ورقة عناصر
مقدمة من جانب جمهورية مصر العربية
في إطار بلورة اتفاقية دولية شاملة في إطار الأمم المتحدة
في مجال مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية

<u>ديباجة:</u>

انطلاقاً من حرص جمهورية مصر العربية على المساهمة إيجابياً في المساعي الدولية المبذولة لبلورة اتفاقية أممية شاملة في مجال مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية، والتزاماً بتعهداتها في المواثيق والتشريعات الوطنية والإقليمية والدولية ذات الصلة بحقوق الإنسان ومكافحة الجرائم العابرة للحدود الوطنية، تم إعداد ورقة تتضمن عناصر مبدئية يُقترح إدراجها في متن الاتفاقية المشار إليها، وذلك أملاً في تحقيق الأهداف المنشودة منها من خلال تعزيز التعاون الدولى وصياغة سياسة جنائية مشتركة تهدف إلى مكافحة كافة أشكال الجرائم المرتبطة بتكنولوجيا الاتصالات والمعلومات، بغية درء أخطار هذه الجرائم على أمن الدول ومصالحها وسلامة مجتمعاتها وأفرادها.

<u>أولاً: الهدف من الاتفاقية:</u>

تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول الأعضاء في الأمم المتحدة في مجال مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية، بغية منع أية إجراءات من شأنها تهديد سلامة وسرية تكنولوجيا المعلومات والاتصالات، وتجريم إساءة استخدام هذه التكنولوجيا لأغراض غير قانونية، وتيسير سبل التحقيق فيها، وملاحقة مرتكبيها، وتنفيذ التدابير الرامية إلى إزالة تداعيات هذه الجرائم، بما في ذلك تعليق المعاملات المتعلقة بالأصول التي تم الحصول عليها نتيجة ارتكاب أي فعل غير قانوني منصوص عليه بموجب هذه الاتفاقية، ومصادرة عائدات هذه الجرائم وإعادتها، وذلك من خلال توفير صلاحيات كافية لمكافحة هذه الجرائم بشكل فعال عن طريق وضع ترتيبات للتعاون الدولي من أجل تسهيل اكتشاف هذه الجرائم والتحقيق فيها وملاحقة مرتكبيها ومقاضاتهم وتسليم المجرمين.

<u>ثانياً: نطاق انطباق الاتفاقية:</u>

١. تطبق هذه الاتفاقية، باستثناء ما تنص عليه خلافا لذلك، على منع الجرائم المنصوص عليها بموجب هذه الاتفاقية.

٢. تتخذ كل دولة طرف جميع التدابير اللازمة لإقامة الولاية القضائية على الجرائم الجنائية وغيرها من الأعمال غير المشروعة المنشأة وفقا لهذه الاتفاقية، عندما ترتكب:

أ) في إقليم تلك الدولة الطرف؛ أو

ب) على متن سفينة ترفع علم تلك الدولة الطرف عندما ارتكبت الجريمة، أو على متن طائرة مسجلة بموجب قانون تلك الدولة الطرف في ذلك الوقت.

ج) حيثما يكون الجرم ذا طابع عبر وطني وتكون جماعة إجرامية منظمة ضالعة في ارتكابه، ويعد الجرم ذا طابع عبر وطني في الأحوال التالية:(أ) ارتُكب في أكثر من دولة واحدة؛ (ب) ارتُكب في دولة واحدة ولكن جرى جانب من الإعداد أو التخطيط له أو توجيهه أو الإشراف عليه في دولة أخرى؛ (ج) ارتُكب في دولة واحدة، ولكن ضلعت في ارتكابه جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة؛ (د) ارتُكب في دولة واحدة، ولكن له آثارا جسيمة في دولة أخرى.

٣. لأغراض تنفيذ هذه الاتفاقية، لا يلزم أن تؤدي الجرائم وغيرها من الأعمال غير القانونية التي تنشأ فيها إلى إلحاق أضرار بالممتلكات، إلا على النحو المنصوص عليه في هذه الاتفاقية.

٤. على كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة بعاليه.

ثالثاً: صون السيادة:

١. تلتزم كل دولة طرف وفقاً لقوانينها الداخلية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.

