العدالة.

المادة 39- الملاحقة والمقاضاة والجزاءات

- 1- تجعل كل دولة طرف ارتكاب أي فعل مجرّم وفقا لهذه الاتفاقية خاضعا لعقوبات تُراعى فيها جسامته ذلك الجرم.
- 2- يجوز لكل دولة طرف أن تفرض عقوبة مشددة على الأفعال المجرّمة وفقا لهذه الاتفاقية، بما في ذلك، على سبيل المثال لا الحصر، الحالات التي تكون فيها الجرائم المرتكبة:
 - (أ) تؤثر على البنية التحتية الحيوية؛
 - (ب) تؤدي إلى الحصول على معلومات حكومية سرية.
 - (ج) تسبب ضررا، بما في ذلك الصدمة الجسدية أو النفسية، للأفراد.

- 3- تتخذ كل دولة طرف، وفقا لنظامها القانوني ومبادئها الدستورية، ما قد يلزم من تدابير لإرساء أو إبقاء توازن مناسب بين أي حصانات أو امتيازات قضائية ممنوحة لموظفيها العموميين من أجل أداء وظائفهم وإمكانية القيام، عند الضرورة، بعمليات تحقيق وملاحقة ومقاضاة فعالة في الأفعال المجرّمة وفقا لهذه الاتفاقية.
- 4- تسعى كل دولة طرف إلى ضمان أن أي صلاحيات قانونية تقديرية يتيحها قانونها الداخلي فيما يتعلق بملاحقة الأشخاص لارتكابهم أفعالا مجرّمة وفقا لهذه الاتفاقية، تمارس من أجل تحقيق الفعالية القصوى لتدابير إنفاذ القانون التي تُتخذ بشأن تلك الجرائم، ومع إيلاء الاعتبار الواجب لضرورة الردع عن ارتكابها.
- 5- تكفل كل دولة طرف تمتع أي شخص يحاكم على أفعال مجرّمة وفقا لهذه الاتفاقية بجميع الحقوق والضمانات وفقا لقانون الدولة التي يوجد ذلك الشخص في إقليمها وللأحكام ذات الصلة والمنطبقة من القانون الدولي لحقوق الإنسان، بما في ذلك الحق في محاكمة عادلة وحقوق الدفاع.
- 6- في حالة الأفعال المجرّمة وفقا لهذه الاتفاقية، تتخذ كل دولة طرف تدابير مناسبة، وفقا لقانونها الداخلي ومع إيلاء الاعتبار الواجب لحقوق الدفاع، تهدف إلى ضمان أن تراعي شروط قرارات الإفراج إلى حين المحاكمة أو الاستئناف ضرورة ضمان حضور المدعى عليه في الإجراءات الجنائية اللاحقة.
- 7- تأخذ كل دولة طرف بعين الاعتبار خطورة الجرائم المعنية لدى النظر في احتمال الإفراج المبكر أو المشروط عن الأشخاص المدانين بارتكاب تلك الجرائم.
- 8- ليس في هذه الاتفاقية ما يمس بالمبدأ القاضي بأن يكون الحق في توصيف الأفعال المجرّمة وفقا لها وتوصيف الدفوع القانونية المنطبقة أو المبادئ القانونية الأخرى التي تحكم مشروعية السلوك محظوظا حصرا للقانون الداخلي للدولة الطرف، وأن تلك الجرائم يجب ملاحقتها قضائيا والمعاقبة عليها وفقا لذلك القانون.
- 9- تسعى الدول الأطراف إلى تشجيع إعادة إدماج الأشخاص المدانين بارتكاب أفعال مجرّمة وفقا لهذه الاتفاقية في مجتمعاتهم.

