COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

مجلس أوروبا

سلسلة المعاهدات الأوروبية رقم 185

التقرير التفسيري لاتفاقية الجريمة الإلكترونية

بودابست، في ٢٣ نوفمبر/تشرين الثاني ٢٠٠١

أولا – تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (٨ نوفمبر/تشرين الثاني ٢٠٠١) وفتح باب التوقيع على الاتفاقية في بودابست، في ٢٣ نوفمبر/تشرين الثاني ٢٠٠١، بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية.

ثانيا – لا يشكل نص هذا التقرير التفسيري أداة توفر تفسيرا ذي حجية للاتفاقية، على الرغم من أنه قد يكون ذا طبيعة تسهل تطبيق الأحكام الواردة فيه.

أولا. المقدمة

١. غيرت ثورة تكنولوجيات المعلومات المجتمع بشكل جوهري، ومن المحتمل أن تستمر في تغييره في المستقبل القريب، علاوة على أنها يسرت إنجاز العديد من المهام. ولئن كانت بعض فئات المجتمع فقط قد نجحت، أصلا، في ترشيد إجراءات عملها بمساعدة تكنولوجيا المعلومات، فإن كافة فئات المجتمع لم تسلم من تأثيرها، حيث اجتاحت تكنولوجيا المعلومات بشكل أو بآخر تقريبا كل جوانب الأنشطة البشرية.

٢. لعل إحدى السمات البارزة لتكنولوجيا المعلومات تتلخص في الوقع الذي أحدثته وستحدثه على تطور تكنولوجيا الاتصالات السلكية واللاسلكية. وقد تجاوزت الاتصالات الهاتفية، التي تنطوي على نقل صوت الإنسان، تبادل كميات هائلة من البيانات، بما في ذلك الصوت، والنص، والموسيقى والصور الثابتة والمتحركة. لم يعد هذا التبادل يحدث سوى بين البشر، ولكن أيضا بين البشر والحواسيب، وبين أجهزة الكمبيوتر نفسها. فضلا عن ذلك، تمت استعاضة عن الاتصالات بدوائر التبديل بشبكات تبديل الرزم. ولم يعد الربط المباشر يكتسي أي أهمية؛ يكفي أن يتم إدخال بيانات في شبكة مع عنوان الوجهة أو إتاحتها لأي شخص يريد النفاذ إليها.

٣. يعتبر الاستخدام واسع النطاق للبريد الإلكتروني والولوج إلى العديد من المواقع الإلكترونية مثالا لهذه التطورات، التي غيرت مجتمعنا بعمق.

٤. أدت سهولة الولوج إلى المعلومات المضمنة في نظم الكمبيوتر وإمكانية البحث عنها، بالإضافة إلى الإمكانات غير المحدودة لتبادلها ونشرها بشمل عملي، بغض النظر عن بعد المسافات الجغرافية، إلى حدوث نمو هائل في حجم المعلومات المتاحة والمعرفة التي يمكن استخلاصها من منها.

٥. أسفرت هذه التطورات عن تغيرات اقتصادية واجتماعية لم يسبق لها مثيل، إلا أنها تنطوي أيضا على جانب مظلم: ظهور أنواع جديدة من الإجرام، فضلا عن ارتكاب جرائم تقليدية عن طريق التكنولوجيات الجديدة. بالإضافة إلى ذلك، يمكن أن يتجاوز مدى عواقب السلوك الإجرامي نطاقها في السابق لأنها غير مقيدة بحدود جغرافية أو وطنية، وأكبر دليل على ذلك، الانتشار الأخير لفيروسات الكمبيوتر الضارة في جميع أنحاء العالم. لهذا، ينبغي تنفيذ التدابير الفنية الرامية إلى حماية نظم الكمبيوتر بالتزامن مع تدابير قانونية للوقاية من السلوك الإجرامي وردعه.

٦. تتحدى التكنولوجيات الحديثة المفاهيم القانونية القائمة، حيث تتدفق المعلومات والاتصالات بسهولة أكبر من جميع أنحاء العالم. ولم تعد الحدود عائقا أمام هذا التدفق. فضلا عن أن المجرمين ما فتئوا يتواجدون في أماكن غير تلك التي تنتج فيها أفعالهم آثارها. ومع ذلك، تظل القوانين الوطنية محصورة بشكل عام في إقليم معين. لهذا، ينبغي أن يوفر القانون الدولي الحلول للمشاكل المطروحة، مما يستلزم اعتماد صكوك قانونية دولية ملائمة. وفي هذا الإطار، تهدف هذه الاتفاقية إلى رفع هذا التحدي، مع إيلاء الاحترام الواجب لحقوق الإنسان في مجتمع المعلومات الجديد.

ثانيا. الأعمال التحضيرية

٧. قررت اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، في قرارها رقم CDPC/١٠٣/٢١١١٩٦ الصادر في نوفمبر/تشرين الثاني ١٩٩٦، إنشاء لجنة خبراء للتعامل مع الجريمة الإلكترونية. واستندت اللجنة في قرارها على الأساس المنطقي التالي:

٨. " تؤثر التطورات السريعة في مجال تكنولوجيا المعلومات بشكل مباشر على جميع فئات وقطاعات المجتمع الحديث، إذ أن تكامل أنظمة الاتصالات والمعلومات، التي تتيح تخزين ونقل جميع أنواع الاتصالات، بغض النظر عن المسافة، يفتح تشكيلة واسعة وكاملة من الإمكانيات الجديدة. وقد تعززت هذه التطورات بظهور طرق وشبكات المعلومات فائقة السرعة، بما في ذلك الإنترنت، والتي يمكن افتراضيا من خلالها لأي شخص النفاذ إلى أي خدمة للمعلومات الإلكترونية بغض النظر عن مكان وجودها في العالم. وبالتالي، فإن المستخدمين، من خلال الربط بخدمات الاتصالات والمعلومات، يخلقون نوعا من الفضاء المشترك يسمى "الفضاء الإلكتروني"، الذي يستخدم لأغراض مشروعة، لكن قد يكون أيضا عرضة لإساءة الاستعمال. وعندئذ، تتلخص "جرائم الفضاء الإلكتروني" هذه إما في جرائم مرتكبة ضد سلامة وتوافر وسرية أنظمة الكمبيوتر وشبكات الاتصالات أو في استخدام هذه الشبكات لارتكاب جرائم تقليدية. ويتعارض الطابع العابر للحدود لهذه الجرائم، عندما يرتكب عن طريق الإنترنت على سبيل المثال، مع إقليمية سلطات إعمال القوانين الوطنية.

٩. لذلك، يجب أن يواكب القانون الجنائي هذه التطورات التكنولوجية التي تتيح فرصا معقدة للغاية لإساءة استخدام مرافق الفضاء الإلكتروني وتسبب أضرارا للمصالح المشروعة. وتقتضي الطبيعة العابرة للحدود لشبكات المعلومات جهودا دولية متسقة من أجل التصدي لإساءة الاستخدام من هذا القبيل. ولئن كانت التوصية رقم ٨٩ (٩) قد أسفرت عن تقريب المفاهيم الوطنية فيما يتعلق بأشكال معينة من إساءة استخدام الحاسوب، فإن الفعالية اللازمة لمكافحة هذه الظواهر الجديدة لن تتحقق إلا من خلال آلية دولية ملزمة. وبالإضافة إلى تدابير التعاون الدولي، ينبغي أن تتم في إطار هذه الآلية معالجة مسائل القانون الموضوعي والإجرائي، علاوة على المسائل المتصلة اتصالا وثيقا باستخدام تكنولوجيا المعلومات."

١٠. فضلا عن ذلك، أخذت اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، في الاعتبار التقرير الذي أعده - بناء على طلبها - البروفيسور ه. كاسبرسين (H.W.K. Kaspersen)، الذي خلص إلى أنه "... ينبغي النظر في إمكانية وضع آلية قانونية أخرى ملزمة بشكل أكبر من التوصية، من قبيل اتفاقية. ولا ينبغي أن تقتصر اتفاقية من هذا القبيل على تناول مسائل القانون الموضوعي الجنائي بل أن تعالج أيضا المسائل الإجرائية الجنائية وكذلك إجراءات واتفاقيات القانون الجنائي الدولي "[1]. وقد برزت نتيجة مماثلة من قبل في التقرير المرفق بالتوصية رقم (٨٩) [2]٩ بشأن القانون الموضوعي وفي التوصية رقم (٩٥) [3]١٣ بشأن مشاكل القانون الإجرائي المتصلة بتكنولوجيا المعلومات.

---

[1] إعمال التوصية رقم (89) 9 بشأن الجرائم المتصلة بالكمبيوتر، تقرير أعده الأستاذ الدكتور ه. كاسبرسين (وثيقة. اللجنة الأوروبية المعنية بمشاكل الإجرام (٩٧) ٥ أند ولجنة الخبراء المتعلقة بالفضاء الإلكتروني (PC-CY) (٩٧) ٥، صفحة ١٠٦).

[2] انظر الجريمة المتصلة بالكمبيوتر، تقرير اللجنة الأوروبية المعنية بمشاكل الإجرام، الصفحة ٨٦.

[3] انظر مشاكل قانون الإجراءات الجنائية المتصلة بتكنولوجيا المعلومات، التوصية رقم (95) 13، المبدأ رقم ١٧.

١١. وكانت البنود المرجعية الخاصة باللجنة الجديدة تتلخص فيما يلي:

أ. " على ضوء التوصيتين رقم (٨٩) ٩ بشأن الجرائم المتصلة بالكمبيوتر ورقم (٩٥) ١٣ بشأن مشاكل قانون الإجراءات الجنائية المتصلة بتكنولوجيا المعلومات، مراجعة المواضيع التالية بالتحديد:

ب. جرائم الفضاء الإلكتروني، لا سيما الجرائم المرتكبة من خلال استخدام شبكات الاتصالات السلكية واللاسلكية مثل الإنترنت، من قبيل المعاملات المالية غير المشروعة، وتقديم خدمات غير قانونية، وانتهاك حقوق التأليف والنشر، علاوة على الجرائم التي تنتهك كرامة الإنسان وحماية القاصرين؛

ت. مسائل أخرى من القانون الجنائي الموضوعي حيث قد يكون من الضروري تبني مقاربة مشتركة لأغراض التعاون الدولي، من قبيل التعاريف والعقوبات ومسؤولية الفاعلين في الفضاء الإلكتروني، بما في ذلك مزودو خدمات الإنترنت؛

ث. استخدام سلطات قسرية، بما في ذلك إمكانية الاستخدام العابر للحدود، وقابلية تطبيقها في بيئة تكنولوجية، مثل اعتراض الاتصالات السلكية واللاسلكية والمراقبة الإلكترونية لشبكات المعلومات، على سبيل المثال عن طريق شبكة الإنترنت، والبحث في نظم معالجة المعلومات ومصادرتها (بما في ذلك مواقع الإنترنت)، مما يجعل مواد غير قانونية غير قابلة للنفاذ ويتطلب من مقدمي الخدمات الامتثال لالتزامات خاصة، مع مراعاة المشاكل الناجمة عن تدابير خاصة بسلامة المعلومات، مثلا: التشفير؛

ج. مسألة الاختصاص فيما يتعلق بجرائم تكنولوجيا المعلومات، على سبيل المثال. من أجل تحديد المكان الذي ارتكبت فيه الجريمة (locus delicti)، ومن ثم تحديد القانون الواجب تطبيقه، بما في ذلك مشكلة " عدم جواز المحاكمة على ذات الجرم مرتين " في حال تعدد الاختصاصات القضائية، ومسألة كيفية حل تنازع الاختصاص الإيجابي وطريقة تفادي النزاعات السلبية المرتبطة بالاختصاص القضائي؛

ح. مسائل التعاون الدولي في مجال التحقيق في جرائم الفضاء الإلكتروني، بالتعاون الوثيق مع لجنة الخبراء المعنية بتشغيل الاتفاقيات الأوروبية في المجال الجنائي (PC-OC).

وهكذا، ينبغي على اللجنة صياغة آلية قانونية ملزمة، قدر الإمكان، بشأن البنود "أ" إلى "ح"، مع التركيز بشكل خاص على المسائل الدولية، وعند الاقتضاء، صياغة توصيات إضافية ذات الصلة بقضايا محددة. ويمكن للجنة أن تقدم اقتراحات بشأن مسائل أخرى في ضوء التطورات التكنولوجية."

١٢. عملا بقرار اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، أنشأت لجنة الوزراء لجنة جديدة تدعى "لجنة الخبراء المعنية بالجريمة في الفضاء الإلكتروني" بموجب القرار رقم CM/Del/Dec(97)583، الصادر في ٤ فبراير/شباط (١٩٩٧). وقد بدأت هذه اللجنة المعروفة بالاختصار الانجليزي (PC-CY) أعمالها في أبريل/نيسان ١٩٩٧ وأجرت مفاوضات بشأن مسودة اتفاقية دولية حول الجريمة الإلكترونية. وفي إطار بنودها المرجعية الأصلية، كان من المقرر أن تنهي اللجنة عملها بحلول ٣١ ديسمبر/كانون الأول ١٩٩٩. وبما أن اللجنة لم تكن آنذاك في وضعية تمكنها من إبرام مفاوضاتها بشأن بعض المسائل الواردة في مشروع الاتفاقية، تم تمديد بنودها المرجعية إلى غاية ٣١ ديسمبر/كانون الأول ٢٠٠٠ بموجب القرار رقم CM/Del/Dec(99)679 الصادر عن نواب الوزراء. وقد أعرب وزراء العدل الأوروبيون مرتين عن تأييدهم للمفاوضات: بموجب القرار رقم ١ المعتمد خلال مؤتمرهم الحادي والعشرين (براغ، يونيو/حزيران ١٩٩٧)، الذي أوصى لجنة الوزراء بدعم العمل الذي اضطلعت به اللجنة الأوروبية المعنية بمشاكل الإجرام بشأن الجريمة الإلكترونية بغية تقريب أحكام القانون الجنائي المحلي من بعضها البعض والتمكين من استخدام وسائل فعالة للتحقيق في جرائم من هذا القبيل، وكذلك بموجب القرار رقم ٣، المعتمد خلال المؤتمر الثالث والعشرين لوزراء العدل الأوروبيين (لندن، يونيو/حزيران ٢٠٠٠)، الذي شجع الأطراف المتفاوضة على مواصلة جهودها بغية إيجاد حلول مناسبة لتمكين أكبر عدد ممكن من الدول لتصبح أطرافا في الاتفاقية واعترف بالحاجة إلى نظام سريع وفعال للتعاون الدولي يأخذ في الاعتبار كما يجب المتطلبات الخاصة

لمكافحة الجريمة الإلكترونية. وأعربت الدول الأعضاء في الاتحاد الأوروبي عن تأييدها لعمل لجنة الخبراء المعنية بالجريمة في الفضاء الإلكتروني من خلال موقف مشترك، اعتمد في مايو/أيار ١٩٩٩.

١٣. في الفترة الممتدة ما بين أبريل/نيسان ١٩٩٧ وديسمبر/كانون الأول ٢٠٠٠، عقدت لجنة (PC-CY) ١٠ اجتماعات في جلسات عامة و١٥ اجتماعا لفريق الصياغة المفتوح باب العضوية. وعقب انتهاء مدة بنودها المرجعية الموسعة، عقد الخبراء، تحت رعاية اللجنة الأوروبية المعنية بمشاكل الإجرام، ثلاثة اجتماعات أخرى لوضع اللمسات النهائية على مشروع المذكرة التوضيحية ومراجعة مسودة الاتفاقية في ضوء رأي الجمعية البرلمانية، التي طلبت منها لجنة الوزراء في أكتوبر/تشرين الأول ٢٠٠٠ إبداء رأيها بشأن مسودة الاتفاقية الذي اعتمدته في الجزء الثاني من دورتها العامة في أبريل/نيسان ٢٠٠١.

١٤. في أعقاب قرار اتخذته لجنة (PC-CY)، تم الكشف عن نسخة مبكرة من مسودة الاتفاقية وصدورها في أبريل/نيسان ٢٠٠٠، تلتها مسودات لاحقة صدرت بعد كل جلسة عامة، بغية تمكين الدول المتفاوضة من التشاور مع كافة الأطراف المهتمة. وقد ثبتت فائدة عملية التشاور.

١٥. قدمت مسودة الاتفاقية المنقحة والنهائية ومذكرتها التفسيرية للموافقة عليهما إلى اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) في دورتها العامة الخمسين المنعقدة في يونيو/حزيران ٢٠٠١، وبعدها، تم عرض نص مسودة الاتفاقية على لجنة الوزراء لاعتماده وفتح باب التوقيع عليه.

ثالثا. الاتفاقية

١٦. ترمي الاتفاقية بشكل أساسي إلى (١) مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية (٢) والتنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم ومتابعتها قضائيا علاوة على الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر أو التي تكون الأدلة المتصلة بها في شكل إلكتروني (٣) وإلى إنشاء نظام سريع وفعال للتعاون الدولي.

١٧. بناء على ذلك، تتضمن الاتفاقية أربعة فصول: (١) استخدام المصطلحات؛ (٢) التدابير الواجب اتخاذها على الصعيد المحلي – القانون الموضوعي والقانون الإجرائي؛ (٣) التعاون الدولي؛ (٤) الأحكام الختامية.

١٨. يتطرق القسم ١ من الفصل الثاني (مسائل القانون الموضوعي) إلى أحكام التجريم والأحكام الأخرى ذات الصلة في مجال الجريمة الإلكترونية أو الجريمة المتصلة بالكمبيوتر: يحدد أولا ٩ جرائم مصنفة في أربع فئات مختلفة، ثم يتناول المسؤولية الفرعية والعقوبات. وتعرف الاتفاقية الجرائم التالية: النفاذ/الولوج غير القانوني، والاعتراض غير القانوني، وتداخل البيانات، وتداخل النظام، وإساءة استخدام الأجهزة، والتزوير المتصل بالكمبيوتر، والاحتيال المتصل بالكمبيوتر، والجرائم المتصلة باستغلال الأطفال في المواد الإباحية، والجرائم المتصلة بحق التأليف والنشر والحقوق المجاورة.

١٩. يحدد القسم ٢ من الفصل الثاني (المسائل المتعلقة بالقانون الإجرائي) – الذي يتجاوز نطاقه الجرائم المحددة في القسم ١ من حيث أنه ينطبق على أي جريمة ترتكب بواسطة نظام الكمبيوتر أو تكون الأدلة المتصلة بها في شكل إلكتروني – أولا الشروط والضمانات المشتركة التي تنطبق على جميع الصلاحيات الإجرائية في هذا الفصل. ثم، يحدد الصلاحيات الإجرائية التالية: التعجيل بحفظ البيانات المخزنة؛ والتعجيل في حفظ بيانات الحركة والإفصاح الجزئي عنها؛ أمر تقديم البيانات؛ البحث عن بيانات الكمبيوتر ومصادرتها؛ جمع بيانات الحركة في الوقت الحقيقي؛ اعتراض بيانات المحتوى. وينتهي الفصل الثاني بأحكام الولاية القضائية.

٢٠. يتضمن الفصل الثالث الأحكام المتعلقة بالمساعدة المتبادلة التقليدية والمتصلة بالجريمة الإلكترونية، فضلا عن قواعد تسليم المجرمين. ويتناول هذا الفصل المساعدة المتبادلة التقليدية في حالتين: ١) غياب الأساس القانوني (معاهدة، تشريع متبادل، وما إلى ذلك) بين الأطراف – وفي هذه الحالة تنطبق أحكامه – ٢) وجود الأساس القانوني – وفي هذه الحالة، تنطبق الترتيبات القائمة أيضا على المساعدة بموجب هذه الاتفاقية. وتنطبق المساعدة الخاصة بالجريمة الإلكترونية أو الجريمة المتصلة بالكمبيوتر على كلا الحالتين وتغطي، مع مراعاة الشروط الإضافية، نفس نطاق الصلاحيات الإجرائية المحددة في الفصل الثاني. وبالإضافة إلى ذلك، يتضمن الفصل الثالث حكما بشأن نوع محدد من النفاذ العابر للحدود إلى بيانات مخزنة على الحواسيب والذي لا يتطلب المساعدة المتبادلة (عبر الموافقة أو عندما تكون متاحة للجمهور)، وينص على إنشاء شبكة على مدار ٢٤ ساعة طوال أيام الأسبوع بغية ضمان المساعدة السريعة بين الاطراف.

٢١. وفي الأخير، يتضمن الفصل الرابع الأحكام الختامية التي – مع بعض الاستثناءات – تكرر الأحكام الموحدة في معاهدات مجلس أوروبا.

تعليق على مواد الاتفاقية

الفصل الأول – استخدام المصطلحات

تقديم التعاريف الواردة في المادة ١

٢٢. استوعب القائمون على الصياغة أن الأطراف لن تكون ملزمة، بموجب هذه الاتفاقية، باستنساخ المفاهيم الأربعة المحددة في المادة ١حرفيا في قوانينها الداخلية، شريطة أن تغطي هذه القوانين تلك المفاهيم بطريقة تتفق مع مبادئ الاتفاقية و توفر إطارا مطابقا لتنفيذها.

المادة ١ (أ) – نظام الكمبيوتر

٢٣. بموجب الاتفاقية، يقصد بنظام الكمبيوتر أي جهاز يتألف من أجهزة وبرمجيات تم تطويرها من أجل المعالجة التلقائية للبيانات الرقمية. ويمكن أن يشمل المدخلات والمخرجات، ومرافق التخزين. ويمكن أن يشتغل لوحده أو أن يكون متصلا بشبكة مع غيرها من الأجهزة المماثلة. ويقصد بمصطلح "تلقائي" دون تدخل بشري مباشر. وتعني "معالجة البيانات" أن البيانات في نظام الكمبيوتر يتم تشغيلها عن طريق تنفيذ برنامج الكمبيوتر. "برنامج الكمبيوتر" هو مجموعة من التعليمات التي يمكن تنفيذها من خلال الكمبيوتر لتحقيق النتيجة المرجوة. ويمكن للكمبيوتر تشغيل برامج مختلفة. وعادة، يتكون نظام الكمبيوتر من أجهزة مختلفة، من قبيل المعالج (processor) أو وحدة المعالجة المركزية، والأجهزة الطرفية. ويعتبر " الجهاز الطرفي" جهازا يؤدي بعض الوظائف المعينة في تفاعل مع وحدة المعالجة، كالآلة الطابعة، شاشة الفيديو، آلة قراءة/تسجيل الأقراص المدمجة أو أي جهاز تخزين آخر.

٢٤. الشبكة هي ترابط بين نظامي كمبيوتر أو أكثر. ويمكن أن تكون الوصلات أرضية (على سبيل المثال، الأسلاك أو الكابلات) أو لاسلكية (مثل الراديو أو الأشعة تحت الحمراء أو القمر الصناعي) أو كليهما. ويمكن أن تكون الشبكة محدودة جغرافيا في منطقة صغيرة (شبكات المنطقة المحلية) أو أن تمتد على مساحة شاسعة (شبكات المنطقة الواسعة)، وهذه الشبكات بدورها يمكن أن تكون مترابطة فيما بينها. ويعتبر الإنترنت شبكة عالمية تتكون من العديد من الشبكات المترابطة تستخدم جميعها نفس البروتوكولات. وتوجد أنواع أخرى من الشبكات، سواء كانت متصلة بالإنترنت أم لا، القادرة على تحويل بيانات الكمبيوتر بين أنظمة الحاسوب. ويمكن أن تكون أنظمة الكمبيوتر متصلة بالشبكة كنقاط نهاية أو كوسيلة للمساعدة في التواصل على الشبكة. الأمر الأساس هو أن تبادل البيانات يتم عبر الشبكة.

المادة ١ (ب) – بيانات الكمبيوتر

٢٥. يستند تعريف بيانات الكمبيوتر إلى تعريف المنظمة الدولية للمواصفات لمصطلح البيانات. ويتضمن هذا التعريف مصطلحات "مناسب للمعالجة"، بمعنى أنه يتم وضع البيانات في شكل يسمح بمعالجتها مباشرة من خلال نظام الكمبيوتر. وتوخيا لتوضيح أن البيانات الواردة في هذه الاتفاقية يجب أن تفهم على أنها بيانات في شكل إلكتروني أو أي شكل آخر قابل للمعالجة التلقائية، تم إدخال مفهوم "بيانات الكمبيوتر". ويمكن أن تكون بيانات الكمبيوتر التي تتم معالجتها تلقائيا موضوع إحدى الجرائم الجنائية المحددة في هذه الاتفاقية وكذلك موضوع تطبيق أحد تدابير التحقيق المحددة في هذه الاتفاقية.

المادة ١ (ج) – مقدم الخدمة

٢٦. يشمل مصطلح "مقدم الخدمات" فئة واسعة من الأشخاص الذين يضطلعون بدور خاص فيما يتعلق بالاتصال أو معالجة البيانات ذات الصلة بأنظمة الكمبيوتر (راجع أيضا التعليقات في القسم ٢). وبموجب الفقرة (١) من التعريف، يتضح أن الكيانات العامة والخاصة التي توفر للمستعملين القدرة على التواصل فيما بينهم مشمولة. لذلك، فإن معرفة ما إذا كان المستخدمون يشكلون مجموعة مغلقة أو ما إذا كان مقدم الخدمة يعرض خدماته للجمهور مجانا أو مقابل رسوم، ليست أمرا مجديا. ويمكن أن تشير المجموعة المغلقة على سبيل المثال إلى موظفي شركة خاصة تقدم لهم هذه الخدمة من خلال شبكة الشركة.

٢٧. بموجب الفقرة (٢) من التعريف، يتضح أن مصطلح "مقدم الخدمات" يشمل أيضا الهيئات التي تخزن البيانات أو تعالجها نيابة عن الأشخاص المذكورين في الفقرة الفرعية (١). علاوة على ذلك، يشمل المصطلح الكيانات التي تقوم بتخزين البيانات أو معالجتها بطريقة أخرى نيابة عن مستخدمي الخدمات التي يوفرها الأشخاص المذكورون في الفقرة الفرعية (١). على سبيل المثال، يتضمن مصطلح مقدم الخدمة، في إطار هذا التعريف، كلا من الخدمات التي توفر خدمة الاستضافة والتخزين المؤقت بالإضافة إلى الخدمات التي توفر الربط بشبكة. ومع ذلك، لا يشمل من هذا التعريف مقدم المحتوى (من قبيل الشخص الذي يتعاقد مع شركة استضافة مواقع الإنترنت لاستضافة موقعه الإلكتروني) إذا كان مقدم المحتوى لا يوفر أيضا خدمات الاتصال أو خدمات معالجة البيانات ذات الصلة.

المادة ١ (د) – بيانات الحركة

٢٨. لأغراض هذه الاتفاقية، تشكل بيانات حركة المرور، على النحو المحدد في المادة ١ في إطار الفقرة الفرعية (د)، فئة من بيانات الكمبيوتر الخاضعة لنظام قانوني خاص. ويتم توليد هذه البيانات من قبل أجهزة الكمبيوتر في خضم سلسلة الاتصالات من أجل توجيه اتصال من المصدر الأصلي إلى الوجهة. لذلك، تعتبر بيانات الحركة فرعية ومساعدة للاتصال في حد ذاته.

٢٩. في حال التحقيق في جريمة جنائية ارتكبت من خلال نظام كمبيوتر، تكون هنالك حاجة إلى بيانات الحركة لتعقب مصدر الاتصال كنقطة انطلاق من أجل جمع أدلة إضافية أو كجزء من الأدلة على الجريمة. لكن بيانات الحركة معرضة للزوال، مما يدعو إلى الأمر بالتعجيل بحفظها. ونتيجة لذلك، قد يكون من الضروري الكشف السريع عنها بغية تحديد طريق الاتصال من أجل جمع المزيد من الأدلة قبل حذفها أو بغية التعرف على المشتبه به. لذلك، قد يكون الإجراء العادي لجمع بيانات الكمبيوتر والكشف عنها غير كاف. فضلا عن ذلك، يعتبر جمع هذه البيانات من حيث المبدأ أقل تطفلا، حيث أنه لا يكشف عن محتوى الاتصال الذي يعتبر أكثر حساسية.

٣٠. وضع التعريف قائمة مستفيضة لفئات بيانات الحركة التي تخضع معالجتها لنظام خاص في هذه الاتفاقية: منشأ الاتصال، وجهته، طريقه، وقته (توقيت غرينتش)، تاريخه، حجمه، مدته ونوع الخدمة التي ينطوي عليها. ولن تكون جميع هذه الفئات متاحة دائما من الناحية الفنية أو قد لا يتمكن مقدم الخدمة من إنتاجها، أو لن تكون ضرورية لإجراء تحقيق جنائي معين. ويشير مصطلح "المنشأ" إلى رقم الهاتف أو عنوان بروتوكول الإنترنت (IP) أو ما شابه ذلك من هوية هيئة الاتصالات التي يزودها مقدم الخدمة بخدماته. ويقصد بمصطلح "الوجهة" العنوان المماثل لهيئة الاتصالات التي تنقل إليها الاتصالات. وتشير عبارة "نوع الخدمة التي ينطوي عليها" إلى نوع الخدمة التي يتم استخدامها داخل الشبكة، مثل نقل الملفات، أو البريد الإلكتروني أو الرسائل الفورية.

٣١. يترك التعريف للمجالس التشريعية الوطنية القدرة على إدخال تمييز في الحماية القانونية لبيانات الحركة وفقا لحساسيتها. وفي هذا السياق، تلزم المادة ١٥ الأطراف بتوفير شروط وضمانات كافية لحماية حقوق الإنسان والحريات. ويعني ذلك، من بين أمور أخرى، أن المعايير الموضوعية وإجراءات تطبيق سلطة التحقيق قد تختلف بحسب حساسية البيانات.

الفصل الثاني – التدابير الواجب اتخاذها على الصعيد الوطني

٣٢. يتضمن الفصل الثاني (من المادة ٢ إلى المادة ٢٢) ثلاثة أقسام: القانون الجنائي الموضوعي (المواد من ٢ إلى ١٣)، والقانون الإجرائي (المواد من ١٤ إلى ٢١) والولاية القضائية (المادة ٢٢).

القسم ١ – القانون الجنائي الموضوعي

٣٣. يتلخص الغرض من القسم ١ من الاتفاقية (المواد من ٢ إلى ١٣) في تحسين وسائل منع وقمع الجرائم الإلكترونية أو المتصلة بالكمبيوتر من خلال وضع معيار أدنى مشترك للجرائم ذات الصلة، فضلا عن أن هذا النوع من المواءمة يخفف مكافحة هذه الجرائم على الصعيدين الوطني والدولي. علاوة على ذلك، تحول المطابقة في القانون المحلي دون انتقال الإساءات إلى دولة طرف ذات معيار أدنى سابق. ونتيجة لذلك، يمكن أيضا تعزيز تبادل الخبرات المشتركة المفيدة في التعامل العملي مع القضايا. ويتم تيسير التعاون الدولي (خصوصا تسليم المجرمين والمساعدة القانونية المتبادلة) على سبيل المثال، فيما يتعلق بشروط التجريم المزدوج.

٣٤. تشمل قائمة الجرائم المدرجة حدا أدنى من التوافق لا يستبعد توسيع نطاق القانون المحلي. ويستند إلى حد كبير إلى المبادئ التوجيهية التي وضعت في ارتباط بالتوصية رقم ٩ (٨٩) الصادرة عن مجلس أوروبا بشأن الجرائم المتصلة بالكمبيوتر وبشأن أعمال منظمات دولية عامة وخاصة أخرى (منظمة التعاون والتنمية الاقتصادية (OECD)، والأمم المتحدة، والجمعية الدولية المعنية بقانون العقوبات (AIDP)، ولكن مع مراعاة تجارب أكثر حداثة لإساءة استخدام شبكات الاتصالات التي ما فتئت تتوسع.

٣٥. ينقسم القسم إلى خمسة أبواب. ويشمل الباب ١ أهم الجرائم المتصلة بالكمبيوتر، والجرائم المخلة بسرية وسلامة وتوافر بيانات وأنظمة الكمبيوتر، التي تمثل التهديدات الأساسية، على النحو المحدد في المناقشات المتعلقة بأمن الكمبيوتر والبيانات، التي تتعرض لها معالجة البيانات الإلكترونية وأنظمة الاتصال. ويقدم هذا الباب وصفا لنوع الجرائم المشمولة، أي النفاذ غير المرخص له إلى الأنظمة، البرامج أو البيانات والتلاعب بها بصورة غير مشروعة. وتتضمن الأبواب من ٢ إلى ٤ أنواعا أخرى من "الجرائم المتصلة بالكمبيوتر" التي تؤدي دورا أكبر في الممارسة وحيث تستخدم أنظمة الكمبيوتر والاتصالات كوسيلة للهجوم على بعض المصالح القانونية التي يحميها القانون الجنائي في معظم الأحيان من الهجمات التي تستخدم طرقا تقليدية. وقد أضيفت جرائم في الباب ٢ (الغش والتزوير المتصلان بالكمبيوتر) طبقا للمقترحات الواردة في المبادئ التوجيهية لتوصية مجلس أوروبا رقم ٩ (٨٩). ويغطي الباب ٣ "الجرائم المتصلة بالمحتوى المتعلقة بالإنتاج أو التوزيع غير المشروع لاستغلال الأطفال في المواد الإباحية عن طريق استخدام أنظمة الكمبيوتر" باعتبارها أحد أخطر أساليب العمل في عصرنا. وناقشت لجنة صياغة الاتفاقية إمكانية إدراج جرائم أخرى ذات الصلة بالمحتوى، من قبيل توزيع الدعاية العنصرية عن طريق أنظمة الكمبيوتر. غير أن اللجنة لم تتمكن من التوصل إلى توافق في الآراء بشأن تجريم هذا السلوك. وعلى الرغم من التأييد الكبير لإدراج هذا الفعل كجريمة، أعربت بعض الوفود عن قلقها الشديد إزاء إدراج حكم من هذا القبيل من منظور حرية التعبير. وبعد أن لاحظت اللجنة تعقد المسألة، تقرر أن تحيل اللجنة مسألة وضع بروتوكول إضافي لهذه الاتفاقية إلى اللجنة الأوروبية المعنية بمشاكل الإجرام. ويحدد الباب ٤ "الجرائم المتعلقة بانتهاكات حقوق التأليف والنشر والحقوق المجاورة". وقد أدرجت هذه الجرائم في الاتفاقية لأن انتهاكات حقوق التأليف والنشر هي أحد أشكال الجرائم الإلكترونية والجرائم المتصلة بالكمبيوتر أو الحاسوب الأكثر انتشارا، لأن تصاعدها يسبب قلقا دوليا. وفي الأخير، يتضمن الباب ٥ أحكاما إضافية بشأن المحاولة والمساعدة والتحريض والعقوبات والتدابير، وامتثالا للصكوك الدولية الحديثة، أحكاما بشأن مسؤولية الشركات.

٣٦. على الرغم من أن أحكام القانون الموضوعي تتعلق بجرائم تستخدم تكنولوجيا المعلومات، تستخدم الاتفاقية لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية.

٣٧. أدرك القائمون على صياغة الاتفاقية أن الأطراف قد تستبعد سوء السلوك البسيط أو غير الهام من تطبيق الجرائم المحددة في المواد من ٢ إلى ١٠.

٣٨. من بين الخصائص المحددة للجرائم المدرجة، ثمة الشرط الصريح الذي يقضي بأن يكون السلوك المعني "بدون حق". ويعكس ذلك الرأي السائد بأن السلوك الموصوف لا يعاقب دائما في حد ذاته، ولكن قد يكون قانونيا أو مبررا ليس فقط في الحالات التي تكون فيها الدفوع القانونية التقليدية قابلة للتطبيق، مثل الموافقة والدفاع عن النفس أو الضرورة، ولكن حيث تؤدي مبادئ أو مصالح أخرى إلى استبعاد المسؤولية الجنائية. ويستمد التعبير "بدون حق" معناه من السياق الذي يستخدم فيه. ومن ثم، ودون تقييد الطريقة التي يمكن بها للأطراف إعمال هذا المفهوم في قوانينها المحلية، يجوز أن تشير هذه العبارة إلى السلوك الذي يتم دون سلطة (سواء كانت تشريعية، تنفيذية، إدارية، قضائية، تعاقدية أو توافقية) أو سلوك لا تشمله خلاف ذلك الدفوع القانونية، الأعذار، المبررات أو المبادئ ذات الصلة القائمة بموجب القانون المحلي. وبالتالي، تترك الاتفاقية السلوك غير المتأثر المتخذ وفقا للسلطة الحكومية الشرعية (على سبيل المثال، عندما تعمل حكومة الدولة الطرف للحفاظ على النظام العام، وحماية الأمن القومي أو التحقيق في الجرائم الجنائية). علاوة على ذلك، لا ينبغي تجريم الأنشطة المشروعة والمشتركة المتأصلة في تصميم الشبكات، أو الممارسات التشغيلية أو التجارية المشروعة والمشتركة. وترد أمثلة محددة على هذه الاستثناءات من التجريم فيما يتعلق بجرائم محددة في النص المطابق في المذكرة التفسيرية أدناه. ويترك للأطراف تحديد كيفية تنفيذ هذه الاستثناءات في إطار أنظمتها القانونية المحلية (بموجب القانون الجنائي أو بطرق أخرى).