٢. ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

رابعاً: الجرائم المقترح أن تشملها الاتفاقية:

١. 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، واكتشافها وملاحقة مرتكبيها ومقاضاتهم وتسليم المجرمين وتسهيل إجراءات التعاون الدولي وجمع الأدلة فيها.

٢. تعتمد أيضا كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية:

المادة الأولى: 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.

المادة الثانية: الدخول غير المشروع و/أو تجاوز حدود الحق فى الدخول:

١. كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدمًا حقًا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول.

٢. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

٣. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

i. محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

ii. الحصول على معلومات حكومية سرية.

المادة الثالثة: الاعتداء على تصميم موقع:

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

المادة الرابعة: الاعتراض غير المشروع:

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

المادة الخامسة: الاعتداء على سلامة البيانات:

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

المادة السادسة: 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 التدمير أو الحجب أو التعديل أو النسخ أو نشر المعلومات الرقمية أو تحييد سماتها الأمنية، باستثناء البحوث المشروعة.

المادة السابعة: التزوير:

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

المادة الثامنة: الاحتيال:

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين – عن قصد وبدون وجه حق – بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، بما في ذلك من خلال جرائم احتيالية إلكترونية متعلقة بالعملات الافتراضية (الرقمية او المشفرة).

المادة التاسعة: التهديد والابتزاز:

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

المادة العاشرة: الإباحية:

١. انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية بغرض الدعارة من خلال تقنيات الاتصالات والمعلومات.

٢. انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية للأطفال والقُصر، بما في ذلك حيازة مواد إباحية للأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية الاتصالات والمعلومات أو وسيط تخزين تلك التقنيات.

المادة الحادية عشر :الجرائم الأخرى المرتبطة بالإباحية:

الاستغلال الجنسي أو التحرش، لاسيما بالنساء والأطفال والقصر.

المادة الثانية عشر: 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 الالكترونية.

المادة الثالثة عشر: تورط الأطفال في ارتكاب أعمال غير مشروعة:

تورط القصر عن طريق تكنولوجيا المعلومات والاتصالات في ارتكاب أفعال غير مشروعة تعرض حياتهم أو صحتهم الجسمانية والنفسية للخطر.

المادة الرابعة عشر: الاعتداء على حرمة الحياة الخاصة بواسطة تكنولوجيا المعلومات والاتصالات، بما في ذلك تجريم كل من اصطنع بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا ونسبه زورًا إلى شخص طبيعي أو اعتبارى.

المادة الخامسة عشر: الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

١. نشر أفكار ومبادئ جماعات إرهابية والدعوة لها أو تبريرها.

٢. تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، وتوفير الدعم اللوجيستي لمرتكبيها.

٣. نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

٤. نشر النعرات والفتن والكراهية والعنصرية.

٥. تتخذ الدول التدابير اللازمة لمنع نشر هذا المحتوى على وسائل تكنولوجيا المعلومات والاتصال، بما في ذلك حجب وإزالة المحتوى المرتبط بهذه الجرائم.

المادة السادسة عشر: الجرائم المالية بما في ذلك المتعلقة بغسل الأموال:

١. استخدام تكنولوجيا المعلومات والاتصالات لارتكاب أية جرائم مالية وإساءة استخدام العملات الافتراضية (الرقمية والمشفرة)

٢. القيام بعمليات غسل أموال، أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.

المادة السابعة عشر: الاستخدام غير المشروع لأدوات الدفع الالكترونية:

١. كل من زوّر أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.

٢. كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.

٣. كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

٤. كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

المادة الثامنة عشر: الجرائم المتعلقة بالجرائم المنظمة أو ذات طابع عبر وطني والمرتكبة بواسطة تقنية المعلومات:

١. الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.

٢. التوزيع غير المشروع للأدوية والمنتجات الطبية المقلدة.

٣. تهريب المهاجرين.

٤. الاتجار بالأشخاص.

٥. الاتجار بالأعضاء البشرية.

٦. الاتجار غير المشروع بالأسلحة.

٧. الاتجار غير المشروع في الممتلكات الثقافية.