الفصل الثالث

التدابير الإجرائية وإنفاذ القانون

المجموعة 1

المادة 40- الولاية القضائية

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير لبسط ولايتها القضائية على الأفعال المجرّمة وفقا لهذه الاتفاقية في الحالتين التاليتين:
- (أ) عندما يُرتكب الجرم في إقليم تلك الدولة الطرف؛ أو
- (ب) عندما يُرتكب الجرم على متن سفينة ترفع علم تلك الدولة الطرف أو طائرة مسجلة بمقتضى قوانين تلك الدولة الطرف وقت ارتكاب الجرم.
- 2- رهنا بأحكام المادة 4 من هذه الاتفاقية، يجوز للدولة الطرف أن تُخضع أيضا أي جرم من هذا القبيل لولايتها القضائية في الحالات التالية:
- (أ) أن يُرتكب الجرم ضد أحد مواطني تلك الدولة الطرف أو ضد أحد شخصياتها الاعتبارية؛ أو
- (ب) أن يرتكب الجرم شخص وطني أو اعتباري من تلك الدولة الطرف أو شخص عديم الجنسية يكون محل إقامته المعتاد في إقليمها؛ أو

- (ج) أن يُرتكب الجرم خارج إقليمها بهدف ارتكاب فعل مجرم وفقا لهذه الاتفاقية داخل إقليمها؛ أو
- (د) أن يُرتكب الجرم ضد الدولة الطرف؛ أو
- (هـ) أن يشمل الجرم [بيانات حاسوبية] [معلومات إلكترونية/رقمية] لمواطني الدولة الطرف، بصرف النظر عن مكان تخزينها المادي أو تجهيزها أو فحصها.
- 3- لأغراض المادة المتعلقة بتسليم المطلوبين من هذه الاتفاقية، تعتمد كل دولة طرف ما قد يلزم من تدابير لبسط ولايتها القضائية على الأفعال المجرمة وفقا لهذه الاتفاقية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تسلم ذلك الشخص لمجرد كونه أحد مواطنيها.
- 4- يجوز لكل دولة طرف أيضا أن تعتمد ما قد يلزم من تدابير لإخضاع الأفعال المجرمة وفقا لهذه الاتفاقية لولايتها القضائية عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه.
- 5- إذا أُبلغت الدولة الطرف التي تمارس ولايتها القضائية بمقتضى الفقرة 1 أو الفقرة 2 من هذه المادة، أو علمت بطريقة أخرى، أن أي دول أطراف أخرى تجري تحقيقا أو ملاحقة قضائية أو تتخذ إجراء قضائيا بشأن السلوك ذاته، وجب على السلطات المختصة في تلك الدول الأطراف أن تتشاور فيما بينها، حسب الاقتضاء، بهدف تنسيق ما تتخذه من إجراءات.
- 6- دون مساس بقواعد القانون الدولي العام، لا تحول هذه الاتفاقية دون ممارسة أي ولاية قضائية جنائية تقيمها دولة طرف وفقا لقانونها الداخلي.

المادة 41- نطاق التدابير الإجرائية

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإقامة الصلاحيات والإجراءات المنصوص عليها في هذا القسم لأغراض التحقيقات أو الإجراءات الجنائية المحددة في هذا الشأن.
- 2- يطبق كل طرف، ما لم ينص على خلاف ذلك في المادة 48 من هذه الاتفاقية، الصلاحيات والإجراءات المشار إليها في الفقرة 1 من هذه المادة على:
- (أ) الجرائم الجنائية المجرمة وفقا لهذه الاتفاقية؛
- (ب) الجرائم الجنائية الأخرى المرتكبة عن طريق [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]؛
- (ج) جمع الأدلة في شكل إلكتروني عن [الجرائم المنصوص عليها في هذه الاتفاقية] [أي فعل إجرامي] [الجرائم الخطيرة].
- 3- (أ) يجوز لكل دولة طرف أن تحتفظ بالحق في تطبيق التدابير المشار إليها في المادة 47 من هذه الاتفاقية حصرا على جرائم أو فئات جرائم تحددها في التحفظ، شريطة ألا يكون نطاق هذه الجرائم أو فئات الجرائم أضيق من نطاق الجرائم التي تطبق عليها الدولة الطرف التدابير المشار إليها في المادة 48. وينظر كل طرف في تقييد مثل هذا التحفظ لإتاحة تطبيق التدابير المتعلقة بجمع بيانات الحركة في الوقت الحقيقي على أوسع نطاق.
- (ب) عندما تفرض قيود في التشريعات السارية لدى الدولة الطرف وقت اعتماد هذه الاتفاقية، مما يؤدي إلى عدم تمكنها من تطبيق التدابير المتعلقة بجمع بيانات الحركة في الوقت الحقيقي وباعتراض بيانات المحتوى على الرسائل المرسلة داخل [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] تابع لمقدم خدمة، وكان ذلك النظام:

1' يُشغّل لصالح مجموعة مغلقة من المستخدمين؛

2' لا يستخدم شبكات اتصالات عامة وليس متصلاً بنظام حاسوبي آخر، سواء أكان عاماً أو خاصاً،

يجوز لتلك الدولة الطرف أن تحتفظ بالحق في عدم تطبيق تلك التدابير على تلك الرسائل. وينظر كل طرف في تقييد مثل هذا التحفظ لإتاحة تطبيق التدابير على أوسع نطاق ممكن فيما يتعلق بجمع بيانات الحركة في الوقت الحقيقي واعتراض بيانات المحتوى.

المادة 42- الشروط والضمانات

1- تكفل كل دولة طرف أن يخضع إنشاء الصلاحيات والإجراءات المنصوص عليها في هذا الفصل وتنفيذها وتطبيقها للشروط والضمانات المنصوص عليها في قانونها الداخلي، الذي يجب أن ينص على توفير الحماية الكافية لحقوق الإنسان والحريات، بما في ذلك الحقوق والحريات الأساسية الناشئة من الالتزامات بموجب ما ينطبق من القانون الدولي لحقوق الإنسان، والذي يجب أن يشمل مبادئ التناسب والضرورة والمشروعية وحماية الخصوصية والبيانات الشخصية.

2- تشمل هذه الشروط والضمانات فيما تشمل، حسب الاقتضاء في ضوء طبيعة الإجراء المعني أو الصلاحية المعنية، الإشراف القضائي أو شكلاً آخر من أشكال الإشراف المستقل، والأسباب التي تبرر التطبيق، والحد من نطاق ومدة هذه الصلاحية أو هذا الإجراء.

3- تنظر كل دولة طرف، بالقدر الذي يتسق مع المصلحة العامة، ولا سيما مع إقامة العدل على نحو سليم، في أثر الصلاحيات والإجراءات المنصوص عليها في هذه المادة على حقوق الأطراف الثالثة ومسؤولياتها ومصالحها المشروعة.

المجموعة 2

المادة 43- التعجيل بالحفاظ على [البيانات الحاسوبية المخزنة]

[المعلومات الإلكترونية/الرقمية المتراكمة]

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من إصدار أوامر أو تعليمات وافية للحصول على [بيانات حاسوبية] [معلومات إلكترونية/رقمية] محددة أو التمكن بوسيلة مماثلة من الحفاظ عليها على وجه السرعة أو ضمان الحفاظ عليها، بما في ذلك بيانات الحركة التي خزنت بواسطة [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]، ولا سيما عند وجود أسباب تدعو إلى الاعتقاد بأن [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] معرضة بوجه خاص للحذف أو النسخ أو الفقدان أو التعديل، بما في ذلك بسبب انتهاء فترة الاحتفاظ المنصوص عليها في التشريعات الداخلية للدولة الطرف أو في شروط الخدمة التي ينشرها مقدم الخدمة.