٣٩. يجب أن ترتكب جميع الجرائم الواردة في الاتفاقية "عمدا" من أجل تطبيق المسؤولية الجنائية. وفي بعض الحالات، يشكل عنصر متعمد محدد إضافي جزءا من الجريمة. فعلى سبيل المثال، في المادة ٨ المتعلقة بالاحتيال المتصل بالكمبيوتر، تشكل النية في الحصول على منفعة اقتصادية عنصرا من العناصر المكونة للجريمة. واتفق القائمون على صياغة الاتفاقية على أن المعنى الدقيق لمصطلح "عمدا" ينبغي أن يترك للتفسير الوطني.

٤٠. تسمح بعض المواد الواردة في هذا القسم بإضافة ظروف مؤهلة عند تنفيذ الاتفاقية في القانون المحلي. وفي حالات أخرى، تمنح إمكانية التحفظ (انظر المادتين ٤٠ و٤٢). وتعكس هذه الطرق المختلفة لمقاربة أكثر تقييدا في التجريم تقييمات مختلفة لخطورة السلوك الذي ينطوي عليه الأمر أو للحاجة إلى استخدام القانون الجنائي كتدبير مضاد. وتوفر هذه المقاربة مرونة للحكومات والبرلمانات في تحديد سياستها الجنائية في هذا المجال.

٤١. ينبغي أن تصاغ القوانين المنشئة لهذه الجرائم بقدر أكبر من الوضوح والخصوصية قدر الإمكان، من أجل توفير الاستشراف الملائم لنوع السلوك الذي سيسفر عن عقوبة جنائية.

٤٢. خلال عملية الصياغة، تدارس القائمون على الصياغة استصواب تجريم سلوك غير السلوكيات المحددة في المواد من ٢ إلى ١١، بما في ذلك ما يسمى "احتلال الفضاء الإلكتروني" أو "السطو الإلكتروني" (cybersquatting)، أي تسجيل اسم نطاق مطابق إما لاسم هيئة قائمة بالفعل وعادة ما يكون اسما جد معروف أو لاسم تجاري أو علامة تجارية لمنتج أو شركة. ولا يوجد لدى محتلي الفضاء الإلكتروني أي نية في الاستخدام النشط لاسم النطاق بل يسعون إلى جني فائدة مالية من خلال إجبار الهيئة المعنية، وإن كان بشكل غير مباشر، على دفع ثمن نقل ملكية اسم النطاق. وفي الوقت الراهن، يعتبر هذا السلوك مسألة ذات صلة بالعلامة التجارية. وبما أن انتهاكات العلامات التجارية غير خاضعة لهذه الاتفاقية، فإن القائمين على الصياغة لم يروا أنه من المناسب تناول مسألة تجريم هذا السلوك.

الباب الأول – الجرائم ضد سرية وسلامة وتوافر بيانات وأنظمة الكمبيوتر

٤٣. يتلخص الغرض من الجرائم المحددة في المواد (من ٢ إلى ٦) في حماية سرية وسلامة وتوافر أنظمة أو بيانات الكمبيوتر وليس في تجريم الأنشطة المشروعة والمشتركة المتأصلة في تصميم الشبكات، أو الممارسات التشغيلية أو التجارية المشروعة والمشتركة.

النفاذ غير القانوني (المادة ٢)

٤٤. تشمل عبارة "النفاذ غير القانوني" الجريمة الأساسية للتهديدات الخطيرة الموجهة ضد أمن أنظمة وبيانات الكمبيوتر (أي السرية والسلامة والتوافر) والهجمات عليها. وتعكس الحاجة إلى الحماية مصالح المنظمات والأفراد في إدارة أنظمتها وتشغيلها ومراقبتها بطريقة غير مضطربة ودون عوائق. وينبغي أن يكون مجرد التسلل غير المرخص، بمعنى "قرصنة" أو "كسر" أو "اختراق الكمبيوتر"، غير قانوني في حد ذاته من حيث المبدأ، حيث أن مثل هذا السلوك قد يضع عوائق أمام المستخدمين الشرعيين للأنظمة والبيانات، وقد يتسبب في إحداث تغيير أو تدمير يسفر إصلاحه عن كلفة عالية. وقد يترتب عن مثل هذا الاختراق النفاذ إلى بيانات سرية (بما في ذلك، كلمات المرور ومعلومات عن النظام المستهدف)، وأسرار، بالإضافة إلى استخدام النظام بدون مقابل أو حتى إلى تشجيع القراصنة على ارتكاب أشكال أكثر خطورة من الجرائم المتصلة بالكمبيوتر، مثل الاحتيال أو التزوير المتصل بالكمبيوتر.

٤٥. إن الوسيلة الأكثر فعالية لمنع النفاذ غير المرخص هي، بطبيعة الحال، إدخال وتطوير تدابير أمنية فعالة. ومع ذلك، يجب أن تشمل الاستجابة الشاملة أيضا التهديد باستخدام تدابير القانون الجنائي واستخدامها. ويمكن للحظر الجنائي للنفاذ غير المرخص أن يوفر حماية إضافية للنظام والبيانات في حد ذاتها وفي مرحلة مبكرة ضد المخاطر المذكورة أعلاه.

٤٦. يتألف "النفاذ" من الدخول الكامل أو الجزئي إلى نظام الكمبيوتر (المعدات، والمكونات والبيانات المخزنة في النظام المثبت، والدلائل، وبيانات الحركة، والبيانات ذات الصلة بالمحتوى). ومع ذلك، لا يتضمن مجرد إرسال رسالة عن طريق البريد الإلكتروني أو ملف إلى هذا النظام. ويشمل "النفاذ" الدخول إلى نظام كمبيوتر آخر، حيث يتم ربطه عبر شبكات الاتصالات العامة، أو بنظام كمبيوتر على نفس الشبكة، مثل شبكة اتصال محلية (LAN) أو شبكة إنترانت داخل منظمة. لا تعتبر طريقة الاتصال مهمة (على سبيل المثال الاتصال عن بعد، بما في ذلك عبر وصلات لاسلكية أو على مسافة قريبة).

٤٧. يجب أن يرتكب الفعل أيضا "بدون حق". بالإضافة إلى التفسير الوارد أعلاه حول هذه العبارة، فهذا يعني أنه لا يوجد تجريم للنفاذ المسموح به من قبل المالك أو أي شخص آخر صاحب الحق على النظام أو جزء منه (مثلا لأغراض الاختبار المرخص أو حماية نظام الكمبيوتر المعني). فضلا عن ذلك، لا يوجد تجريم للنفاذ إلى نظام كمبيوتر يتيح للجمهور الولوج المجاني والمفتوح، باعتبار هذا النفاذ "بحق".

٤٨. قد يؤدي تطبيق أدوات تقنية محددة إلى النفاذ بموجب المادة ٢، مثل الدخول إلى صفحة على شبكة الإنترنت، مباشرة أو من خلال الوصلات التشعبية، بما في ذلك الوصلات العميقة أو تطبيق "ملفات تعريف الارتباط" (كوكيز) أو "بوتات الإنترنت" (bots) لتحديد موقع و استرجاع المعلومات باسم الاتصال. ولا يعتبر تطبيق هذه الأدوات في حد ذاتها "بدون حق". فصيانة موقع عمومي على شبكة الإنترنت تنطوي على موافقة مالك الموقع الإلكتروني على إمكانية النفاذ إليه من قبل أي مستعمل آخر للإنترنت. ولا يعتبر تطبيق الأدوات القياسية المنصوص عليها في بروتوكولات وبرامج الاتصالات التي يتم تطبيقها بشكل عام، في حد ذاته "بدون حق"، لا سيما عندما يمكن اعتبار أن صاحب حق النظام الذي تم النفاذ إليه قد قبل بتطبيقه، على سبيل المثال في حالة "الكوكيز"، بعدم رفض التركيب الأولي أو عدم إزالته.

٤٩. تتضمن العديد من التشريعات الوطنية بالفعل أحكاما بشأن جرائم "الاختراق"، غير أن نطاقها والعناصر المكونة لها تختلف بشكل كبير. ولا تعتبر المقاربة الواسعة للتجريم المشار إليها في الجملة الأولى من المادة ٢ موضع نزاع، لكن تنبع المعارضة من الحالات التي لا تنشأ فيها أخطار بمجرد الاقتحام أو التي تؤدي فيها أعمال القرصنة إلى الكشف عن ثغرات ومكامن ضعف في أمن الأنظمة. وقد أدى ذلك في مجموعة من البلدان إلى تبني مقاربة ضيقة تفرض شروطا مؤهلة إضافية، وهي أيضا المقاربة الذي اعتمدت في التوصية رقم ٩ (٨٩) واقتراح الفريق العامل التابع لمنظمة التعاون والتنمية الاقتصادية في عام ١٩٨٥.

٥٠. يمكن للأطراف أن تعتمد المقاربة الواسعة وأن تجرم مجرد الاختراق طبقا للجملة الأولى من المادة ٢. كما يمكن لها، بدلا من ذلك، أن ترفق، كليا أو جزئيا، العناصر المؤهلة المدرجة في الجملة الثانية: اختراق التدابير الأمنية، النية الخاصة في الحصول على بيانات الكمبيوتر، أو نوايا أخرى غير شريفة تبرر المسؤولية الجنائية، أو اشتراط ارتكاب الجريمة ذات صلة بنظام كمبيوتر متصل عن بعد بنظام كمبيوتر آخر. ويتيح الخيار الأخير للأطراف استبعاد الحالة التي ينفذ فيها الشخص فعليا إلى جهاز كمبيوتر مستقل دون استخدام أي نظام كمبيوتر آخر. ويمكن أن تقيد الأطراف هذه الجريمة بالنفاذ غير المشروع إلى أنظمة الكمبيوتر الشبكية (بما في ذلك، الشبكات العمومية التي توفرها خدمات الاتصال والشبكات الخاصة من قبيل الشبكات الداخلية "إنترانت" أو الشبكة الخارجية "إكسترانت").

الاعتراض غير القانوني (المادة ٣)

٥١. يهدف هذا الحكم إلى حماية الحق في خصوصية نقل البيانات. وتمثل الجريمة نفس الانتهاك لخصوصية الاتصالات مثل التنصت والتسجيل التقليديين للمحادثات الهاتفية الشفوية بين الأشخاص. وتكرس المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان الحق في خصوصية المراسلات. وتطبق الجريمة المنصوص عليها في المادة ٣ هذا المبدأ على جميع أشكال نقل البيانات الإلكترونية، سواء عن طريق الهاتف أو الفاكس أو البريد الإلكتروني أو نقل الملفات.

٥٢. اقتبس نص الحكم أساسا من جريمة "الالتقاط غير المرخص" الواردة في التوصية ٩ (٨٩). وتوضح هذه الاتفاقية أن الاتصالات المعنية تتعلق "بإرسال بيانات الكمبيوتر" فضلا عن الإشعاع الكهرومغناطيسي، في ظل الظروف المبينة أدناه.

٥٣. ينطوي الاعتراض بواسطة "وسائل فنية" على التنصت على محتوى الاتصالات أو رصده أو مراقبته، أو شراء محتوى البيانات سواء بطريقة مباشرة من خلال الولوج إلى نظام الكمبيوتر واستخدامه، أو بطريقة غير مباشرة عن طريق استخدام أجهزة اختلاس السمع أو التنصت الإلكترونية. ويمكن أن ينطوي الاعتراض أيضا على التسجيل. وتشمل الوسائل الفنية الأجهزة التقنية المثبتة على خطوط النقل وكذلك أجهزة جمع وتسجيل الاتصالات اللاسلكية. ويمكن أن تشمل استخدام البرمجيات وكلمات المرور والرموز. ويعتبر شرط استخدام الوسائل الفنية مؤهلا تقييديا لتجنب التجريم المفرط.

٥٤. تنطبق الجريمة على عمليات الإرسال "غير العامة" لبيانات الكمبيوتر. ويحدد مصطلح "غير عام" طبيعة عملية الإرسال (الاتصالات) وليس طبيعة البيانات المرسلة. ويمكن أن تكون البيانات التي يتم إرسالها معلومات متاحة للجمهور، ولكن الأطراف ترغب في التواصل بشكل سري. كما يمكن الاحتفاظ بسرية البيانات لأغراض تجارية حتى يتم دفع مقابل الخدمة، كما هو الحال في خدمة التلفزيون المدفوع. لذلك، لا يستبعد مصطلح "غير عام" في حد ذاته الاتصالات عبر الشبكات العامة. من جهة أخرى، تعتبر اتصالات الموظفين، سواء كانت لأغراض مهنية أو غيرها، والتي تشكل "نقلا غير عام لبيانات الكمبيوتر" مشمولة بالحماية من الاعتراض بدون حق بموجب المادة ٣ (انظر مثلا حكم المحكمة الأوروبية لحقوق الإنسان في قضية هالفورد ضد المملكة المتحدة، ٢٥ يونيو/حزيران ١٩٩٧، ٩٢/٢٠٦٠٥).

٥٥. يمكن أن يحدث الاتصال في شكل إرسال بيانات الكمبيوتر داخل نظام كمبيوتر واحد (بحيث يتدفق من وحدة المعالجة المركزية نحو الشاشة أو الآلة الطابعة، على سبيل المثال)، بين نظامين للكمبيوتر ينتميان إلى نفس الشخص، بين جهازين متصلان ببعضهما البعض، أو بين جهاز كمبيوتر وشخص (مثلا من خلال لوحة المفاتيح). ومع ذلك، قد تطالب الأطراف كعنصر إضافي أن يتم نقل الاتصال بين أنظمة الكمبيوتر المتصلة عن بعد.

٥٦. تجدر الإشارة إلى أن تضمن مفهوم "نظام الكمبيوتر" للاتصالات اللاسلكية لا يعني أن الطرف ملزم بتجريم اعتراض أي بث إذاعي، الذي، وإن كان "غير عام"، يتم بطريقة مفتوحة نسبيا ويمكن الولج إليه بسهولة، وبالتالي يمكن اعتراضه، على سبيل المثال من قبل هواة الراديو.

٥٧. إن إنشاء جريمة مرتبطة "بالانبعاثات الكهرومغناطيسية" سيضمن نطاقا أشمل. ويمكن أن تصدر الانبعاثات الكهرومغناطيسية عن الكمبيوتر أثناء تشغيله. ولا تعتبر هذه الانبعاثات "بيانات" وفقا للتعريف الوارد في المادة ١. ومع

ذلك، يمكن إعادة بناء البيانات انطلاقا من تلك الانبعاثات. لذلك، تم إدراج اعتراض البيانات من الانبعاثات الكهرومغناطيسية الصادر من نظام الكمبيوتر باعتبارها جريمة بموجب هذا الحكم.

٥٨. لإلحاق المسؤولية الجنائية، يجب أن يرتكب الاعتراض غير المشروع "عمدا" و "بدون حق". ويكون هذا الفعل مبررا، على سبيل المثال، إذا كان للشخص المعترض الحق في القيام بذلك، إذا تصرف بناء على تعليمات أو بإذن من المشاركين في الإرسال (بما في ذلك الاختبار المرخص أو أنشطة الحماية التي وافق عليها المشاركون)، أو إذا كانت المراقبة مخولة قانونيا لمصلحة الأمن القومي أو للكشف عن الجرائم من قبل سلطات التحقيق. وكان من المفهوم أيضا أن استخدام الممارسات التجارية المشتركة، من قبيل استخدام "ملفات تعريف الارتباط" (كوكيز)، لا يقصد به أن يجرم على هذا النحو، باعتبار أنه لا يشكل اعتراضا "بدون حق". وفيما يتعلق بالاتصالات غير العامة بين الموظفين المحمية بموجب المادة ٣ (انظر الفقرة ٥٤ أعلاه)، يمكن أن يوفر القانون المحلي سببا للاعتراض المشروع على هذه الاتصالات. وبموجب المادة ٣، يعتبر الاعتراض في مثل هذه الظروف على أنه تم "عن حق".

٥٩. قد يكون الاعتراض، في بعض البلدان، مرتبطا ارتباطا وثيقا بجريمة النفاذ غير المرخص إلى نظام الكمبيوتر. ومن أجل ضمان الاتساق في الحظر والتطبيق بموجب القانون، يمكن للبلدان، التي تتطلب وجود نوايا غير مشروعة أو أن ترتكب الجريمة في إطار علاقة بنظام حاسوبي متصل بنظام كمبيوتر آخر وفقا للمادة ٢، أن تشترط أيضا وجود عناصر مؤهلة مماثلة لإسناد المسؤولية الجنائية في هذه المادة. وينبغي تفسير هذه العناصر وتطبيقها بالاقتران مع العناصر الأخرى للجريمة، كالارتكاب "عمدا" و "بدون حق".

التدخل في البيانات (المادة ٤)

٦٠. يتلخص الهدف من هذا الحكم في توفير حماية لبيانات الكمبيوتر وبرامج الكمبيوتر تكون مماثلة لتلك التي تتمتع بها الأشياء المادية ضد إلحاق الضرر المتعمد. وتتمثل المصلحة القانونية المحمية هنا في سلامة بيانات أو برامج الكمبيوتر المخزنة وفي حسن تشغيلها أو استخدامها.

٦١. في الفقرة ١، يرتبط "الإضرار" و"التخريب"، باعتبارهما عملان متداخلان، على وجه الخصوص بالتغيير السلبي في سلامة البيانات والبرامج أو محتواها الإعلامي. ويعتبر "حذف" البيانات مطابقا لتدمير الشيء المادي، حيث يتم تدميرها وجعلها غير قابلة للتعرف. ويقصد بإتلاف بيانات الكمبيوتر أي عمل يمنع أو ينهي توافر البيانات للشخص الذي لديه حق النفاذ إلى الكمبيوتر أو لوسيلة حفظ البيانات التي تم تخزين البيانات عليها. ويعني مصطلح "التغيير" تعديل البيانات القائمة. وبالتالي، فإن إدخال رموز خبيثة، مثل الفيروسات وأحصنة طروادة، مشمولة في هذه الفقرة، كما هو الحال بالنسبة للتعديل الناجم عن البيانات.

٦٢. لا يعاقب على الأفعال المذكورة أعلاه إلا إذا ارتكبت "بدون حق". وهكذا، فإن الأنشطة المشتركة المتأصلة في تصميم الشبكات أو الممارسات التشغيلية أو التجارية المشتركة، مثل اختبار أو حماية أمن نظام الكمبيوتر المرخص به من قبل المالك أو المشغل، أو إعادة تشكيل نظام تشغيل الكمبيوتر الذي يتم عندما يقتني مشغل النظام برمجية جديدة (على سبيل المثال، البرمجيات التي تسمح بالولوج إلى الإنترنت والتي تعطل البرامج المماثلة المركبة سابقا)، تعتبر "بحق" وبالتالي لا تجرمها هذه المادة. وينبغي، من حيث المبدأ، اعتبار تعديل بيانات الحركة بغرض تيسير الاتصالات مجهولة المصدر (مثل أنشطة أنظمة إعادة الإرسال المجهولة)، أو تعديل البيانات لأغراض الاتصالات الآمنة (مثل التشفير) بمثابة حماية مشروعة للخصوصية، ومن تم، اعتبار أنها تنجز "بحق". ومع ذلك، قد ترغب الأطراف في تجريم بعض التجاوزات المتعلقة بالاتصالات المجهولة، مثلا عند تغيير المعلومات الرأسية للرزمة من أجل إخفاء هوية مرتكب الجريمة.

٦٣. بالإضافة إلى ذلك، يجب أن يكون الجاني قد تصرف "عمدا".

٦٤. تسمح الفقرة ٢ للأطراف بالتحفظ بشأن الجرم من حيث أنها قد تقتضي أن يؤدي التصرف إلى ضرر جسيم. ويترك للتشريع المحلي تفسير ما يشكل ضررا جسيما، لكن ينبغي للأطراف إشعار الأمين العام لمجلس أوروبا بتفسيرها إذا ما تم استخدام هذا التحفظ.

التدخل في النظام (المادة ٥)

٦٥. يشار إلى ذلك في التوصية رقم ٩ (٨٩) بتخريب الكمبيوتر. ويهدف هذا الحكم إلى تجريم العرقلة المتعمدة للاستعمال المشروع لأنظمة الكمبيوتر بما في ذلك مرافق الاتصالات السلكية واللاسلكية من خلال استخدام بيانات الكمبيوتر أو التأثير عليها. وتتمثل المصلحة القانونية المحمية في مصلحة مشغلي ومستخدمي أنظمة الكمبيوتر أو الاتصالات حتى يكونوا قادرين على تشغيلها بشكل سليم. وقد تمت صياغة النص بطريقة محايدة بحيث يمكن حماية جميع أنواع الوظائف بموجبه.

٦٦. يشير مصطلح "العرقلة" إلى الإجراءات التي تعترض التشغيل السليم لنظام الكمبيوتر. ويجب أن تتم هذه العرقلة عبر إدخال بيانات الكمبيوتر، نقلها، إتلافها، حذفها، تغييرها أو تدميرها.

٦٧. فضلا عن ذلك، يجب أن تكون العرقلة "جسيمة" لإنشاء عقوبة جنائية. ويتعين على كل طرف تحديد معاييره الخاصة التي يجب استيفاؤها من أجل اعتبار العرقلة "جسيمة". فعلى سبيل المثال، يمكن لدولة طرف أن تشترط حدا أدنى من الضرر حتى يتم اعتبار العرقلة جسيمة. واعتبر القائمون على الصياغة كفعل "جسيم" عملية إرسال البيانات إلى نظام معين في شكل أو حجم أو تواتر بحيث يكون له تأثير ضار كبير على قدرة المالك أو المشغل على استخدام النظام، أو التواصل مع أنظمة أخرى (على سبيل المثال، عن طريق البرامج التي تولد هجمات "الحرمان من الخدمة"، والرموز الخبيثة مثل الفيروسات التي تمنع أو تبطئ بشكل كبير تشغيل النظام، أو البرامج التي ترسل كميات هائلة من البريد الإلكتروني إلى المتلقي من أجل إعاقة وظائف الاتصال في النظام).

٦٨. يجب أن تكون العرقلة "بدون حق". تعتبر الأنشطة المشتركة المتأصلة في تصميم الشبكات، أو الممارسات التشغيلية أو التجارية المشتركة "بحق"، وتشمل، على سبيل المثال، مثل اختبار أو حماية أمن نظام الكمبيوتر المرخص به من قبل المالك أو المشغل، أو إعادة تشكيل نظام تشغيل الكمبيوتر الذي يتم عندما يقتني مشغل النظام برمجية جديدة (على سبيل المثال، البرمجيات التي تسمح بالولوج إلى الإنترنت والتي تعطل البرامج المماثلة المركبة سابقا). لذلك، لا تجرم هذه المادة هذا السلوك حتى وإن تسبب في عرقلة جسيمة.

٦٩. يمكن أن يؤدي إرسال بريد إلكتروني غير مرغوب فيه لأغراض تجارية أو لأغراض أخرى إلى إزعاج المتلقي، لا سيما عندما ترسل هذه الرسائل بكميات كبيرة أو بوتيرة عالية ("الرسائل غير المرغوب فيها"). وبحسب رأي القائمين على الصياغة، لا ينبغي تجريم هذا السلوك إلا إذا عرقل الاتصال عمدا وبشكل جسيم. ومع ذلك، قد تتوفر الأطراف على مقاربة مختلفة بشأن العرقلة بموجب قانونها، على سبيل المثال، من خلال اعتبار بعض الأفعال المرتبطة بالتدخل كجرائم إدارية أو إخضاعها لعقوبة أخرى. ويترك النص للأطراف إمكانية تحديد نطاق عرقلة تشغيل النظام – جزئيا أو كليا، بصورة مؤقتة أو دائمة – لبلوغ عتبة الضرر التي تبرر العقوبة الإدارية أو الجنائية بموجب قانونها.

٧٠. يجب أن ترتكب الجريمة عمدا، بمعنى أن تكون لدى مرتكب الجريمة نية العرقلة الجسيمة.

إساءة استخدام الأجهزة (المادة ٦)

٧١. ينص هذا الحكم على ارتكاب فعل خاص متعمد وغير قانوني، باعتباره جريمة جنائية منفصلة ومستقلة، فيما يتعلق بأجهزة معينة أو بيانات النفاذ التي يساء استخدامها لغرض ارتكاب الجرائم المذكورة أعلاه ضد سرية وسلامة وتوافر أنظمة أو بيانات الكمبيوتر. وبما أن ارتكاب هذه الجرائم غالبا ما يتطلب حيازة وسائل النفاذ ("أدوات القراصنة") أو غيرها من الأدوات، فهناك حافز قوي لاكتسابها لأغراض إجرامية قد تؤدي بالتالي إلى خلق نوع من السوق السوداء لإنتاجها وتوزيعها. ومن أجل مكافحة هذه الأخطار بمزيد من الفعالية، ينبغي أن يحظر القانون الجنائي أفعالا يحتمل أن تكون خطرة من الأصل، قبل ارتكاب الجرائم بموجب المواد من ٢ إلى ٥. وفي هذا الصدد، يستند الحكم إلى التطورات الأخيرة داخل مجلس أوروبا (الاتفاقية الأوروبية بشأن الحماية القانونية للخدمات القائمة أو المنطوية على النفاذ المشروط (سلسلة المعاهدات الأوروبية رقم ١٧٨) والاتحاد الأوروبي (التوجيه رقم 98/84/EC الصادر عن البرلمان الأوروبي والمجلس والمؤرخ في ٢٠ نوفمبر /تشرين الثاني ١٩٩٨ بشأن الحماية القانونية للخدمات القائمة أو المنطوية على النفاذ المشروط) والأحكام ذات الصلة في بعض البلدان. وقد تم تبني مقاربة مماثلة في اتفاقية جنيف لعام ١٩٢٩ بشأن تزييف النقد.

٧٢. تجرم الفقرة ١ (أ) ١ الإنتاج أو البيع أو الشراء للاستعمال أو الاستيراد أو التوزيع أو الإتاحة بوسيلة أخرى لأي برنامج حاسوبي مصمم أو معد خصيصا لغرض ارتكاب أي من الجرائم المقررة في المواد من ٢ إلى ٥ من هذه الاتفاقية. ويشير مصطلح "التوزيع" إلى الفعل النشط لنقل البيانات إلى الغير، بينما يحيل مصطلح "إتاحة" على توفير أجهزة عبر الإنترنت

ليستخدمها الغير. ويهدف هذا المصطلح أيضا إلى تغطية إنشاء أو تجميع وصلات تشعبية من أجل تيسير النفاذ إلى هذه الأجهزة. ويشير إدراج "برنامج حاسوبي" إلى البرامج المصممة على سبيل المثال من أجل تغيير أو حتى إتلاف البيانات أو التدخل في تشغيل الأنظمة، من قبيل برامج الفيروسات أو البرامج المصممة أو المكيفة للحصول على إمكانية النفاذ إلى أنظمة الكمبيوتر.

٧٣. ناقش القائمون على الصياغة بشكل مطول ضرورة حصر الأجهزة في تلك المصممة حصريا أو خصيصا لارتكاب الجرائم، وبالتالي استبعاد الأجهزة ذات الاستخدام المزدوج. واعتبر هذا الأمر ضيقا للغاية حيث يمكن أن يؤدي إلى صعوبات لا يمكن التغلب عليها للإثبات في الإجراءات الجنائية، مما يجعل الحكم غير قابل للتطبيق عمليا أو ينطبق فقط في حالات نادرة. كما تم رفض البديل المقترح بإدراج جميع الأجهزة حتى ولو كان إنتاجها وتوزيعها قانونيا. وبالتالي، فإن عنصر النية الشخصي في ارتكاب جريمة إلكترونية هو فقط الحاسم عند فرض العقوبة. وفي هذا المجال، لم تعتمد هذه المقاربة حتى فيما يتعلق بتزييف النقود. وكحل وسط معقول، قيدت الاتفاقية نطاقه في الحالات التي يتم فيها تصميم أو تكييف الأجهزة بشكل موضوعي أساسا لغرض ارتكاب جريمة. هذا وحده من شأنه أن يستبعد عادة الأجهزة ذات الاستخدام المزدوج.

٧٤. تجرم الفقرة ١ (أ) ٢ الإنتاج أو البيع أو الشراء للاستعمال أو الاستيراد أو التوزيع أو الإتاحة بوسيلة أخرى لكلمة مرور حاسوبية أو رمز النفاذ أو بيانات مماثلة يمكن من خلالها الولوج إلى نظام الكمبيوتر كليا أو جزئيا.

٧٥. تنشئ الفقرة ١ (ب) جريمة حيازة المواد المبينة في الفقرة ١ (أ) ١ أو ١ (أ) ٢. ويسمح للأطراف، بموجب الجملة الأخيرة من الفقرة ١ (ب)، أن تقتضي بموجب القانون امتلاك عدد من هذه المواد. ويساعد عدد العناصر المملوكة مباشرة في إثبات النية الجنائية. ويتعين على كل طرف أن يقرر عدد المواد المطلوبة قبل إلحاق المسؤولية الجنائية.

٧٦. تتطلب الجريمة ارتكابها عمدا وبدون حق. ومن أجل تجنب خطر التجريم المفرط عند إنتاج وتوفير الأجهزة في السوق لأغراض مشروعة، على سبيل المثال. في مواجهة الهجمات ضد أنظمة الكمبيوتر، تم إضافة عناصر أخرى لتقييد الجريمة. وبصرف النظر عن شرط النية العام، يجب أن تكون هناك نية محددة (أي مباشرة) تفيد بأن الجهاز يستخدم لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من ٢ إلى ٥ من الاتفاقية.

٧٧. تبين الفقرة ٢ بوضوح أن هذا الحكم لا يشمل تلك الأدوات التي أنشئت لأغراض الاختبار المرخص أو حماية نظام الكمبيوتر. وهذا المفهوم وارد بالفعل في عبارة "بدون حق". على سبيل المثال، تصمم وتنتج الشركات أجهزة الاختبار ("أجهزة كسر كلمات المرور") وأجهزة تحليل الشبكة من أجل رصد موثوقية منتوجاتها في مجال تكنولوجيا المعلومات أو اختبار أمن النظام لأغراض مشروعة، وبالتالي، تعتبر أدوات منتجة "بحق" .

٧٨. نظرا لمختلف عمليات التقييم لضرورة تطبيق جريمة "إساءة استعمال الأجهزة" على جميع أنواع جرائم الكمبيوتر المختلفة الواردة في المواد من ٢ إلى ٥، تسمح الفقرة ٣، على أساس التحفظ (انظر المادة ٤٢)، بتقييد الجريمة في القانون المحلي. إلا أن كل طرف ملزم بتجريم بيع أو توزيع أو إتاحة كلمة مرور حاسوبية أو النفاذ إلى البيانات على النحو المبين في الفقرة ١ (أ) ٢.

الباب ٢ – الجرائم المتصلة بالكمبيوتر

٧٩. تتعلق المواد من ٧ إلى ١٠ بالجرائم العادية التي كثيرا ما ترتكب من خلال استخدام نظام الكمبيوتر. وقد جرمت معظم الدول بالفعل هذه الجرائم العادية، وقد تكون قوانينها القائمة واسعة بما فيه الكفاية أو لا تكون بحيث تمتد لتشمل الحالات التي تنطوي على شبكات الكمبيوتر (على سبيل المثال، قد لا تشمل القوانين القائمة المتعلقة باستغلال الأطفال في المواد الإباحية لبعض الدول الصور الإلكترونية). لذلك، يتعين على الدول، أثناء تنفيذ هذه المواد، أن تراجع قوانينها القائمة لتحديد ما إذا كانت تنطبق على الحالات التي تنطوي على أنظمة أو شبكات الكمبيوتر. وإذا كانت الجرائم القائمة تغطي بالفعل هذا السلوك، فلا حاجة إلى تعديل الجرائم القائمة أو سن قوانين جديدة بشأنها.

٨٠. يتناول "التزوير المتصل بالكمبيوتر" و"الغش المتصل بالكمبيوتر" بعض الجرائم المتصلة بالكمبيوتر، أي التزوير والاحتيال المتصل بالكمبيوتر، باعتبارهما نوعين محددين من التلاعب بأنظمة أو بيانات الكمبيوتر. ويعتبر إدراجهما اعترافا أن بعض المصالح القانونية التقليدية لا تحظى في كثير من البلدان بالحماية الكافية من الأشكال الجديدة للتدخل والهجمات.

التزوير المتصل بالكمبيوتر (المادة ٧)

٨١. ترمي هذه المادة إلى إنشاء جريمة موازية لتزوير الوثائق الملموسة. وهكذا، فهي تهدف إلى سد الثغرات في القانون الجنائي المتعلقة بالتزوير التقليدي والتي تتطلب قراءة بصرية للبيانات أو التصريحات المجسدة في وثيقة والتي لا تنطبق على البيانات المخزنة إلكترونيا. وقد يكون للتلاعب بمثل هذه البيانات ذات القيمة الإثباتية نفس العواقب الخطيرة التي تترتب على أعمال التزوير التقليدية إذا تم تضليل طرف ثالث. وينطوي التزوير المتصل بالكمبيوتر على إنشاء أو تغيير بيانات مخزنة بشكل غير مرخص بحيث تكتسب قيمة إثباتية مختلفة في سياق المعاملات القانونية التي تعتمد على صحة المعلومات الواردة في البيانات، وبالتالي، تصبح موضوع الخدع. وتتمثل المصلحة القانونية المحمية في أمن وموثوقية البيانات الإلكترونية التي قد تكون لها عواقب على العلاقات القانونية.

٨٢. تجدر الإشارة إلى أن المفاهيم الوطنية للتزوير تختلف بشكل كبير. ويستند أحد المفاهيم إلى صحة الوثيقة، من حيث مؤلفها، بينما يتركز بعضها إلى صدق التصريح الوارد في الوثيقة. إلا أنه من المتفق عليه أن الخداع فيما يتعلق بصحة الوثيقة يشير على الأقل إلى الجهة التي تصدر البيانات، بصرف النظر عن صحة أو صدق محتويات البيانات. ويمكن للأطراف أن تذهب أبعد من ذلك وأن تدرج في مصطلح "أصلي" صحة البيانات.

٨٣. يغطي هذا الحكم البيانات التي تعادل وثيقة عامة أو خاصة، والتي تترتب عنها آثار قانونية. ويسفر "الإدخال" غير المرخص لبيانات صحيحة أو خاطئة عن حالة مطابقة لصناعة وثيقة مزورة. وبشكل عام، تعتبر التغييرات اللاحقة (التعديلات، والاختلافات، والتغييرات الجزئية)، والحذف (إزالة بعض البيانات من وسيلة لتخزين البيانات) والإتلاف (إعاقة، إخفاء البيانات) بمثابة تزوير وثيقة أصلية.

٨٤. تشير عبارة "لأغراض قانونية" إلى المعاملات والوثائق القانونية ذات الصلة قانونيا.

٨٥. تتيح الجملة الأخيرة من الحكم للأطراف، عند تنفيذ الجريمة في القانون المحلي، إمكانية إضافة شرط نية الاحتيال أو نية مشبوهة مماثلة، قبل إلحاق المسؤولية الجنائية.

الاحتيال المتصل بالكمبيوتر (المادة ٨)

٨٦. مع وصول الثورة التكنولوجية، تضاعفت فرص ارتكاب جرائم اقتصادية مثل الاحتيال، بما في ذلك الاحتيال على بطاقات الائتمان. وأصبحت الأصول الممثلة أو المسيرة على أنظمة الكمبيوتر (التحويلات الإلكترونية للأموال، إيداع الأموال) هدفا للتلاعب على غرار الأشكال التقليدية للملكية. وتتكون هذه الجرائم أساسا من التلاعب بالمدخلات، حيث يتم إدخال بيانات غير صحيحة في الكمبيوتر، أو عن طريق التلاعب بالبرنامج وتدخلات أخرى في مسار معالجة البيانات. وهكذا، ترمي هذه المادة إلى تجريم أي تلاعب غير مشروع أثناء معالجة البيانات بنية النقل غير المشروع للملكية.

٨٧. بغية ضمان تغطية جميع التلاعبات المحتملة ذات الصلة، تم استكمال العناصر المكونة ل "الإدخال"، "التغيير"، "الحذف" أو "الإتلاف" الواردة في المادة ٨(أ) بالفعل العام المتمثل في "التدخل في أداء برنامج أو نظام الكمبيوتر "في المادة ٨ (ب). وتكتسي عناصر "الإدخال، التغيير، الحذف أو الاتلاف" نفس المعنى الوارد في المواد السابقة. وتغطي المادة ٨ (ب) أفعالا من قبيل التلاعب بالأجهزة، والأفعال التي تنطوي على إتلاف المطبوعات والأفعال التي تؤثر على تسجيل البيانات أو تدفقها، أو التسلسل الذي يتم فيه تشغيل البرامج.