المادة التاسعة عشر: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة:

انتهاك حق المؤلف والحقوق المجاورة ذات الصلة كما هي مُعّرفة فى قانون الدولة الطرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد.

المادة العشرون: الدخول غير المصرح به في البنية التحتية للمعلومات الحيوية:

١. لإنشاء 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 فيه أو تحييد ميزات الأمان.

٢. 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 طالما أنها تضر بالبنية التحتية الحيوية للمعلومات.

المادة الحادية والعشرين: التحريض على الأنشطة التخريبية أو المسلحة أو الجرائم الجنائية الأخرى:

تجريم الدعوات الصادرة عن طريق تكنولوجيا المعلومات والاتصالات من أجل الدعوة 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 الثانية والعشرين: الجرائم المتعلقة بالتطرف:

تجريم 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 لكراهية عرقية أو دينية أو العداء بصفة عامة، وتجريم الدعوة وتبرير مثل هذه الأعمال أو توفير النفاذ إليها.

المادة الثالثة والعشرين: الشروع في ارتكاب جريمة:

١. 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 الرابعة والعشرين: الأفعال الأخرى غير القانونية:

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

خامساً: المسئولية القانونية والإجراءات الجنائية وإنفاذ القانون والمساعدة القانونية الدولية:

المادة الأولى: مسئولة الأشخاص الاعتبارية:

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

المادة الثانية: مسئولية مقدمي الخدمات/ مديري المواقع:

مع عدم الإخلال بالأحكام الواردة بهذه الاتفاقية، يلتزم مقدمو الخدمات/ مديرو المواقع والتابعون لهم بما يلي، مع تجريمه في حالة مخالفة أي من تلك الالتزامات: –

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

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

٢. 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

٣. تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها.

٤. يجب على مقدم الخدمة/ مدير الموقع أن يوفر لمستخدمي خدماته ولأى جهة مختصة، بالشكل والطريقة التي يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية:
– 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.

٥. يوفر مقدم الخدمة/ مدير الموقع –حال طلب السلطات المختصة التي تم تحديدها من قبل الدولة– كافة الإمكانيات الفنية التي تتيح لتلك السلطات ممارسة اختصاصاتها.

المادة الثالثة: الإجراءات الجنائية:

١. تتخذ كل دولة طرف ما يلزم من تدابير تشريعية وتدابير أخرى لتحديد السلطات والإجراءات لأغراض منع وتحديد وكشف الجرائم وغيرها من الأعمال غير المشروعة والتحقيق فيها، واتخاذ الإجراءات القضائية المتعلقة بهذه الجرائم.

٢. تطبق كل دولة طرف الصلاحيات والإجراءات المشار إليها على:

أ) الأفعال الإجرامية وغيرها من الأفعال غير المشروعة المقررة في هذه الاتفاقية؛

ب) الجرائم الجنائية الأخرى وغيرها من الأعمال غير المشروعة المرتكبة بواسطة تكنولوجيا المعلومات والاتصالات؛

ج) جمع الأدلة عن الجرائم بشكل الكتروني.

٣. تتضمن الإجراءات الجنائية ما يلي:

أ. التحفظ العاجل على البيانات المخزنة في تقنية المعلومات والاتصالات

بما في ذلك معلومات تتبع المستخدمين والتي خُزنت على تقنية معلومات وخصوصاً إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل، وذلك من خلال إصدار أمر إلى شخص من أجل إلزامه بحفظ سلامة هذه المعلومات الموجودة بحيازته أو تحت سيطرته من أجل تمكين السلطات المختصة من البحث والتقصي، مع الحفاظ على سرية أية إجراءات تتخذ في هذا الشأن.

ب. التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات، وضمان قيام السلطات المختصة بالكشف العاجل لمقدار عادل من المعلومات لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.

ج. أمر تسليم المعلومات في حوزة شخص في إقليم دولة طرف والمخزنة على تقنية معلومات أو وسيط تخزين، أو في حوزة مزود خدمة يقدم خدماته في إقليم الدولة الطرف أو تحت سيطرته.