2- عندما تُفَعّل دولة طرف الفقرة 1 أعلاه عن طريق إصدار أمر إلى شخص ما، قد يكون طبيعياً أو اعتبارياً، للحفاظ على [بيانات حاسوبية] [معلومات إلكترونية/رقمية] مخزنة محددة توجد في حوزة ذلك الشخص أو تحت سيطرته، تعتمد الدولة الطرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام ذلك الشخص بالحفاظ على تلك [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] وصون سلامتها للفترة اللازمة من الزمن، وبحد أقصى 90 يوماً، لتمكين السلطات المختصة من التماس الكشف عنها. ويجوز للدولة الطرف أن تنص على تجديد هذا الأمر في وقت لاحق.

- 3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإلزام الوديع أو أي شخص آخر يتولى الحفاظ على [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية]، بأن يحافظ على سرية الاضطلاع بهذه الإجراءات للفترة الزمنية المنصوص عليها في تشريعاتها الداخلية.
- 4- تحدد السلطات والإجراءات المشار إليها في هذه المادة وفقا للمادتين 41 و42 من هذه الاتفاقية.

المادة 44- التعجيل بالحفاظ على بيانات الحركة والكشف الجزئي عنها

- 1- تعتمد كل دولة طرف، بشأن بيانات الحركة التي يتعين الحفاظ عليها بمقتضى المادة المتعلقة بالتعجيل بالحفاظ على [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية]، ما قد يلزم من تدابير تشريعية وتدابير أخرى من أجل:
- (أ) ضمان إتاحة هذا الحفاظ السريع على بيانات الحركة بغض النظر عن مشاركة مقدم خدمة واحد أو أكثر في إرسال تلك الرسالة؛
- (ب) ضمان الكشف السريع للسلطة المختصة في الدولة الطرف، أو لشخص تعيينه تلك السلطة، عن كمية من بيانات الحركة تكفي لتمكين الدولة الطرف من تحديد مقدمي الخدمات الذين أرسلت من خلالها الرسالة أو المعلومات المشار إليها والمسار الذي أرسلت من خلاله.
- 2- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 41 و42.

المادة 45- أمر تقديم المعلومات

- 1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة، حيثما تكون هناك أسباب معقولة تدعو للاعتقاد بأن فعلا إجراميا قد ارتكب أو يجري ارتكابه، من اتخاذ الإجراءات التالية:
- (أ) أن تأمر شخصا في إقليمها بأن يقدم إليها ما بحوزته أو تحت سيطرته من [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] المحددة في الأمر والمخزنة في نظام حاسوبي أو في واسطة لتخزين البيانات الحاسوبية؛
- (ب) أن تأمر مقدم خدمة في إقليم الدولة الطرف بأن يقدم إليها ما بحوزته أو تحت سيطرته من معلومات عن المشتركين في خدماته.
- 2- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 41 و42.
- 3- لأغراض هذه المادة، يعني مصطلح "معلومات المشتركين" أي معلومات متضمنة في شكل [بيانات حاسوبية] [معلومات إلكترونية/رقمية] أو أي شكل آخر يحتفظ بها مقدم خدمة، وتتعلق بالمشتركين في خدماته، غير بيانات الحركة أو بيانات المحتوى، ويمكن من خلالها إثبات ما يلي:
- (أ) نوع خدمة تكنولوجيا المعلومات والاتصالات المستخدمة، والتدابير التقنية المطبقة بشأنها، ومدة الخدمة؛
- (ب) هوية المشترك وعنوانه البريدي أو الجغرافي ورقم الهاتف وغيره من أرقام الوصول ومعلومات تحرير الفواتير والدفع المتاحة على أساس اتفاق الخدمة أو ترتيبها؛
- (ج) المعلومات المتعلقة بمكان معدات المعلومات والاتصالات المتاحة على أساس اتفاق الخدمة أو ترتيبها.