٨٨. تجرم عمليات التلاعب للاحتيال عبر الكمبيوتر عندما تتسبب في خسارة اقتصادية أو حيازية مباشرة لممتلكات شخص آخر وعندما يكون مرتكب الجريمة يتصرف بقصد الحصول على مكسب اقتصادي غير مشروع لحسابه أو لفائدة شخص آخر. وتشمل عبارة "خسارة الملكية"، باعتباره مفهوما واسعا، خسارة الأموال، والأصول الملموسة والأصول غير الملموسة ذات قيمة اقتصادية.

٨٩. يجب أن يرتكب الجرم "بدون حق" كما يجب الحصول على المنفعة الاقتصادية دون حق. وبطبيعة الحال، فإن الممارسات التجارية المشروعة المشتركة، التي ترمي إلى تحقيق منفعة اقتصادية، لا تندرج في الجريمة المقررة بموجب هذه المادة لأنها تتم بحق. وعلى سبيل المثال، فإن الأنشطة المنجزة في إطار عقد صحيح بين الأشخاص المعنيين هي عن حق (مثلا تعطيل موقع على شبكة الإنترنت على النحو الذي الواجب وفقا لشروط العقد).

٩٠. يجب أن ترتكب الجريمة "عمدا". يشير عنصر النية العام إلى التلاعب أو التدخل عبر الكمبيوتر الذي يتسبب في فقدان الملكية لحساب شخص آخر. وتقتضي الجريمة أيضا وجود نية غش معينة أو نية أخرى غير شريفة للحصول على منفعة اقتصادية أو غيرها من المنافع لحساب مرتكب الجريمة بنفسه أو لفائدة شخص آخر. وهكذا وعلى سبيل المثال، لا تندرج الممارسات التجارية المرتبطة بالمنافسة في السوق التي قد تسبب ضررا اقتصاديا لشخص ما أو تستفيد منها دون نية الاحتيال أو نية غير شريفة، في الجريمة المنصوص عليها في هذه المادة. وبالتالي، ليس القصد هو تجريم أفعال من قبيل استخدام برامج جمع المعلومات لمقارنة التسوق على الإنترنت ("البوتات")، حتى وإن لم يكن مرخصا به من قبل موقع تتم زيارته عن طريق "البوت".

الباب ٣ – الجرائم ذات الصلة بالمحتوى

الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية (المادة ٩)

٩١. تسعى المادة ٩ المتعلقة باستغلال الأطفال في المواد الإباحية إلى تعزيز التدابير الحمائية للأطفال، بما في ذلك حمايتهم من الاستغلال الجنسي، وذلك بتحديث أحكام القانون الجنائي بغية تقييد استخدام أنظمة الكمبيوتر في ارتكاب جرائم جنسية ضد الأطفال بشكل أكثر فعالية.

٩٢. يستجيب هذا الحكم لقلق رؤساء دول وحكومات مجلس أوروبا، المعرب عنه خلال مؤتمر القمة الثاني (ستراسبورغ، ١٠-١١ أكتوبر/تشرين الأول ١٩٩٧) في خطة عملهم (البند الثالث – ٤) ويتوافق مع التوجه الدولي الذي يسعى إلى حظر استغلال الأطفال في إنتاج المواد الإباحية، كما يتضح من اعتماد البروتوكول الاختياري لاتفاقية الأمم المتحدة بشأن حقوق الطفل مؤخرا، وبشأن بيع الأطفال واستغلالهم في البغاء وفي المواد الإباحية، ومن مبادرة المفوضية الأوروبية الأخيرة بشأن مكافحة الاستغلال الجنسي للأطفال (COM2000 / 854).

٩٣. يجرم هذا الحكم مختلف جوانب الإنتاج الإلكتروني والحيازة والتوزيع للمواد الإباحية التي تعرض صورا للأطفال. وتجرم معظم الدول بالفعل الإنتاج التقليدي والتوزيع المادي للمواد الإباحية المتعلقة بالأطفال، لكن مع الاستخدام المتزايد للإنترنت كأداة رئيسية لتداول هذه المواد، كان هناك شعور قوي بضرورة تبني أحكام محددة في آلية قانونية دولية من أجل مكافحة هذا الشكل الجديد من أشكال الاستغلال الجنسي للأطفال وتعريضهم للخطر. وثمة اعتقاد على نطاق واسع أن مثل هذه الممارسات المادية أو الإلكترونية، مثل تبادل الأفكار والنزوات الجنسية والمشورة بين أصحاب الميول الجنسي للأطفال، تؤدي دورا في دعم، تشجيع أو تيسير الجرائم الجنسية المرتكبة ضد الأطفال.

٩٤. تجرم الفقرة ١(أ) إنتاج المواد الإباحية المتعلقة بالأطفال لأغراض التوزيع عن طريق نظام الكمبيوتر. واعتبرت أن هذا الحكم ضروري لمكافحة الأخطار المذكورة أعلاه من مصدرها.

٩٥. تجرم الفقرة ١(ب) "عرض" المواد الإباحية المتعلقة بالأطفال عن طريق نظام الكمبيوتر. ويرمي "العرض" إلى تغطية التماس الآخرين للحصول على المواد الإباحية المتعلقة بالأطفال. وهذا يعني، ضمنيا، أن بإمكان الشخص الذي يعرض المادة أن يوفرها فعلا. ويتوخى من مصطلح "إتاحة" تغطية وضع المواد الإباحية المتعلقة بالأطفال على الإنترنت ليستخدمها

أشخاص آخرون، على سبيل المثال، عن طريق إنشاء مواقع إباحية عن الأطفال. وتهدف هذه الفقرة أيضا إلى تغطية إنشاء أو تجميع وصلات تشعبية لمواقع إباحية للأطفال بغية تيسير النفاذ إلى المواد الإباحية المتعلقة بالأطفال.

٩٦. تجرم الفقرة ١(ج) توزيع أو نقل المواد الإباحية المتعلقة بالأطفال عن طريق نظام الكمبيوتر. ويعرف "التوزيع" بأنه النشر النشط للمادة. وتتناول مسألة إرسال المواد الإباحية المتعلقة بالأطفال عن طريق نظام الكمبيوتر إلى شخص آخر في إطار جريمة "نقل" المواد الإباحية المتعلقة بالأطفال.

٩٧. يقصد بعبارة "الشراء لحساب الشخص نفسه أو لفائدة شخص آخر" الواردة في الفقرة ١(د)، السعي بنشاط إلى الحصول على المواد الإباحية المتعلقة بالأطفال، مثلا عن طريق تحميلها.

٩٨. تجرم الفقرة ١(ه) حيازة المواد الإباحية المتعلقة بالأطفال داخل نظام الكمبيوتر أو على دعامة لتخزين البيانات، مثل القرص المرن أو القرص المدمج. وتحفز حيازة المواد الإباحية المتعلقة بالأطفال الطلب على هذه المواد. ولعل من بين الوسائل الفعالة للحد من إنتاج المواد الإباحية المتعلقة بالأطفال إلحاء عواقب جنائية على سلوك كل مشارك في السلسلة من الإنتاج إلى الحيازة.

٩٩. يخضع مصطلح "المواد الإباحية" الوارد في الفقرة ٢ إلى المعايير الوطنية المتعلقة بتصنيف المواد على أنها فاحشة، لا تتفق مع الآداب العامة أو ما يماثلها من فساد. لذلك، يمكن اعتبار المواد التي لها ميزة فنية، طبية، علمية أو ما شابه ذلك غير إباحية. ويشمل التصور المرئي كافة البيانات المخزنة على قرص مرن أو على وسائل التخزين الإلكترونية الأخرى، والتي تكون قادرة على تحويلها إلى صورة مرئية.

١٠٠. تشمل عبارة "السلوك الجنسي الواضح" على الأقل أي ممارسة حقيقة أو بالمحاكاة: (أ) للاتصال الجنسي، بما في ذلك الأعضاء التناسلية، أو اتصال العضو التناسلي بالفم، أو اتصال العضو التناسلي بالشرج، أو اتصال الفم بالشرج، بين أشخاص قاصرين، أو بين شخص بالغ وشخص قاصر، من نفس الجنس أو من الجنس الآخر؛ ب) إيتان البهيمة؛ ج) الاستمناء؛ (د) الإساءة السادية أو المازوشية (التلذذ بالألم أو القسوة) في سياق جنسي؛ أو ه) عرض لأعضاء التناسلية أو منطقة العانة لدى شخص قاصر بشكل يثير الشهوة الجنسية. ولا يهم إذا كان السلوك المصور حقيقيا أو بالمحاكاة.

١٠١. تغطي الأنواع الثلاثة من المواد المحددة في الفقرة ٢ لأغراض ارتكاب الجرائم الواردة في الفقرة ١ صور الاعتداء الجنسي على طفل من دم ولحم (٢.أ)، والصور الإباحية التي يظهر في شخص يبدو أنه قاصر وهو يمارس سلوكا جنسي واضحا (٢.ب)، وفي الأخير الصور، التي، على الرغم من أنها تبدو "واقعية"، لا تنطوي في الواقع على طفل من دم ولحم وهو يمارس سلوكا جنسيا واضحا (٢.ج). ويشمل هذا السيناريو الأخير الصور التي أدخلت عليها تغييرات، مثل الصور المركبة من أشخاص طبيعيين أو حتى تلك التي يتم توليدها بالكامل بواسطة الكمبيوتر.

١٠٢. في الحالات الثلاث المشمولة بالفقرة ٢، تختلف المصالح القانونية المحمية اختلافا طفيفا. وتركز الفقرة ٢(أ) بصورة مباشرة على الحماية من سوء معاملة الأطفال. وتهدف الفقرتان ٢(ب) و٢(ج) إلى توفير الحماية من السلوك الذي، إن لم يكن يؤدي بالضرورة إلى إلحاق الضرر بـ "الطفل" المصور في المادة الإباحية، حيث قد لا يكون هناك طفل من لحم ودم، من شأنه أن يستخدم لتشجيع أو إغواء الأطفال على المشاركة في مثل هذه الأفعال، وبالتالي تشكل جزءا من ثقافة فرعية تحابي استغلال الأطفال.

١٠٣. لا يستثني مصطلح "بدون حق" الدفوع القانونية أو الأعذار أو المبادئ المشابهة ذات الصلة التي تخفف من مسؤولية شخص ما في ظروف محددة. وبالتالي، يسمح مصطلح "بدون حق" للدولة الطرف بأن تأخذ في الاعتبار الحقوق الأساسية، مثل حرية الفكر والتعبير والخصوصية. فضلا عن ذلك، يجوز للدولة الطرف أن تقدم دفاعا فيما يتعلق بالسلوك المتصل بـ "المواد الإباحية" التي لها مزايا فنية، طبية، علمية أو ما شابه ذلك. وفيما يتعلق بالفقرة ٢(ب)، يمكن أن تسمح الإشارة إلى مصطلح "بدون حق"، على سبيل المثال، للدولة الطرف أن تنص على إعفاء شخص من المسؤولية الجنائية إذا ثبت أن الشخص المصور ليس قاصرا بالمعنى الوارد في هذا الحكم.

١٠٤.تعرف الفقرة ٣ مصطلح "القاصر" في سياق المواد الإباحية عن الأطفال بصفة عامة، باعتباره أي شخص دون سن ١٨ عاما، وفقا لتعريف "الطفل" في اتفاقية الأمم المتحدة لحقوق الطفل (المادة ١). وقد اعتبر وضع معيار دولي موحد بشأن السن مسألة سياسية بالغة الأهمية. وتجدر الإشارة إلى أن السن يشير إلى تشييء أطفال (حقيقيين أو وهميين) جنسيا، وهذا السن غير مرتبط بسن الموافقة على العلاقات الجنسية.
ومع ذلك، وإدراكا بأن بعض الدول تقتضي حدا أقل للسن في التشريعات الوطنية المتعلقة باستغلال الأطفال في المواد الإباحية، فإن العبارة الأخيرة من الفقرة ٣ تسمح للأطراف بأن تقضي بحدود عمرية مختلفة، شريطة ألا تقل عن ١٦ سنة.

١٠٥.تسرد هذه المادة أنواعا مختلفة من الأفعال غير المشروعة المتعلقة باستغلال الأطفال في المواد الإباحية التي تلزم الأطراف، كما هو الحال في المواد من ٢ إلى ٨، بتجريمها عندما ترتكب "عمدا". وبموجب هذا المعيار، لا يكون الشخص مسؤولا ما لم تكن لديه نية عرض المواد الإباحية المتعلقة بالأطفال، إتاحتها، توزيعها، نقلها، إنتاجها أو حيازتها. ويجوز للأطراف أن تعتمد معيارا أكثر تحديدا (انظر، على سبيل المثال، قانون الجماعة الأوروبية المطبق فيما يتعلق بمسؤولية مقدم الخدمة)، وفي هذه الحال، يحكم هذا المعيار. يمكن، مثلا، فرض المسؤولية إذا كانت هناك "معرفة ومراقبة" على المعلومات التي يتم إرسالها أو تخزينها. وليس كافيا، على سبيل المثال، أن يكون مقدم الخدمة بمثابة قناة، أو أن يستضيف موقعا على شبكة الإنترنت أو غرفة إخبارية تحتوي على هذه المواد، دون وجود النية المطلوبة بموجب القانون المحلي في هذه الحالة الخاصة. علاوة على ذلك، لا يكون مقدم الخدمة مطالبا برصد السلوك لتجنب المسؤولية الجنائية.

١٠٦.تسمح الفقرة ٤ للأطراف بإبداء تحفظات بشأن الفقرة ١(د) و(ه) والفقرة ٢(ب) و(ج). ويمكن أن يكون الحق في عدم تطبيق هذه الأجزاء من الحكم جزئيا أو كليا. وينبغي الإعلان عن أي تحفظ من هذا القبيل لدى الأمين العام لمجلس أوروبا وقت التوقيع أو عند إيداع صكوك الدولة الطرف للتصديق أو القبول أو الموافقة أو الانضمام، وفقا للمادة ٤٢.

الباب ٤ – الجرائم المتعلقة بانتهاكات حق التأليف والنشر والحقوق المجاورة

الجرائم المتعلقة بانتهاكات حق التأليف والنشر والحقوق المجاورة (المادة ١٠)

١٠٧.تعتبر انتهاكات حقوق الملكية الفكرية، ولا سيما حق التأليف والنشر، من بين أكثر الجرائم التي ترتكب عادة على شبكة الإنترنت، مما يثير قلق أصحاب حقوق التأليف والنشر وأولئك الذين يعملون مهنيا على شبكات الكمبيوتر. ويعتبر استنساخ المصنفات المحمية ونشرها على شبكة الإنترنت، دون موافقة صاحب حق التأليف والنشر، أمرا واردا ومتكررا للغاية. وتشمل هذه المصنفات المحمية الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية وغيرها من المصنفات. ولعل سهولة النسخ غير المرخص بسبب التكنولوجيا الرقمية وكذلك حجم الاستنساخ والنشر في سياق الشبكات الإلكترونية هما ما حثا على إدراج أحكام بشأن العقوبات في القانون الجنائي وتعزيز التعاون الدولي في هذا المجال.

١٠٨.كل دولة طرف ملزمة بتجريم الانتهاكات المتعمدة على حق التأليف والنشر والحقوق ذات الصلة، التي يشار إليها أحيانا بالحقوق المجاورة، الناشئة عن الاتفاقات المدرجة في المادة، عندما ترتكب هذه الانتهاكات عن طريق نظام الكمبيوتر وعلى نطاق تجاري. وتنص الفقرة ١ على عقوبات جنائية ضد انتهاكات حق التأليف والنشر عن طريق نظام الكمبيوتر. ويعتبر انتهاك حق التأليف والنشر بالفعل جريمة في جميع الدول تقريبا. وتتناول الفقرة ٢ انتهاك الحقوق ذات الصلة عن طريق نظام الكمبيوتر.

١٠٩.يعرف انتهاك كل من حق التأليف والنشر والحقوق ذات الصلة على النحو المحدد في قانون كل طرف ووفقا للالتزامات التي تعهد بها الطرف بموجب صكوك دولية معينة. ولما كان كل طرف مطالبا بتجريم هذه الانتهاكات، فإن الطريقة الدقيقة التي تحدد بها هذه الانتهاكات بموجب القانون المحلي قد تختلف من دولة إلى أخرى. ومع ذلك، فإن التزامات التجريم بموجب الاتفاقية لا تشمل انتهاكات الملكية الفكرية غير تلك التي تتناولها المادة ١٠ بصريح العبارة، وبالتالي تستبعد الانتهاكات المتعلقة ببراءات الاختراع أو العلامات التجارية.

١١٠.بخصوص الفقرة ١، فإن الاتفاقات المشار إليها هي قانون باريس المؤرخ ٢٤ يوليو/تموز ١٩٧١، واتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (TRIPS)، ومعاهدة حقوق

المؤلف للمنظمة العالمية للملكية الفكرية (الويبو). وفيما يتعلق بالفقرة ٢، تتلخص الصكوك الدولية المذكورة في الاتفاقية الدولية لحماية فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة (اتفاقية روما)، والاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة المنظمة العالمية للملكية الفكرية (الويبو) بشأن الأداء والتسجيل الصوتي. ويوضح استخدام عبارة "عملا بالالتزامات التي تعهدت بها" في الفقرتين أن الطرف المتعاقد في هذه الاتفاقية ليس ملزما بتطبيق الاتفاقات المذكورة التي لا يكون طرفا فيها؛ فضلا عن ذلك، إذا كان الطرف قد أبدى تحفظا أو قدم إعلانا مسموحا به بموجب أحد الاتفاقات، فإن هذا التحفظ قد يحد من نطاق التزامه بموجب هذه الاتفاقية.

١١١.لم تكن معاهدة الويبو بشأن حقوق المؤلف ومعاهدة الويبو بشأن الأداء والتسجيل الصوتي قد دخلت حيز التنفيذ وقت إبرام هذه الاتفاقية. ومع ذلك، فإن هاتين المعاهدتين مهمتان لأنهما تستكملان بشكل كبير الحماية الدولية للملكية الفكرية (وخاصة فيما يتعلق بالحق الجديد في "توفير" المواد المحمية "عند الطلب" عبر الإنترنت) وتساهمان في تحسين وسائل مكافحة انتهاكات حقوق الملكية الفكرية في جميع أنحاء العالم. غير أنه من المفهوم أن انتهاكات الحقوق التي تنص عليها هاتان المعاهدتان لا ينبغي تجريمها بموجب هذه الاتفاقية إلى أن تدخل هاتان المعاهدتان حيز النفاذ بالنسبة لأي دولة طرف.

١١٢.إن الالتزام بتجريم انتهاكات حق التأليف والنشر والحقوق ذات الصلة وفقا للالتزامات المتعهد بها في الصكوك الدولية لا يشمل أي حقوق معنوية تمنحها الصكوك المذكورة (من قبيل ما ورد في المادة ٦ مكرر من اتفاقية برن وفي المادة ٥ من معاهدة الويبو بشأن حقوق المؤلف).

١١٣.يجب أن ترتكب الجرائم ضد حق التأليف والنشر والحقوق ذات الصلة "عمدا" من أجل تطبيق المسؤولية الجنائية. وعلى نقيض كافة أحكام القانون الموضوعي الأخرى من هذه الاتفاقية، يستخدم مصطلح "عمدا" بدلا من "قصدا" في الفقرتين ١ و٢، لأن هذا هو المصطلح المستخدم في الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (اتفاق تريبس) (المادة ٦١)، الذي يحكم الالتزام بتجريم انتهاكات حقوق التأليف والنشر.

١١٤.تهدف الأحكام إلى التنصيص على عقوبات جنائية ضد الانتهاكات "على نطاق تجاري" وعن طريق نظام الكمبيوتر. وهذا يتماشى مع المادة ٦١ من المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (TRIPS)، التي تطالب بعقوبات جنائية في مسائل حقوق المؤلف فقط في حالة "القرصنة على نطاق تجاري". ومع ذلك، قد ترغب الأطراف في تجاوز عتبة "النطاق التجاري" وتجريم أنواع أخرى من انتهاكات حق التأليف والنشر أيضا.

١١٥.حذفت عبارة "بدون حق" من نص هذه المادة باعتبارها تكرارا، بما أن مصطلح "الانتهاك" يشير بالفعل إلى استخدام المادة المحمية بموجب حقوق التأليف والنشر دون ترخيص. ولا يستبعد غياب مصطلح "بدون حق" تطبيق الدفوع القانونية والمبررات والمبادئ التي تحكم استبعاد المسؤولية الجنائية المرتبطة بمصطلح "بدون حق" في مكان آخر من الاتفاقية.

١١٦.تسمح الفقرة ٣ للأطراف بعدم فرض المسؤولية الجنائية بموجب الفقرتين ١ و٢ في "ظروف محدودة" (مثل الواردات الموازية وحقوق الاستئجار)، ما دامت وسائل الانتصاف الفعالة الأخرى، بما في ذلك التدابير المدنية و/أو الإدارية، متاحة. ويتيح هذا الحكم أساسا للأطراف إعفاء محدودا من الالتزام بفرض المسؤولية الجنائية، شريطة ألا تتخلى عن الالتزامات المنصوص عليها في المادة ٦١ من الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (اتفاق تريبس) الذي يشكل الحد الأدنى المطلوب من شروط التجريم القائمة.

١١٧.لا تفسر هذه المادة بأي حال من الأحوال على أنها توسع نطاق الحماية الممنوحة للمؤلفين، منتجي الأفلام، فناني الأداء، منتجي التسجيلات الصوتية، هيئات الإذاعة أو غيرهم من أصحاب الحقوق ليشمل الأشخاص الذين لا يستوفون معايير الأهلية بموجب القانون المحلي أو الاتفاق الدولي.

الباب ٥ – المسؤولية الإضافية والعقوبات

المحاولة والمساعدة أو التحريض (المادة ١١)

١١٨. تهدف هذه المادة إلى إنشاء جرائم إضافية تتعلق بمحاولة ارتكاب الجرائم المحددة في الاتفاقية والمساعدة في ارتكابها أو التحريض على ارتكابها، وكما هو مبين أدناه، لا يشترط على الطرف أن يجرم محاولة ارتكاب كل جريمة منصوص عليها في الاتفاقية.

١١٩. تقتضي الفقرة ١ من الأطراف تجريم المساعدة أو التحريض على ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من ٢ إلى ١٠. وتنشأ المسؤولية عن المساعدة أو التحريض حيثما يكون الشخص الذي يرتكب جريمة منصوصا عليها في الاتفاقية يحظى بمساعدة شخص آخر لديه أيضا نية أن ترتكب الجريمة. على سبيل المثال، على الرغم من أن نقل بيانات المحتوى المضرة أو الرموز الخبيثة من خلال الإنترنت يتطلب مساعدة مقدمي الخدمات كقناة، فإن مزود الخدمة الذي لا تكون لديه النية الجنائية لا يمكن أن يتحمل المسؤولية بموجب هذا القسم. وبالتالي، ليس من واجب مقدم الخدمة رصد المحتوى بفعالية لتجنب المسؤولية الجنائية بموجب هذا الحكم.

١٢٠. فيما يخص الفقرة ٢ المتعلقة بالمحاولة، اعتبرت بعض الجرائم المحددة في الاتفاقية أو بعض عناصر هذه الجرائم، صعبة من الناحية النظرية (مثلا، عناصر عرض أو إتاحة المواد الإباحية المتعلقة بالأطفال). فضلا عن ذلك، فإن بعض الأنظمة القانونية تحد من الجرائم التي يعاقب فيها على المحاولة. وبناء على ذلك، يقتضي الأمر تجريم المحاولة فيما يتعلق بالجرائم المقررة وفقا للمواد ٣، ٤، ٥، ٧، ٨ و ٩ (١) (أ) و ٩ (١) (ج).

١٢١. كما هو الحال بالنسبة لجميع الجرائم المقررة وفقا للاتفاقية، يجب أن ترتكب المحاولة، المساعدة أو التحريض "عمدا".

١٢٢. أضيفت الفقرة ٣ لمعالجة الصعوبات التي قد تواجهها الأطراف من حيث الفقرة ٢، بالنظر إلى المفاهيم المتباينة على نطاق واسع في مختلف التشريعات، على الرغم من الجهود المبذولة في الفقرة ٢ لاستثناء بعض الجوانب من الحكم المتعلق بالمحاولة. ويجوز لأي طرف أن يعلن تحفظه بالحق في عدم تطبيق الفقرة ٢ جزئيا أو كليا. وهذا يعني أن كل طرف يبدي تحفظا على ذلك الحكم لن يكون ملزما بتجريم المحاولة على الإطلاق، أو يجوز له أن يختار الجرائم أو أجزاء من الجرائم التي تلحقها عقوبات جنائية فيما يتعلق بالمحاولة. ويهدف التحفظ إلى تمكين التصديق على الاتفاقية على أوسع نطاق ممكن مع السماح للأطراف بالحفاظ على بعض مفاهيمها القانونية الأساسية.

مسؤولية الشركات (المادة ١٢)

١٢٣. تتناول المادة ١٢ مسؤولية الأشخاص الاعتباريين، وهذا ما يتفق مع التوجه القانوني الحالي للاعتراف بمسؤولية الشركات. ويتلخص الغرض من ذلك في فرض المسؤولية على الشركات والجمعيات والأشخاص الاعتباريين المماثلين عن الأفعال الإجرامية التي يقوم بها شخص في منصب قيادي داخل المؤسسة، عندما يتم ارتكابها لصالح ذلك الشخص الاعتباري. وتنص المادة ١٢ أيضا على المسؤولية في حال عدم قيام ذلك الشخص بالإشراف على موظف أو وكيل أو مراقبته، حيث يؤدي هذا الإخفاق إلى ارتكاب ذلك الموظف أو الوكيل لأحد الجرائم المنصوص عليها في الاتفاقية.

١٢٤. بموجب الفقرة ١، يلزم استيفاء أربعة شروط من أجل إلحاق المسؤولية. أولا، يجب أن ترتكب إحدى الجرائم الموصوفة في الاتفاقية. ثانيا، يجب أن تكون الجريمة قد ارتكبت لفائدة الشخص الاعتباري. ثالثا، يجب أن ترتكب الجريمة من قبل شخص يشغل منصبا قياديا (بما في ذلك المساعدة والتحريض). تشير عبارة "الشخص الذي يشغل منصبا قياديا" إلى الشخص الطبيعي الذي لديه منصب رفيع في المؤسسة، من قبيل المدير. رابعا، يجب أن يكون الشخص الذي يشغل منصبا قياديا قد تصرف على أساس إحدى هذه الصلاحيات – سلطة تمثيلية أو سلطة تقريرية أو رقابية – مما يدل على أن هذا الشخص الطبيعي تصرف في نطاق سلطته من أجل تحميل الشخص الاعتباري المسؤولية. وباختصار، تلزم الفقرة ١ الأطراف بأن تكون قادرة على فرض المسؤولية على الشخص الاعتباري فقط على الجرائم التي يرتكبها هؤلاء القادة.

١٢٥. بالإضافة إلى ذلك، تلزم الفقرة ٢ الأطراف بأن تكون لديها القدرة على فرض المسؤولية على شخص اعتباري عندما لا ترتكب الجريمة من قبل الشخص القائد الوارد وصفه في الفقرة ١، بل من لدن شخص آخر يتصرف تحت سلطة الشخص الاعتباري القانونية، أي أحد موظفيها أو وكلائها العاملين ضمن نطاق سلطتهم. ويجب استيفاء الشروط التالية قبل إلحاق

المسؤولية (١) ارتكاب جريمة من قبل موظف أو وكيل الشخص الاعتباري، (٢) ارتكاب الجريمة لفائدة الشخص الاعتباري؛ و(٣) تسنى ارتكاب الجريمة بسبب فشل الشخص القائد في الإشراف على الموظف أو الوكيل. وفي هذا السياق، ينبغي تفسير عدم الاشراف على أنه يشمل عدم اتخاذ التدابير المناسبة والمعقولة لمنع الموظفين أو الوكلاء من ارتكاب أنشطة إجرامية نيابة عن الشخص الاعتباري. ويمكن تحديد هذه التدابير المناسبة والمعقولة من خلال عوامل مختلفة، من قبيل نوع النشاط التجاري وحجمه، والمعايير أو أفضل الممارسات التجارية المعمول بها، وما إلى ذلك. ولا ينبغي تفسير ذلك على أنه يتطلب نظاما عاما لمراقبة اتصالات الموظفين (انظر الفقرة ٥٤ أيضا). ولا يتحمل مقدم الخدمة المسؤولية بسبب كون الجريمة قد ارتكبت على نظامه من قبل العميل/الزبون أو المستخدم أو أي شخص ثالث آخر، لأن مصطلح "يتصرف تحت سلطته" ينطبق حصريا على الموظفين والوكلاء الذين يعملون ضمن نطاق سلطتهم.

١٢٦. بموجب هذه المادة، يمكن أن تكون المسؤولية جنائية، مدنية أو إدارية. يتمتع كل طرف بالمرونة في اختيار التنصيص على أي من أشكال هذه المسؤولية أو كلها، وفقا للمبادئ القانونية لكل طرف، طالما أنه يستوفي معايير الفقرة ٢ من المادة ١٣، بأن تكون العقوبة أو التدبير " فعالة، متناسبة ورادعة "وأن تشمل العقوبات المالية.

١٢٧. توضح الفقرة ٤ أن مسؤولية الشركات لا تستبعد المسؤولية الفردية.

العقوبات والتدابير (المادة ١٣)

١٢٨. ترتبط هذه المادة ارتباطا وثيقا بالمواد من ٢ إلى ١١ التي تحدد مختلف الجرائم الإلكترونية أو الجرائم المتصلة بالكمبيوتر التي ينبغي أن يعاقب عليها القانون الجنائي. ووفقا للالتزامات التي تفرضها تلك المواد، يلزم هذا الحكم الأطراف المتعاقدة باستخلاص العواقب من الطبيعة الخطيرة لهذه الجرائم من خلال التنصيص على عقوبات جنائية "فعالة ومتناسبة ورادعة"، تشمل، فيما يتعلق بالأشخاص الطبيعيين، إمكانية فرض عقوبات بالسجن.

١٢٩. يخضع الأشخاص الاعتباريون الذين تنشأ مسؤوليتهم وفقا للمادة ١٢ أيضا لعقوبات "فعالة ومتناسبة ورادعة" يمكن أن تكون جنائية، إدارية أو مدنية بطبيعتها. ويتعين على الأطراف المتعاقدة، بموجب الفقرة ٢، أن تنص على إمكانية فرض عقوبات مالية على الأشخاص الاعتباريين.

١٣٠. تترك المادة الباب مفتوحا أمام إمكانية فرض عقوبات أو تدابير أخرى تجسد خطورة الجرائم. وعلى سبيل المثال، يمكن أن تشمل التدابير إصدار أمر قضائي أو المصادرة. ويترك للأطراف السلطة التقديرية لإنشاء نظام للجرائم والعقوبات الجنائية يتوافق مع أنظمتها القانونية الوطنية القائمة.

القسم الثاني – القانون الإجرائي

١٣١. تصف المواد الواردة في هذا القسم بعض التدابير الإجرائية الواجب اتخاذها على الصعيد الوطني لأغراض التحقيق الجنائي في الجرائم المنصوص عليها في القسم ١، والجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر، وجمع الأدلة على جريمة جنائية في شكل إلكتروني. ووفقا للفقرة ٣ من المادة ٣٩، لا يوجد في الاتفاقية ما يطالب أو يدعو طرفا إلى إنشاء سلطات أو إجراءات غير تلك الواردة في هذه الاتفاقية، ولا ما يمنع طرفا من القيام بذلك.

١٣٢. أدت الثورة التكنولوجية، التي تشمل "الطريق الإلكتروني السريع" حيث تترابط وتتفاعل أشكال عديدة من الاتصالات والخدمات من خلال تقاسم وسائط ودعامات النقل المشتركة، إلى تغيير مجال القانون الجنائي والإجراءات الجنائية. وتفتح شبكة الاتصالات التي ما فتئت تتوسع، أبوابا جديدة للأنشطة الإجرامية في مجال الجرائم التقليدية والجرائم التكنولوجية الجديدة على حد سواء. ولا يجب أن يواكب هذه التجاوزات الجديدة القانون الجنائي الموضوعي فحسب بل أيضا قانون الإجراءات الجنائية وتقنيات التحقيق. وبالمثل، ينبغي أيضا ملاءمة الضمانات أو تطويرها لمواكبة البيئة التكنولوجية الجديدة والصلاحيات الإجرائية الجديدة.

١٣٣. يتمثل أحد التحديات الرئيسية لمكافحة الجريمة في البيئة الشبكية في صعوبة تحديد هوية مرتكب الجريمة وتقييم مدى تأثير الفعل الإجرامي وأثره. وثمة مشكلة أخرى ناجمة عن تقلب البيانات الإلكترونية، التي يمكن تغييرها، نقلها أو حذفها في

ثوان. على سبيل المثال، يمكن للمستخدم الذي يتحكم في البيانات استخدام نظام الكمبيوتر لمحو البيانات الخاضعة لتحقيق جنائي، وبالتالي إتلاف الأدلة. وغالبا ما تكون السرعة، وأحيانا السرية، أمرا حاسما في نجاح التحقيق.

١٣٤.تعمل الاتفاقية على ملاءمة التدابير الإجرائية التقليدية، من قبيل البحث والضبط، مع البيئة التكنولوجية الجديدة. وبالإضافة إلى ذلك، تم وضع تدابير جديدة، مثل التعجيل بحفظ البيانات، من أجل الحفاظ على فعالية التدابير التقليدية لجمعها، كالبحث والضبط، في البيئة التكنولوجية المتقلبة. وبما أن البيانات في البيئة التكنولوجية الجديدة ليست دائما ثابتة، بل قد تتدفق في خضم عملية الاتصال، تم أيضا تكييف إجراءات جمع تقليدية أخرى لجمع البيانات ذات الصلة بالاتصالات السلكية واللاسلكية، مثل جمع بيانات الحركة في الوقت الحقيقي واعتراض بيانات المحتوى، من أجل السماح بتجميع البيانات الإلكترونية التي تنطوي عليها عملية الاتصال. وترد بعض هذه التدابير في توصية مجلس أوروبا رقم 13 (95) بشأن مشاكل قانون الإجراءات الجنائية المتصلة بتكنولوجيا المعلومات.

١٣٥.تهدف جميع الأحكام المشار إليها في هذا القسم إلى تمكين الحصول على البيانات أو جمعها لأغراض التحقيقات أو الإجراءات الجنائية الخاصة. وناقش القائمون على صياغة هذه الاتفاقية ضرورة أن تفرض الاتفاقية التزاما على مقدمي الخدمات بجمع بيانات الحركة والاحتفاظ بها بصورة روتينية لفترة محددة من الزمن، لكنهم لم يدرجوا أي التزام من هذا القبيل بسبب عدم التوصل إلى توافق في الآراء.

١٣٦.تشير الإجراءات بوجه عام إلى جميع أنواع البيانات، بما في ذلك ثلاثة أنواع محددة من بيانات الكمبيوتر (بيانات الحركة، وبيانات المحتوى، وبيانات المنخرطين)، التي قد تتخذ شكلين (مخزنة أو في خضم عملية الاتصال). وترد تعريفات لبعض هذه المصطلحات في المادتين ١ و١٨. وتتوقف إمكانية تطبيق أي إجراء على نوع معين أو شكل من أشكال البيانات الإلكترونية على طبيعة وشكل البيانات وطبيعة الإجراء، على النحو المبين تحديدا في كل مادة.

١٣٧.عند مواءمة القوانين الإجرائية التقليدية مع البيئة التكنولوجية الجديدة، تنشأ مسألة المصطلحات المناسبة في أحكام هذا الباب. وشملت الخيارات الإبقاء على اللغة التقليدية ("البحث" و"المصادرة")، أو استخدام مصطلحات حاسوبية جديدة وأكثر توجها من الناحية التكنولوجية ("النفاذ" و"الاستنساخ")، بصيغتها المعتمدة في نصوص المنتديات الدولية الأخرى بشأن هذا الموضوع (مثل الفريق الفرعي المعني بجرائم التكنولوجيا العالية التابع لمجموعة الثماني"G8")، أو استخدم حل وسط يتمثل في لغة مختلطة ("البحث أو النفاذ بطريقة مماثلة"، و "المصادرة أو التأمين بطريقة مماثلة"). ولما كانت هناك حاجة إلى تجسيد تطور المفاهيم في البيئة الإلكترونية، فضلا عن تحديد جذورها التقليدية والحفاظ عليها، تم تبني مقاربة مرنة تتيح للدول استخدام المفاهيم القديمة "للبحث والمصادرة" أو المفاهيم الجديدة " النفاذ والاستنساخ ".