د. تفتيش المعلومات المخزنة أو الوصول إلى المعلومات المخزنة في تقنية المعلومات أو وسيط تخزين.

هـ. ضبط المعلومات المخزنة وعمل نسخة منها والاحتفاظ بها من أجل إتمام إجراءات تفتيش والوصول إلى المعلومات المخزنة.

و. الجمع الفوري لمعلومات تتبع المستخدمين وإلزام مزود الخدمة ضمن اختصاصه بجمع وتسجيل المعلومات والاحتفاظ بسرية أية معلومات.

ز. اعتراض معلومات المحتوى من خلال تمكين السلطات المختصة بالجمع والتسجيل من خلال الوسائل الفنية بشكل فوري للمعلومات التي تبث بواسطة تكنولوجيا المعلومات والاتصالات.

ح. تتخذ كل دولة طرف ما يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاتها المختصة من وقف بث وإذاعة أي محتوي يشكل الجرائم المنصوص عليها في هذه الاتفاقية.

٤. قبول الأدلة الرقمية:

يكون للأدلة الرقمية المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الالكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات والاتصالات ذات قيمة وحجية الأدلة الجنائية المادية في الأثبات الجنائي متى توافرت بها الشروط الفنية وفقاً لقوانين الدول الأطراف.

المادة الرابعة: التعاون القانوني والقضائي الدولي:

١. تعمل الدول الأطراف على تيسير التعاون فيما بينها وفقاً لهذه الاتفاقية أو تطبيق مبدأ المعاملة بالمثل، من أجل تبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها.

٢. تتعاون الدول الأطراف إلى أقصى حد ممكن وفقا لأحكام هذه المادة وعملا بالصكوك الدولية الأخرى المتعلقة بالتعاون الدولي في المسائل الجنائية ومبدأ المعاملة بالمثل، وكذلك القوانين الداخلية ذات الصلة بهدف منع وقمع وكشف والتحقيق في الجرائم المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات.

٣. لأغراض تسليم المجرمين والمساعدة القانونية المتبادلة في المسائل الجنائية، لا تعتبر أي من الجرائم المنصوص عليها في هذا الاتفاقية جريمة سياسية. وبناء عليه، لا يجوز رفض طلب التسليم أو المساعدة القانونية في المسائل الجنائية المتصلة بهذه الجرائم، بدعوى ان الطلب يتعلق بجريمة سياسية أو جريمة مرتبطة بجريمة سياسية أو بجريمة ذات دوافع سياسية.

٤. الاختصاص: تلتزم كل دولة بتبني الإجراءات الضرورية لمد اختصاصها على الجرائم المنصوص عليها سلفاً إذا ما ارتُكبت الجريمة كلياً أو جزئيا أو تحققت:

أ. في إقليم الدولة الطرف

ب. على متن سفينة تحمل علم الدولة الطرف

ج. على متن طائرة مسجلة تحت قوانين الدولة الطرف

د. من جانب أحد مواطني الدولة الطرف إذا كانت الجريمة يُعاقب عليها حسب القانون المحلي في مكان ارتكابها، أو إذا كان ارتُكبت خارج منطقة الاختصاص القضائي لأية دولة.

هـ. إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

٥. تسليم المجرمين:

أ. يتم تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها بعاليه، بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الأطراف المعنية، ويجوز للدولة الطرف – التي يسمح قانونها بذلك – أن توافق على طلب تسليم شخص ما بسبب أي من الجرائم المشمولة بهذه الاتفاقية والتي لا يعاقب عليها بموجب قانونها الداخلي.

ب. إن الجرائم المنصوص عليها بعاليه تعتبر جرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف.

ج. إذا قامت دولة طرف بجعل تسليم المجرمين مشروطاً بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم، فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين.

د. يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة، بما في ذلك الأسس التي يمكن للدول الطرف الاستناد إليها لرفض طلب التسليم.

هـ. يجوز لكل دولة طرف أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية، وذلك إذا ما وجهت إليها الدول الطرف الأخرى طلباً بالملاحقة مصحوباً بالملفات والوثائق والمعلومات والدلائل التي تكون في حيازتها، وتحاط الدولة الطرف الطالبة علماً بما تم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم.