المادة 46- البحث عن [المعلومات المخزنة أو المعالجة إلكترونياً/رقمياً]
[البيانات الحاسوبية المخزنة] والاستحواذ عليها

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة، عندما تكون هناك أسباب معقولة تدعو للاعتقاد بأن فعلاً إجرامياً قد ارتكب أو يجري ارتكابه، من إجراء بحث في البندين التاليين في الأراضي أو الولايات القضائية التابعة للدولة الطرف، أو الوصول إليهما بوسيلة مماثلة:

(أ) [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] [نظام حاسوبي]، أو جزء منه، و[بيانات حاسوبية] [معلومات إلكترونية/رقمية] مخزنة فيه؛

(ب) واسطة تخزين [بيانات حاسوبية] [معلومات إلكترونية/رقمية] قد تكون [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] التي يبحث عنها مخزنة فيها.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان أنه عندما تكون لدى سلطاتها المختصة، التي تجري بحثاً عملاً بأحكام الفقرة 1 (أ) من هذه المادة، أسباب معقولة تدعو إلى الاعتقاد بأن [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] التي يُبحث عنها مخزنة على [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] [نظام حاسوبي] آخر في إقليم تلك الدولة الطرف، ويكون من الممكن الوصول إلى هذه [البيانات] [المعلومات] من النظام الأول أو تكون متاحة له بشكل قانوني، فإن تلك السلطات ستتمكن من تسريع خطوات البحث للحصول على إمكانية الوصول إلى [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] [النظام الحاسوبي] المذكور الآخر أو [البيانات] [المعلومات] التي توجد فيه.

3- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من الاستحواذ على [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] التي توجد في إقليم تلك الدولة الطرف أو تحت ولايتها القضائية والتي تم الوصول إليها وفقاً للفقرتين 1 و 2، أو تأمين تلك المعلومات بطريقة مشابهة. وتشمل هذه التدابير صلاحيات للقيام بما يلي:

(أ) الاستحواذ على [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] [نظام حاسوبي] أو جزء منه، أو على واسطة تستخدم لتخزين [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] أو تأمين ما سيق بطريقه أخرى؛

(ب) عمل نسخ من هذه [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] والاحتفاظ بها في شكل إلكتروني/رقمي؛

(ج) صون سلامة [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] المخزنة ذات الصلة؛

(د) جعل الوصول متعذراً إلى تلك [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] في [النظام الحاسوبي] [جهاز/نظام لتكنولوجيا المعلومات والاتصالات] الذي تم الوصول إليه، أو إزالتها منه.

4- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من أن تأمر أي شخص لديه معرفة خاصة بتشغيل [النظام الحاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] المعني، أو شبكة المعلومات والاتصالات، أو الأجزاء المكونة لهما، أو التدابير المطبقة لحماية [البيانات الحاسوبية] [المعلومات الإلكترونية/الرقمية] الواردة فيها، بأن يقدم، في حدود المعقول، المعلومات اللازمة للتمكين من اتخاذ التدابير المشار إليها في الفقرتين 1 و 3 من هذه المادة.

5- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 41 و 42.

المادة 47- جمع بيانات الحركة الحاسوبية في الوقت الحقيقي

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة، عندما تكون هناك أسباب معقولة للاعتقاد بأن فعلاً إجرامياً قد ارتكب أو يجري ارتكابه، من اتخاذ الإجراءات التالية فيما يتعلق ببيانات الحركة المرتبطة برسائل محددة في إقليمها ترسل بواسطة [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات] في إقليم تلك الدولة الطرف:

(أ) جمع وتسجيل البيانات المرتبطة بمعلومات محددة في إقليم تلك الدولة الطرف، في الوقت الحقيقي، ومن خلال تطبيق وسائل تقنية في إقليم تلك الدولة الطرف؛

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

1' جمع وتسجيل تلك البيانات، في الوقت الحقيقي، من خلال تطبيق وسائل تقنية في إقليم تلك الدولة الطرف؛ أو

2' التعاون ومساعدة السلطات المختصة في جمع وتسجيل تلك البيانات في الوقت الحقيقي؛

2- إذا لم تتمكن الدولة الطرف، بسبب المبادئ الراسخة لنظامها القانوني الداخلي، من اعتماد التدابير المشار إليها في الفقرة 1 (أ)، فيجوز لها بدلاً من ذلك أن تعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات الحركة المرتبطة برسائل محددة أرسلت في إقليمها، وذلك باستخدام الوسائل التقنية اللازمة في ذلك الإقليم.