١٣٨.تشير جميع المواد الواردة في القسم إلى "السلطات المختصة" والصلاحيات التي ينبغي منحها لأغراض التحقيقات أو الإجراءات الجنائية الخاصة. وفي بعض البلدان، لا يكون للقضاة سوى سلطة إصدار الأوامر أو الترخيص بجمع الأدلة أو تقديمها، بينما يعهد إلى المدعين العامين أو غيرهم من الموظفين المكلفين بإنفاذ القوانين في بلدان أخرى بنفس الصلاحيات أو بسلطات مماثلة. لذلك، تشير عبارة "السلطة المختصة" إلى سلطة قضائية أو إدارية أو غيرها من سلطات إنفاذ القانون التي يخول لها القانون المحلي أن تأمر باتخاذ تدابير إجرائية لأغراض جمع أو تقديم الأدلة فيما يتعلق بالتحقيقات الجنائية الخاصة أو الترخيص بها أو تنفيذها.

الباب ١ – أحكام عامة

١٣٩.يبدأ هذا القسم بحكمين عامين ينطبقان على جميع المواد المتعلقة بالقانون الإجرائي.

نطاق الأحكام الإجرائية (المادة ١٤)

١٤٠.تلتزم كل دولة طرف باعتماد ما يلزم من تدابير تشريعية وغيرها من التدابير، وفقا لقانونها الداخلي وإطارها القانوني، لإقرار السلطات والإجراءات المنصوص عليها في هذا القسم لأغراض "التحقيقات أو الإجراءات الجنائية الخاصة".

١٤١.مع مراعاة استثناءين، تطبق كل دولة طرف السلطات والإجراءات المنصوص عليها في هذا القسم على ما يلي: (١) الجرائم الجنائية المقررة وفقا للقسم ١ من الاتفاقية؛ (٢) الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر؛ و(٣) جمع الأدلة الخاصة بجريمة جنائية في شكل إلكتروني.
وبالتالي، تطبق السلطات والإجراءات المشار إليها في هذا القسم، لأغراض التحقيقات أو الإجراءات الجنائية الخاصة، على الجرائم المقررة وفقا للاتفاقية، وعلى الجرائم الأخرى المرتكبة بواسطة نظام الكمبيوتر، وعلى جمع أدلة الجريمة الجنائية في شكل إلكتروني. وهذا يضمن الحصول على الأدلة في شكل إلكتروني على أي جريمة جنائية أو جمعها عن طريق الصلاحيات والإجراءات المنصوص عليها في هذا القسم، كما يوفر قدرة مكافئة أو موازية للحصول على بيانات الكمبيوتر أو جمعها طبقا لما يتم في إطار الصلاحيات التقليدية والإجراءات المتعلقة بالبيانات غير الإلكترونية. وتنص الاتفاقية صراحة على أنه ينبغي للأطراف أن تدرج في قوانينها إمكانية استخدام المعلومات المضمنة في شكل رقمي أو أي شكل إلكتروني آخر كدليل أمام محكمة في الدعاوى الجنائية، بصرف النظر عن طبيعة الجريمة التي تتم مقاضاتها.

١٤٢.ثمة استثناءان لنطاق التطبيق هذا. أولا، تنص المادة ٢١ على أن صلاحية اعتراض بيانات المحتوى تقتصر على مجموعة من الجرائم الخطيرة التي يحددها القانون المحلي. وتقيد العديد من الدول سلطة اعتراض الاتصالات الشفوية أو الاتصالات السلكية واللاسلكية على مجموعة من الجرائم الخطيرة، اعترافا منها بخصوصية الاتصالات الشفوية والاتصالات السلكية واللاسلكية وبالطابع التطفلي لهذا التدبير التحقيقي. وبالمثل، لا تطالب هذه الاتفاقية الأطراف إلا بإنشاء صلاحيات وإجراءات الاعتراض فيما يتعلق ببيانات المحتوى ذات الصلة باتصالات محددة عبر الكمبيوتر والمرتبطة بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي.

١٤٣.وثانيا، يجوز لأي طرف أن يحتفظ بالحق في تطبيق التدابير الواردة في المادة ٢٠ (جمع بيانات الحركة في الوقت الحقيقي) على الجرائم أو فئات الجرائم المحددة في التحفظ، شريطة ألا يكون نطاق هذه الجرائم أو فئاتها أكثر تقييدا من نطاق الجرائم التي تطبق عليها تدابير الاعتراض المشار إليها في المادة ٢١. وتعتبر بعض الدول جمع بيانات الحركة بمثابة جمع بيانات المحتوى من حيث الخصوصية والطابع التطفلي. ولعل حق التحفظ من شأنه أن يسمح لهذه الدول بتقييد تطبيق تدابير جمع بيانات الحركة في الوقت الحقيقي على نفس مجموعة الجرائم التي تطبق عليها سلطات وإجراءات اعتراض بيانات المحتوى في الوقت الحقيقي. ومع ذلك، لا تعتبر العديد من الدول اعتراض بيانات المضمون وجمع بيانات الحركة على أنهما متكافئان من حيث مصالح الخصوصية ودرجة التدخل، لأن جمع بيانات الحركة وحده لا يجمع محتوى الاتصال أو يكشف عنه. وبما أن جمع بيانات الحركة في الوقت الفعلي قد يكتسي أهمية بالغة في تعقب مصدر الاتصالات عبر الكمبيوتر أو وجهتها (ومن تم المساعدة في التعرف على المجرمين)، تدعو الاتفاقية الدول الأطراف التي تمارس حق التحفظ إلى الحد من تحفظها لتمكين تطبيق السلطات والإجراءات المنصوص عليها لجمع بيانات الحركة في الوقت الحقيقي على أوسع نطاق ممكن.

١٤٤.تنص الفقرة (ب) على تحفظ بالنسبة للبلدان التي لا تستطيع، بسبب القيود القائمة في قوانينها الداخلية وقت اعتماد الاتفاقية، أن تعترض الاتصالات على أنظمة الكمبيوتر التي تعمل لصالح مجموعة مغلقة من المستخدمين ولا تستخدم شبكات الاتصالات العامة ولا ترتبط بأنظمة كمبيوتر أخرى. تشير عبارة "مجموعة مغلقة من المستخدمين"، على سبيل المثال، إلى مجموعة من المستخدمين محدودة بحكم ارتباطها بمزود الخدمة، من قبيل الموظفين لدى شركة توفر لهم إمكانية التواصل فيما بينها باستخدام شبكة كمبيوتر. وتعني عبارة "غير متصلة بأنظمة كمبيوتر أخرى" أنه في الوقت الذي يصدر فيه أمر بموجب المادتين ٢٠ أو ٢١، لا يكون للنظام الذي تتم فيه الاتصالات أي اتصال مادي أو منطقي بشبكة كمبيوتر أخرى. وتستثني عبارة "لا تستخدم شبكات الاتصالات العامة" الأنظمة التي تستخدم شبكات الكمبيوتر العامة (بما في ذلك الإنترنت)، وشبكات الهواتف العمومية أو غيرها من مرافق الاتصالات العامة، من أجل نقل الاتصالات، سواء كان هذا الاستخدام واضحا بالنسبة للمستخدمين أم لا.

الشروط والضمانات (المادة ١٥)

١٤٥.يخضع وضع وتنفيذ وتطبيق الصلاحيات والإجراءات المنصوص عليها في هذا القسم من الاتفاقية للشروط والضمانات المنصوص عليها في القانون الداخلي لكل طرف. وعلى الرغم من أن الأطراف ملزمة بإدخال بعض أحكام القانون الإجرائي في قوانينها الداخلية، فإن طرق إنشاء وتنفيذ هذه الصلاحيات والإجراءات في نظامها القانوني، وتطبيق الصلاحيات والإجراءات في حالات محددة، متروكة للقانون الداخلي والإجراءات الخاصة بكل طرف. وينبغي أن تشمل هذه القوانين

والإجراءات المحلية، كما هو مفصل بشكل أكثر تحديدا أدناه، الشروط أو الضمانات التي يمكن التنصيص عليها دستوريا، تشريعا، قضائيا أو خلاف ذلك. وينبغي أن تشمل الطرائق إضافة عناصر معينة من قبيل الشروط أو الضمانات التي توفق بين متطلبات إنفاذ القانون وحماية حقوق الإنسان والحريات. وبما أن الاتفاقية تنطبق على دول أطراف ذات العديد من الأنظمة والثقافات القانونية المختلفة، فإنه من غير الممكن تحديد الشروط والضمانات الواجب تطبيقها بالنسبة لكل صلاحية أو إجراء بشكل مفصل. وينبغي على الأطراف ضمان تنصيص هذه الشروط والضمانات على الحماية الكافية لحقوق الإنسان والحريات، علما أن هنالك بعض المعايير المشتركة أو حد أدنى من الضمانات التي يجب أن تلتزم بها الأطراف في الاتفاقية والتي تشمل المعايير أو الحد الأدنى من الضمانات الناشئة عن الالتزامات التي تعهد بها الطرف بموجب الصكوك الدولية السارية لحقوق الإنسان. وتشمل هذه الصكوك الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لعام ١٩٥٠ والبروتوكولات الإضافية رقم ١ و٤ و٦ و٧ و١٢ (سلسلة المعاهدات الأوروبية رقم ٥[4] و٩ و٤٦ و١١٤ و١١٧ و١٧٧)، فيما يتعلق بالدول الأوروبية الأطراف فيها. وبالإضافة إلى ذلك، فهي تتضمن صكوك حقوق الإنسان الأخرى المعمول بها في دول أخرى من العالم (مثل الاتفاقية الأمريكية لحقوق الإنسان لعام ١٩٦٩ والميثاق الأفريقي لحقوق الإنسان وحقوق الشعوب لعام ١٩٨١) والتي هي أطراف في هذه الآليات، علاوة على العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦. فضلا عن ذلك، ثمة أشكال مماثلة من الحماية تنص عليها قوانين معظم الدول.

١٤٦. ثمة ضمانة أخرى في الاتفاقية تتمثل في ضرورة أن تعمل الصلاحيات والإجراءات على "تضمين مبدأ التناسب". ويطبق كل طرف التناسب وفقا للمبادئ ذات الصلة في قانونه الداخلي. وبالنسبة للبلدان الأوروبية، يستمد ذلك من مبادئ اتفاقية مجلس أوروبا لعام ١٩٥٠ بشأن حماية حقوق الإنسان والحريات الأساسية، والاجتهاد القضائي الساري، والتشريعات والاجتهادات الوطنية، التي تفيد أن تكون السلطة أو الإجراء متناسبين مع طبيعة الجريمة وظروفها. وتطبق دول أخرى مبادئ ذات الصلة في قانونها، من قبيل القيود المفروضة على الإفراط في أوامر التقديم ومتطلبات المعقولية لعمليات التفتيش والمصادرة. كما أن التحديد الصريح الوارد في المادة ٢١ بشأن الالتزامات المتعلقة بتدابير الاعتراض تتعلق بمجموعة من الجرائم الخطيرة، التي يحددها القانون المحلي، يعتبر مثالا واضح على تطبيق مبدأ التناسب.

١٤٧. دون تقييد أنواع الشروط والضمانات التي يمكن تطبيقها، تقتضي الاتفاقية على وجه التحديد أن تشمل هذه الشروط والضمانات، حسب الاقتضاء بالنظر إلى طبيعة السلطة أو الإجراء، أو الإشراف القضائي أو أي إشراف مستقل آخر، الأسباب المبررة لتطبيق السلطة أو الإجراء والقيود المفروضة على النطاق أو مدته. ويتعين على الهيئات التشريعية الوطنية أن تحدد، عند تطبيق التزامات دولية ملزمة ومبادئ محلية راسخة، أن تحدد السلطات والإجراءات ذات طبيعة تطفلية بما فيه الكفاية والتي تتطلب تنفيذ شروط وضمانات معينة. وكما ورد في الفقرة ٢١٥، ينبغي للأطراف أن تطبق بوضوح شروطا وضمانات مثل تلك المتعلقة بالاعتراض، بالنظر إلى طابعها التطفلي. وفي الوقت نفسه، ليست هنالك حاجة على سبيل المثال، لتطبيق هذه الضمانات بشكل متساوي على الحفظ. وتشمل الضمانات الأخرى التي ينبغي تناولها في إطار القانون المحلي، الحق في عدم تجريم الذات، والامتيازات القانونية وخصوصية الأفراد أو الأماكن التي تكون موضوع تطبيق التدبير.

١٤٨. بالنظر إلى المسائل التي نوقشت في الفقرة ٣، تعتبر "المصلحة العامة"، ولا سيما مصالح "الإدارة السليمة للعدالة"، ذات أهمية قصوى. وينبغي للأطراف، إلى أقصى حد يتفق مع المصلحة العامة، أن تتدارس عوامل أخرى، مثل تأثير السلطة أو الإجراء على "حقوق ومسؤوليات ومصالح مشروعة" لأطراف ثالثة، بما في ذلك مقدمي الخدمات، الناجم عن تدابير التنفيذ، وما إذا كان بالإمكان اتخاذ وسائل مناسبة للتخفيف من هذا الأثر. وباختصار، يولى الاعتبار في المقام الأول للإدارة السليمة للعدالة ومصالح عامة أخرى (مثل السلامة العامة والصحة العمومية وغيرها من المصالح، بما في ذلك مصالح الضحايا واحترام الحياة الخاصة). وينبغي، إلى أقصى حد يتفق مع المصلحة العامة، إيلاء الاعتبار عادة لمسائل من قبيل التقليل إلى أدنى حد من تعطيل خدمات المستهلكين، والحماية من المسؤولية عن الكشف أو تسهيل الكشف بموجب هذا الفصل، أو حماية مصالح المالكين.

---

[4] تم تعديل نص الاتفاقية وفقا لأحكام البروتوكول رقم ٣ (سلسلة المعاهدات الأوروبية رقم ٤٥) الذي دخل حيز النفاذ في ٢١ سبتمبر/أيلول ١٩٧٠، والبروتوكول رقم ٥ (سلسلة المعاهدات الأوروبية رقم ٥٥) الذي دخل حيز النفاذ في ٢٠ ديسمبر/كانون الأول ١٩٧١، والبروتوكول رقم ٨ (سلسلة المعاهدات الأوروبية رقم ١١٨) الذي دخل حيز النفاذ في ١ يناير/كانون الثاني ١٩٩٠، وشمل أيضا نص البروتوكول رقم ٢ (سلسلة المعاهدات الأوروبية رقم ٤٤) الذي يشكل، طبقا للمادة ٥، الفقرة ٣ منه، جزء لا يتجزأ من الاتفاقية منذ دخولها حيز النفاذ في ٢١ سبتمبر/أيلول ١٩٧٠. وتم استبدال جميع الأحكام التي عدلت أو أضيفت بموجب هذه البروتوكولات، بالبروتوكول رقم ١١ (سلسلة المعاهدات الأوروبية رقم ١٥٥) اعتبارا من تاريخ دخوله حيز النفاذ في ١ نوفمبر/تشرين الثاني ١٩٩٨. ومنذ ذلك التاريخ، ألغي البروتوكول رقم ٩ (سلسلة المعاهدات الأوروبية رقم ١٤٠) الذي دخل حيز النفاذ في ١ أكتوبر/تشرين الأول ١٩٩٤، وفقد البروتوكول رقم ١٠ (سلسلة المعاهدات الأوروبية رقم ١٤٦) الغرض المتوخى منه.

الباب ٢ – تعجيل حفظ بيانات الكمبيوتر المخزنة

١٤٩.تنطبق التدابير الواردة في المادتين ١٦ و١٧ على البيانات المخزنة التي تم جمعها وحفظ بها من قبل أصحاب البيانات، مثل مقدمي الخدمات. ولا تنطبق على جمع بيانات الحركة في الوقت الحقيقي وحفظ بيانات الحركة المستقبلية أو على النفاذ في الوقت الحقيقي إلى محتوى الاتصالات. ويتناول الباب ٥ هذه المسائل.

١٥٠.لا تعمل التدابير الموصوفة في المواد إلا عندما توجد بالفعل بيانات حاسوبية ويجري تخزينها حاليا. ولأسباب كثيرة، قد تكون بيانات حاسوبية ذات الصلة بالتحقيقات الجنائية غير موجودة أو لم تعد مخزنة. وعلى سبيل المثال، من الممكن ألا تكون البيانات الدقيقة قد تم جمعها والاحتفاظ بها، أو في حال تم جمعها فمن المحتمل أنه لم يتم الاحتفاظ بها. ومن الممكن أن تكون قوانين حماية البيانات قد أكدت على المطالبة بإتلاف بيانات هامة قبل أن يدرك أي شخص أهميتها في الدعاوى الجنائية. في بعض الأحيان، قد لا يكون هناك سبب تجاري لجمع وحفظ البيانات، مثلا عندما يدفع العملاء سعرا ثابتا مقابل خدمات أو عندما تكون الخدمات مجانية. ولا تعالج المادتان ١٦ و١٧ هذه المشاكل.

١٥١.يجب تمييز "حفظ البيانات" عن "الاحتفاظ بالبيانات". ولئن كانت هاتان العبارتان تقاسمان معاني مماثلة في اللغة المشتركة، فإن معانيها مميزة فيما يتعلق باستخدام الكمبيوتر. وهكذا، يعني حفظ البيانات إبقاء بيانات، توجد بالفعل في شكل مخزن، محمية من أي شيء من شأنه أن يتسبب في تغيير جودتها أو وضعها الراهنين أو تدهورها. بينما يعني الاحتفاظ بالبيانات إبقاء بيانات، يتم توليدها حاليا، في حوزة الشخص لاستخدامها في المستقبل. وينطوي الاحتفاظ بالبيانات على مراكمة البيانات في الوقت الحاضر وإبقائها أو حيازتها لفترة زمنية مقبلة. ويعتبر الاحتفاظ بالبيانات بمثابة عملية تخزين البيانات. أما حفظ البيانات، من ناحية أخرى، فيمثل النشاط الذي يبقي تلك البيانات المخزنة سليمة وآمنة.

١٥٢.تشير المادتان ١٦ و١٧ فقط إلى حفظ البيانات، وليس الاحتفاظ بالبيانات، ولا تأمران بجمع وحفظ جميع البيانات أو بعضها من قبل مقدم خدمة أو أي هيئة أخرى في سياق أنشطتهم. وتنطبق تدابير الحفظ على بيانات الكمبيوتر التي "تم تخزينها بواسطة نظام كمبيوتر"، وهو ما يفترض مسبقا أن البيانات موجودة بالفعل، وقد تم جمعها وتخزينها. وعلاوة على ذلك، وكما هو مبين في المادة ١٤، فإن جميع الصلاحيات والإجراءات المطلوب إنشاؤها في القسم ٢ من الاتفاقية موجهة "لأغراض تحقيقات أو إجراءات جنائية محددة"، مما يحصر تطبيق التدابير في التحقيق في قضية خاصة. بالإضافة إلى ذلك، عندما يقوم الطرف بتنفيذ تدابير الحفظ بواسطة أمر، فإن هذا الأمر يخص "بيانات كمبيوتر مخزنة وخاصة تكون في حوزة الشخص أو تحت سيطرته" (الفقرة ٢). ومن تم، لا تنص المواد إلا على صلاحية المطالبة بحفظ البيانات المخزنة الموجودة، ريثما يتم الكشف لاحقا عن البيانات وفقا لسلطات قانونية أخرى، فيما يتعلق بالتحقيقات أو الإجراءات الجنائية المحددة.

١٥٣. لا يرمي الالتزام بضمان حفظ البيانات إلى مطالبة الأطراف بتقييد عرض أو استخدام الخدمات التي لا تقوم عادة بجمع أنواع معينة من البيانات والاحتفاظ بها، مثل بيانات الحركة أو المنخرط، كجزء من ممارساتها التجارية المشروعة. كما أنه لا يطالبها بتنفيذ قدرات تقنية جديدة للقيام بذلك، مثلا بغية حفظ بيانات مؤقتة قد تكون متاحة على النظام لفترة وجيزة بحيث لا يمكن الحفاظ عليها بشكل معقول استجابة لطلب أو أمر.

١٥٤.تتوفر بعض الدول على قوانين تقتضي بأنه لا يجب الاحتفاظ ببعض أنواع البيانات، مثل البيانات الشخصية التي يحتفظ بها أشخاص معينون، وأنه يجب حذفها إذا لم يعد هناك غرض تجاري للاحتفاظ بها. وفي الاتحاد الأوروبي، ينفذ المبدأ العام بموجب المبدإ التوجيهي رقم 95/46/EC، وفي السياق الخاص لقطاع الاتصالات السلكية واللاسلكية، ينفذ بموجب المبدإ التوجيهي رقم 97/66/EC. وينص هذان المبدآن التوجيهيان على الالتزام بحذف البيانات بمجرد أن يصبح تخزينها غير ضروري. إلا أنه يجوز للدول الأعضاء أن تعتمد تشريعا ينص على استثناءات عند الضرورة لغرض منع الجرائم الجنائية أو التحقيق فيها أو مقاضاتها. ولا يمنع هذان المبدآن التوجيهيان الدول الأعضاء في الاتحاد الأوروبي من إنشاء سلطات وإجراءات بموجب قانونها الداخلي لحفظ بيانات محددة لغرض تحقيقات محددة.

١٥٥.يعتبر حفظ البيانات بالنسبة لمعظم البلدان سلطة أو إجراء قانونيا جديدا تماما في القانون الوطني. فهو أداة جديدة هامة للتحقيق في معالجة الجرائم الإلكترونية و الجرائم المتصلة بالكمبيوتر، لا سيما الجرائم المرتكبة عن طريق الإنترنت. أولا، تعتبر البيانات، بسبب تقلب بيانات الكمبيوتر، معرضة بسهولة للتلاعب أو التغيير. وهكذا، يمكن بسهولة تضييع أدلة قيمة على الجريمة من خلال المناولة غير المتقنة وممارسات التخزين، والتلاعب المتعمد أو الحذف بهدف إتلاف الأدلة أو الحذف الروتيني للبيانات التي لم تعد هناك حاجة للاحتفاظ بها. وتتمثل إحدى وسائل الحفاظ على سلامتها في أن تقوم السلطات المختصة بالبحث أو النفاذ بطرق مماثلة إلى البيانات أو مصادرتها أو تأمينها بطرق مماثلة. ومع ذلك، عندما تكون الجهة الوديعة للبيانات موثوقة، مثل الشركات ذات السمعة الطيبة، يمكن تأمين سلامة البيانات بسرعة أكبر من خلال أمر بحفظ البيانات. وبالنسبة للشركات التجارية المشروعة، قد يكون أمر الحفظ أيضا أقل إخلالا بأنشطتها العادية وسمعتها من تنفيذ عمليات التفتيش والمصادرة داخل مرافقها. وثانيا، ترتكب الجرائم الإلكترونية والجرائم المتصلة بالكمبيوتر إلى حد كبير نتيجة لنقل الاتصالات عن طريق نظام الكمبيوتر. وقد تحتوي هذه الاتصالات على محتوى غير قانوني، مثل المواد الإباحية المتعلقة بالأطفال أو فيروسات الكمبيوتر أو غيرها من التعليمات التي تتسبب في التدخل في البيانات أو في التشغيل السليم لنظام الكمبيوتر أو في دليل على ارتكاب جرائم أخرى، من قبيل الاتجار في المخدرات أو الاحتيال. ومن جهة أخرى، يمكن أن يساعد تحديد مصدر هذه الاتصالات السابقة أو وجهتها في التعرف على الجناة. تكون بيانات الحركة الخاصة بهذه الاتصالات السابقة مطلوبة من أجل تتبع هذه الاتصالات لتحديد مصدرها أو وجهتها (انظر المزيد من التوضيح بشأن أهمية بيانات الحركة الواردة أدناه بموجب المادة ١٧). وثالثا، عندما تحتوي هذه الاتصالات على محتوى غير قانوني أو دليل على نشاط إجرامي، يحتفظ مقدمو الخدمات بنسخ من هذه الرسائل، مثل البريد الإلكتروني. ويعتبر حفظ هذه الاتصالات مهما من أجل ضمان عدم إتلاف أدلة بالغة الأهمية. ولعل الحصول على نسخ من هذه الاتصالات السابقة (مثل البريد الإلكتروني المخزن الذي تم إرساله أو استلامه) من شأنه أن يكشف عن أدلة على الإجرام.

١٥٦.تهدف صلاحية التعجيل بحفظ بيانات الكمبيوتر إلى معالجة هذه المشاكل. ومن تم، فإن الأطراف مطالبة بإدخال صلاحية تأمر بحفظ بيانات حاسوبية محددة كتدبير مؤقت، بحيث يتم حفظ البيانات لفترة من الوقت طالما كان ذلك ضروريا، أقصاها ٩٠ يوما. ويجوز لأي طرف أن ينص على تجديد الأمر لاحقا. وهذا لا يعني أنه يتم الكشف عن تلك البيانات لسلطات إنفاذ القانون خلال فترة الحفظ. ولكي يحدث ذلك، يجب أن إصدار أمر بإجراء تدبير إضافي من أجل الكشف أو البحث. وفيما يتعلق بالكشف عن البيانات المحفوظة لإنفاذ القانون، انظر الفقرتين ١٥٢ و١٦٠.

١٥٧.يعتبر من المهم أيضا وجود تدابير للحفظ على الصعيد الوطني من أجل تمكين الأطراف من مساعدة بعضها البعض على الصعيد الدولي في التعجيل بحفظ البيانات المخزنة الموجودة على أراضيها. وهذا من شأنه أن يساعد في ضمان عدم إتلاف البيانات الهامة أثناء إجراءات المساعدة القانونية المتبادلة التي كثيرا ما تستغرق وقتا طويلا والتي تمكن الطرف المطلوب منه المساعدة من الحصول فعليا على البيانات والإفصاح عنها للطرف مقدم الطلب.

التعجيل في حفظ بيانات الكومبيوتر المخزنة (المادة ١٦)

١٥٨.تهدف المادة ١٦ إلى ضمان قدرة السلطات الوطنية المختصة على أن تأمر أو تحصل بطريقة مماثلة على التعجيل في حفظ بيانات كمبيوتر مخزنة محددة ومتعلقة بتحقيق جنائي أو دعوى جنائية محددة.

١٥٩.يقتضي "الحفظ" أن تكون البيانات، الموجودة بالفعل في شكل مخزن، محمية من أي شيء قد يتسبب في تغيير أو تدهور جودتها أو وضعها القائم. كما أنه يتطلب أن تبقى آمنة من التعديل أو الإفساد أو الحذف. ولا يعني الحفظ بالضرورة أن البيانات "مجمدة" (بمعنى أنه يتعذر النفاذ إليها) وأنه لا يمكن استخدامها أو استخدام نسخ منها من قبل المستخدمين الشرعيين. ويبقى للشخص الذي يوجه له الأمر، وفقا للمواصفات الدقيقة للأمر، إمكانية النفاذ إلى البيانات. لا تحدد المادة كيفية حفظ البيانات، وبالتالي، يترك لكل طرف تحديد الطريقة المناسبة لحفظ البيانات، وما إذا كان ينبغي في بعض الحالات المناسبة أن ينطوي حفظ البيانات أيضا على "تجميدها".

١٦٠.ترمي الإشارة إلى "الأمر أو الحصول بطريقة مماثلة" إلى تمكين استخدام أساليب قانونية أخرى لتحقيق الحفظ بدلا من الاكتفاء بأمر قضائي أو إداري أو توجيهات (مثلا من الشرطة أو المدعي العام). وفي بعض الدول، لا توجد أوامر الحفظ في قانونها الإجرائي، ولا يمكن حفظ البيانات والحصول عليها إلا من خلال أمر البحث والاستيلاء أو التقديم. وتتيح هذه العبارة مرونة مقصودة تتجلى في "أو الحصول بطريقة مماثلة" بغية تمكين هذه الدول من تنفيذ هذه المادة باستخدام هذه

الوسائل. ومع ذلك، يوصى بأن تنظر الدول في إنشاء سلطات وإجراءات لكي تأمر فعليا الجهة المتلقية بحفظ البيانات، لأن اتخاذ إجراء سريع من قبل هذا الشخص يمكن أن يؤدي إلى تعزيز تسريع تنفيذ تدابير الحفظ في حالات معينة.

١٦١. تنطبق صلاحية الأمر بالتعجيل بحفظ بيانات كمبيوتر محددة أو الحصول عليها بطريقة مماثلة على أي نوع من بيانات الكمبيوتر المخزنة. ويمكن أن يتضمن ذلك أي نوع من البيانات المحددة في الأمر بالحفظ. ويمكن أن تشمل، على سبيل المثال، سجلات الأعمال، والسجلات الصحية أو الشخصية أو غيرها من السجلات. ويتعين على الأطراف وضع هذه التدابير لاستخدامها "خاصة إذا كانت هناك أسباب تدعو إلى الاعتقاد بأن بيانات الكمبيوتر معرضة بوجه خاص للضياع أو التعديل". ويمكن أن يشمل ذلك الحالات التي تخضع فيها البيانات للاحتفاظ لفترة قصيرة من الزمن، مثل حالة وجود سياسة تجارية بحذف البيانات بعد فترة زمنية معينة أو عندما يتم عادة حذف بيانات عند استخدام دعامة للتخزين لتسجيل بيانات أخرى عليها. ويمكن أن تشير أيضا إلى طبيعة الجهة الوديعة للبيانات أو الطريقة غير الآمنة التي يتم بها تخزين البيانات. ومع ذلك، إذا كانت الجهة الوديعة للبيانات غير جدير بالثقة، لعه سيكون أكثر أمانا إجراء الحفظ عن طريق البحث والمصادرة، بدلا من إصدار أمر من المحتمل ألا يتم الامتثال له. وترد إشارة محددة إلى "بيانات الحركة" في الفقرة ١ للإشارة إلى الأحكام التي تنطبق بوجه خاص على هذا النوع من البيانات، والتي إذا جمعها واحتفظ بها مقدم الخدمة، عادة ما تكون لفترة قصيرة من الزمن. وتتصل الإشارة إلى "بيانات الحركة" أيضا بالتدابير الواردة في المادتين ١٦ و١٧.

١٦٢. تحدد الفقرة ٢ أنه عندما تفعل دولة طرف الحفظ عن طريق إصدار أمر، يكون الأمر بالحفظ يتعلق ب "بيانات كمبيوتر مخزنة محددة في حيازة شخص أو تحت سيطرته". وهكذا، قد تكون البيانات المخزنة في الواقع في حوزة الشخص أو قد تكون مخزنة في مكان آخر ولكن تخضع لسيطرة هذا الشخص. ويتعين على الشخص الذي يتسلم الأمر أن "يحافظ على سلامة بيانات الكمبيوتر المعنية لفترة من الوقت طالما كان ذلك ضروريا، دون أن تتجاوز ٩٠ يوما، وذلك لتمكين السلطات المختصة من التماس الكشف عنها". وينبغي أن يحدد القانون الداخلي للطرف فترة زمنية قصوى لحفظ البيانات بموجب أمر، وينبغي أن يوضح الأمر المدة الزمنية المحددة لحفظ البيانات المعنية. وينبغي أن تكون الفترة الزمنية للمدة الضرورية، والتي أقصاها ٩٠ يوما، للسماح للسلطات المختصة باتخاذ تدابير قانونية أخرى، مثل التفتيش أو المصادرة أو النفاذ والتأمين بطريقة مماثلة، أو إصدار أمر التقديم، بغية الحصول على الكشف عن البيانات. يجوز للطرف أن ينص على التجديد اللاحق لأمر التقديم. وفي هذا السياق، ينبغي الإشارة إلى المادة ٢٩ التي تتعلق بطلب المساعدة المتبادلة للحصول على التعجيل بحفظ البيانات المخزنة بواسطة نظام الكمبيوتر. وتحدد تلك المادة أن الحفظ الذي يتم تنفيذه استجابة لطلب المساعدة المتبادلة "يجب أن يكون لمدة لا تقل عن ٦٠ يوما لتمكين الطرف مقدم الطلب من تقديم طلب للبحث أو النفاذ بطريقة مماثلة، أو المصادرة أو التأمين بطريقة مماثلة أو الكشف عن البيانات."

١٦٣. تفرض الفقرة ٣ إلزاما بالسرية فيما يخص إجراءات الحفظ على الجهة الوديعة للبيانات التي يتعين حفظها أو على الشخص الذي أمر بحفظ البيانات لفترة من الزمن طبقا لما هو منصوص عليه في القانون المحلي. ويتطلب ذلك من الأطراف إدراج تدابير السرية فيما يتعلق بالتعجيل بحفظ البيانات المخزنة، ومدة زمنية فيما يخص الفترة المشمولة بالسرية. وينبغي أن يتواءم هذا التدبير مع احتياجات إنفاذ القانون حتى لا يعرف المشتبه به بالتحقيق الجاري في حقه، وكذلك مع حق الأفراد في الخصوصية. ويشكل التعجيل بحفظ البيانات، بالنسبة لسلطات إنفاذ القانون، جزءا من التحقيقات الأولية، وبالتالي قد تكون السرية هامة في هذه المرحلة. ويعتبر الحفظ تدبيرا أوليا ريثما يتم اتخاذ تدابير قانونية أخرى للحصول على البيانات أو الكشف عنها. فالسرية مطلوبة لكي لا يحاول الآخرون التلاعب بالبيانات أو حذفها. وبالنسبة للشخص الذي يوجه له الأمر، أو موضوع البيانات أو الأشخاص الآخرين الذين يمكن ذكرهم أو تحديدهم في البيانات، يكون هناك حد زمني واضح لطول مدة التدبير. وتساعد الالتزامات المزدوجة للحفاظ على سلامة البيانات وأمنها والحفاظ على سرية اتخاذ تدبير الحفظ على حماية خصوصية موضوع البيانات أو الأشخاص الآخرين الذين يمكن ذكرهم أو تحديد هويتهم في تلك البيانات.

١٦٤. بالإضافة إلى القيود المبينة أعلاه، تخضع الصلاحيات والإجراءات المشار إليها في المادة ١٦ أيضا للشروط والضمانات المنصوص عليها في المادتين ١٤ و١٥.

التعجيل في حفظ بيانات الكومبيوتر والكشف الجزئي عن بيانات الحركة (المادة ١٧)

١٦٥.تنص هذه المادة على التزامات محددة ذات الصلة بحفظ بيانات الحركة بموجب المادة ١٦، وتنص على التعجيل بالكشف عن بعض بيانات الحركة من أجل التعرف على مقدمي الخدمات الآخرين المنخرطين في نقل الاتصالات المحددة. ويرد تعريف "بيانات الحركة" في المادة ١.

١٦٦.يمكن أن يكون الحصول على بيانات الحركة المخزنة ذات الصلة باتصالات سابقة أمرا حاسما من أجل تحديد مصدر أو وجهة اتصال سابق، وهو أمر بالغ الأهمية لتحديد هوية الأشخاص الذين قاموا، على سبيل المثال، بتوزيع مواد إباحية متعلقة بالأطفال، أو بتوزيع تحريفات مزيفة كجزء من مخططات احتيالية، أو بنشر فيروسات حاسوبية، أو بمحاولة النفاذ إلى أنظمة الكمبيوتر بصورة غير مشروعة أو نجحوا في النفاذ إليها، أو بنقل اتصالات إلى نظام كمبيوتر تداخلت مع البيانات الموجودة في النظام أو أثرت على اشتغاله السليم. ومع ذلك، يتم تخزين هذه البيانات في كثير من الأحيان لفترات قصيرة فقط، حيث أن القوانين المصممة لحماية الخصوصية قد تحظر أو قد تثبط قوى السوق تخزين هذه البيانات على المدى الطويل. لذلك، من الأهمية بمكان اتخاذ تدابير الحفظ لضمان سلامة هذه البيانات (انظر المناقشة المتعلقة بالحفظ، أعلاه).

١٦٧.كثيرا ما يشارك أكثر من مقدم خدمة واحد في نقل الاتصال. ويجوز لكل مزود الخدمة أن يمتلك بعض بيانات الحركة المتصلة بنقل الاتصالات المحددة التي تم توليدها والاحتفاظ بها من قبل مقدم الخدمة فيما يتعلق بمرور الاتصال عبر نظامه أو تم توفيرها من لدن غيرهم من مقدمي الخدمة. وفي بعض الأحيان، يتم تقاسم بيانات الحركة، أو على الأقل بعض أنواعها، بين مقدمي الخدمة المشاركين في إرسال الاتصالات لأغراض تجارية، أمنية أو تقنية. وفي مثل هذه الحالات، قد تتوفر لدى أي من مقدمي الخدمة بيانات الحركة الحاسمة والضرورية لتحديد مصدر أو وجهة الاتصال. ومع ذلك، لا يوجد في كثير من الأحيان، مزود خدمة واحد يتوفر على ما يكفي من بيانات الحركة الحاسمة للتمكن من تحديد المصدر الفعلي للاتصال أو وجهته. فكل واحد يمتلك قطعة من اللوحة، وثمة حاجة إلى فحص كل القطع وتجميعها حتى تكتمل الصورة من أجل تحديد المصدر أو الوجهة.