و. تسعى الدول الأطراف، رهنا بقوانينها الداخلية، إلى التعجيل بإجراءات التسليم وتبسيط ما يتصل بها من متطلبات إثباتية فيما يخص أي جُرم تنطبق عليه هذه المادة .

ز. يجوز للدولة الطرف متلقية الطلب، رهنا بأحكام قانونها الداخلي ومعاهداتها المتعلقة بالتسليم، وبناء على طلب من الدولة الطرف الطالبة، أن تحتجز الشخص المطلوب تسليمه والموجود في إقليمها، أو أن تتخذ تدابير مناسبة أخرى لضمان حضوره إجراءات التسليم، متى اقتنعت بأن الظروف تستدعي ذلك وبأنها ظروف ملحّة.

ح. إذا رُفض طلب تسليم مقدَّم لغرض تنفيذ حكم قضائي بحجة أن الشخص المطلوب تسليمه هو من مواطني الدولة الطرف متلقية الطلب، وجب على الدولة الطرف متلقية الطلب، إذا كان قانونها الداخلي يسمح بذلك ووفقا لمقتضيات ذلك القانون، أن تنظر، بناء على طلب من الدولة الطرف الطالبة، في إنفاذ العقوبة المفروضة بمقتضى القانون الداخلي للدولة الطرف الطالبة أو ما تبقى منها .

ط. تُكفل لأي شخص تُتخذ بشأنه إجراءات فيما يتعلق بأي من الجرائم التي تنطبق عليها هذه المادة معاملة منصفة في كل مراحل الإجراءات، بما في ذلك التمتع بجميع الحقوق والضمانات التي ينص عليها القانون الداخلي للدولة الطرف التي يوجد ذلك الشخص في إقليمها .

ي. لا يجوز تفسير أي حكم في هذه الاتفاقية على أنه يفرض التزاما بالتسليم إذا كان لدى الدولة الطرف متلقية الطلب أسباب وجيهة لاعتقاد أن الطلب قدّم لغرض ملاحقة أو معاقبة شخص بسبب جنسه أو عرقه أو ديانته أو جنسيته، أو أن الامتثال للطلب سيلحق ضررا بوضعية ذلك الشخص لأي سبب من هذه الأسباب .

ك. لا يجوز للدول الأطراف أن ترفض طلب تسليم لمجرد أن الجرم يعتبر جرما يتعلق بأمور مالية .

ل. قبل رفض التسليم، تتشاور الدولة الطرف متلقية الطلب، حيثما اقتضى الأمر، مع الدولة الطرف الطالبة لكي تتيح لها فرصة وافية لعرض آرائها وتقديم معلومات داعمة لادعائها .

م. تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإبلاغ بيانات السلطة المسئولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي إلى (جهاز متخصص يتم الاتفاق عليه) وتحديثها بشكل دوري.

٢. المساعدة المتبادلة:

أ. على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم.

ب. يتم تقديم طلب المساعدة الثنائية والاتصالات المتعقلة بها كتابةً، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك استخدام التشفير) وتأكيد الإرسال حسبما تطلب الدولة الطرف.

ج. باستثناء ما يرد فيه نص في هذه الاتفاقية، فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون.

د. حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فإن هذا الشرط يعتبر حاصلاً بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة.

٣. المعلومات العرضية المُتلقاة:

يجوز لأي دولة طرف – ضمن حدود قانونها الداخلي –وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف.

٤. الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة:

أ. تطبق مواد هذه الفقرة في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطرف الطالبة أو المطلوب منها، أما في حال وجودها فلا تطبق الفقرات المشار إليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي.

ب. على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها، مع تحديث بيانات هذه السلطة بشكل دوري.

ج. يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة.

د. يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها.

هـ. قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة، بعد استشارة الدولة الطرف الطالبة لها، أن تقرر فيما إذا سيتم تلبية الطلب جزئياً أو يكون خاضعاً للشروط التي قد تراها ضرورية.

و. تلتزم الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب، وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب

منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير.

ز. يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية أي طلب ما عدا القدر الكافي لتنفيذ الطلب، وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب.