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

4- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 41 و42.

المادة 48- اعتراض بيانات المحتوى

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها قانونها الداخلي، لتمكين سلطاتها المختصة من اتخاذ الإجراءات التالية فيما يتعلق بـ[بيانات المحتوى] [المعلومات الإلكترونية/الرقمية، بما في ذلك بيانات المحتوى، المرسلّة بواسطة تكنولوجيا المعلومات والاتصالات] لرسائل محددة في إقليمها ترسل بواسطة [نظام حاسوبي] [نظام/جهاز لتكنولوجيا المعلومات والاتصالات]:

(أ) جمع وتسجيل تلك [البيانات] [المعلومات]، في الوقت الحقيقي، من خلال تطبيق وسائل تقنية في إقليم تلك الدولة الطرف؛

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

1' جمع وتسجيل تلك [البيانات] [المعلومات]، في الوقت الحقيقي، من خلال تطبيق وسائل تقنية في إقليم تلك الدولة الطرف؛ أو

2' التعاون ومساعدة السلطات المختصة في جمعها وتسجيلها في الوقت الحقيقي؛

2- إذا لم تتمكن الدولة الطرف، بسبب المبادئ الراسخة لنظامها القانوني الداخلي، من اعتماد التدابير المشار إليها في الفقرة 1 (أ)، فيجوز لها بدلاً من ذلك أن تعتمد ما قد يلزم من تدابير تشريعية وتدابير أخرى

لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات المحتوى عن رسائل محددة في إقليمها، وذلك باستخدام الوسائل التقنية اللازمة في ذلك الإقليم.

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

4- تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 41 و42.

المادة 49- قبول الأدلة الإلكترونية/الرقمية

يكون للأدلة الإلكترونية/الرقمية المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الإلكترونية/الرقمية أو من نظم معلومات أو برامج حاسوبية، أو من أي وسيلة لتكنولوجيات المعلومات والاتصالات قيمة وحجية الأدلة الجنائية المادية في الإجراءات الجنائية إذا تحققت فيها الشروط الفنية وفقاً لقوانين الدول الأطراف المعنية.

المجموعة 3

المادة 50- تجميد عائدات الجريمة وحجزها ومصادرتها

1- تعتمد كل دولة طرف، إلى أقصى حد ممكن في نظمها القانونية الداخلية، ما قد يلزم من تدابير للتمكين من مصادرة:

(أ) العائدات الإجرامية المتأتية من أفعال مجرّمة وفقاً لهذه الاتفاقية، أو ممتلكات تعادل قيمتها قيمة تلك العائدات؛

(ب) الممتلكات أو المعدات أو الأدوات الأخرى التي استُخدمت أو كانت معدة للاستخدام في ارتكاب أفعال مجرّمة وفقاً لهذه الاتفاقية.

2- تعتمد كل دولة طرف ما قد يلزم من تدابير تمكن من تحديد أي من البنود المشار إليها في الفقرة 1 من هذه المادة أو اقتفاء أثره أو تجميده أو حجزه، لغرض مصادرته في نهاية المطاف.

3- تتخذ كل دولة طرف، وفقاً لقانونها الداخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتنظيم إدارة السلطات المختصة للممتلكات المجمدة أو المحجوزة أو المصادرة التي تتناولها الفقرتان 1 و2 من هذه المادة.

4- إذا حُولت هذه العائدات الإجرامية إلى ممتلكات أخرى أو بُدلت بها، جزئياً أو كلياً، تكون تلك الممتلكات، بدلاً من العائدات، خاضعة للتدابير المشار إليها في هذه المادة.