١٦٨.تضمن المادة ١٧ في حال مشاركة مقدم خدمة واحد أو أكثر في إرسال اتصال، تفعيل التعجيل بحفظ بيانات الحركة بين جميع مقدمي الخدمة. ولا تحدد المادة الوسائل التي يمكن من خلالها تحقيق ذلك، مما يترك للقانون المحلي المجال لتحديد الوسائل التي تتفق مع نظامها القانوني والاقتصادي. ومن الوسائل الكفيلة بتحقيق التعجيل بالحفظ أن تصدر السلطات المختصة على وجه السرعة أمرا منفصلا بالحفظ إلى كل مقدم خدمة على حدة. إلا أن الحصول على سلسلة من أوامر منفصلة يستهلك وقتا طويلا لا لزوم له. ولعل أحد البدائل المفضلة يتمثل في الحصول على أمر واحد ينطبق نطاقه على جميع مقدمي الخدمة الذين تم تحديد مشاركتهم في إرسال الاتصالات المحددة. ويمكن توجيه هذا الأمر الشامل بالتتابع إلى كل مزود خدمة محدد. ويمكن أن تشمل البدائل الممكنة الأخرى إشراك مقدمي الخدمة في هذه العملية. على سبيل المثال، يمكن مطالبة مقدم الخدمة الذي تسلم الأمر بإخطار مقدم الخدمة الموالي في تسلسل القائمة بوجود أمر الحفظ وشروطه. ويمكن أن يكون لهذا الإشعار، رهنا بالقانون المحلي، كأثر إما ترخيص مقدم الخدمة الآخر بالحفظ الطوعي لبيانات الحركة ذات الصلة، على الرغم من أي التزامات بحذفها، أو الإلزامية بحفظ بيانات الحركة ذات الصلة. وبالمثل، يمكن لمزود الخدمة الثاني أن يشعر مقدم الخدمة الموالي في السلسلة، وهكذا دواليك.

١٦٩.نظرا إلى عدم الكشف عن بيانات الحركة لسلطات إنفاذ القانون عند تقديم أمر الحفظ إلى مقدم الخدمة (ولكن يتم الحصول عليها أو الإفصاح عنها لاحقا عند اتخاذ تدابير قانونية أخرى)، فإن هذه السلطات لن تعرف ما إذا كان مزود الخدمة يمتلك جميع بيانات الحركة الحاسمة أو ما إذا كان هناك مقدمو خدمات آخرون يشاركون في سلسلة إرسال الاتصال. لذلك، تقضي هذه المادة بأن يقوم مقدم الخدمة، الذي يتلقى أمر الحفظ أو تدبيرا مماثلا، بالإفصاح على وجه السرعة إلى السلطات المختصة، أو أي شخص آخر معين، عن كمية كافية من بيانات الحركة لتمكين تلك السلطات المختصة من التعرف على أي من مقدمي الخدمات الآخرين والطريق الذي تم من خلاله إرسال الاتصال. وينبغي للسلطات المختصة أن تحدد بوضوح نوع بيانات الحركة المطلوب الكشف عنها. ولعل استلام هذه المعلومات من شأنه أن يمكن السلطات المختصة من تقرير جدوى اتخاذ تدابير الحفظ فيما يتعلق بمقدمي الخدمات الآخرين. وبهذه الطريقة، يمكن لسلطات التحقيق تعقب الاتصال إلى مصدره أو وجهته، والتعرف على مرتكب أو مرتكبي الجريمة المحددة التي تخضع للتحقيق. وتخضع التدابير الواردة في هذه المادة أيضا للقيود والشروط والضمانات المنصوص عليها في المادتين ١٤ و١٥.

الباب ٣ – أمر التقديم

أمر التقديم (المادة ١٨)

١٧٠.تدعو الفقرة ١ من هذه المادة الأطراف إلى تمكين سلطاتها المختصة من إرغام شخص في إقليمها على تقديم بيانات حاسوبية مخزنة محددة أو مقدم خدمة يقدم خدماته في إقليم الطرف على تقديم معلومات بشأن المنخرطين. وتكون البيانات المعنية مخزنة أو بيانات موجودة، ولا تتضمن البيانات التي لم تخرج بعد إلى حيز الوجود مثل بيانات الحركة أو بيانات المحتوى المتعلقة بالاتصالات المستقبلية. وبدلا من مطالبة الدول بتطبيق تدابير قسرية منتظمة فيما يتعلق بالأطراف الثالثة، من قبيل البحث عن البيانات ومصادرتها، من الضروري أن تتوفر الدول في قوانينها الداخلية على سلطات تحقيق بديلة توفر وسائل أقل تطفلا للحصول على المعلومات ذات الصلة بالتحقيقات الجنائية.

١٧١.يوفر " أمر التقديم" تدبيرا مرنا يمكن لسلطات إعمال القانون تطبيقه في كثير من الحالات، لا سيما بدلا عن التدابير التي تكون أكثر تطفلا أو أكثر كلفة. ولعل تنفيذ هذه الآلية الإجرائية من شأنه أن يكون مفيدا أيضا للأطراف الثالثة الوديعة للبيانات، مثل مقدمي خدمات الإنترنت، الذين غالبا ما يكونون على استعداد لمساعدة سلطات إنفاذ القانون على أساس طوعي من خلال توفير البيانات الخاضعة لسيطرتهم، ولكن يفضلون أساسا قانونيا مناسبا من أجل تقديم هذه المساعدة، وتجريدهم من أي مسؤولية تعاقدية أو غير تعاقدية.

١٧٢.يشير أمر التقديم إلى بيانات الكمبيوتر أو المعلومات عن المنخرط التي تكون في حوزة أو تحت سيطرة شخص أو مقدم خدمة. ولا ينطبق هذا التدبير إلا عندما يحتفظ الشخص أو مقدم الخدمة بتلك البيانات أو المعلومات. فبعض مقدمي الخدمات، على سبيل المثال، لا يحتفظون بالسجلات المتعلقة بالمنخرطين في خدماتهم.

١٧٣.ينبغي على الدولة الطرف، بموجب الفقرة ١(أ)، أن تكفل لسلطات إنفاذ القانون المختصة لديها صلاحية أمر الشخص الموجود في إقليمها بتقديم بيانات حاسوبية محددة مخزنة في نظام كمبيوتر أو على جهاز لتخزين البيانات يكون في حيازة ذلك الشخص أو تحت سيطرته. ويشير مصطلح "الحيازة أو السيطرة" إلى الحيازة المادية للبيانات المعنية في إقليم الطرف الذي يصدر الأمر، وإلى الحالات التي لا تكون فيها البيانات التي يجب تقديمها في حيازة الشخص المادية ولكن يمكن لذلك الشخص التحكم بحرية في تقديم البيانات من داخل إقليم الطرف الذي يصدر الأمر (على سبيل المثال، رهنا بالامتيازات المطبقة، يجب على الشخص الذي يتوصل بأمر تقديم معلومات مخزنة على حسابه عن طريق خدمة تخزين على الإنترنت عن بعد، أن يقدم تلك المعلومات المطلوبة). وفي الوقت نفسه، لا تشكل القدرة الفنية على النفاذ إلى بيانات مخزنة عن بعد (على سبيل المثال، قدرة المستخدم على النفاذ من خلال رابط على الشبكة إلى بيانات مخزنة عن بعد ليست تحت سيطرته المشروعة) بالضرورة "سيطرة" بالمعنى المقصود في هذا البند. وفي بعض الدول، يغطي المفهوم الواسع لمصطلح "الحيازة" في القانون، الحيازة المادية والبناءة بما يكفي لتلبية شرط "الحيازة أو السيطرة".
وبموجب الفقرة ١(ب)، ينص الطرف أيضا على صلاحية الأمر بأن يقوم مقدم خدمات يعرض خدماته في إقليمه "بتقديم المعلومات عن المنخرطين التي في حوزته أو تحت سيطرته". وكما هو الحال في الفقرة ١(أ)، يشير مصطلح "الحيازة أو السيطرة" إلى المعلومات عن المنخرط التي توجد في الحيازة المادية لمقدم الخدمة وإلى المعلومات عن المنخرط المخزنة عن بعد التي توجد تحت سيطرة مقدم الخدمة (على سبيل المثال في على جهاز لتخزين البيانات عن بعد توفره شركة أخرى) . وتعني عبارة "المتعلقة بهذه الخدمة" أن تكون الصلاحية متاحة لغرض الحصول على معلومات المنخرط المتعلقة بالخدمات المقدمة في إقليم الطرف الذي يصدر الأمر.

١٧٤.يمكن أن تستثني الشروط والضمانات المشار إليها في الفقرة ٢ من المادة، وفقا للقانون الداخلي لكل طرف، البيانات أو المعلومات الامتيازية. وقد يرغب أحد الأطراف في تحديد شروط وسلطات مختصة وضمانات مختلفة فيما يتعلق بتقديم أنواع معينة من بيانات الكمبيوتر أو المعلومات عن المشتركين التي تحتفظ بها فئات معينة من الأشخاص أو مقدمي الخدمات. فعلى سبيل المثال، يجوز لأي طرف فيما يتعلق ببعض أنواع البيانات، مثل المعلومات عن المنخرطين المتاحة للعموم، أن يسمح لعناصر إنفاذ القانون بإصدار أمر من هذا القبيل يتطلب في حالات أخرى أن يصدر عن محكمة. ومن ناحية أخرى، قد يطلب الطرف، في بعض الحالات، أو يكون مطالبا بموجب ضمانات حقوق الإنسان، أن يصدر أمر التقديم عن السلطات القضائية فقط بغية التمكن من الحصول على أنواع معينة من البيانات. وقد ترغب الأطراف في حصر الكشف عن هذه البيانات لأغراض إنفاذ القانون في الحالات التي يكون فيها أمر التقديم من أجل لكشف عن هذه المعلومات صادرا

عن سلطات قضائية. ويوفر مبدأ التناسب أيضا بعض المرونة فيما يتعلق بتطبيق التدبير، الذي تلجأ له كثير من الدول مثلا من أجل استبعاد تطبيقه على الحالات البسيطة.

١٧٥. يمكن أن تنظر الأطراف أيضا في إمكانية إدراج تدابير تتعلق بالسرية. لا يتضمن الحكم إشارة محددة إلى السرية، من أجل الحفاظ على التوازي مع العالم غير الإلكتروني حيث لا تفرض السرية بشكل عام فيما يتعلق بأوامر التقديم. ومع ذلك، يمكن في بعض الأحيان استخدام أمر التقديم في العالم الإلكتروني، لا سيما على الإنترنت، كتدبير أولي في التحقيق، الذي يسبق تدابير أخرى مثل البحث عن بيانات أخرى أو مصادرتها أو اعتراضها في الوقت الحقيقي. وقد تكون السرية أساسية لنجاح التحقيق.

١٧٦. فيما يتعلق بأساليب التقديم، يمكن للأطراف أن تضع التزامات بأن يتم تقديم بيانات الكمبيوتر المحددة أو المعلومات عن المنخرطين بالطريقة المحددة في الأمر. ويمكن أن يشمل ذلك إشارة إلى فترة زمنية يجب خلالها أن يتم الكشف عن تلك البيانات أو المعلومات أو إلى الشكل الذي يجب فيه تقديمها، مثلا في شكل "نص عادي" أو على الإنترنت أو مطبوعة على ورق أو على قرص مرن.

١٧٧. يرد تعريف "المعلومات عن المنخرط" في الفقرة ٣، مبدئيا، تشير هذه العبارة إلى أي معلومات تحتفظ بها إدارة مقدم خدمة تتعلق بمنخرط في خدماتها. ويمكن تضمين المعلومات عن المنخرط في شكل بيانات الكمبيوتر أو أي شكل آخر، مثل السجلات الورقية. وبما أن المعلومات عن المنخرط تتضمن أشكالا من البيانات غير بيانات الكمبيوتر فقط، فقد أدرج حكم خاص في المادة لمعالجة هذا النوع من المعلومات. واستخدم مصطلح "المنخرط" قصدا ليشمل مجموعة واسعة من عملاء مقدمي الخدمات، من الأشخاص الذين يتوفرون على اشتراكات مدفوعة الأجر، وأولئك الذين يدفعون على أساس كل استخدام، إلى أولئك الذين يتلقون خدمات مجانية. كما يشمل المعلومات بشأن الأشخاص الذين يحق لهم استخدام حساب المنخرط.

١٧٨. في سياق التحقيق الجنائي، قد تكون هناك حاجة إلى المعلومات عن المنخرط أساسا في حالتين محددتين. أولا، ثمة حاجة إلى المعلومات عن المنخرط لتحديد نوع الخدمات أو التدابير التقنية ذات الصلة التي استخدمها أو يستخدمها المنخرط، مثل نوع الخدمة الهاتفية المستخدمة (مثلا الهاتف النقال) ونوع الخدمات الأخرى المرتبطة (مثل إعادة توجيه المكالمات، والبريد الصوتي، وما إلى ذلك)، ورقم الهاتف أو عنوان فني آخر (على سبيل المثال، عنوان البريد الإلكتروني). ثانيا، عندما يكون العنوان الفني معروفا، تكون هنالك حاجة إلى المعلومات عن المنخرط من أجل المساعدة في تحديد هوية الشخص المعني. ويمكن أن تكون معلومات أخرى عن المنخرط، مثل المعلومات التجارية حول سجلات الفوترة والدفع الخاصة بالمنخرط، صميمية أيضا بالنسبة للتحقيقات الجنائية، خاصة عندما تنطوي الجريمة قيد التحقيق على احتيال على الكمبيوتر أو جرائم اقتصادية أخرى.

١٧٩. لذلك، تتضمن المعلومات عن المنخرط أنواعا مختلفة من المعلومات عن استخدام الخدمة ومستخدمي تلك الخدمة. وفيما يتعلق باستخدام الخدمة، يقصد بالمصطلح أي معلومات، من غير بيانات الحركة أو المحتوى، يمكن من خلالها تحديد نوع خدمة الاتصالات المستخدمة، والأحكام الفنية المتعلقة بها، والفترة الزمنية التي اشترك فيها الشخص في الخدمة. ويشمل مصطلح "الأحكام الفنية" جميع التدابير المتخذة لتمكين المنخرط من التمتع بخدمة الاتصالات المقدمة. وتشمل هذه الأحكام حجز رقم أو عنوان فني (رقم الهاتف أو عنوان الموقع الإلكتروني أو اسم النطاق وعنوان البريد الإلكتروني وما إلى ذلك)، فضلا عن توفير وتسجيل معدات الاتصال المستخدمة من قبل المنخرط، مثل أجهزة الهاتف، ومراكز الاتصال أو شبكات المناطق المحلية (LANs).

١٨٠. لا تقتصر المعلومات عن المنخرط على المعلومات المرتبطة مباشرة باستخدام خدمة الاتصالات. فهي تعني أيضا أي معلومات، بخلاف بيانات الحركة أو بيانات المحتوى، يمكن من خلالها تحديد هوية المستخدم أو عنوانه البريدي أو الجغرافي، ورقم هاتفه أو رقم اتصال آخر ومعلومات الفوترة والدفع، والتي تتوفر على أساس اتفاق أو ترتيب الخدمة بين المنخرط ومقدم الخدمة. كما يقصد بها أي معلومات أخرى، بخلاف بيانات الحركة أو بيانات المحتوى، ذات الصلة بالموقع أو المكان الذي تم فيه تركيب معدات الاتصالات، والمتاحة على أساس اتفاق أو ترتيب الخدمة. وقد تكون هذه المعلومات

الأخيرة صميمية فقط من الناحية العملية عندما تكون المعدات غير محمولة، لكن معرفة قابلية المعدات للنقل أو موقعها المزعوم (على أساس المعلومات المقدمة وفقا لاتفاق الخدمة أو ترتيبها) يمكن أن تساعد في التحقيق.

١٨١.إلا أنه لا ينبغي فهم هذه المادة على أنها تفرض التزاما على مقدمي الخدمات للاحتفاظ بسجلات منخرطيهم، كما أنها لا تطالب مقدمي الخدمات بضمان صحة هذه المعلومات. وبالتالي، فإن مقدم الخدمة غير ملزم بتسجيل معلومات هوية مستخدمي ما يسمى بالبطاقات مسبقة الدفع لخدمات الهاتف الجوال. كما أنهم غير ملزمين بالتحقق من هوية المنخرطين أو مقاومة استخدام أسماء مستعارة من قبل مستخدمي خدماتهم.

١٨٢.بما أن الصلاحيات والإجراءات الواردة في هذا القسم وضعت لأغراض تحقيقات أو إجراءات جنائية محددة (المادة ١٤)، ينبغي استخدام أوامر التقديم في حالات فردية تتعلق، عادة، بمنخرطين معينين. على سبيل المثال، بناء على توفير اسم معين مذكور في أمر التقديم، يمكن طلب رقم هاتف أو عنوان بريد إلكتروني مرتبط بذلك الاسم. ويجوز، انطلاقا من رقم هاتف أو عنوان بريد إلكتروني معين، طلب اسم وعنوان المنخرط المعني. ولا يرخص هذا الحكم للأطراف بإصدار أمر قانوني بالإفصاح عن كميات عشوائية من المعلومات عن المنخرطين من مقدم الخدمة بشأن مجموعات من المنخرطين، مثلا لغرض التنقيب في البيانات.

١٨٣.ينبغي أن تفسر الإشارة إلى "اتفاق أو ترتيب الخدمة" بمعنى واسع وأن تشمل أي نوع من العلاقات التي يقوم على أساسها الزبون/العميل باستخدام خدمات مقدم الخدمة.

الباب ٤ – البحث عن بيانات الكومبيوتر المخزنة ومصادرتها

البحث عن بيانات الكومبيوتر المخزنة ومصادرتها (المادة ١٩)

١٨٤.تهدف هذه المادة إلى تحديث وتنسيق القوانين المحلية المتعلقة بالبحث عن بيانات الكمبيوتر المخزنة ومصادرتها لأغراض الحصول على أدلة فيما يتعلق بالتحقيقات أو الإجراءات الجنائية المحددة. ويشمل أي قانون إجرائي جنائي داخلي صلاحيات للبحث عن الأشياء الملموسة ومصادرتها. ومع ذلك، لا تعتبر، في عدد من الولايات القضائية، بيانات الكمبيوتر المخزنة في حد ذاتها شيئا ملموسا وبالتالي لا يمكن تأمينها باسم تحقيقات ودعاوى جنائية بطريقة موازية كأشياء ملموسة إلا من خلال تأمين الجهاز الذي يتم تخزين البيانات عليه. وترمي المادة ١٩ من هذه الاتفاقية إلى إنشاء صلاحية معادلة خاصة بالبيانات المخزنة.

١٨٥.ينطوي البحث، في مجال البحث التقليدي المتعلق بالوثائق أو السجلات، على جمع الأدلة التي تم تسجيلها أو تقييدها في الماضي في شكل ملموس، مثلا حبرا على ورق. ويقوم المحققون بالبحث في هذه البيانات المسجلة أو فحصها، ومصادرة السجل الملموس أو إبعاده فعليا. ويتم جمع البيانات خلال فترة البحث وبالنظر إلى البيانات المتاحة عندئذ. ويتلخص الشرط المسبق للحصول على السلطة القانونية لإجراء البحث في وجود أسباب للاعتقاد، على النحو المنصوص عليه في القانون المحلي والضمانات المتعلقة بحقوق الإنسان، بأن هذه البيانات موجودة في مكان معين ومن شأنها أن توفر أدلة على جريمة جنائية محددة.

١٨٦.في إطار البحث عن الأدلة، لا سيما بيانات الكمبيوتر، لا تزال العديد من خصائص البحث التقليدي قائمة في البيئة التكنولوجية الجديدة. على سبيل المثال، يتم جمع البيانات خلال فترة البحث وبالنظر إلى البيانات المتاحة عندئذ. وتنطبق نفس الشروط المسبقة للحصول على سلطة قانونية لإجراء البحث. ولا تختلف درجة الاعتقاد المطلوبة للحصول على الترخيص قانوني لإجراء البحث سواء تعلق الأمر ببيانات في شكل ملموس أو في شكل إلكتروني. وبالمثل، فإن الاعتقاد والبحث يتعلقان بالبيانات الموجودة بالفعل والتي من شأنها أن توفر أدلة على جريمة محددة.

١٨٧.إلا أنه من الضروري، فيما يتعلق بالبحث عن بيانات الكمبيوتر، وضع أحكام إجرائية إضافية بغية تأمين الحصول على بيانات الكمبيوتر بنفس الدرجة من الفعالية كالبحث في سجل مادي للبيانات ومصادرته، وذلك لأسباب عدة: أولا، البيانات متوفرة في شكل غير ملموس، مثلا في شكل كهرومغناطيسي؛ ثانيا، لئن كان من الممكن قراءة البيانات باستخدام أجهزة الكمبيوتر،

فإن مصادرتها وإبعادها بنفس المعنى الوارد بخصوص السجلات الورقية أمر غير ممكن. ويجب مصادرة الدعامة المادية التي تخزن عليها البيانات غير الملموسة (مثل الأقراص الصلبة للكمبيوتر أو الأقراص المرنة) أو حجزها، أو الحصول على نسخة ها إما في شكل ملموس (مثلا عبر طباعتها) أو في شكل غير ملموس، على دعامة مادية (مثلا، على قرص مرن)، قبل التمكن من مصادرة وإبعاد الدعامة الملموسة التي تحتوي على نسخة. وفي الحالتين الأخيرتين، عندما يتم إجراء نسخ من هذه البيانات، تبقى نسخة من البيانات في نظام الكمبيوتر أو جهاز التخزين. وينبغي أن ينص القانون المحلي على صلاحية إجراء هذه النسخ. وثالثا، نظرا لترابط أنظمة الكمبيوتر، قد لا يتم تخزين البيانات في جهاز الكمبيوتر المعين الذي يتم فيه البحث، ولكن قد تكون هذه البيانات في قابلة للنفاذ انطلاقا من هذا النظام. كما يمكن أن تكون مخزنة على جهاز لتخزين البيانات متصل بشكل مباشر بالكمبيوتر، أو بشكل غير مباشر من خلال أنظمة الاتصالات، مثل الإنترنت. وقد يتطلب ذلك أو لا يتطلب سن قوانين جديدة تسمح بتوسيع نطاق البحث ليشمل أي دعامة يتم عليها تخزين البيانات فعليا (أو باستخراج البيانات من تلك الدعامة إلى الكمبيوتر الذي يجري البحث فيه)، أو باستخدام صلاحيات البحث التقليدية بطريقة أكثر تنسيقا وتعجيلا في كلا الحالتين.

١٨٨.تقتضي الفقرة ١ من الأطراف أن تمكن سلطات إنفاذ القانون من النفاذ والبحث في بيانات الكمبيوتر المتاحة سواء داخل نظام الكمبيوتر أو في جزء منه (مثلا جهاز متصل لتخزين البيانات)، أو على دعامة مستقلة لتخزين البيانات (مثلا قرص مدمج أو قرص مرن). وحيث يشير تعريف "نظام الكمبيوتر" الوارد في المادة ١ إلى "أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة"، فإن الفقرة ١ تتعلق بالبحث في نظام حاسوبي وعناصره ذات الصلة التي يمكن اعتبار أنها تشكل نظام كمبيوتر واحد متكامل (مثلا، جهاز الكمبيوتر وآلة الطباعة وأجهزة التخزين ذات الصلة، أو شبكة المنطقة المحلية). علاوة على ذلك، يمكن في بعض الأحيان النفاذ قانونيا إلى البيانات التي يتم تخزينها فعليا على نظام أو جهاز تخزين آخر من خلال نظام الكمبيوتر الذي يتم فيه البحث عن طريق إنشاء رابط مع أنظمة كمبيوتر مستقلة أخرى. وتتناول الفقرة ٢ هذه الحالة التي تنطوي على روابط مع أنظمة حاسوبية أخرى عن طريق شبكات الاتصالات داخل نفس الإقليم (مثل شبكة المنطقة الواسعة أو شبكة الإنترنت).

١٨٩.على الرغم من إمكانية إجراء البحث في " دعامة تخزين بيانات الكمبيوتر التي يمكن أن تكون بيانات كمبيوتر مخزنة داخلها " (الفقرة ١ (ب)) ومصادرتها من خلال استخدام صلاحيات البحث التقليدية، غالبا ما يتطلب تنفيذ البحث على الكمبيوتر البحث في نظام الكمبيوتر وأي دعامة لتخزين بيانات الكمبيوتر ذات الصلة (مثل الأقراص المرنة) توجد في منطقة في الجوار المباشر لنظام الكمبيوتر. ونظرا لهذه العلاقة، تنص الفقرة ١ على سلطة قانونية شاملة تغطي كلا الحالتين.

١٩٠.تنطبق المادة ١٩ على بيانات الكمبيوتر المخزنة. وفي هذا الصدد، يطرح السؤال ما إذا كانت رسالة البريد الإلكتروني غير المفتوحة التي تظل في علبة البريد من مزود خدمة الإنترنت إلى أن يقوم المرسل إليه بتحميلها على حاسوبه، يجب أن تعتبر بيانات كمبيوتر مخزنة أم بيانات عابرة. وبموجب قانون بعض الأطراف، تعتبر رسالة البريد الإلكتروني هاته جزءا من الاتصال، وبالتالي لا يمكن الحصول على مضمونها إلا من خلال تطبيق صلاحية الاعتراض، بينما تعتبر أنظمة قانونية اخرى هذه الرسالة بمثابة بيانات مخزنة تنطبق عليها المادة ١٩. لذلك، ينبغي على الأطراف مراجعة قوانينها فيما يتعلق بهذه المسألة لتحديد ما هو ملائم في أنظمتها القانونية المحلية.

١٩١.ثمة إشارة إلى عبارة "البحث أو النفاذ بطريقة مماثلة". ويحمل استخدام كلمة "البحث" التقليدية في طياته فكرة ممارسة الدولة للقوة القسرية، ويشير إلى أن الصلاحية المشار إليها في هذه المادة مشابهة لصلاحية البحث التقليدي. ويعني مصطلح "البحث" السعي إلى إيجاد بيانات أو قراءتها أو فحصها أو مراجعتها، ويتضمن مفاهيم البحث عن البيانات والبحث في (فحص) البيانات. ومن ناحية أخرى، يحمل مصطلح "النفاذ" معنى محايدا، لكنه يعكس بمزيد من الدقة المصطلحات الحاسوبية. ويستخدم كلا المصطلحان من أجل إقران المفاهيم التقليدية بالمصطلحات الحديثة.

١٩٢.وردت الإشارة إلى عبارة "في إقليمها" كتذكير بأن هذا الحكم، على غرار جميع المواد الواردة في هذا القسم، لا يتعلق إلا بالتدابير التي يلزم اتخاذها على الصعيد الوطني.

١٩٣.تسمح الفقرة ٢ لسلطات التحقيق بتوسيع بحثها أو النفاذ بطريقة أخرى إلى نظام كمبيوتر آخر أو جزء منه عندما تكون لديها أسباب تدعو إلى الاعتقاد بأن البيانات المطلوبة مخزنة في ذلك النظام. لكن، يجب أن يكون نظام الكمبيوتر الآخر أو الجزء منه متواجدا أيضا "في أراضيها".

١٩٤.لا تنص الاتفاقية على كيفية السماح بتوسيع عملية بحث أو إجرائها. ويترك هذا الأمر للقانون المحلي. ومن الأمثلة على الشروط الممكنة نذكر ما يلي: تمكين السلطة القضائية أو أي سلطة أخرى التي تأذن بالبحث في نظام كمبيوتر معين، بترخيص توسيع البحث أو النفاذ بطريقة أخرى إلى نظام متصل إذا كان لديها أسباب للاعتقاد (في حدود الدرجة التي يقتضيها القانون الوطني وضمانات حقوق الإنسان) أن نظام الكمبيوتر المتصل قد يحتوي على البيانات المحددة التي يجري البحث عنها؛ أو تمكين سلطات التحقيق من توسيع نطاق البحث المرخص أو النفاذ بطريقة مماثلة إلى نظام كمبيوتر معين ليشمل نظام كمبيوتر متصل عندما توجد أسباب مماثلة للاعتقاد بأن البيانات المحددة التي يجري البحث عنها مخزنة في نظام الكمبيوتر الآخر؛ أو ممارسة صلاحيات البحث أو النفاذ بطريقة مماثلة في كلا الحالتين بطريقة منسقة ومعجلة. وفي جميع الحالات، يجب أن تكون البيانات الواجب البحث فيها قابلة للنفاذ من الناحية القانونية أو متاحة لنظام الكمبيوتر الأولي.

١٩٥.لا تتناول هذه المادة "عمليات البحث والمصادرة العابرة للحدود" التي يمكن للدول بموجبها البحث عن بيانات ومصادرتها في أراضي دول أخرى دون الاضطرار إلى المرور عبر القنوات المعتادة للمساعدة القانونية المتبادلة. وتناقش هذه المسألة أدناه في الفصل المتعلق بالتعاون الدولي.

١٩٦.تتناول الفقرة ٣ مسائل تمكين السلطات المختصة من مصادرة أو تأمين بيانات الكمبيوتر التي تم البحث فيها أو النفاذ إليها بطريقة مماثلة بموجب الفقرتين ١ أو ٢. ويشمل ذلك صلاحية مصادرة معدات الكمبيوتر ودعائم تخزين بيانات الكمبيوتر. في حالات معينة، على سبيل المثال عندما يتم تخزين البيانات على أنظمة تشغيل فريدة من نوعها بحيث لا يمكن استنساخها، فلا يمكن إلا مصادرة حامل البيانات برمته. وقد يكون ذلك ضروريا أيضا عندما يتعين فحص حامل البيانات من أجل استخراج البيانات القديمة التي تم استبدالها والكتابة عليها لكن مع ذلك تركت آثارا على حامل للبيانات.

١٩٧.يعني مصطلح "المصادرة" في هذه الاتفاقية، حجز وإبعاد الدعامة المادية التي سجلت عليها البيانات أو المعلومات، أو إجراء نسخة من هذه البيانات أو المعلومات والاحتفاظ بها. ويشمل مصطلح "المصادرة" استخدام أو حجز البرامج اللازمة للنفاذ إلى البيانات التي تتم مصادرتها. فضلا عن استخدام مصطلح "المصادرة" التقليدي، تم إدراج مصطلح "التأمين بطريقة مماثلة" ليشمل الوسائل الأخرى التي يتم من خلالها إزالة بيانات غير ملموسة، التي يتعذر النفاذ إليها أو التي يتم التحكم فيها بطريقة أخرى في بيئة الحاسوب. وبما أن التدابير تتعلق بالبيانات غير الملموسة المخزنة، قد تقتضي السلطات المختصة اتخاذ تدابير إضافية لتأمين البيانات؛ بمعنى "الحفاظ على سلامة البيانات"، أو الحفاظ على "سلسلة احتجاز" البيانات، وهذا يعني أن البيانات التي يتم استنساخها أو إزالتها يتم الاحتفاظ بها في الدولة التي وجدت فيها وقت مصادرتها وحفظها من أي تغيير خلال فترة الدعاوى الجنائية. وتشير هذه العبارة إلى التحكم في البيانات أو إبعادها.

١٩٨.يشمل تعذر النفاذ إلى البيانات تشفير البيانات أو منع أي شخص من النفاذ الفني إليها. ويمكن تطبيق هذا التدبير بطريقة مفيدة في الحالات التي تنطوي على خطر أو ضرر اجتماعيين، مثل برامج الفيروسات أو التعليمات المتعلقة بكيفية صنع الفيروسات أو القنابل، أو عندما تكون البيانات أو محتواها غير قانونية، مثل المواد الإباحية المتعلقة بالأطفال. ويقصد من مصطلح "إزالة" التعبير عن فكرة أنه عندما يتم إزالة البيانات أو يتعذر النفاذ إليها، فإنه لا يتم تدميرها، ولكنها تظل موجودة. وبالتالي، يحرم المشتبه به مؤقتا من البيانات، مع إمكانية إعادتها وفقا لنتيجة التحقيق الجنائي أو الدعوى الجنائية.

١٩٩.وبالتالي، تحقق مصادرة البيانات أو تأمينها بطريقة مماثلة وظيفتين: ١) جمع الأدلة، مثلا عن طريق استنساخ البيانات، أو ٢) مصادرة البيانات، مثلا من خلال استنساخها وجعل نسختها الأصلية غير قابلة للنفاذ أو عن طريق إزالتها. ولا تنطوي المصادرة على الحذف النهائي للبيانات المصادرة.

٢٠٠.تدرج الفقرة ٤ تدبيرا قسريا يرمي إلى تيسير البحث عن بيانات الكمبيوتر ومصادرتها. وتتناول الإشكال العملي المطروح عندما يكون من الصعب النفاذ إلى البيانات المطلوبة كدليل وتحديدها بسبب كمية البيانات التي يمكن معالجتها وتخزينها، ونشر التدابير الأمنية، فضلا عن طبيعة العمليات الحاسوبية. وتعترف هذه الفقرة أن الأمر قد يقتضي استشارة المسؤولين عن إدارة النظام، الذين لديهم معرفة خاصة بنظام الكمبيوتر، بشأن الأساليب الفنية لإجراء البحث بأفضل طريقة. وبالتالي، فإن يسمح هذا الحكم لسلطات إنفاذ القانون بإرغام مسؤول النظام على تقديم المساعدة، بالقدر المعقول، في إجراء عمليات البحث والمصادرة.

٢٠١.لا تعتبر هذه الصلاحية مفيدة لسلطات التحقيق فقط. في غياب هذا النوع من التعاون، يمكن أن تقضي سلطات التحقيق فترات طويلة في أماكن البحث وأن تمنع النفاذ إلى نظام الكمبيوتر أثناء إجراء البحث، مما قد يشكل عبئا اقتصاديا على الأنشطة التجارية المشروعة أو العملاء والمنخرطين الذين يحرمون من النفاذ إلى البيانات خلال هذه الفترة. ولعل إيجاد وسيلة لتعاون الأشخاص ذوي الخبرة من شأنه أن يساعد في تعزيز فعالية عمليات البحث وكفاءتها من حيث التكلفة، سواء بالنسبة لسلطات إنفاذ القانون أو للأفراد الأبرياء المتضررين. فضلا عن ذلك، يؤدي الإجبار القانوني للمسؤول عن إدارة النظام على المساعدة إلى إعفائه من أي التزامات تعاقدية أو غيرها من الالتزامات بعدم الكشف عن البيانات.

٢٠٢.المعلومات التي يمكن الأمر بتقديمها هي تلك المعلومات اللازمة لتمكين إجراء عمليات البحث والمصادرة أو النفاذ أو التأمين بطريقة مماثلة. غير أن تقديم هذه المعلومات يقتصر على ما هو "معقول". وفي بعض الحالات، يمكن أن يشمل الحكم المعقول الإفصاح عن كلمة السر أو أي تدابير أمنية أخرى لسلطات التحقيق. ومع ذلك، في ظروف أخرى، قد لا يكون ذلك معقولا؛ على سبيل المثال، عندما يؤدي الكشف عن كلمة السر أو أي تدبير أمني آخر إلى تهديد غير معقول لخصوصية مستخدمين آخرين أو بيانات أخرى غير مرخص بالبحث فيها. وفي مثل هذه الحالة، يمكن أن ينطوي توفير "المعلومات الضرورية" على الكشف عن البيانات الفعلية التي تلتمسها السلطات المختصة، في شكل يمكن فهمه وقراءته.

٢٠٣.بموجب الفقرة ٥ من هذه المادة، تخضع هذه التدابير للشروط والضمانات المنصوص عليها في القانون المحلي على أساس المادة ١٥ من هذه الاتفاقية. وقد تشمل هذه الشروط أحكاما تتعلق بمشاركة الشهود والخبراء وتعويضهم المالي.

