ورقة عناصر
مقدمة من جانب جمهورية مصر العربية
في إطار الجلسة الثانية للجنة الخاصة ببلورة اتفاقية دولية شاملة في إطار الأمم المتحدة
في مجال مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية
(الأحكام العامة، التجريم، المسائل الإجرائية وإنفاذ القانون)

انطلاقاً من الحرص على مواجهة التغيرات التكنولوجية على الساحة الدولية والتي قد تؤثر سلباً على أمن الدول وسيادتها ومصالحها وسلامة مجتمعاتها وأفرادها من خلال استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية، فإنه من الهام إيجاد اتفاقية دولية تضمن الحفاظ على الأمن القومي للدول أعضاء الأمم المتحدة، وعلى النحو الذى يتماشى مع أحكام حقوق الانسان ذات الصلة، وفي اطار متوازن ويتلائم مع احترام سيادة الدول وعدم التدخل في شئونها الداخلية، وأن يكون الهدف من هذه الاتفاقية هو تعزيز التعاون الدولي في مجال مكافحة الجريمة السيبرانية مع التأكيد على أهمية قيام الدول ذات الخبرات التكنولوجية المتقدمة بتقديم المساعدات الفنية وبرامج بناء القدرات اللازمة لنظرائها من الدول ذات الخبرة الأقل في هذا المجال، وبخاصة الدول النامية، وعلى النحو الذى يساعد فى تسهيل نقل المعرفة والتكنولوجيا لهذه الدول وفقاً لاحتياجاتها، ودون شروط أو معوقات.

وفى هذا السياق، تتقدم جمهورية مصر العربية بالمقترحات التالية في إطار الإعداد للجلسة الثانية للجنة الخاصة ببلورة اتفاقية دولية شاملة في إطار الأمم المتحدة في مجال مكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية، والمقرر أن يتم خلالها التفاوض حول الموضوعات التالية: الأحكام العامة، التجريم، المسائل الإجرائية وإنفاذ القانون.

الفصل الأول: الأحكام العامة:

يُقترح أن يتضمن هذا الفصل الهدف من الاتفاقية، وأهم المصطلحات المستخدمة، بالإضافة إلى ما يضمن صون السيادة، إلى جانب مجالات التطبيق؛ وذلك على النحو التالي:

المادة الأولى (الهدف من الاتفاقية)

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.

المادة الثانية (المصطلحات)

يُقصد بالمصطلحات التالية في هذه الاتفاقية التعريف المبين إزاء كل منها:

١. ***تقنية المعلومات:*** **أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزونة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة.**

٢. ***مزود الخدمة:*** **أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.**

٣. ***البيانات:*** **كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها.**

٤. ***النظام المعلوماتي:*** **مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.**

٥. ***الشبكة المعلوماتية:*** **ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.**

٦. ***الموقع:*** **مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.**

٧. ***الإلتقاط:*** **مشاهدة البيانات أو المعلومات أو الحصول عليها.**

٨. ***مدير الموقع:*** **كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع أو أكثر على الشبكة المعلوماتية، بما في ذلك حقوق الوصول لمختلف المستخدمين على ذلك الموقع أو تصميمه، أو توليد وتنظيم صفحاته أو محتواه أو المسئول عنه.**

٩. ***الحساب الخاص:*** **مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له الحق دون غيره الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي.**

١٠. ***البريد الإلكتروني:*** **وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلي وما في حكمها.**

١١. *الاعتراض:* مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل، أو تغيير المحتوى، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق.

١٢. *الاختراق:* الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة، إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية، وما في حكمها.

١٣. *المحتوى:* أي بيانات تؤدى بذاتها، أو مجتمعة مع بيانات أو معلومات أخرى إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معنى أو الإشارة إلى بيانات أخرى.

١٤. *الدليل الرقمي:* أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.

١٥. *حركة الاتصال (بيانات المرور):* بيانات ينتجها نظام معلوماتي تبين مصدر الاتصال، وجهته والوجهة المرسل منها والمرسل إليها والطريق الذي سلكه، وساعته وتاريخه وحجمه ومدته، ونوع الخدمة.

المادة الثالثة (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.

المادة الرابعة (مجالات التطبيق)

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

٢. 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.

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

الفصل الثانى: التجريم:

المادة الخامسة (التجريم)

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 مع التأكيد على أهمية مبدأ الحيادية التكنولوجية، 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 السادسة (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.

المادة السابعة (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 الثامنة (الاعتداء على تصميم موقع)

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

المادة التاسعة (الاعتراض غير المشروع)

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

المادة العاشرة (الاعتداء على سلامة البيانات)

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

المادة الحادية عشر (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 الثانية عشر (التزوير)

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

المادة الثالثة عشر (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 الرابعة عشر (التهديد والابتزاز)

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

المادة الخامسة عشر (الإباحية)

١.انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية بغرض الدعارة واستغلال السيدات والقصر من خلال تقنيات الاتصالات والمعلومات وفقا للقانون الداخلي لكل دولة.

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 السادسة عشر (الجرائم الأخرى المرتبطة بالإباحية)

الاستغلال الجنسي أو التحرش، لاسيما بالنساء والأطفال والقصر.

المادة السابعة 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 الثامنة 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 التاسعة عشر (الاعتداء على حرمة الحياة الخاصة)

وذلك 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 العشرون (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 الحادية والعشرين (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 الثانية والعشرين (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 الثالثة والعشرين (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 غير المشروع بالأشخاص و الاتجار بالأعضاء البشرية.
٥. الاتجار غير المشروع بالأسلحة.

٦. الاتجار غير المشروع في الممتلكات الثقافية.

المادة الرابعة والعشرين (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 الخامسة والعشرين (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 السادسة والعشرين (التحريض على الأنشطة التخريبية أو المسلحة أو الجرائم الجنائية الأخرى)

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

المادة الثامنة والعشرين (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 التاسعة 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.

المادة الثلاثون (مسئولة الأشخاص الاعتبارية)

١. 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.

٢. 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:

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، 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.

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.

الفصل الثالث: المسائل الإجرائية وإنفاذ القانون:

يُقترح أن يتضمن هذا الفصل ٣ مواد رئيسية، وذلك على النحو التالي:

المادة الحادية والثلاثين (نطاق المسائل الإجرائية)

١. تتخذ كل دولة طرف ما يلزم من تدابير تشريعية 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 إلكتروني.

المادة الثانية والثلاثين (المسائل الإجرائية)

تتضمن الإجراءات الجنائية ما يلي:

١. 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.

٢. 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.

٣. 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.

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

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

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

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

٨. 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.

المادة الثالثة والثلاثين (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.