5- إذا كانت العائدات الإجرامية قد اختلطت بممتلكات اكتسبت من مصادر مشروعة، وجب إخضاع تلك الممتلكات للمصادرة في حدود القيمة المقدرة للعائدات المختلطة، دون مساس بأي صلاحيات تتعلق بتجميدها أو حجزها.

6- تخضع أيضاً للتدابير المشار إليها في هذه المادة، على نفس النحو وبنفس القدر الساريين على العائدات الإجرامية، الإيرادات أو المنافع الأخرى المتأتية من العائدات الإجرامية، أو من الممتلكات التي حُولت العائدات الإجرامية إليها أو بُدلت بها، أو من الممتلكات التي اختلطت بها العائدات الإجرامية.

7- لأغراض هذه المادة والمادة [المتعلقة بالتعاون الدولي لأغراض المصادرة] من هذه الاتفاقية، تحوّل كل دولة طرف محاكمها أو سلطاتها المختصة الأخرى أن تأمر بتقديم السجلات المصرفية أو المالية أو التجارية أو بالتحفظ عليها. ولا يجوز لدولة طرف أن ترفض العمل بموجب أحكام هذه الفقرة بحجة السرية المصرفية.

- 8- يجوز لكل دولة طرف أن تنتظر في إمكانية إلزام الجاني بأن يبين المصدر المشروع للعائدات الإجرامية المزعومة أو الممتلكات الأخرى المعرضة للمصادرة، بقدر ما يتفق ذلك الإلزام مع مبادئ قانونها الداخلي ومع طبيعة الإجراءات القضائية والإجراءات الأخرى.
- 9- لا يجوز تأويل أحكام هذه المادة بما يمس حقوق أطراف ثالثة حسنة النية.
- 10- ليس في هذه المادة ما يمس مبدأ أن يكون تحديد وتنفيذ التدابير التي تشير إليها متوافقين مع أحكام القانون الداخلي لدولة طرف.

المادة 51- إنشاء سجل جنائي

يجوز لكل دولة طرف أن تعتمد ما قد يلزم من تدابير تشريعية أو تدابير أخرى لكي يؤخذ في الاعتبار، حسبما تراه مناسباً من شروط وأغراض، أي حكم إدانة سبق أن صدر بحق الجاني المزعوم في دولة أخرى، بغية استخدام تلك المعلومات في إجراءات جنائية ذات صلة بفعل مجرم وفقاً لهذه الاتفاقية.

المادة 52- حماية الشهود

- 1- تتخذ كل دولة طرف تدابير مناسبة، في حدود إمكانياتها، لتوفير حماية فعالة من الترهيب والانتقام الذي يحتمل أن يتعرض له الشهود الذين يدلون بشهادتهم، أو يقدمون، بحسن نية ولأسباب معقولة، معلومات عن الأفعال المجرمة وفقاً لهذه الاتفاقية أو يتعاونون بطريقة أخرى مع سلطات التحقيق أو السلطات القضائية، وتوفير تلك الحماية، عند الاقتضاء، لأقاربهم وغيرهم من الأشخاص المقربين منهم.
- 2- يجوز أن تشمل التدابير المتوخاة في الفقرة 1 من هذه المادة، في جملة أمور، ودون مساس بحقوق المدعى عليه، بما في ذلك حقه في محاكمة وفق الأصول القانونية، ما يلي:
- (أ) وضع إجراءات لتوفير الحماية المادية لأولئك الأشخاص، كالقيام مثلاً، بالقدر اللازم والممكن عملياً، بتغيير أماكن إقامتهم، والسماح عند الاقتضاء بعدم إفشاء المعلومات المتعلقة بهوية أولئك الأشخاص وأماكن وجودهم أو بفرض قيود على إفشائها؛
- (ب) توفير قواعد لتقديم الأدلة تتيح الإدلاء بشهادة الشهود على نحو يكفل سلامة الشاهد، مثل السماح بالإدلاء بالشهادة باستخدام تكنولوجيا الاتصالات، من قبيل وصلات الفيديو أو غيرها من الوسائل الملائمة.
- 3- تنتظر الدول الأطراف في إبرام اتفاقات أو ترتيبات مع دول أخرى بشأن تغيير أماكن إقامة الأشخاص المشار إليهم في الفقرة 1 من هذه المادة.
- 4- تسري أحكام هذه المادة أيضاً على الضحايا الذين يتقدمون للشهادة.