٢٠٤.واصل القائمون على الصياغة في إطار الفقرة ٥ مناقشة ضرورة إشعار الأطراف المهتمة بعملية البحث المنجزة على الإنترنت حيث أنه قد لا يكون واضحا أنه تم تفتيش بيانات ومصادرتها (استنساخها) بقدر وضوح ذلك خارج الإنترنت، حيث يظهر جليا أن الأشياء المصادرة غائبة ماديا. ولا تنص قوانين بعض الأطراف على إلزامية الإشعار في حال البحث التقليدي. وبالتالي، إذا اقتضت الاتفاقية الإخطار فيما يتعلق بالبحث في الكمبيوتر، فإن من شأن ذلك أن يخلق تباينا في قوانين هذه الأطراف. ومن جهة أخرى، قد تعتبر بعض الأطراف أن الإشعار سمة أساسية من سمات هذا الإجراء، من مواصلة التمييز بين عملية البحث في الكمبيوتر عن بيانات مخزنة (التي لا يتوقع منها عموما أن تكون تدبيرا سريا) وعملية اعتراض البيانات المتدفقة (التي تكون عملية سرية، انظر المادتين ٢٠ و٢١). ومن تم، ترك تحديد مسألة الإشعار للقوانين المحلية. عندما تنظر الأطراف في إمكانية وضع نظام إلزامي لإشعار الأشخاص المعنيين، ينبغي ألا يغيب عن البال أن هذا الإشعار قد يلحق الضرر بالتحقيق. وفي حال وجود خطر من هذا القبيل، وجب النظر في تأجيل الإشعار.

الباب ٥ – جمع بيانات الكمبيوتر في الوقت الحقيقي

٢٠٥.تنص المادتان ٢٠ و٢١ على جمع بيانات الحركة في الوقت الحقيقي والاعتراض في الوقت الحقيقي لبيانات المحتوى المرتبطة باتصالات محددة التي ينقلها عبر نظام الكمبيوتر. وتتناول هذه الأحكام قيام السلطات المختصة بجمع واعتراض هذه البيانات في الوقت الحقيقي، فضلا عن جمعها أو اعتراضها من قبل مقدمي الخدمات. كما تتناول التزامات السرية.

٢٠٦.يشير اعتراض الاتصالات السلكية واللاسلكية عادة إلى شبكات الاتصالات التقليدية. ويمكن أن تشمل هذه الشبكات البنى التحتية للكابلات، سواء الكابلات السلكية أو البصرية، وكذلك الوصلات البينية مع الشبكات اللاسلكية، بما في ذلك أنظمة الهاتف النقال وأنظمة إرسال الموجات الدقيقة. وحاليا، تتم الاتصالات النقالة أيضا بواسطة نظام الشبكات الساتلية (الأقمار الصناعية) الخاصة. ويمكن أن تتألف شبكات الكمبيوتر أيضا من بنية تحتية مستقلة للكابلات الثابتة، لكنها تشتغل

بشكل متزايد كشبكة افتراضية عن طريق وصلات تتم من خلال البنى التحتية للاتصالات السلكية واللاسلكية، مما يسمح بإنشاء شبكات الكمبيوتر أو روابط الشبكات التي تكون عالمية بطبيعتها. وقد أدت التقائية تكنولوجيات الاتصالات والمعلومات إلى تلاشي إمكانية التمييز بين الاتصالات السلكية واللاسلكية والاتصالات عبر الكمبيوتر. وبالتالي، لا يقيد تعريف "نظام الكمبيوتر" الوارد في المادة ١ طريقة ترابط الأجهزة أو مجموعة من الأجهزة. ومن ثم، تنطبق المادتان ٢٠ و٢١ على الاتصالات المحددة المرسلة بواسطة نظام الكمبيوتر، والتي يمكن أن تشمل نقل الاتصال من خلال شبكات الاتصالات قبل استلامها بواسطة نظام كمبيوتر آخر.

٢٠٧.لا تميز المادتان ٢٠ و٢١ بين نظام الاتصال أو الكمبيوتر العام أو الخاص أو بين استخدام الأنظمة وخدمات الاتصالات المعروضة من قبل الجمهور العام أو مجموعات مغلقة من المستخدمين أو أطراف خاصة. ويشير تعريف "مقدم الخدمة" الوارد في المادة ١ إلى الهيئات العامة والخاصة التي توفر لمستخدمي خدماتها القدرة على الاتصال عن طريق نظام كمبيوتر.

٢٠٨.يحكم هذا الباب جمع الأدلة الواردة في الاتصالات المولدة في الوقت الحاضر، والتي تجمع في وقت إجراء الاتصال (أي "الوقت الحقيقي"). وتعتبر هذه البيانات غير ملموسة من حيث الشكل (مثلا، في شكل إرسالات صوتية أو نبضات إلكترونية). ولا يتأثر تدفق البيانات بشكل هام من عملية جمع البيانات، ويصل الاتصال إلى المتلقي المقصود منه. وبدلا من المصادرة الفعلية للبيانات، يتم تسجيل (أي استنساخ) البيانات التي يتم إرسالها عبر الاتصال. ويحدث جمع هذه الأدلة خلال فترة معينة من الزمن. ويجب التوفر على صلاحية قانونية ترخص بجمع البيانات المتعلقة بحدث مستقبلي (أي إرسال بيانات في المستقبل).

٢٠٩.ثمة نوعان من البيانات التي يمكن جمعها: بيانات الحركة وبيانات المحتوى. وتعرف المادة ١ (د) "بيانات الحركة " بأنها أي بيانات كومبيوتر متعلقة باتصال عن طريق نظام الكومبيوتر والتي تنشأ عن نظام كومبيوتر يشكل جزءاً في سلسلة الاتصالات، توضح المنشأ والوجهة، والمسار، والزمن، والتاريخ، والحجم، والمدة، أو نوع الخدمة الأساسية. لكن الاتفاقية لم تعرف "بيانات المحتوى" إلا أنها تشير إلى محتوى الاتصال؛ أي معنى أو فحوى الاتصال، الرسالة أو المعلومات التي ينقلها الاتصال (غير بيانات الحركة).

٢١٠.في العديد من الدول، ثمة تمييز بين اعتراض بيانات المحتوى في الوقت الحقيقي وجمع بيانات الحركة في الوقت الحقيقي من حيث الشروط القانونية المسبقة المطلوبة للترخيص بإجراء هذا التحقيق وبين الجرائم التي يمكن أن يطبق عليها هذا التدبير. ولئن كانت الدول تعرف بإمكانية تواجد مصالح ذات الصلة بالخصوصية في كلا النوعين من البيانات، فإنها العديد من الدول تعتبر أن مصالح الخصوصية المرتبطة ببيانات المحتوى أكبر بالنظر لطبيعة محتوى الاتصال أو الرسالة. وبالتالي، يمكن فرض قيود على جمع بيانات المحتوى في الوقت الحقيقي أكثر من على بيانات الحركة. وإذ تفعل الاتفاقية الاعتراف بجمع وتسجيل البيانات في كلتا الحالتين، فإنها تشير، من أجل المساعدة في الاعتراف بهذا التمييز لدى هذه الدول، في عناوين المواد إلى جمع بيانات الحركة باعتباره "جمع في الوقت الحقيقي" وإلى جمع بيانات المحتوى باعتباره "اعتراض في الوقت الحقيقي" بشكل معياري.

٢١١.في بعض الدول، لا يفرق التشريع القائم بين جمع بيانات الحركة واعتراض بيانات المحتوى، إما بسبب عدم التمييز في القانون بين الاختلافات في مصالح الخصوصية أو نظرا للتشابه الكبير في تقنيات الجمع التكنولوجي لكلا التدبيرين. وبالتالي، تكون الشروط القانونية المطلوبة للترخيص باتخاذ التدابير، والجرائم التي يمكن بشأنها استخدام تلك التدابير، هي نفسها. وتعترف الاتفاقية أيضا بهذا الوضع من خلال الاستخدام الوظيفي المشترك لمصطلح "جمع أو تسجيل" في النص الراهن لكل من المادتين ٢٠ و٢١.

٢١٢.بخصوص اعتراض بيانات المحتوى في الوقت الحقيقي، ينص القانون في كثير من الأحيان على أن التدبير متاح فقط فيما يتعلق بالتحقيق في الجرائم الخطيرة أو فئات من الجرائم الخطيرة. وتحدد هذه الجرائم في القانون المحلي على أنها خطيرة لهذا الغرض، غالبا من خلال إدراجها في قائمة الجرائم المنطبقة أو بإدراجها في هذه الفئة بالإشارة إلى عقوبة حبسية قصوى تنطبق على الجريمة. لذلك، تنص المادة ٢١ تحديدا، فيما يتعلق باعتراض بيانات المحتوى، على أن الأطراف مطالبة فقط بوضع التدبير "فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي".

٢١٣.من ناحية أخرى، تعتبر المادة ٢٠ المتعلقة بجمع بيانات الحركة غير محدودة ومن حيث المبدأ تنطبق على أي جريمة جنائية تشملها الاتفاقية. غير أن الفقرة ٣ من المادة ١٤ تنص على أنه يجوز لأي طرف أن يحتفظ بالحق في تطبيق التدبير فقط على الجرائم أو فئات الجرائم المحددة في التحفظ، شريطة ألا يكون نطاق الجرائم أو فئات الجرائم أكثر تقييدا من نطاق الجرائم التي يطبق عليها تدبير اعتراض بيانات المحتوى. ومع ذلك، ينبغي للطرف، عند استخدام هذا التحفظ، النظر في تقييد هذا التحفظ من أجل تمكين أوسع نطاق من تطبيق تدبير جمع بيانات الحركة.

٢١٤.بالنسبة لبعض الدول، لا تعتبر عادة الجرائم المقررة في الاتفاقية خطيرة بما فيه الكفاية للترخيص باعتراض بيانات المحتوى أو في بعض الحالات حتى جمع بيانات الحركة. ومع ذلك، فإن هذه التقنيات غالبا ما تكون حاسمة بالنسبة للتحقيق في بعض الجرائم المقررة في الاتفاقية، مثل تلك التي تنطوي على النفاذ غير المشروع إلى أنظمة الكمبيوتر، وتوزيع الفيروسات والمواد الإباحية عن الأطفال. على سبيل المثال، لا يمكن في بعض الحالات تحديد مصدر التطفل أو التوزيع دون جمع بيانات الحركة في الوقت الفعلي. في بعض الحالات، لا يمكن اكتشاف طبيعة الاتصال دون اعتراض بيانات المحتوى في الوقت الحقيقي. وتنطوي هذه الجرائم، بطبيعتها أو حسب وسائل نقلها، على استخدام تكنولوجيات الكمبيوتر؛ لذلك ينبغي السماح باستخدام الوسائل التكنولوجية للتحقيق في هذه الجرائم. غير أن الاتفاقية تترك تحديد نطاق هذا التدبير للقانون المحلي بالنظر للحساسيات المحيطة بمسألة اعتراض بيانات المحتوى. وبما أن بعض البلدان تربط في قوانينها جمع بيانات الحركة باعتراض بيانات المحتوى، يسمح بإمكانية التحفظ على تقييد تطبيق التدبير السابق، ولكن ليس لدرجة من شأنها أن تقيد تدبير اعتراض بيانات المحتوى في الوقت الفعلي. ومع ذلك، ينبغي للأطراف أن تنظر في تطبيق التدبيرين على الجرائم المنصوص عليها في الاتفاقية في القسم ١ من الفصل الثاني، بغية توفير وسيلة فعالة للتحقيق في جرائم الكمبيوتر والجرائم المتصلة بالكمبيوتر.

٢١٥.تخضع الشروط والضمانات المتعلقة بالصلاحيات والإجراءات المتعلقة باعتراض بيانات المحتوى في الوقت الحقيقي وجمع بيانات الحركة في الوقت الحقيقي لأحكام المادتين ١٤ و١٥. وحيث أن اعتراض بيانات المحتوى تدبير بالغ التدخل في الحياة الخاصة، يقتضى توفير ضمانات صارمة لضمان توازن مناسب بين مصالح العدالة والحقوق الأساسية للفرد. وفي مجال الاعتراض، لا تنص هذه الاتفاقية على ضمانات محددة غير حصر ترخيص اعتراض بيانات المحتوى على التحقيقات في الجرائم الجنائية الخطيرة كما هو محدد في القانون المحلي. ومع ذلك، تتلخص الشروط والضمانات الهامة في هذا المجال والمطبقة في القوانين المحلية، في ما يلي: المراقبة القضائية أو أي مراقبة مستقلة أخرى؛ مواصفات الاتصالات أو الأشخاص موضوع الاعتراض (مثلا، الأسباب القانونية التي تبرر اتخاذ التدبير؛ وتدابير أخرى أقل تطفلا غير مفعلة)؛ تحديد مدة الاعتراض؛ حق الانتصاف. وتعكس العديد من هذه الضمانات ما ورد في الاتفاقية الأوروبية لحقوق الإنسان وفقهها القضائي اللاحق (انظر الأحكام الصادرة في قضية كلاس[5] (Klass) وكروسلين[6] (Kruslin) وهوفيج[7] (Huvig) ومالون[8] (Malone) وهالفورد[9] (Halford) ولامبرت[10] (Lambert). بعض هذه الضمانات تنطبق أيضا على جمع بيانات حركة المرور في الوقت الحقيقي.

جمع بيانات الحركة في الوقت الحقيقي (المادة ٢٠)

٢١٦.في كثير من الأحيان، قد تصبح بيانات الحركة المرور التاريخية غير متاحة أو غير صميمية عندما يقوم الدخيل بتغيير مسار الاتصال. لذلك، يعتبر جمع بيانات الحركة في الوقت الحقيقي إجراء بالغ الأهمية بالنسبة للتحقيق. وتتناول المادة ٢٠ موضوع جمع وتسجيل بيانات الحركة في الوقت الحقيقي لأغراض تحقيقات أو إجراءات جنائية محددة.

٢١٧.عادة، كان جمع بيانات الحركة ذات الصلة بالاتصالات السلكية واللاسلكية (مثل المحادثات الهاتفية) أداة مفيدة للتحقيق من أجل تحديد مصدر أو وجهة الاتصال (مثل أرقام الهواتف) وبيانات ذات الصلة (مثل الوقت والتاريخ والمدة) بأنواع مختلفة من الاتصالات غير القانونية (من قبيل التهديدات والمضايقات الإجرامية، والمؤامرة الجنائية، والادعاءات الكاذبة

---

[5] الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية كلاس (Klass) وآخرين ضد ألمانيا، أ.٢٨، ٦ سبتمبر/أيلول ١٩٧٨.

[6] الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية كروسلين (Kruslin) ضد فرنسا، ١٧٦-أ، ٢٤ أبريل/نيسان ١٩٩٠.

[7] الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية هوفيج (Huvig) ضد فرنسا، ١٧٦-ب، ٢٤ أبريل/نيسان ١٩٩٠

[8] الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية مالون (Malone) ضد المملكة المتحدة، أ.٨٢، ٢ أغسطس/آب ١٩٨٤.

[9] الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية هالفورد (Halford) ضد المملكة المتحدة، تقارير ١٩٩٧ – الجزء ٣، ٢٥ يونيو/حزيران ١٩٩٧.

[10] الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية لامبرت (Lambert) ضد فرنسا، تقارير ١٩٩٨ – الجزء ٤، ٢٤ أغسطس/آب ١٩٩٨.

الاحتيالية)، وباتصالات توفر أدلة على جرائم سابقة أو مستقبلية (مثل الإتجار بالمخدرات، والقتل والجرائم الاقتصادية وغيرها).

٢١٨.يمكن أن تشكل أو توفر الاتصالات عبر الكمبيوتر أدلة على نفس أنواع الإجرام، إلا أنه بالنظر إلى القدرة الهائلة لتكنولوجيا الحاسوب على نقل كميات هائلة من البيانات، بما في ذلك النصوص المكتوبة والصور المرئية والصوت، فإنها توفر أيضا إمكانيات أكبر لارتكاب جرائم تنطوي على توزيع محتوى غير قانوني (مثل المواد الإباحية المتعلقة بالأطفال). وبالمثل، وحيث أن أجهزة الكمبيوتر توفر إمكانية تخزين كميات هائلة من البيانات، غالبا ذات طابع خاص، فإن احتمال إلحاق الضرر، سواء كان اقتصاديا، اجتماعيا أو شخصيا، يكون مهما إذا تم التدخل في سلامة هذه البيانات. علاوة على ذلك، وبما أن علم تكنولوجيا الحاسوب قائم على معالجة البيانات، سواء كمنتج نهائي أو كجزء من وظيفته التشغيلية (مثل تنفيذ برامج الحاسوب)، فإن أي تدخل في هذه البيانات يمكن أن يسفر عن آثار كارثية على التشغيل السليم لأنظمة الكمبيوتر. وعندما يرتكب توزيع غير مشروع للمواد الإباحية المتعلقة بالأطفال أو نفاذ غير مشروع إلى نظام كمبيوتر أو تدخل في حسن الاشتغال السليم لنظام كمبيوتر أو في سلامة البيانات، لا سيما من مسافة بعيدة عن طريق الإنترنت مثلا، يصبح من الضروري تقفي مسار الاتصالات من الضحية إلى الجاني. لذلك، تكتسي القدرة على جمع بيانات الحركة المرور المرتبطة بالاتصالات عبر الكمبيوتر نفس القدر من الأهمية، إن لم تكن أكثر أهمية، التي تولى للاتصالات التقليدية المحضة. ويمكن لتقنية التحقيق هاته أن تربط بين وقت وتاريخ ومصدر ووجهة اتصالات المشتبه به بوقت اقتحام أنظمة الضحايا، وأن تحدد ضحايا آخرين أو تظهر روابط مع شركاء.

٢١٩.بموجب هذه المادة، يجب أن ترتبط بيانات الحركة المعنية باتصالات محددة في إقليم الطرف. وقد استخدم مصطلح "الاتصالات" المحددة في صيغة الجمع، حيث قد يلزم جمع بيانات الحركة الخاصة بعدة اتصالات من أجل تحديد الشخص المرسل (المصدر) أو المتلقي (الوجهة) (على سبيل المثال، عندما تكون هنالك أسرة معيشية يستخدم فيها عدة أشخاص مختلفين نفس أجهزة الاتصالات، قد يكون من الضروري ربط عدة اتصالات باحتمال استخدام أفراد هذه الأسرة لنظام الكمبيوتر). ومع ذلك، يجب تحديد الاتصالات التي يمكن جمع أو تسجيل بيانات الحركة بشأنها. وبالتالي، لا تقتضي الاتفاقية ولا تسمح بالمراقبة العامة أو العشوائية وجمع كميات كبيرة من بيانات الحركة. كما أنها لا ترخص بحالة "تصيد المعلومات بنيةٍ مبيتة" التي يتوخى منها اكتشاف أنشطة إجرامية، بدلا من التحقيق في حالات محددة من الجرائم. ويجب أن يرد في الأمر القضائي أو أي أمر آخر يأذن بالجمع تحديد للاتصالات المعنية بجمع بيانات الحركة.

٢٢٠.رهنا بأحكام الفقرة ٢، تلزم الأطراف، بموجب الفقرة ١(أ)، بأن تكفل لسلطاتها المختصة القدرة على جمع بيانات الحركة أو تسجيلها بالوسائل التقنية. ولا تحدد هذه المادة من الناحية التقنية كيفية إجراء عملية الجمع، كما لا تحدد أي التزامات من الناحية التقنية.

٢٢١.بالإضافة إلى ذلك، فإن الأطراف ملزمة، بموجب الفقرة ١(ب)، بضمان أن سلطاتها المختصة تتمتع بصلاحية إجبار مقدم خدمة على جمع بيانات الحركة أو تسجيلها أو التعاون مع السلطات المختصة في جمع أو تسجيل تلك البيانات. ولا ينطبق هذا الالتزام فيما يتعلق بمقدمي الخدمات إلا في حدود القدرات التقنية المتوفرة لدى مقدم الخدمة للقيام بالجمع أو التسجيل أو التعاون والمساعدة. ولا تلزم المادة مقدمي الخدمات بضمان امتلاكهم القدرة التقنية على القيام بالجمع أو التسجيل أو التعاون أو المساعدة. كما أنها لا تقتضي منهم الحصول على معدات جديدة أو تطويرها، أو استئجار دعم الخبراء أو الانخراط في إعادة تصميم مكلفة لأنظمتها. إلا أن المادة تقتضي منها، في حال توفرت لأنظمتها وموظفيها القدرة التقنية على توفير خدمة الجمع أو التسجيل أو التعاون أو المساعدة، اتخاذ التدابير اللازمة لاستخدام هذه القدرة. على سبيل المثال، قد يكون نظام مقدم الخدمة أو تكون برامج الكمبيوتر التي يمتلكها مصممة بشكل يسمح باتخاذ هذه التدابير، لكن لا يتم تنفيذها عادة أو استخدامها في السياق العادي لاشتغال مقدم الخدمة. وبالتالي، يمكن أن تطالب هذه المادة مقدم الخدمة بتفعيل أو تشغيل هذه التدابير، وفقا لما يقتضيه القانون.

٢٢٢.لما كان هذا التدبير من التدابير التي يتعين تنفيذها على الصعيد الوطني، تطبق التدابير على جمع أو تسجيل اتصالات محددة في إقليم الطرف. وهكذا، تنطبق الالتزامات عموما، من الناحية العملية، حيثما يتوفر مقدم الخدمة على بنى تحتية أو معدات مادية في ذلك الإقليم تكون قادرة على اتخاذ تلك التدابير، دون اشتراط أن يكون ذلك في موقع عملياته الرئيسية أو مقره الرئيسي. ولأغراض هذه الاتفاقية، من المفهوم أن الاتصال يتم في إقليم طرف عندما يكون أحد أطراف الاتصال

(من البشر أو الحواسيب) متواجدا في ذلك الإقليم أو عندما يكون جهاز الكمبيوتر أو معدات الاتصالات التي يمر منها الاتصال موجودا داخل ذلك الإقليم.

٢٢٣. بصفة عامة، لا تعتبر الإمكانيتان المنصوص عليها لجمع بيانات الحركة في الفقرتين ١(أ) و(ب) بدائل. وباستثناء ما هو منصوص عليه في الفقرة ٢، يجب على الطرف أن يكفل إمكانية تنفيذ كلا التدبيرين. وهذا الشرط ضروري لأنه في حال عدم توفر مقدم الخدمة على القدرة التقنية لإجراء جمع أو تسجيل بيانات الحركة (١"ب")، وجب على الطرف التوفر على إمكانية اضطلاع سلطات إنفاذ القانون بنفسها بهذه المهمة (١"أ"). وبالمثل، فإن الالتزام بموجب الفقرة ١(ب)"٢" بالتعاون مع السلطات المختصة في جمع بيانات الحركة أو تسجيلها أمر لا معنى له إن لم تكن السلطات المختصة مخولة لجمع بيانات الحركة أو تسجيلها بنفسها. فضلا عن ذلك، عندما يتعلق الأمر ببعض شبكات المناطق المحلية (LANs)، حيث قد لا يوجد مقدم الخدمة، فإن الطريقة الوحيدة للجمع أو التسجيل التي يتعين القيام بها هي أن تنجزها سلطات التحقيق بنفسها. ولا يلزم استخدام كل من التدبيرين الواردين في الفقرتين ١(أ) و(ب) في كل مرة، لكن تطالب المادة بتوافر هاتين الطريقتين.

٢٢٤. طرح هذا الالتزام المزدوج، مع ذلك، صعوبات بالنسبة لبعض الدول التي لم تكن سلطات إنفاذ القانون فيها قادرة إلا على اعتراض البيانات في نظم الاتصالات السلكية واللاسلكية من خلال مساعدة مقدم الخدمة أو لم تتمكن من إجراء ذلك بشكل سري دون معرفة مقدم الخدمة على الأقل. لهذا السبب، تضمنت الفقرة ٢ هذه الحالة. ففي الحالات التي لا يمكن فيها للطرف، بسبب "المبادئ الثابتة في نظامه القانوني المحلي"، أن يتبنى التدابير المشار إليها في الفقرة ١(أ)، يمكنه أن يعتمد بدلا من ذلك مقاربة مختلفة، من قبيل الاكتفاء بإلزام مقدمي الخدمات بتوفير المرافق التقنية الضرورية لضمان جمع بيانات الحركة في الوقت الحقيقي من قبل سلطات إنفاذ القانون. وفي هذه الحالة، تبقى كافة القيود الأخرى المتعلقة بالإقليم، وخصوصية الاتصالات واستخدام الوسائل التقنية سارية.

٢٢٥. على غرار اعتراض بيانات المحتوى في الوقت الحقيقي، فإن جمع بيانات الحركة في الوقت الحقيقي لا يكون فعالا إلا إذا نفذ دون معرفة الأشخاص الذين يجري التحقيق بشأنهم. ويكون الاعتراض سريا ويجب أن تنفيذه بطريقة تجعل الأطراف المنخرطة في الاتصال على غفلة من العملية المنجزة. لذلك، يجب على مقدمي الخدمات وموظفيهم الذين يعلمون بالاعتراض المنجز أن يلتزموا بالسرية حتى يتسنى تنفيذ الإجراء على نحو فعال.

٢٢٦. تلزم الفقرة ٣ الأطراف بأن تعتمد ما يلزم من تدابير تشريعية أو غيرها من التدابير لإجبار مقدم الخدمة على الحفاظ على سرية تنفيذ أي من التدابير المنصوص عليها في هذه المادة وأي معلومات تتعلق بهذا الإجراء بشأن جمع بيانات الحركة في الوقت الفعلي. ولا يكفل هذا الحكم سرية التحقيق فحسب، بل يعفي أيضا مقدم الخدمة من أي التزامات تعاقدية أو التزامات قانونية أخرى بإشعار المنخرطين بجمع بيانات تخصهم. ويمكن تنفيذ الفقرة ٣ من خلال إنشاء التزامات واضحة في القانون. ومن ناحية أخرى، يمكن للطرف أن يكفل سرية التدبير على أساس أحكام قانونية محلية أخرى، من قبيل سلطة محاكمة الأشخاص الذين يساعدون المجرمين بإعاقة سير العدالة عن طريق إخبارهم بالتدبير. وعلى الرغم من أن شرط السرية المحددة (مع فرض عقوبات فعالة في حال الانتهاك) يعتبر إجراء مفضلا، فإن استخدام جريمة إعاقة سير العدالة يمكن أن يكون وسيلة بديلة لمنع الكشف غير الملائم، وبالتالي يكون كافيا أيضا لتنفيذ هذه الفقرة. وفي الحالات التي تنشأ فيها التزامات صريحة بالسرية، تخضع هذه الالتزامات للشروط والضمانات المنصوص عليها في المادتين ١٤ و١٥. وينبغي أن تفرض هذه الضمانات أو الشروط فترات زمنية معقولة بالنسبة لمدة الالتزام، نظرا للطابع السري لتدابير التحقيق.

٢٢٧. كما تمت الإشارة أعلاه، يولى الاعتبار عموما لمصلحة الخصوصية فيما يتعلق بجمع بيانات الحركة بشكل أقل من عندما يتعلق الأمر باعتراض بيانات المحتوى. فبيانات الحركة بشأن وقت الاتصال ومدته وحجمه تكشف القليل من المعلومات الشخصية عن الشخص أو أفكاره. ومع ذلك، قد تطرح مسألة الخصوصية بحدة فيما يتعلق بالبيانات المرتبطة بمصدر الاتصال أو وجهته (مثلا المواقع الإلكترونية التي تمت زيارتها). وقد يسمح جمع هذه البيانات، في بعض الحالات، بتجميع السمات المحددة لمصالح الشخص وشركائه وسياقه الاجتماعي. وبناء على ذلك، ينبغي للأطراف أن تضع هذه الاعتبارات في الحسبان عند إنشاء الضمانات المناسبة والشروط القانونية المسبقة اللازمة لإعمال هذه التدابير، طبقا للمادتين ١٤ و١٥.

اعتراض بيانات المحتوى (المادة ٢١)

٢٢٨.لطالما كان جمع بيانات المحتوى فيما يتعلق بالاتصالات السلكية واللاسلكية (مثل المحادثات الهاتفية) أداة مفيدة للتحقيق من أجل تحديد أن الاتصال ذو طابع غير قانوني (مثلا، تحديد إذا ما كان الاتصال يشكل تهديدا إجراميا أو تحرشا، أو مؤامرة جنائية أو ادعاءات كاذبة احتيالية) وجمع الأدلة على الجرائم السابقة أو المستقبلية (مثل الاتجار بالمخدرات، والقتل، والجرائم الاقتصادية، وما إلى ذلك). ويمكن أن تشكل أو توفر الاتصالات عبر الكمبيوتر أدلة على نفس أنواع الإجرام. إلا أنه بالنظر إلى القدرة الهائلة لتكنولوجيا الحاسوب على نقل كميات هائلة من البيانات، بما في ذلك النصوص المكتوبة والصور المرئية والصوت، فإنها توفر أيضا إمكانيات أكبر لارتكاب جرائم تنطوي على توزيع محتوى غير قانوني (مثل المواد الإباحية المتعلقة بالأطفال)، تنطوي العديد من الجرائم المرتكبة عبر الكمبيوتر على إرسال أو نقل بيانات كجزء من ارتكابها؛ على سبيل المثال، الاتصالات المرسلة من أجل تيسير النفاذ غير المشروع لنظام كمبيوتر أو توزيع فيروسات الكمبيوتر. ولا يمكن في الوقت الحقيقي تحديد الطبيعة الضارة وغير القانونية لهذه الاتصالات دون اعتراض مضمون الرسالة. ولعل انعدام القدرة على تحديد ومنع حدوث الجريمة الجاري ارتكابها من شأنه ألا يترك لسلطات إنفاذ القانون سوى التحقيق في الجرائم السابقة والمرتبكة فعلا مع ما ترتب عنها من ضرر. لذلك، يكتسي اعتراض في بيانات محتوى الاتصالات عبر الكمبيوتر في الوقت الحقيقي نفس القدر من الأهمية، إن لم يكن أكثر، التي تولى لاعتراض الاتصالات السلكية واللاسلكية في الوقت الحقيقي.

٢٢٩.تشير عبارة "بيانات المحتوى" إلى محتوى الاتصال؛ أي معنى أو فحوى الاتصال، أو الرسالة أو المعلومات التي يتم نقلها عبر الاتصال. فهي كل ما يتم نقله كجزء من الاتصال غير بيانات الحركة.

٢٣٠.معظم عناصر هذه المادة مماثلة لتلك الواردة في المادة ٢٠. لذلك فإن التعليقات الواردة أعلاه بشأن جمع أو تسجيل بيانات الحركة والالتزامات بالتعاون والمساعدة والالتزامات المتعلقة بالسرية تنطبق بالتساوي على اعتراض بيانات المحتوى. ونظرا لمصلحة الخصوصية العليا المرتبطة ببيانات المحتوى، يقتصر تدبير إجراء التحقيق على "مجموعة من الجرائم الخطيرة التي يحددها القانون المحلي".

٢٣١.كما هو مبين في التعليقات الواردة أعلاه بشأن المادة ٢٠، يمكن أن تكون الشروط والضمانات المنطبقة على اعتراض بيانات المحتوى في الوقت الحقيقي أكثر صرامة من الشروط المطبقة على جمع بيانات الحركة في الوقت الفعلي، أو على البحث في بيانات مخزنة، ومصادرتها أو تأمينها بطريقة مماثلة.

القسم ٢: الولاية القضائية

الولاية القضائية (المادة ٢٢)

٢٣٢.تنص هذه المادة على مجموعة من المعايير التي تلزم بموجبها الأطراف المتعاقدة بإقامة ولايتها القضائية على الجرائم الجنائية المنصوص عليها في المواد من ٢ إلى ١١ من الاتفاقية.

٢٣٣.تستند الفقرة ١ إلى مبدأ الإقليمية. ويتعين على كل طرف أن يعاقب على ارتكاب الجرائم المنصوص عليها في هذه الاتفاقية والمرتكبة في إقليمه. فعلى سبيل المثال، يمكن لطرف أن يؤكد ولايته القضائية الإقليمية إذا كان الشخص الذي يهاجم نظام الكمبيوتر وكان نظام الضحية موجودا داخل إقليم ذلك الطرف، وعندما يكون نظام الكمبيوتر الخاضع للهجوم داخل إقليمه، حتى لو كان مرتكب الهجوم خارج ذلك الإقليم.

٢٣٤.جرى النظر في إدراج حكم يقضي بأن ينشئ كل طرف ولاية قضائية على الجرائم التي تنطوي على أقمار صناعية مسجلة باسمه. وقرر القائمون على الصياغة أن هذا الحكم غير ضروري لأن مصدر و/أو وجهة الاتصالات غير القانونية التي تنطوي على استخدام الأقمار الصناعية تكون دائما على الأرض. وهكذا، فإن أحد الأسس التي تستند إليها الولاية القضائية للطرف المنصوص عليها في الفقرة ١(أ)-(ج) سيكون متاحا إذا كان مصدر أو وجهة الاتصال في أحد المواقع المحددة فيها. فضلا عن ذلك، عندما ترتكب الجريمة التي تنطوي على اتصال عبر الأقمار الصناعية من قبل أحد رعايا الدولة الطرف خارج الولاية الإقليمية لأي دولة، سيكون هناك أساس للولاية القضائية بموجب الفقرة ١(د). وفي الأخير، تساءل القائمون على الصياغة جدوى اعتبار التسجيل كأساس ملائم لتأكيد الولاية القضائية الجنائية باعتبار أنه لن يكون هناك في كثير من الحالات صلة ذات مغزى بين الجريمة المرتكبة ودولة التسجيل لأن القمر الصناعي يستخدم كمجرد قناة للإرسال.

٢٣٥.تستند الفقرة ١، الفقرتان الفرعيتان (ب) و(ج) إلى خيار مبدأ الإقليمية. وتقتضي هتان الفقرتان الفرعيتان من كل طرف أن ينشئ ولاية قضائية جنائية على الجرائم المرتكبة على السفن التي ترفع علمه أو طائراته المسجلة بموجب قوانينه. وينفذ هذا الالتزام بالفعل كمسألة عامة في قوانين العديد من الدول، نظرا لأن هذه السفن والطائرات كثيرا ما تعتبر امتدادا لإقليم الدولة. وهذا النوع من الولاية القضائية يكون مفيدا للغاية عندما لا تكون السفينة أو الطائرة متواجدة في إقليمها وقت ارتكاب الجريمة، ونتيجة لذلك لن تكون الفقرة ١ من هذا القانون متاحة كأساس لتأكيد الولاية القضائية. وإذا ارتكبت الجريمة على متن سفينة أو طائرة تقع خارج إقليم طرف العلم، لا يجوز أن تكون هناك دولة أخرى تستطيع ممارسة هذه الولاية دون هذا الشرط. بالإضافة إلى ذلك، إذا ارتكبت جريمة على متن سفينة أو طائرة تمر عبر مياه أو مجال جوي لدولة أخرى، فإن الدولة الأخيرة قد تواجه معيقات عملية هامة أمام ممارسة ولايتها القضائية، ومن ثم فإنه من المفيد لدولة التسجيل أن تتوفر أيضا على ولايتها القضائية.

٢٣٦.تستند الفقرة ١ إلى مبدأ الجنسية. غالبا ما تطبق نظرية الجنسية من قبل الدول التي تطبق تقاليد القانون المدني. وتنص الفقرة على أن مواطني الدولة ملزمون بالامتثال للقانون المحلي حتى عندما يكونون خارج أراضيها. وبموجب الفقرة (د)، إذا ارتكب أحد المواطنين جريمة في الخارج، يكون الطرف ملزما بالتوفر على قدرة ملاحقته إذا كان السلوك يعتبر جريمة أيضا بمقتضى قانون الدولة التي ارتكب فيها أو كان السلوك قد حدث خارج الاختصاص الإقليمي لأي دولة.

٢٣٧.تسمح الفقرة ٢ للأطراف بتقديم تحفظ على أسباب الولاية القضائية المنصوص عليها في الفقرة ١، والفقرات (ب) و(ج) و(د). غير أنه لا يسمح بأي تحفظ فيما يتعلق بإقامة الاختصاص الإقليمي بموجب الفقرة (أ)، أو فيما يتعلق بالالتزام بإقامة الولاية القضائية في الحالات التي تندرج في إطار مبدأ "التسليم أو المحاكمة" (*aut dedere aut judicare*) بموجب الفقرة ٣، بمعنى عندما يرفض ذلك الطرف تسليم الجاني المزعوم على أساس جنسيته ويكون الجاني موجودا في إقليمه. وتعتبر الولاية القضائية المنشأة على أساس الفقرة ٣ ضرورية لضمان أن تكون لدى الأطراف التي ترفض تسليم مواطن ما القدرة القانونية على إجراء التحقيقات والمتابعات على الصعيد المحلي بدلا من ذلك، في حال طلب الطرف الذي طلب التسليم ذلك عملا بمتطلبات "تسليم المجرمين"، الفقرة ٦ من المادة ٢٤ من هذه الاتفاقية.

٢٣٨.لا تعتبر أسس الولاية القضائية المنصوص عليها في الفقرة ١ حصرية. وتسمح الفقرة ٤ من هذه المادة للأطراف بأن تنشئ، وفقا لقانونها الداخلي، أنواعا أخرى من الولاية القضائية الجنائية أيضا.