ح. في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها، وفي مثل هذه الحالات يجب إرسال نسخة في نفس الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها.

ط. يجوز عمل الاتصالات وتقديم الطلبات حسب الفقرة السابقة بواسطة الإنتربول.

٥. <u>رفض المساعدة:</u>

أ. يجوز للدولة الطرف المطلوب منها المساعدة – بالإضافة إلى أسس الرفض المنصوص عليها في المواد السابقة أعلاه– أن ترفض المساعدة إذا اعتبر أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لسيادتها أو أمنها أو نظامها أو مصالحها الأساسية.

ب. لا يجوز رفض المساعدة القضائية في الجرائم المنصوص عليها في هذه الاتفاقية تأسيسا على كون تلك الجرائم من الجرائم السياسية أو ما في حكمها.

٦. <u>السرية وحدود الاستخدام:</u>

عندما لا يكون هناك معاهدة أو اتفاق للمساعدة المتبادلة على أساس التشريع النافذ بين الدول الأطراف الطالبة والمطلوب منها فيجب تطبيق هذه المادة، ولا يتم تطبيقها إذا وجدت مثل هذه الاتفاقية أو المعاهدة إلا إذا اتفقت الدول الأطراف المعنية على تطبيق هذه المادة جزئيا أو كلها.

٧. <u>الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات:</u>

أ. لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات التي تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلباً بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

ب. يمكن للدولة الطرف المطلوب منها المساعدة أن ترفض تنفيذ طلب الحفظ إذا اعتبرته قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها.

٨. <u>الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة:</u>

حيثما تكتشف الدولة الطرف المطلوب منها – في سياق تنفيذ الطلب الخاص بحفظ معلومات تتبع المستخدمين الخاصة باتصالات معينة – بأن مزود خدمة في دولة أخرى قد اشترك في بث الاتصال فيجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدراً كافياً من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الاتصالات.

٩. التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة:

أ. يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها.

ب. تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية.

ج. تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضة للفقدان أو التعديل.

١٠. الوصول إلى معلومات تقنية المعلومات عبر الحدود:

يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرف أخرى أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات.

١١. التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين:

أ. على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينه في أقاليمها والتي تبث بواسطة تقنية المعلومات.

ب. على كل دولة طرف توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المستخدمين لمثيلتها من القضايا الداخلية.

١٢. التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى:

تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينه تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية.

١٣. جهاز متخصص:

أ. تكفل كل دولة طرف، وفقاً للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة طوال الأسبوع لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة ويجب أن تشمل مثل هذه المساعدة تسهيل أو تنفيذ:

- **توفير المشورة الفنية.**
- **حفظ المعلومات استناداً للمواد ذات الصلة.**
- **جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين.**

ب. يجب أن يكون لدى ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة.

ج. إذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزءاً من سلطات تلك الدولة الطرف المسؤولة عن المساعدة الثنائية الدولية فيجب على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة.

د. على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز المذكور أعلاه.

خامساً: المساعدة التقنية والتدريب:

١. المبادئ العامة للمساعدة التقنية:

أ) تنظر الدول الأطراف في منح بعضها بعضا أكبر قدر من المساعدة التقنية، وخصوصا لصالح البلدان النامية من أجل دعم خططها وبرامجها الرامية إلى مكافحة الجرائم في مجال تكنولوجيا المعلومات والاتصالات، بما في ذلك الدعم المادي والتدريب في المجالات المشار إليها في هذه الاتفاقية، إضافة إلى التدريب والمساعدة ونقل التكنولوجيا والمعرفة وتبادل أفضل التجارب والخبرات المكتسبة ذات الصلة، مما ييسر التعاون الدولي بين الدول الأطراف فيما يتعلق بتسليم المجرمين والمساعدة القانونية المتبادلة.

ب) تعزز الدول الأطراف جهودها الرامية إلى زيادة فعالية الأنشطة التنفيذية والتدريبية إلى أقصى حد في المنظمات الدولية والإقليمية وفي إطار الاتفاقات أو الترتيبات الثنائية والمتعددة الأطراف ذات الصلة.