المادة 53- مساعدة الضحايا وحمايتهم

- 1- تتخذ كل دولة طرف تدابير ملائمة في حدود إمكانياتها لتوفير المساعدة والحماية لضحايا الأفعال المجرمة وفقاً لهذه الاتفاقية، لا سيما في حالات التهديد بالانتقام أو الترهيب.
- 2- تضع كل دولة طرف إجراءات ملائمة لتوفير سبل الحصول على التعويض ورد الحقوق لضحايا الأفعال المجرمة وفقاً لهذه الاتفاقية.
- 3- تتيح كل دولة طرف، رهناً بقانونها الداخلي، إمكانية عرض آراء وشواغل الضحايا والنظر فيها في المراحل المناسبة من الإجراءات الجنائية المتخذة ضد الجناة، على نحو لا يمس بحقوق الدفاع.

المادة 54- التعويض عن الضرر

تتخذ كل دولة طرف ما قد يلزم من تدابير، وفقاً لمبادئ قانونها الداخلي، لضمان حصول الكيانات أو الأشخاص الذين أصابهم ضرر نتيجة لـ [استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية] [الجريمة السيبرانية] على الحق في رفع دعوى قضائية ضد المسؤولين عن إحداث ذلك الضرر، بغية الحصول على تعويض.

المادة 55- تدابير تعزيز التعاون مع أجهزة إنفاذ القانون

1- تتخذ كل دولة طرف تدابير ملائمة لتشجيع الأشخاص الذين يشاركون أو شاركوا في أفعال مجرّمة وفقاً لهذه الاتفاقية على ما يلي:

(أ) إمداد السلطات المختصة بمعلومات مفيدة لأغراض التحري والإثبات فيما يخص أموراً منها:

1' هوية المشاركين في أفعال مجرّمة وفقاً لهذه الاتفاقية أو طبيعتهم أو تركيبتهم أو هيكلهم أو مكانهم أو أنشطتهم؛

2' الصلات، بما فيها الصلات الدولية، بأشخاص آخرين يشاركون في أفعال مجرّمة وفقاً لهذه الاتفاقية؛

3' الجرائم الأخرى التي ارتكبها أو قد يرتكبها المشاركون في أفعال مجرّمة وفقاً لهذه الاتفاقية؛

(ب) تقديم مساعدة فعلية وملموسة للسلطات المختصة يمكن أن تساهم في تجريد المشاركين في أفعال مجرّمة وفقاً لهذه الاتفاقية من مواردهم أو من عائدات الجريمة.

2- تنتظر كل دولة طرف في أن تتيج، في الحالات المناسبة، إمكانية تخفيف عقوبة المتهم الذي يقدم عوناً كبيراً في عمليات التحقيق أو الملاحقة بشأن فعل مجرّم وفقاً لهذه الاتفاقية.

3- تنتظر كل دولة طرف في إمكانية منح الحصانة من الملاحقة القضائية، وفقاً للمبادئ الأساسية لقانونها الداخلي، لأي شخص يقدم عوناً كبيراً في عمليات التحقيق أو الملاحقة بشأن فعل مجرّم وفقاً لهذه الاتفاقية.

4- تُكفل حماية هؤلاء الأشخاص على النحو المنصوص عليه في المادة المتعلقة بحماية الشهود من هذه الاتفاقية.

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 تنتظرا في إبرام اتفاقات أو ترتيبات، وفقاً لقانونهما الداخلي، بشأن إمكان قيام الدولة الطرف الأخرى بتوفير المعاملة المبينة في الفقرتين 2 و 3 من هذه المادة.