٢٣٩.عندما يتعلق الأمر بجرائم ارتكبت باستخدام أنظمة الكمبيوتر، تكون هناك حالات تنطوي على أكثر من طرف واحد تكون له الولاية القضائية على بعض أو جميع المشاركين في الجريمة. على سبيل المثال، تستهدف العديد من هجمات الفيروسات، وعمليات الاحتيال وانتهاكات حقوق التأليف والنشر التي ترتكب من خلال استخدام الإنترنت، ضحايا يتواجدون في دول عدة. ومن أجل تفادي ازدواجية الجهود أو الإزعاج غير الضروري للشهود أو المنافسة بين الموظفين المكلفين بإنفاذ القوانين في الدول المعنية أو بغية تيسير فعالية الإجراءات أو وعدالتها، يتعين على الأطراف المتضررة أن تتشاور لتحديد المكان المناسب للملاحقة القضائية. وفي بعض الحالات، سيكون من الأكثر فعالية أن تختار الدول المعنية مكانا واحدا للمقاضاة؛ بينما يكون من الأفضل، في حالات أخرى، أن يعهد إلى دولة واحدة بمحاكمة بعض المشاركين، في حين تقوم دولة أخرى أو أكثر بملاحقة مشاركين آخرين. ويسمح بأي من هذين الخيارين بموجب هذه الفقرة. وفي الأخير، لا يعتبر الالتزام بالتشاور مطلقا، بل يجب أن يتم "عند الاقتضاء". وهكذا، إذا كان أحد الأطراف، على سبيل المثال، يعلم أن التشاور ليس ضروريا (في حال تلقى تأكيدا بأن الطرف الآخر لا يعتزم المتابعة، مثلا)، أو إذا رأى أحد الأطراف أن التشاور قد يضر بالتحقيق أو المتابعة، جاز له تأخير أو رفض التشاور.

الفصل الثالث: التعاون الدولي

٢٤٠.يتضمن الفصل الثالث عددا من الأحكام المتعلقة بتسليم المجرمين والمساعدة القانونية المتبادلة بين الأطراف.

القسم ١: المبادئ العامة

الباب الأول: المبادئ العامة ذات الصلة بالتعاون الدولي

المبادئ العامة ذات الصلة بالتعاون الدولي (المادة ٢٣)

٢٤١.تحدد المادة ٢٣ ثلاثة مبادئ عامة فيما يتعلق بالتعاون الدولي بموجب الفصل الثالث.

٢٤٢.توضح المادة، في المقام الأول، أن التعاون الدولي سيقدم إلى الأطراف "على أوسع نطاق ممكن". ويقتضي هذا المبدأ من الأطراف أن تقدم تعاونا واسعا فيما بينها، وأن تقلل إلى أدنى حد من العوائق التي تحول دون التدفق السلس والسريع للمعلومات والأدلة على الصعيد الدولي.

٢٤٣.ثانيا، يرد النطاق العام للالتزام بالتعاون في المادة ٢٣: ينبغي توسيع نطاق التعاون ليشمل جميع الجرائم ذات الصلة بأنظمة وبيانات الكمبيوتر (أي الجرائم المشمولة بالفقرة ٢ من المادة ١٤، البندين "أ" و"ب")، فضلا عن جمع الأدلة في شكل إلكتروني عن جريمة جنائية. ويعني ذلك أن أحكام الفصل الثالث تنطبق سواء ارتكبت الجريمة باستخدام نظام كمبيوتر، أو انطوت جريمة عادية لم ترتكب باستخدام نظام كمبيوتر (مثل القتل) على أدلة إلكترونية. ومع ذلك، تجدر الإشارة إلى أن المواد ٢٤ (تسليم المجرمين) (المساعدة المتبادلة بشأن جمع بيانات الحركة في الوقت الحقيقي) و٣٤ (المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى) تسمح للأطراف بتوفير نطاق مختلف لتطبيق هذه التدابير.

٢٤٤.وفي الأخير، يجب إنجاز التعاون "وفقا لأحكام هذا الفصل" و "من خلال تطبيق الاتفاقات الدولية ذات الصلة بالتعاون الدولي في المسائل الجنائية، والترتيبات المتفق عليها على أساس التشريع الموحد أو المتبادل والقوانين المحلية " على حد سواء. وينص البند الأخير على المبدأ العام الذي مفاده أن أحكام الفصل الثالث لا تلغي أحكام الاتفاقات الدولية المتعلقة بالمساعدة القانونية المتبادلة وتسليم المجرمين، والترتيبات المتبادلة بين الأطراف في إطارها (والتي يرد وصفها بمزيد من التفصيل في مناقشة المادة ٢٧ أدناه)، أو والأحكام ذات الصلة في القانون المحلي والمتعلقة بالتعاون الدولي. ويعزز هذا المبدأ الأساسي بشكل صريح في المواد ٢٤ (تسليم المجرمين)، و٢٥ (المبادئ العامة المتعلقة بالمساعدة المتبادلة)، و٢٦ (المعلومات التلقائية)، و٢٧ (الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق)، و٢٨ (السرية والقيود على الاستخدام) و(٣١) (المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكمبيوتر المخزنة) و٣٣ (المساعدة المتبادلة ذات الصلة بجمع بيانات الحركة في الوقت الحقيقي) و٣٤ (المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى).

الباب الثاني – المبادئ ذات الصلة بتسليم المجرمين

المادة ٢٤ – تسليم المجرمين (المادة ٢٤)

٢٤٥.تنص الفقرة ١ على أن الالتزام بالتسليم لا ينطبق إلا على الجرائم المقررة طبقا للمواد من ٢ إلى ١١ من الاتفاقية التي يعاقب عليها بموجب قوانين الطرفين المعنيين بعقوبة سالبة للحرية لمدة أقصاها سنة واحدة على الأقل أو بعقوبة أشد. وقرر القائمون على الصياغة إدراج حد أدنى للعقوبة لأن الأطراف قد تعاقب، بموجب الاتفاقية، على بعض الجرائم بعقوبة حبسية تكون مدتها القصوى قصيرة نسبيا (مثلا، المادة ٢ – النفاذ غير القانوني – والمادة ٤ – التدخل في البيانات). وبالنظر إلى ذلك، لم يعتقد القائمون على الصياغة أنه من الملائم اشتراط اعتبار كل جريمة من الجرائم المنصوص عليها في المواد من ٢ إلى ١١ في حد ذاتها قابلة لتطبيق إجراء تسليم المجرمين. وبناء على ذلك، تم التوصل إلى اتفاق بشأن شرط عام يقضي بأن تعتبر الجريمة جريمة قابلة لتطبيق إجراء تسليم المجرمين عندما تكون العقوبة القصوى التي يمكن فرضها على الجريمة المطلوب التسليم من أجلها عقوبة حبسية لمدة سنة واحدة على الأقل – كما هو وارد في المادة ٢ من الاتفاقية الأوروبية لتسليم المجرمين (سلسلة المعاهدات الأوروبية رقم ٢٤). ولا يتوقف تحديد قابلية الجريمة لتطبيق إجراء تسليم المجرمين على العقوبة الفعلية المفروضة في القضية المعينة قيد النظر، ولكن بدلا من ذلك على المدة القصوى التي يجوز فرضها قانونيا على الجريمة المطلوب التسليم من أجلها.

٢٤٦.في الوقت نفسه، ووفقا للمبدأ العام الذي يقضي بأن التعاون الدولي في إطار الفصل الثالث ينبغي أن ينفذ عملا بالصكوك الجاري بها العمل بين الأطراف، تنص الفقرة ١ أيضا على أنه في حال وجود معاهدة بشأن تسليم المجرمين أو ترتيب على

أساس تشريع موحدة أو متبادل سارية المفعول بين طرفين أو أكثر (انظر وصف هذا المصطلح في مناقشة المادة ٢٧ أدناه) ينص على حد أدنى مختلف لتسليم المجرمين، يطبق ذلك الحد الأدنى المنصوص عليه في هذه المعاهدة أو الترتيب. وعلى سبيل المثال، تنص العديد من معاهدات تسليم المجرمين بين البلدان الأوروبية والبلدان غير الأوروبية أن الجريمة تعتبر قابلة لتطبيق إجراء تسليم المجرمين عندما تكون العقوبة القصوى التي يمكن فرضها على الجريمة المطلوب التسليم من أجلها عقوبة حبسية لمدة سنة واحدة على الأقل أو عندما تكون العقوبة أشد. وفي مثل هذه الحالات، يواصل ممارسو التسليم الدوليون تطبيق الحد الأدنى العادي بموجب ممارساتهم التعاهدية من أجل تحديد ما إذا كانت الجريمة قابلة لتطبيق إجراء تسليم المجرمين. وحتى في إطار الاتفاقية الأوروبية لتسليم المجرمين (سلسلة المعاهدات الأوروبية رقم ٢٤)، يمكن أن تحدد التحفظات عقوبة دنيا مختلفة لتسليم المجرمين. ومن بين الأطراف في تلك الاتفاقية، عندما يطلب التسليم من طرف أبدى هذا التحفظ، تطبق العقوبة المنصوص عليها في التحفظ لتحديد ما إذا كانت الجريمة قابلة لتطبيق إجراء تسليم المجرمين.

٢٤٧. تنص الفقرة ٢ على أن الجرائم المبينة في الفقرة ١ تعتبر جرائم قابلة لتطبيق إجراء تسليم المجرمين في أي معاهدة لتسليم المجرمين بين الأطراف أو فيما بينها، وينبغي إدراجها في المعاهدات المقبلة التي قد تتفاوض بشأنها فيما بينها. وهذا لا يعني أن التسليم يجب أن يمنح في كل مرة يقدم فيها الطلب، بل أنه ينبغي أن تكون إمكانية الموافقة على تسليم الأشخاص لارتكابهم جرائم من هذا القبيل متاحة. وبموجب الفقرة ٥، تكون الأطراف قادرة على توفير شروط أخرى لتسليم المجرمين.

٢٤٨. بموجب الفقرة ٣، يجوز للطرف الذي لا يمنح التسليم، إما بسبب غياب معاهدة لتسليم المجرمين مع الطرف مقدم الطلب أو لأن المعاهدات القائمة لا تشمل الطلب المقدم بشأن الجرائم المقررة وفقا لهذه الاتفاقية، أن يستخدم الاتفاقية نفسها كأساس لتسليم الشخص المطلوب، رغم أنه غير ملزم بذلك.

٢٤٩. عندما يستخدم طرف نظاما قانونيا عاما لتنفيذ التسليم بدلا من الاعتماد على معاهدات تسليم المجرمين، تقضي الفقرة ٤ بأن تدرج في ذلك النظام الجرائم المبينة في الفقرة ١ ضمن الجرائم التي يتاح بشأنها التسليم.

٢٥٠. تنص الفقرة ٥ على أن الطرف متلقي الطلب لا يحتاج إلى تسليم المجرمين إذا لم يقتنع باستيفاء كافة الشروط والأحكام المنصوص عليها في المعاهدة أو القانون المنطبق. وهذا مثال آخر على ضرورة تطبيق مبدأ التعاون وفقا لبنود الآليات الدولية سارية المفعول بين الأطراف أو الترتيبات المتبادلة أو القانون المحلي. وعلى سبيل المثال، تنطبق الشروط والقيود المنصوص عليها في الاتفاقية الأوروبية لتسليم المجرمين (سلسلة المعاهدات الأوروبية رقم ٢٤) وبروتوكوليها الإضافيين (سلسلة المعاهدات الأوروبية ٨٦ و٩٨) على الأطراف في تلك الاتفاقات، ويمكن رفض التسليم على هذه الأسس (على سبيل المثال، تنص المادة ٣ من الاتفاقية الأوروبية لتسليم المجرمين على رفض تسليم المجرمين إذا اعتبرت الجريمة ذات طابع سياسي، أو إذا اعتبر أن الطلب قدم لغرض مقاضاة أو معاقبة شخص ما بسبب جملة أمور منها العرق أو الدين أو الجنسية أو الرأي السياسي).

٢٥١. تنطبق الفقرة ٦ على مبدأ "التسليم أو المحاكمة" (*aut dedere aut judicare*). وبما أن العديد من الدول ترفض تسليم رعاياها، فإن المجرمين الموجودين في الطرف الذي هم من رعاياه قد يتجنبون المسؤولية عن جريمة ارتكبت في طرف آخر ما لم تكن السلطات المحلية ملزمة بالمقاضاة. وبموجب الفقرة ٦، إذا طلب طرف آخر تسليم الجاني، وتم رفض التسليم على أساس أن الجاني من مواطني الطرف متلقي الطلب، وجب على هذا الأخير، بناء على طلب الطرف مقدم الطلب، أن يعرض القضية على سلطاته من أجل المقاضاة. وإذا لم يطلب الطرف الذي قوبل طلبه بالتسليم بالرفض عرض القضية للتحقيق والملاحقة القضائية على الصعيد المحلي، فإن الطرف متلقي الطلب غير ملزم بالمقاضاة. فضلا عن ذلك، إذا لم يتم تقديم أي طلب بالتسليم، أو في حال رفض التسليم لأسباب أخرى غير الجنسية، فإن هذه الفقرة لا تفرض على الطرف متلقي الطلب أي التزام بعرض القضية للمقاضاة محليا. وبالإضافة إلى ذلك، تقتضي الفقرة ٦ إجراء التحقيق والملاحقة القضائية على الصعيد المحلي بسرعة؛ ويجب التعامل مع هذه القضية بشكل جدي "كما هو الحال بالنسبة لأي جريمة أخرى ذات طبيعة مماثلة" في الدولة الطرف التي تعرض القضية. ويتعين على ذلك الطرف أن يقدم تقريرا عن نتيجة تحقيقاته وإجراءاته إلى الطرف الذي قدم الطلب.

٢٥٢.بغية أن يعلم كل طرف إلى من ينبغي توجيه طلباتهم بشأن الاعتقال المؤقت أو التسليم، تقتضي الفقرة ٧ من الأطراف إبلاغ الأمين العام لمجلس أوروبا باسم وعنوان سلطاتها المسؤولة عن تقديم أو تلقي طلبات التسليم أو الاعتقال المؤقت في حال عدم وجود معاهدة. ويقتصر هذا الحكم على الحالات التي لا توجد فيها معاهدة لتسليم المجرمين سارية بين الأطراف المعنية، لأنه إذا دخلت معاهدة ثنائية أو متعددة الأطراف لتسليم المجرمين حيز النفاذ بين الأطراف (من قبيل سلسلة المعاهدات الأوروبية رقم ٢٤)، فإن الأطراف ستعرف إلى من يجب توجيه طلبات التسليم أو الاعتقال المؤقت دون ضرورة إدراج شرط التسجيل. ويجب إخبار الأمين العام وقت التوقيع أو عند إيداع الطرف صك التصديق أو القبول أو الموافقة أو الانضمام. وتجدر الإشارة إلى أن تعيين السلطة لا يستبعد إمكانية استخدام القناة الدبلوماسية.

الباب الثالث – المبادئ العامة ذات الصلة بالمساعدة المتبادلة

المبادئ العامة ذات الصلة بالمساعدة المتبادلة (المادة ٢٥)

٢٥٣.ترد المبادئ العامة التي تنظم الالتزام بتقديم المساعدة المتبادلة في الفقرة ١. وينبغي توفير التعاون "على أوسع نطاق ممكن". وهكذا، وكما ورد في المادة ٢٣ ("المبادئ العامة ذات الصلة بالتعاون الدولي")، تكون المساعدة المتبادلة من حيث المبدأ واسعة النطاق، والمعيقات التي تقيدها محدودة للغاية. ثم، وكما ورد في المادة ٢٣، ينطبق الالتزام بالتعاون من حيث المبدأ على كل من الأفعال الإجرامية المتعلقة بأنظمة وبيانات الكمبيوتر (أي الجرائم المشمولة بالفقرة ٢ من المادة ١٤، والبندين "أ" و "ب")، وبجمع أدلة خاصة بجريمة جنائية في شكل إلكتروني. وقد تم الاتفاق على فرض التزام بالتعاون فيما يتعلق بهذه المجموعة الواسعة من الجرائم لأن ثمة حاجة مماثلة إلى آليات مبسطة للتعاون الدولي فيما يتعلق بكلتا هاتين الفئتين. ومع ذلك، تسمح المادتان ٣٤ و٣٥ للأطراف بتوفير نطاق مختلف لتطبيق هذه التدابير.

٢٥٤.ستوضح أحكام أخرى من هذا الفصل أن الالتزام بتقديم المساعدة المتبادلة يتم عموما وفقا لأحكام معاهدات وقوانين وترتيبات المساعدة القانونية سارية التطبيق. وبمقتضى الفقرة ٢، كل طرف مطالب بالتوفر على أساس قانوني لتنفيذ أشكال التعاون المحددة المبينة في باقي الفصل، إذا كانت معاهداته وقوانينه وترتيباته لا تتضمن بالفعل أحكاما من هذا القبيل. ويعد توافر هذه الآليات، ولا سيما تلك الواردة في المواد من ٢٩ إلى ٣٥ (أحكام خاصة - الأبواب ١ و٢ و٣) أمرا حيويا للتعاون الفعال في المسائل الجنائية المتعلقة بالكمبيوتر.

٢٥٥.لن تقتضي بعض الأطراف أي تشريع تنفيذي لتطبيق الأحكام المشار إليها في الفقرة ٢، حيث أن أحكام المعاهدات الدولية التي تنشئ أنظمة مفصلة للمساعدة المتبادلة تعتبر أحكاما ذاتية التنفيذ بطبيعتها. ومن المتوقع أن تكون الأطراف قادرة على التعامل مع هذه الأحكام على أنها ذاتية التنفيذ، وأن تكون لديها بالفعل مرونة كافية في إطار تشريعات المساعدة المتبادلة القائمة لتنفيذ تدابير المساعدة المتبادلة المقررة بموجب هذا الفصل، أو أن تكون قادرة على سن أي تشريع مطلوب للقيام بذلك، على وجه السرعة.

٢٥٦.تعتبر بيانات الكمبيوتر شديدة التقلب. ويمكن حذفها ببضع نقرات على لوحة المفاتيح أو عن طريق تشغيل برامج تلقائية، مما يجعل من المستحيل تتبع الجريمة للوصول إلى مرتكبها أو يؤدي إلى إتلاف الأدلة الهامة على الجريمة. يتم تخزين بعض أشكال بيانات الكمبيوتر لفترات قصيرة فقط قبل حذفها. وفي حالات أخرى، قد يتأذى أشخاص أو يلحق ضرر جسيم بممتلكات إن لم يتم جمع الأدلة بسرعة. وفي مثل هذه الحالات العاجلة، يجب التسريع ليس فقط بالطلب، بل وكذلك بالرد. لذلك، تهدف الفقرة ٣ إلى تيسير التعجيل بعملية الحصول على المساعدة المتبادلة بحيث لا تضيع المعلومات أو الأدلة الهامة بسبب حذفها قبل إعداد طلب المساعدة وإرساله والاستجابة له. وتحقق الفقرة ٣ ذلك من خلال: (١) تمكين الأطراف من تقديم طلبات عاجلة للتعاون من خلال وسائل الاتصال السريعة، بدلا من الوسائل التقليدية البطيئة التي تنطوي على نقل الوثائق المكتوبة والمختومة عبر الحقائب الدبلوماسية أو البريد؛ و(٢) مطالبة الطرف متلقي الطلب باستخدام وسائل سريعة للاستجابة للطلبات في مثل هذه الظروف. ويطلب من كل طرف أن تتوفر لديه القدرة على تطبيق هذا التدبير في حال لم تنص معاهدات أو قوانين أو ترتيبات المساعدة المتبادلة على ذلك. يعتبر إدراج الفاكس والبريد الإلكتروني ذا طبيعة إرشادية؛ ويجوز استخدام أي وسيلة اتصال سريعة أخرى حسبما يكون ملائما في الظروف الخاصة المطروحة. ومع تقدم التكنولوجيا، سيتم تطوير المزيد من وسائل الاتصال السريعة التي يمكن استخدامها لطلب المساعدة المتبادلة. وفيما يتعلق بمتطلبات الصحة والأمن الواردة في الفقرة، يجوز للأطراف أن تقرر فيما بينها كيفية ضمان صحة الاتصالات وما إذا كانت هناك حاجة إلى حمايات أمنية خاصة (بما في ذلك التشفير) قد تكون ضرورية في الحالات الحساسة بشكل خاص. وفي

الأخير، تسمح الفقرة أيضا للطرف متلقي الطلب بأن يطلب تأكيدا رسميا يرسل عن طريق القنوات التقليدية لمتابعة الإرسال المعجل، إذا اختار ذلك.

٢٥٧.تنص الفقرة ٤ على مبدأ خضوع المساعدة المتبادلة لأحكام معاهدات المساعدة المتبادلة (MLATs) والقوانين المحلية. وتوفر هذه الأنظمة ضمانات لحقوق الأشخاص الموجودين في الطرف متلقي الطلب الذين قد يصبحون موضوع طلب المساعدة المتبادلة. على سبيل المثال، لا يتم تنفيذ تدبير تدخلي، مثل البحث والمصادرة، نيابة عن الطرف مقدم الطلب ما لم تستوف الشروط الأساسية للطرف متلقي الطلب بشأن هذا التدبير المنطبق في قضية محلية. ويجوز للأطراف أيضا أن تكفل حماية حقوق الأشخاص فيما يتعلق بالمواد التي تمت مصادرتها وتوفيرها عبر المساعدة القانونية المتبادلة.

٢٥٨.ومع ذلك، لا تنطبق الفقرة ٤ إذا "ورد التنصيص تحديدا على خلاف ذلك في هذا الفصل". ويهدف هذا البند إلى الإشارة إلى أن الاتفاقية تتضمن عدة استثناءات هامة من المبدأ العام. وورد أول استثناء من هذا القبيل في الفقرة ٢ من هذه المادة التي تلزم كل طرف بأن ينص على أشكال التعاون المنصوص عليها في المواد المتبقية من الفصل (مثل الحفظ، وجمع البيانات في الوقت الحقيقي، والبحث والمصادرة، وصيانة الشبكة ٧/٢٤) بغض النظر عما إذا كانت أحكام معاهدات المساعدة المتبادلة (MLATs) أو الترتيبات المماثلة أو قوانين المساعدة المتبادلة تنص على هذه التدابير، في الوقت الراهن. وثمة استثناء آخر ورد في المادة ٢٧ التي ينبغي دائما تطبيقها على تنفيذ الطلبات بدلا من القانون الداخلي للطرف متلقي الطلب الذي يحكم التعاون الدولي في غياب معاهدة متعددة الأطراف أو ترتيب مماثل بين الأطراف المقدمة والمتلقية للطلب. وتنص المادة ٢٧ على نظام من الشروط وأسباب الرفض. وثمة استثناء آخر، منصوص عليه تحديدا في هذه الفقرة، مفاده أنه لا يجوز رفض التعاون، على الأقل فيما يتعلق بالجرائم المحددة في المواد من ٢ إلى ١١ من الاتفاقية، على أساس أن الطرف متلقي الطلب يعتبر أن الطلب ينطوي على جريمة "مالية". وفي الأخير، تعتبر المادة ٢٩ استثناء من حيث أنها تنص على أنه لا يجوز رفض الحفظ على أسس ازدواجية التجريم، وإن ورد التنصيص على إمكانية إبداء تحفظ في هذا الصدد.

٢٥٩.الفقرة ٥ هي، في الأساس، تعريف لازدواجية التجريم لأغراض المساعدة المتبادلة في إطار هذا الفصل. عندما يسمح للطرف متلقي الطلب باشتراط ازدواجية التجريم لتقديم المساعدة (مثلا، عندما يحتفظ الطرف متلقي الطلب بحقه في طلب ازدواجية التجريم فيما يتعلق بحفظ البيانات بموجب الفقرة ٤ من المادة ٢٩ "التعجيل بحفظ بيانات الكمبيوتر المخزنة")، تعتبر ازدواجية التجريم موجودة إذا كان السلوك الذي تنطوي عليه الجريمة التي تطلب المساعدة بشأنها يعتبر جريمة جنائية بموجب قوانين الطرف متلقي الطلب، حتى وإن صنفت قوانينه الجريمة ضمن فئة مختلفة من الجرائم أو استخدمت مصطلحات مختلفة لتسمية الجريمة. وقد اعتبر هذا الحكم ضروريا لضمان ألا تعتمد الأطراف متلقية الطلب اختبارا صارما للغاية عند تطبيق ازدواجية التجريم. ونظرا للاختلافات في الأنظمة القانونية الوطنية، لا بد من ظهور اختلافات في المصطلحات وتصنيف السلوك الإجرامي. وإذا كان السلوك يشكل انتهاكا جنائيا في كلا النظامين، فإن هذه الاختلافات التقنية ينبغي ألا تعرقل المساعدة. وبدلا من ذلك، ينبغي، في المسائل التي ينطبق عليها معيار التجريم المزدوج، التطبيق بطريقة مرنة تيسر تقديم المساعدة.

المعلومات التلقائية (المادة ٢٦)

٢٦٠.تستمد هذه المادة من أحكام صكوك مجلس أوروبا السابقة، مثل المادة ١٠ من الاتفاقية المعنية بغسل الأموال والبحث عن عائدات الجريمة وضبطها ومصادرتها (سلسلة المعاهدات الأوروبية رقم ١٤١) والمادة ٢٨ من اتفاقية القانون الجنائي بشأن الفساد (سلسلة المعاهدات الأوروبية رقم ١٧٣). ويملك الطرف، بشكل متزايد، معلومات قيمة يعتقد أنها قد تساعد طرفا آخر في تحقيق جنائي أو إجراء جنائي والتي لا يدرك الطرف الذي يجري التحقيق أو الإجراء بوجودها. وفي مثل هذه الحالات، لن يتم تقديم أي طلب للمساعدة المتبادلة. لذلك، تمكن الفقرة ١ الدولة التي تتوفر لديها المعلومات من إحالتها إلى الدولة الأخرى دون طلب مسبق. واعتبر هذا الحكم مفيدا لأنه ثمة حاجة، بموجب قوانين بعض الدول، إلى هذا التقديم الإيجابي للسلطة القانونية من أجل تقديم المساعدة في حال انعدام الطلب. ولا يكون الطرف ملزما بتقديم المعلومات تلقائيا إلى طرف آخر؛ ويجوز له أن يمارس سلطته التقديرية في ضوء ظروف القضية قيد النظر. فضلا عن ذلك، لا يحول الكشف التلقائي للمعلومات دون قيام الطرف المفصح، إذا كانت له الولاية القضائية، بالتحقيق أو إقامة إجراءات تتعلق بالوقائع التي تم الكشف عنها.

٢٦١.تتناول الفقرة ٢ مسألة قيام الطرف، في بعض الظروف، بإرسال المعلومات تلقائيا فقط إذا كانت المعلومات الحساسة ستظل سرية أو إذا أمكن فرض شروط أخرى على استخدام المعلومات. وتكون السرية، على وجه الخصوص، من الاعتبارات الهامة في الحالات التي قد تتعرض فيها المصالح الهامة للدولة مقدمة المعلومات للخطر إذا ما أتيحت تلك المعلومات للعموم، مثلا، حيثما تكون هناك حاجة لحماية هوية الوسيلة المستعملة لجمع المعلومات أو لإخفاء التحقيق الجاري بشأن جماعة إجرامية. وإذا كشف التحقيق المسبق أن الطرف المتلقي لا يستطيع الامتثال لشروط يسعى إليها الطرف مقدم المعلومات (مثلا، عندما لا يستطيع الامتثال لشروط السرية لأن المعلومات مطلوبة كدليل في محاكمة علنية)، يقوم الطرف المتلقي بإبلاغ الطرف المقدم، الذي يبقى له بعد ذلك خيار عدم تقديم المعلومات. أما إذا وافق الطرف المتلقي، مع ذلك، على هذا الشرط، فيجب عليه احترامه. ومن المتوقع أن تكون الشروط المفروضة بموجب هذه المادة متسقة مع الشروط التي يمكن أن يفرضها الطرف مقدم المعلومات عملا بطلب المساعدة المتبادلة من الطرف المتلقي.

الباب الرابع – الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق (المادة ٢٧)

٢٦٢.تلزم المادة ٢٧ الأطراف بتطبيق بعض إجراءات وشروط المساعدة المتبادلة في حالة عدم وجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة سارية بين الأطراف المقدمة والمتلقية للطلب. ومن ثم، تعزز هذه المادة المبدأ العام القائم على أن المساعدة المتبادلة ينبغي أن تنفذ من خلال تطبيق المعاهدات ذات الصلة والترتيبات المماثلة للمساعدة المتبادلة. ورفض القائمون على الصياغة إنشاء نظام عام منفصل للمساعدة المتبادلة في هذه الاتفاقية يطبق بدلا من الصكوك والترتيبات الأخرى واجبة التطبيق، واتفقوا بدلا من ذلك على أنه سيكون من العملي أكثر الاعتماد على أحكام معاهدات المساعدة المتبادلة (MLATs) القائمة في هذا المجال كموضوع عام، وبالتالي السماح لممارسي المساعدة المتبادلة باستخدام الصكوك والترتيبات المستأنسين بها وتجنب الارتباك الذي قد ينجم عن إنشاء أنظمة متنافسة. وكما ذكر سابقا، فإن كل طرف مطالب، فقط فيما يتعلق بالآليات اللازمة بشكل خاص للتعاون الفعال والسريع في المسائل الجنائية المتصلة بالكمبيوتر، مثل الآليات الواردة في المواد من ٢٩ إلى ٣٥ (أحكام خاصة - الأبواب ١ و٢ و٣) بإنشاء أساس قانوني بغية تمكين تنفيذ مثل هذه الأشكال من التعاون إن لم تكن معاهدات أو ترتيبات أو قوانين المساعدة المتبادلة الراهنة تنص على ذلك بالفعل.

٢٦٣.بناء على ذلك، يتواصل تنفيذ معظم أشكال المساعدة المتبادلة بموجب هذا الفصل عملا بالاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية (سلسلة المعاهدات الأوروبية رقم ٣٠) وبروتوكولها (سلسلة المعاهدات الأوروبية رقم ٩٩) بين الأطراف في تلك الصكوك . وكبديل عن ذلك، تواصل الأطراف في هذه الاتفاقية التي تتوفر على معاهدات المساعدة المتبادلة (MLATs) ثنائية الأطراف سارية المفعول بينها، أو غيرها من الاتفاقات المتعددة الأطراف التي تنظم المساعدة المتبادلة في القضايا الجنائية (مثل الدول الأعضاء في الاتحاد الأوروبي) تطبيق شروطها، التي تكملها الآليات المتعلقة بالجريمة المرتكبة عبر الكمبيوتر أو ذات الصلة بالكمبيوتر الوارد وصفها في الجزء المتبقي من الفصل الثالث، ما لم توافق على تطبيق أي من أحكام هذه المادة أو كلها، بدلا منها. ويمكن أن تستند المساعدة المتبادلة أيضا إلى الترتيبات المتفق عليها على أساس تشريعات موحدة أو متبادلة، مثل نظام التعاون الذي وضعته بلدان الشمال الأوروبي، والذي تقبله أيضا الاتفاقية الأوروبية المعنية بالمساعدة المتبادلة في المسائل الجنائية (المادة ٢٥، الفقرة ٤)، وفيما بين أعضاء الكومنولث. وفي الأخير، لا تقتصر الإشارة إلى معاهدات أو ترتيبات المساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة على الصكوك السارية وقت بدء نفاذ هذه الاتفاقية، بل تشمل أيضا الصكوك التي يمكن اعتمادها في المستقبل.

٢٦٤.تنص المادة ٢٧ (الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق)، الفقرات من ٢ إلى ١٠، على عدد من القواعد لتقديم المساعدة المتبادلة في غياب أحكام معاهدات المساعدة المتبادلة (MLATs) أو ترتيب على أساس تشريعات موحدة أو متبادلة، بما في ذلك إنشاء سلطات مركزية، وفرض شروط وأسباب وإجراءات في حالات التأجيل أو الرفض، وسرية الطلبات، والاتصالات المباشرة. وفيما يتعلق بهذه المسائل المشمولة

بصريح العبارة، في حالة غياب اتفاق أو ترتيب للمساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة، تطبق أحكام هذه المادة بدلا من القوانين المحلية المنطبقة التي تنظم المساعدة المتبادلة. وفي الوقت نفسه، لا تنص المادة ٢٧ على قواعد لقضايا أخرى تتناولها عادة التشريعات المحلية التي تنظم المساعدة المتبادلة الدولية. فعلى سبيل المثال، لا توجد أحكام تتناول شكل الطلبات ومحتواها، وتلقي شهادة الشهود لدى الأطراف المقدمة أو المتلقية للطلب، وتوفير السجلات الرسمية أو التجارية، ونقل الشهود المحتجزين، أو المساعدة في مسائل المصادرة. وفيما يتعلق بهذه المسائل، تنص الفقرة ٤ من المادة ٢٥ على أنه في حال عدم وجود حكم محدد في هذا الفصل، ينبغي أن ينظم قانون الطرف متلقي الطلب الطرائق الخاصة بتقديم هذا النوع من المساعدة.

٢٦٥.تقتضي الفقرة ٢ إنشاء سلطة مركزية أو سلطات مسؤولة عن إرسال طلبات المساعدة والرد عليها. ويعد إنشاء السلطات المركزية سمة مشتركة من سمات الصكوك الحديثة التي تتناول المساعدة المتبادلة في المسائل الجنائية، وتعتبر مفيدة بشكل خاص لضمان نوع الرد السريع الذي يكون مفيدا للغاية في مكافحة جرائم الكمبيوتر أو الجرائم المتصلة بالكمبيوتر. وفي البداية، يكون النقل المباشر بين هذه السلطات أسرع وأكثر فعالية من الإرسال عبر القنوات الدبلوماسية. بالإضافة إلى ذلك، يؤدي إنشاء سلطة مركزية نشطة وظيفة هامة في ضمان متابعة الطلبات الواردة والصادرة على حد سواء، وفي تقديم المشورة إلى الشركاء الأجانب المكلفين بإنفاذ القوانين حول أفضل السبل لتلبية المتطلبات القانونية في الطرف متلقي الطلب، وفي التعامل مع الطلبات العاجلة أو الحساسة بشكل صحيح.

٢٦٦.تشجع الأطراف من باب الفعالية على تعيين سلطة مركزية واحدة لأغراض المساعدة المتبادلة؛ وعادة تكون السلطة المعينة لهذا الغرض بموجب أحكام معاهدات المساعدة المتبادلة (MLATs) أو القانون المحلي أكثر فعالية عندما تعمل أيضا باعتبارها السلطة المركزية عند تطبيق هذه المادة. ومع ذلك، يتوفر الطرف على المرونة اللازمة لتعيين أكثر من سلطة مركزية واحدة حيثما يكون ذلك مناسبا في إطار نظام المساعدة المتبادلة. وفي حال إنشاء أكثر من سلطة مركزية واحدة، ينبغي للطرف الذي يقوم بذلك أن يكفل أن تفسر كل سلطة أحكام الاتفاقية بنفس الطريقة، وأن تعالج الطلبات الواردة والصادرة على حد سواء بسرعة وفعالية. ويقوم كل طرف بإبلاغ الأمين العام لمجلس أوروبا بأسماء وعناوين (بما في ذلك البريد الإلكتروني وأرقام الفاكس) السلطة أو السلطات المعينة لتلقي طلبات المساعدة المتبادلة والرد عليها بموجب هذه المادة، ويتعين على الأطراف ضمان تحيين المعلومات ذات الصلة بتعيين تلك السلطات.

٢٦٧.كثيرا ما يتمثل أحد الأهداف الرئيسية للدولة التي تطلب المساعدة المتبادلة في ضمان استيفاء قوانينها الداخلية التي تنظم مقبولية الأدلة، حتى يتسنى لها استخدام الأدلة أمام محاكمها. ولضمان استيفاء شروط الإثبات هذه، تلزم الفقرة ٣ الطرف متلقي الطلب بتنفيذ الطلبات وفقا للإجراءات التي يحددها الطرف مقدم الطلب، ما لم يكن ذلك متعارضا مع قانونه. ويجدر التأكيد على أن هذه الفقرة لا تتعلق إلا بالالتزام باحترام المتطلبات الإجرائية التقنية، وليس بالحمايات الإجرائية الأساسية. وهكذا، لا يمكن على سبيل المثال، للطرف مقدم الطلب أن يطلب من الطرف متلقي الطلب تنفيذ عملية بحث ومصادرة لا تفي بالمتطلبات القانونية الأساسية للطرف المتلقي من أجل هذا الإجراء. وفي ضوء الطبيعة المحدودة لهذا الالتزام، تم الاتفاق على أن عدم معرفة النظام القانوني للطرف متلقي الطلب بمثل هذا الإجراء لا يشكل أساسا كافيا لرفض تطبيق الإجراء الذي يطلبه الطرف مقدم الطلب؛ بل يجب، بدلا من ذلك، أن يكون الإجراء غير متوافق مع المبادئ القانونية للطرف متلقي الطلب. على سبيل المثال، بموجب قانون الطرف مقدم الطلب، يمكن أن تشمل الشروط الإجرائية تقديم إفادة الشاهد مشفوعة بيمين، وحتى إن لم يكن الطرف متلقي الطلب يشترط على الصعيد الداخلي أن تقدم الإفادات بعد أداء القسم، ينبغي له أن يفي بطلب الطرف مقدم الطلب.