ج) تنظر الدول الأطراف في مساعدة بعضها بعضا، عند الطلب، لإجراء تقييمات ودراسات وبحوث بشأن أنواع الجرائم المرتكبة في مجال تكنولوجيا المعلومات والاتصالات في بلدانها والأسباب الكامنة وراءها والآثار الناجمة عنها، لكي تضع بمشاركة السلطات المختصة والفاعلين الرئيسيين استراتيجيات وخطط عمل لمكافحة هذه الأنواع من الجرائم.

د) تنظر الدول الأطراف في إنشاء آليات تمويل بهدف توفير المساعدة للجهود التي تبذلها البلدان النامية من خلال برامج ومشروعات المساعدة الفنية.

هـ) تنظر الدول الأطراف في تبادل المعلومات بشأن التطورات القانونية، السياسية أو التكنولوجية ذات الصلة بالجريمة الإلكترونية وجمع الأدلة في شكل إلكتروني.

٢. التدريب وبناء القدرات:

أ. تتولى كل دولة طرف، حسب الاقتضاء، وضع أو تنفيذ أو تحسين برامج تدريب خاصة لأعضاء السلطات المسؤولين عن منع الجرائم في مجال تكنولوجيا المعلومات والاتصالات ومكافحتها. ويمكن أن تشمل برامج التدريب هذه عدة مجالات، منها ما يلي:

- التدابير الفعالة لمنع الجرائم في مجال تكنولوجيا المعلومات والاتصالات والكشف عنها والتحقيق فيها والمعاقبة عليها ومكافحتها، بما في ذلك استخدام الوسائل الإلكترونية لجمع الأدلة وأساليب التحقيق
- منع تحويل عائدات الجرائم المحددة بموجب هذه الاتفاقية واسترداد تلك العائدات؛
- الكشف عن المعاملات المتصلة بتحويل عائدات الجرائم المحددة وفقا لهذه الاتفاقية واعتراضها؛ ومراقبة حركة عائدات الجرائم المحددة وفقا لهذه الاتفاقية والأساليب المستخدمة في تحويل تلك العائدات أو إخفائها أو تمويهها؛
- إنشاء آليات وأساليب قانونية وإدارية ملائمة وذات كفاءة؛ تسهل ضبط والتحفظ ومصادرة واسترداد عائدات الجرائم المنشأة وفقا لهذه الاتفاقية؛
- الأساليب المستخدمة في حماية الضحايا والشهود والمبلغين الذين يتعاونون مع السلطات القضائية؛

- **إعداد وتخطيط سياسة استراتيجية لمكافحة الجرائم في مجال تكنولوجيا المعلومات والاتصالات، كما ينبغي للبلدان أن تستثمر في بناء وتعزيز قدرات التحليل الجنائي الرقمي، بما في ذلك توفير التدريب والتأهيل الأمني، فضلاً عن نظم إدارة أمن المعلومات لدعم الملاحقات القضائية الناجحة في الجرائم السيبرانية عن طريق فحص الأجهزة الإلكترونية من أجل جمع الأدلة بطريقة موثوقة؛**
- **إعداد طلبات للمساعدة القانونية المتبادلة تستوفي الشروط التي تنص عليها هذه الاتفاقية؛**
- **التحقيق في الجريمة السيبرانية والتعامل مع الأدلة الإلكترونية وتسلسل العهدة والتحليل الجنائي؛**
- **توفير التدريب اللغوي والمهني بكافة الأنشطة المتعلقة بمكافحة استخدام تكنولوجيا الاتصالات والمعلومات وحماية وسرعة التواصل مع الأجهزة المتخصصة لضبط وكشف الجرائم ذات الصلة.**

ب. ينبغي للدول الأعضاء التي لديها قدرات وهياكل أساسية أكثر تقدما في مجال الجريمة السيبرانية أن تتحمل مسؤوليات تتناسب مع تلك القدرات عند تقديم المساعدة القانونية إلى الدول الأخرى وخاصة النامية وتقديم الدعم والمشورة ونقل المعرفة لهم في مجالات مكافحة الجريمة السيبرانية.