٢٦٨.تنص الفقرة ٤ على إمكانية رفض طلبات المساعدة المتبادلة المقدمة بموجب هذه المادة. ويمكن رفض تقديم المساعدة بناء على الأسباب المنصوص عليها في الفقرة ٤ من المادة ٢٥ (أي الأسباب المنصوص عليها في قانون الطرف متلقي الطلب)، بما في ذلك المساس بسيادة الدولة أو الأمن أو النظام العام أو المصالح الأساسية الأخرى، وعندما يعتبر الطرف متلقي الطلب الجريمة كجريمة سياسية أو ذات الصلة بجريمة سياسية. ومن أجل تعزيز المبدأ الأساسي المتمثل في توفير أوسع قدر ممكن من التعاون (انظر المواد ٢٣ و٢٥)، ينبغي أن تكون أسباب الرفض التي يحددها الطرف متلقي الطلب ضيقة وأن تمارس بتريث. ولا ينبغي أن تكون واسعة النطاق بحيث تخلق إمكانية رفض المساعدة رفضا قاطعا، أو إخضاعها لشروط مكلفة، فيما يتعلق بفئات واسعة من الأدلة أو المعلومات.

٢٦٩.تمشيا مع هذه المقاربة، كان من المفهوم أنه باستثناء الأسباب المبينة في المادة ٢٨، لا يجوز التذرع برفض المساعدة على أسس حماية البيانات إلا في حالات استثنائية. ويمكن أن تنشأ مثل هذه الحالة عندما يحتمل، في إطار التوفيق بين المصالح الهامة التي تنطوي عليها الحالة الخاصة (من جهة الإدارة السليمة للعدالة، ومن جهة أخرى، مصالح الخصوصية)، أن يثير تقديم البيانات المحددة التي يسعى الطرف مقدم الطلب إلى الحصول عليها صعوبات جوهرية قد يعتبرها الطرف متلقي الطلب ضمن أسباب الرفض القائمة على المصالح الأساسية. لذلك، يحظر تطبيق مبادئ حماية البيانات على نطاق واسع أو فئوي أو منهجي لرفض التعاون. وبالتالي، فإن توفر الأطراف المعنية على أنظمة مختلفة لحماية خصوصية البيانات (مثل عدم امتلاك الطرف مقدم الطلب لسلطة متخصصة في حماية البيانات) أو على وسائل مختلفة لحماية البيانات الشخصية (مثلا عندما يستخدم الطرف مقدم الطلب وسائل أخرى غير عملية حذف البيانات لحماية خصوصية أو دقة البيانات الشخصية التي تتلقاها سلطات إنفاذ القانون)، لا يشكل في حد ذاته سببا للرفض. وقبل الاحتجاج "بالمصالح الأساسية" كأساس لرفض التعاون، ينبغي أن يحاول الطرف متلقي الطلب وضع شروط تسمح بنقل البيانات. (انظر الفقرة ٦ من المادة ٢٧ والفقرة ٢٧١ من هذا التقرير).

٢٧٠.تسمح الفقرة ٥ للطرف متلقي الطلب بتأجيل المساعدة بدلا من رفضها حيثما كان الإجراء الفوري المتعلق بالطلب من شأنه أن يلحق الضرر بالتحقيقات أو الإجراءات الجارية في الطرف متلقي الطلب. فعلى سبيل المثال، عندما يسعى الطرف مقدم الطلب للحصول على أدلة أو إفادة شهود لأغراض تحقيق أو محاكمة، وكانت نفس الأدلة أو الشهود ضرورية لاستخدامها في محاكمة على وشك أن تبدأ في الطرف متلقي الطلب، يكون مبررا لهذا الأخير تأجيل تقديم المساعدة.

٢٧١.تنص الفقرة ٦ على أنه يجوز، في الحالات التي يرفض فيها طلب المساعدة أو يرجئ خلاف ذلك، للطرف متلقي الطلب أن يقدم بدلا من ذلك مساعدة مرهونة بشروط. وفي حال كانت الشروط غير مقبولة للطرف مقدم الطلب، يجوز للطرف متلقي الطلب أن يعدلها، أو يجوز له أن يمارس حقه في رفض المساعدة أو تأجيلها. وبما أن الطرف متلقي الطلب ملزم بتقديم أكبر قدر ممكن من المساعدة، تم الاتفاق على أنه ينبغي ممارسة أسباب الرفض والشروط على السواء بتريث.

٢٧٢.تلزم الفقرة ٧ الطرف متلقي الطلب بإخبار الطرف مقدم الطلب بنتيجة الطلب، ويقتضي تقديم أسباب رفض المساعدة أو تأجيلها. ومن شأن تقديم الأسباب، في جملة أمور، أن يساعد الطرف مقدم الطلب على فهم الطريقة التي يفسر بها الطرف متلقي الطلب متطلبات هذه المادة، وأن يوفر أساسا للتشاور من أجل تحسين الكفاءة المستقبلية للمساعدة المتبادلة، وأن يوفر للطرف مقدم الطلب معلومات وقائعية لم تكن معروفة من قبل بشأن توافر أو وضع الشهود أو الأدلة.

٢٧٣.أحيانا، يقدم أحد الأطراف طلبا في قضية حساسة بشكل خاص، أو في قضية يمكن أن تترتب عليها عواقب كارثية إذا كانت الوقائع التي يقوم عليها الطلب ستعلن للعموم قبل الأوان. لذلك، تسمح الفقرة ٨ للطرف مقدم الطلب بالتماس إبقاء الطلب ومحتواه سريين. ومع ذلك، لا يجوز التماس السرية لدرجة تقوض قدرة الطرف متلقي الطلب على الحصول على الأدلة أو المعلومات المطلوبة، مثلا عندما يلزم الكشف عن المعلومات من أجل الحصول على أمر محكمة يلزم بتقديم المساعدة، أو حيث يلزم إطلاع الأشخاص الخواص الذين تتوفر لديهم أدلة، بالطلب حتى يتسنى تنفيذه بنجاح. وإذا لم يتمكن الطرف متلقي الطلب من الامتثال لطلب السرية، فإنه يخطر بذلك الطرف مقدم الطلب، الذي يبقى لديه بعد ذلك خيار سحب الطلب أو تعديله.

٢٧٤.ينبغي للسلطات المركزية المعينة وفقا للفقرة ٢ أن تتواصل مباشرة فيما بينها. ومع ذلك، يمكن في الحالات الطارئة، للقضاة والمدعين العامين في الطرف مقدم الطلب إرسال طلبات المساعدة القانونية المتبادلة مباشرة إلى القضاة والمدعين العامين في الطرف متلقي الطلب. ويتعين على القاضي أو المدعي العام الذي يتبع هذا الإجراء أن يوجه أيضا نسخة من الطلب المقدم إلى سلطته المركزية بغية إحالته إلى السلطة المركزية لدى الطرف متلقي الطلب. وبموجب الفقرة (ب)، يمكن توجيه الطلبات عن طريق الإنتربول. ويقع على سلطات الطرف متلقي الطلب التي تتلقى طلبا خارج نطاق اختصاصها، عملا بالفقرة (ج)، التزام ذو شقين: أولهما أنه يجب عليها إحالة الطلب إلى السلطة المختصة لدى الطرف متلقي الطلب، وثانيهما، أنه يجب عليها أن تبلغ سلطات الطرف مقدم الطلب بالإحالة المنجزة. ويمكن أيضا، بموجب الفقرة (د)، أن ترسل الطلبات مباشرة، دون تدخل السلطات المركزية حتى وإن لم تكن هناك حالة طارئة، طالما توفرت لدى سلطة الطرف متلقي الطلب القدرة على الامتثال للطلب دون اللجوء إلى إجراءات قسرية. وفي الأخير، تمكن الفقرة (ه) الطرف بإخبار

الأطراف الأخرى، من خلال الأمين العام لمجلس أوروبا، بأنه ينبغي، لأسباب تتعلق بالفعالية، توجيه المراسلات المباشرة إلى السلطة المركزية.

السرية والقيود على الاستخدام (المادة ٢٨)

٢٧٥. ينص هذا الحكم تحديدا على فرض قيود على استخدام المعلومات أو المواد، لتمكين الطرف متلقي الطلب، في الحالات التي تكون فيها هذه المعلومات أو المواد حساسة بشكل خاص، من ضمان أن يقتصر استعمالها على غرض المساعدة الذي منحت من أجله، أو لضمان عدم نشرها خارج نطاق موظفي سلطة إنفاذ القانون في الطرف مقدم الطلب. وتوفر هذه القيود ضمانات متاحة لأغراض منها حماية البيانات، من بين أمور أخرى.

٢٧٦. على غرار المادة ٢٧، لا تنطبق المادة ٢٨ إلا في غياب معاهدة للمساعدة المتبادلة أو ترتيب على أساس تشريعات موحدة أو متبادلة سارية بين الأطراف المقدمة والمتلقية للطلب. وفي حالة سريان هذه المعاهدة أو الترتيب، تطبق أحكامها المتعلقة بالسرية والقيود على الاستخدام بدلا من أحكام هذه المادة، ما لم يتفق الطرفان على خلاف ذلك. وهذا يسمح بتفادي التداخل مع معاهدات المساعدة القانونية ثنائية ومتعددة الأطراف القائمة والترتيبات المماثلة، مما يمكن الممارسين من مواصلة العمل في إطار النظام العادي المستوعب بشكل جيد بدلا من السعي إلى تطبيق آليتين متنافسين، وربما متناقضين.

٢٧٧. تسمح الفقرة ٢ للطرف متلقي الطلب، عند الاستجابة لطلب المساعدة المتبادلة، بفرض نوعين من الشروط. أولهما، يجوز له أن يطلب الحفاظ على سرية المعلومات أو المواد المقدمة في الحالات التي لا يمكن فيها الامتثال للطلب في حال غياب مثل هذا الشرط، مثلا عندما تكون هوية مخبر سري مهددة. وليس من الملائم المطالبة بالسرية المطلقة في الحالات التي يكون فيها الطرف متلقي الطلب ملزما بتقديم المساعدة المطلوبة، لأن ذلك من شأنه أن يقوض، في كثير من الحالات، قدرة الطرف مقدم الطلب على التحقيق في الجرائم أو محاكمتها بنجاح، مثلا من خلال استخدام الأدلة في محاكمة علنية (بما في ذلك الكشف الإلزامي).

٢٧٨. ثانيا، يجوز للطرف متلقي الطلب أن يقرن تقديم المعلومات أو المواد بشرط ألا يتم استخدامها في تحقيقات أو إجراءات غير تلك المشار إليها في الطلب. ولكي ينطبق هذا الشرط، يجب أن يشير إليه الطرف متلقي الطلب بصريح العبارة، وإلا، لا يوجد أي قيد من هذا القبيل على استخدامها من قبل الطرف مقدم الطلب. وفي الحالات التي يتم فيها إبداء هذا الشرط، فإنه يضمن عدم استخدام المعلومات والمواد إلا للأغراض المتوخاة في الطلب، مما يستبعد استخدام المادة لأغراض أخرى دون موافقة الطرف متلقي الطلب. وقد اعترف المفاوضون باستثناءين للقدرة على الحد من الاستخدام وهما مشمولان ضمنيا في أحكام الفقرة. أولا، في إطار المبادئ القانونية الأساسية لكثير من الدول، إذا كانت المواد الموفرة تمثل دليلا على تبرئة شخص متهم، فيجب الكشف عنها لهيئة الدفاع أو لسلطة قضائية. بالإضافة إلى ذلك، تكون معظم المواد الموفرة في إطار أنظمة المساعدة المتبادلة موجهة للاستخدام خلال المحاكمة، عادة دعوى عامة (بما في ذلك، الكشف الإجباري). وحالما يتم الكشف عن هذه المعلومات، فإن المادة تكون قد انتقلت بشكل أساسي إلى النطاق العام. وفي هذه الحالات، لا يمكن ضمان سرية التحقيق أو الإجراء الذي تطلب بشأنه المساعدة المتبادلة.

٢٧٩. تنص الفقرة ٣ على أنه في حال تعذر على الطرف الذي ترسل إليه المعلومات الامتثال للشرط المفروض، تعين عليه إشعار الطرف مقدم الطلب، الذي يبقى له بعد ذلك خيار عدم تقديم تلك المعلومات. أما إذا وافق الطرف المتلقي على هذا الشرط، فيجب عليه احترامه.

٢٨٠. تنص الفقرة ٤ على أنه يجوز أن يطلب من الطرف مقدم الطلب تفسير الاستخدام المخصص للمعلومات أو المواد التي تلقاها بموجب الشروط المبينة في الفقرة ٢، لكي يتسنى للطرف متلقي الطلب التأكد من الامتثال لهذا الشرط. وتم الاتفاق على أنه لا يجوز للطرف متلقي الطلب المطالبة بمساءلة مرهقة للغاية، في كل مرة يتم فيها النفاذ إلى المواد أو المعلومات المقدمة، على سبيل المثال.

القسم ٢: أحكام خاصة

٢٨١.يرمي هذا القسم إلى توفير آليات محددة من أجل اتخاذ إجراءات دولية فعالة ومتشاور بشأنها في الحالات التي تنطوي على جرائم متصلة بالكمبيوتر والأدلة في شكل إلكتروني.

الباب الأول – المساعدة المتبادلة بشأن التدابير المؤقتة

التعجيل في حفظ بيانات الكومبيوتر المخزنة (المادة ٢٩)

٢٨٢.تنص هذه المادة على آلية على الصعيد الدولي مطابقة لتلك المنصوص عليها في المادة ١٦ من أجل الاستخدام على الصعيد الوطني. وتخول الفقرة ١ من هذه المادة للطرف أن يقدم طلبا للحصول على التعجيل بحفظ البيانات المخزنة في إقليم الطرف متلقي الطلب، وتقتضي الفقرة ٣ أن يكون لكل طرف القدرة القانونية على تحقيق ذلك عبر نظام الكمبيوتر، بغية تفادي تغيير البيانات أو إزالتها أو حذفها خلال الفترة الزمنية اللازمة لإعداد وإرسال وتنفيذ طلب المساعدة المتبادلة للحصول على تلك البيانات. ويعتبر الحفظ تدبيرا مؤقتا محدودا تتوخى منه السرعة بشكل أكبر بكثير من تنفيذ المساعدة المتبادلة التقليدية. وكما أشير سابقا، تعتبر بيانات الكمبيوتر شديدة التقلب. ويمكن حذفها ببضع نقرات على لوحة المفاتيح أو عن طريق تشغيل برامج تلقائية، مما يجعل من المستحيل تتبع الجريمة للوصول إلى مرتكبها أو يؤدي إلى إتلاف الأدلة الهامة على الجريمة. يتم تخزين بعض أشكال بيانات الكمبيوتر لفترات قصيرة فقط قبل حذفها. وهكذا، تم الاتفاق على أن هناك حاجة إلى آلية لضمان توافر هذه البيانات ريثما يتم تنفيذ العملية الأطول والأشمل لطلب المساعدة المتبادلة الرسمية التي قد تستغرق أسابيع أو شهور.

٢٨٣.ولئن كان هذا التدبير أسرع بكثير من ممارسة المساعدة المتبادلة العادية، فإنه في الوقت نفسه أقل تطفلا. ولا يطلب من الموظفين المسؤولين عن المساعدة المتبادلة في الطرف متلقي الطلب الحصول على البيانات من الجهة الوديعة. ولعل الإجراء المفضل للطرف متلقي الطلب يتمثل في ضمان أن تقوم الجهة الوديعة (التي غالبا ما تكون مقدم خدمة أو طرفا ثالثا) بحفظ البيانات (أي، عدم حذفها) ريثما تصدر عملية تقضي بتسليمها إلى موظفي إنفاذ القانون في مرحلة لاحقة. وتتميز هذه العملية بالسرعة وحماية خصوصية الشخص الذي تخصه البيانات، حيث لن يتم الكشف عنها أو فحصها من قبل أي مسؤول حكومي حتى يتم استيفاء معايير الكشف الكامل وفقا لأنظمة المساعدة المتبادلة العادية. وفي الوقت نفسه، يسمح للطرف متلقي الطلب باستخدام إجراءات أخرى لضمان الحفظ السريع للبيانات، بما في ذلك التعجيل بإصدار وتنفيذ أمر التقديم أو أمر البحث عن البيانات. ويتمثل الشرط الأساسي في التوفر على عملية سريعة للغاية لتفادي ضياع البيانات بصورة لا رجعة فيها.

٢٨٤.تبين الفقرة ٢ محتويات طلب الحفظ عملا بهذه المادة. وإذ تضع اللجنة في اعتبارها أن هذا الإجراء تدبير مؤقت وأن يتعين إعداد الطلب وإرساله بسرعة، فإن المعلومات المقدمة تكون موجزة وتشمل فقط الحد الأدنى من المعلومات المطلوبة لتمكين حفظ البيانات. وبالإضافة إلى تحديد السلطة التي تسعى إلى الحفظ والجريمة التي يطلب من أجلها الحفظ، يجب أن يتضمن الطلب موجزا للوقائع، ومعلومات كافية لتحديد البيانات التي يتعين حفظها وموقعها، وأن يبين أن البيانات ذات صلة بالتحقيق في الجريمة المعنية أو ملاحقتها قضائيا، وأن حفظها ضروري. وفي الأخير، يتعين على الطرف مقدم الطلب أن يتقدم بعد ذلك بطلب للمساعدة المتبادلة حتى يتسنى له الحصول على البيانات.

٢٨٥.تنص الفقرة ٣ على أنه لا ينبغي فرض مبدأ ازدواجية التجريم كشرط لتوفير الحفظ. بشكل عام، يسفر تطبيق مبدأ ازدواجية التجريم عن نتيجة عكسية في سياق الحفظ. أولا، في إطار الممارسة الحديثة في مجال المساعدة المتبادلة، ثمة ميول إلى إلغاء شرط ازدواجية التجريم بالنسبة لكافة التدابير، ما عدا التدابير الإجرائية الأكثر تطفلا، مثل البحث والمصادرة أو الاعتراض. غير أن الحفظ، وفقا لتصور القائمين على الصياغة، لا يعتبر تطفلا بشكل خاص لأن الجهة الوديعة يحتفظ بحيازة البيانات التي بحوزته بصورة قانونية، ولا يتم الكشف عن البيانات للمسؤولين لدى الطرف المتلقي أو فحصها من قبلهم إلى أن يتم تنفيذ طلب المساعدة المتبادلة الرسمية الذي يلتمس الكشف عن البيانات. وثانيا، وكمسألة عملية، غالبا ما يستغرق تقديم التوضيحات اللازمة لإثبات وجود ازدواجية التجريم بصورة قاطعة وقتا طويلا لدرجة يمكن في غضونه حذف البيانات، إزالتها أو تغييرها. فعلى سبيل المثال، قد يدرك الطرف مقدم الطلب في المراحل المبكرة من التحقيق أنه قد تم اقتحام جهاز كمبيوتر في إقليمه، لكن قد لا يستوعب جيدا طبيعة الضرر ونطاقه إلا في وقت لاحق. وفي احتمال تأخير الطرف متلقي الطلب لحفظ بيانات الحركة التي من شأنها أن تتقفى مصدر الاقتحام في انتظار إقامة ازدواجية التجريم، فإن البيانات الهامة غالبا ما تحذف بصورة روتينية من قبل مقدمي الخدمات الذين يحتفظون بها لساعات أو أيام

فقط بعد الإرسال. وحتى إذا ما تمكن الطرف مقدم الطلب بعد ذلك من إنشاء ازدواجية التجريم، فإنه لا يتمكن من استرداد بيانات الحركة الحاسمة ولن يتم أبدا تحديد هوية مرتكب الجريمة.

٢٨٦.وهكذا، تتمثل القاعدة العامة في استغناء الأطراف عن أي شرط بازدواجية التجريم لأغراض الحفظ. إلا أن الفقرة ٤ توفر إمكانية إبداء تحفظ محدود. فإذا كان طرف ما يقتضي ازدواجية التجريم كشرط للاستجابة لطلب المساعدة المتبادلة لتقديم البيانات، وإذا كان لديه ما يدعو للاعتقاد بأنه عند الكشف، لن يتم استيفاء شرط ازدواجية التجريم، لأمكنه الاحتفاظ بالحق في طلب ازدواجية التجريم كشرط مسبق لحفظ البيانات. وفيما يتعلق بالجرائم المقررة وفقا للمواد من ٢ إلى ١١، يفترض أن شرط ازدواجية التجريم يلبى تلقائيا بين الأطراف، رهنا بأي تحفظات قد تكون قد أبدتها على هذه الجرائم حيثما تسمح بذلك الاتفاقية. لذلك، لا يجوز للأطراف أن تفرض هذا الشرط إلا فيما يتعلق بجرائم غير تلك المحددة في الاتفاقية.

٢٨٧.على خلاف ذلك، لا يجوز للطرف متلقي الطلب، بموجب الفقرة ٥، أن يرفض طلبا للحفظ إلا إذا كان تنفيذه يمس بسيادته أو أمنه أو نظامه العام أو مصالحه الأساسية الأخرى، أو عندما يعتبر الجريمة جريمة سياسية أو جريمة ذات الصلة بجريمة سياسية. ونظرا لمركزية هذا التدبير في التحقيق الفعال والملاحقة القضائية للجرائم المرتكبة عبر الكمبيوتر أو المتصلة بالكمبيوتر، تم الاتفاق على أن تأكيد أي أساس آخر لرفض طلب الحفظ أمر مستبعد.

٢٨٨.في بعض الأحيان، يدرك الطرف متلقي الطلب أنه من المرجح أن تتخذ الجهة الوديعة للبيانات إجراءات من شأنها أن تهدد سرية التحقيق الذي يجريه الطرف مقدم الطلب، أو أن تلحق بها الضرر بطريقة أخرى (على سبيل المثال، عندما تودع البيانات الواجب حفظها لدى مقدم للخدمة تسيطر عليه جماعة إجرامية، أو لدى الجهة المستهدفة بالتحقيق نفسها). وفي هذه الحالات، يجب بموجب الفقرة ٦، إشعار الطرف مقدم الطلب على وجه السرعة، حتى يتسنى له تقييم ما إذا كان سيتحمل الخطر الذي ينطوي عليه تنفيذ طلب الحفظ أو سيسعى إلى شكل أكثر تطفلا ولكن أكثر أمانا من أشكال المساعدة المتبادلة، كالتقديم أو البحث والمصادرة.

٢٨٩.وفي الأخير، تلزم الفقرة ٧ كل طرف بضمان الاحتفاظ بالبيانات المحفوظة عملا بهذه المادة، لمدة ٦٠ يوما على الأقل ريثما يتم تسلم طلب رسمي بالمساعدة المتبادلة يسعى للكشف عن البيانات، واستمرارية الاحتفاظ بها بعد استلام الطلب.

تعجيل الكشف عن بيانات الحركة المحفوظة (المادة ٣٠)

٢٩٠.تنص هذه المادة على المقابل الدولي للقوة للسلطة المنصوص عليها من أجل الاستخدام المحلي في المادة ١٧. وكثيرا ما يقوم الطرف متلقي الطلب، بناء على طلب طرف ارتكبت فيه جريمة، بحفظ بيانات الحركة فيما يتعلق بإرسال انتقل عبر حواسيبه، من أجل تتبع انتقاله إلى مصدره وتحديد مرتكب الجريمة، أو تحديد الأدلة القاطعة. ويمكن أن يكتشف الطرف متلقي الطلب، عند قيامه بذلك، أن بيانات الحركة الموجودة في إقليمه تبين أنه تم توجيه الإرسال من مقدم خدمة في دولة ثالثة أو من مقدم خدمة في الدولة مقدمة الطلب نفسها. وفي مثل هذه الحالات، يتعين على الطرف متلقي الطلب أن يقدم على وجه السرعة إلى الطرف مقدم الطلب كمية كافية من بيانات الحركة لتمكين التعرف على هوية مقدم الخدمة في الدولة الأخرى وتحديد مسار الاتصال من الدولة الأخرى المعنية. وإذا كان الإرسال صادرا من دولة ثالثة، فإن هذه المعلومات ستمكن الطرف مقدم الطلب من تقديم طلب حفظها والتعجيل بالمساعدة المتبادلة إلى تلك الدولة الأخرى بغية تتبع انتقاله إلى مصدره النهائي. وإذا أعيد الإرسال إلى الطرف مقدم الطلب، سيكون هذا الأخير قادرا على الحصول على بيانات إضافية عن الحركة والكشف عنها من خلال العمليات المحلية.

٢٩١.بموجب الفقرة ٢، لا يجوز للطرف متلقي الطلب أن يرفض الكشف عن بيانات الحركة إلا عندما يحتمل أن يلحق الكشف الضرر بسيادته، أمنه، نظامه العام أو بأي مصالح أساسية أخرى، أو حيثما اعتبر الجريمة جريمة سياسية أو ذات صلة بجريمة سياسية. وكما ورد في المادة ٢٩ (التعجيل بحفظ بيانات الكمبيوتر المخزنة)، نظرا لأن هذا النوع من المعلومات بالغ الأهمية لتحديد هوية مرتكبي الجرائم في نطاق هذه الاتفاقية أو تحديد مكان الأدلة الحاسمة، فإن أسباب الرفض تكون محدودة للغاية، وتم الاتفاق على أن تأكيد أي أساس آخر لرفض المساعدة أمر مستبعد.

المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكومبيوتر المخزنة (المادة ٣١)

٢٩٢. يجب أن تتوفر لدى كل طرف القدرة على إجراء، لفائدة طرف آخر، البحث أو النفاذ بطريقة مماثلة، المصادرة أو التأمين بطريقة مماثلة والكشف عن بيانات مخزنة بواسطة نظام كمبيوتر يوجد داخل إقليمه، كما ورد في المادة ١٩ (البحث عن بيانات الكمبيوتر المخزنة ومصادرتها) حيث يجب أن يتوفر على القدرة على القيام بذلك للأغراض المحلية. وتجيز الفقرة ١ للطرف بطلب هذا النوع من المساعدة المتبادلة، وتقضي الفقرة ٢ بأن يكون الطرف متلقي الطلب قادرا على تقديمه. وتطبق الفقرة ٢ أيضا مبدأ ضرورة تطابق أحكام وشروط تقديم هذا التعاون لتلك الأحكام والشروط المنصوص عليها في المعاهدات والترتيبات والقوانين المحلية المنطبقة التي تحكم المساعدة القانونية المتبادلة في المسائل الجنائية. وبموجب الفقرة ٣، يجب التعجيل بالرد على هذا الطلب عندما (١) تكون هنالك أسباب تدعو إلى الاعتقاد بأن البيانات ذات الصلة معرضة بشكل خاص للإتلاف أو التعديل، أو (٢) عندما تنص هذه المعاهدات، الترتيبات أو القوانين على خلاف ذلك.

النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم (المادة ٣٢)

٢٩٣. ناقش القائمون على صياغة الاتفاقية بشكل مستفيض مسألة متى يسمح لطرف بالنفاذ من جانب واحد إلى بيانات الكمبيوتر المخزنة في طرف آخر دون التماس المساعدة المتبادلة. وتم بشكل مفصل تدارس الحالات التي يمكن فيها للدول أن تقبل العمل من جانب واحد وتلك التي لا تكون مقبولة. وقرر القائمون على الصياغة في نهاية المطاف أنه لم يكن من الممكن بعد إعداد نظام شامل وملزم قانونيا ينظم هذا المجال. ويعزى ذلك من جهة إلى انعدام الخبرة الملموسة في مثل هذه الحالات حتى الآن؛ ومن جهة أخرى إلى استيعاب أن الحل المناسب غالبا ما يحيل على الظروف الدقيقة للحالة الفردية، مما يجعل من الصعب صياغة قواعد عامة. وفي الأخير، قرر القائمون على الصياغة أن يتم التنصيص في المادة ٣٢ من الاتفاقية فقط على الحالات التي اتفق فيها الجميع على أن العمل من جانب واحد مسموح به. واتفقوا على عدم تنظيم حالات أخرى إلى أن يتم جمع المزيد من الخبرة وإجراء مزيد من المناقشات في ضوء ذلك. وفي هذا الصدد، تنص الفقرة ٣ من المادة ٣٩ على أن الحالات الأخرى ليست لا مرخصة ولا مستبعدة.

٢٩٤. تتناول المادة ٣٢ (النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم) حالتين: الأولى، عندما تكون البيانات التي يتم النفاذ إليها متاحة للجمهور، وثانيا، عندما يكون الطرف قد استفاد من بيانات أو توصل بها من خارج إقليمه عبر نظام كمبيوتر في إقليمه، وحصل على الموافقة القانونية والطوعية للشخص الذي يتمتع بالسلطة القانونية بالكشف عن البيانات إلى الطرف من خلال ذلك النظام. وقد يختلف نوع الشخص "المرخص له قانونيا" بالكشف عن البيانات حسب الظروف، وطبيعة الشخص والقانون واجب التطبيق المعنيين. على سبيل المثال، يمكن أن يتم تخزين البريد الإلكتروني للشخص في بلد آخر من قبل مقدم الخدمة، أو أن يقوم شخص بتخزين بيانات عمدا في بلد آخر. ويجوز لهؤلاء الأشخاص استرجاع البيانات، كما يمكنهم أن يكشفوا طوعا عن البيانات إلى الموظفين المكلفين بإنفاذ القانون، أو أن يسمحوا لهؤلاء الموظفين بالنفاذ إلى البيانات، كما هو المنصوص عليه في المادة، شريطة أن تتوفر لهم السلطة القانونية.

المساعدة المتبادلة ذات الصلة بجمع بيانات الحركة في الوقت الحقيقي (المادة ٣٣)

٢٩٥. في كثير من الحالات، لا يستطيع المحققون ضمان تمكنهم من تتبع اتصال إلى مصدره باتباع المسار من خلال سجلات للإرسالات السابقة، نظرا لاحتمال الحذف التلقائي لبيانات الحركة الأساسية من قبل مقدم الخدمة في سلسلة الإرسال قبل التمكن من حفظها. ولذلك فمن الأهمية بمكان أن يكون لدى المحققين في كل طرف القدرة على الحصول على بيانات الحركة في الوقت الحقيقي فيما يتعلق بالاتصالات التي تمر عبر نظام الكمبيوتر في أطراف أخرى. وبناء عليه، فإن كل طرف ملزم، بموجب المادة ٣٣ (المساعدة المتبادلة بشأن جمع بيانات الحركة في الوقت الحقيقي)، بجمع بيانات الحركة في الوقت الحقيقي لفائدة طرف آخر. ولئن كانت هذه المادة تقتضي من الأطراف أن تتعاون بشأن هذه المسائل، فإنه ينبغي في هذا المقام على غرار أي جوانب أخرى، مراعاة الطرائق القائمة للمساعدة المتبادلة. ومن ثم، فإن الأحكام والشروط التي يتعين بموجبها تقديم هذا التعاون هي عموما تلك المنصوص عليها في المعاهدات والترتيبات والقوانين السارية التي تحكم المساعدة القانونية المتبادلة في المسائل الجنائية.

٢٩٦.في كثير من البلدان، تقدم المساعدة المتبادلة على نطاق واسع فيما يتعلق بجمع بيانات الحركة في الوقت الحقيقي، لأن هذا النوع من الجمع يعتبر أقل تطفلا من اعتراض بيانات المحتوى أو عمليات البحث والمصادرة. ومع ذلك، يتبنى عدد من الدول مقاربة أضيق. وبناء على ذلك، تسمح الفقرة ٢، فيما يتعلق بنطاق التدبير الداخلي المطابق، للأطراف بحصر نطاق تطبيق هذا التدبير على نطاق أضيق من الجرائم المنصوص عليها في المادة ٢٣ (المبادئ العامة المتعلقة بالتعاون الدولي) بنفس الطريقة التي يجوز بها للأطراف أن يبدوا تحفظا بموجب المادة ١٤ (نطاق الأحكام الإجرائية). وورد تحذير مفاده أنه لا يجوز بأي حال من الأحوال أن يكون نطاق الجرائم أضيق من نطاق الجرائم التي يتاح بشأنها تدبير من هذا القبيل في قضية محلية مماثلة. وفي الواقع، ونظرا لأن جمع بيانات الحركة في الوقت الحقيقي يكون في بعض الأحيان الطريقة الوحيدة للتحقق من هوية مرتكب الجريمة، ولأن هذا التدبير أقل تطفلا، فإن استخدام مصطلح "على الأقل" في الفقرة ٢ يهدف إلى تشجيع الأطراف على السماح بأكبر قدر ممكن من المساعدة، أي حتى في غياب ازدواجية التجريم.

المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى (المادة ٣٤)

٢٩٧.نظرا لشدة التدخل التي تتسم بها عملية الاعتراض، تم تقييد إلزامية تقديم المساعدة المتبادلة لاعتراض بيانات المحتوى. ويجب تقديم المساعدة في حدود ما تسمح به معاهدات وقوانين الأطراف المعمول بها. وبما أن توفير التعاون من أجل اعتراض المحتوى هو مجال ناشئ من ممارسات المساعدة المتبادلة، فقد تقرر إرجاء أنظمة المساعدة المتبادلة القائمة والقوانين المحلية فيما يتعلق بنطاق وحدود إلزامية المساعدة. وفي هذا الصدد، وردت إشارة إلى التعليقات على المواد ١٤ و١٥ و٢١ وكذلك إلى التوصية رقم 10 (85) بشأن التطبيق العملي للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابات القضائية من أجل اعتراض الاتصالات.

الباب الثالث – شبكة على مدار الساعة و٧ أيام في الأسبوع

شبكة على مدار الساعة و٧ أيام في الأسبوع (المادة ٣٥)

٢٩٨.كما سبق مناقشة ذلك، تتطلب المكافحة الفعالة للجرائم التي ترتكب عن طريق استخدام أنظمة الكمبيوتر والجمع الفعال للأدلة في شكل إلكتروني استجابة سريعة للغاية. فضلا عن ذلك، يمكن، من خلال نقرات قليلة على لوحة المفاتيح، اتخاذ إجراء في منطقة من العالم تترتب عنه فورا آثار عدة على بعد آلاف الكيلومترات والعديد من المناطق الزمنية. لهذا السبب، يتطلب التعاون القائم بين الشرطة وآليات المساعدة المتبادلة وجود قنوات تكميلية للتصدي لتحديات عصر الكمبيوتر بشكل فعال. وتستند القناة المنشأة في هذه المادة إلى الخبرة المكتسبة من شبكة تعمل بالفعل تحت رعاية مجموعة الدول الثمانية. وبموجب هذه المادة، يقع على كل طرف التزام بتعيين نقطة اتصال متاحة ٢٤ ساعة في اليوم و٧ أيام في الأسبوع لضمان تقديم المساعدة الفورية في التحقيقات والإجراءات في نطاق هذا الفصل، خاصة كما هو محدد بموجب المادة ٣٥، الفقرة ١، البندين "أ" – "ج"). وتم الاتفاق على أن إنشاء هذه الشبكة يعتبر من بين أهم الوسائل المنصوص عليها في هذه الاتفاقية لضمان قدرة الأطراف على الاستجابة بفعالية لتحديات إنفاذ القانون التي تطرحها الجرائم المرتكبة عبر الكمبيوتر أو ذات الصلة بالكمبيوتر.

٢٩٩.يتعين على كل نقطة اتصال على مدار الساعة وطوال أيام الأسبوع يعينها الطرف أن تقوم إما بتيسير أو الاضطلاع مباشرة بتقديم المشورة التقنية وحفظ البيانات وجمع الأدلة وتوفير المعلومات القانونية وتحديد مكان المشتبه بهم، من بين أمور أخرى. ويقصد بمصطلح "المعلومات القانونية" في الفقرة ١ تقديم المشورة لطرف آخر يطلب التعاون بأي شروط قانونية مسبقة مطلوبة لتوفير التعاون غير الرسمي أو الرسمي.

٣٠٠.يتمتع كل طرف بحرية تحديد المكان الذي تستقر فيه نقطة الاتصال داخل بنية إنفاذ القانون. وقد ترغب بعض الأطراف في جعل مقر نقطة الاتصال ٧/٢٤ داخل سلطتها المركزية للمساعدة المتبادلة، وقد يعتبر البعض الآخر أن أفضل مكان لإيواء نقطة الاتصال هو وحدة الشرطة المتخصصة في مكافحة الجريمة المرتكبة عبر الكمبيوتر – أو الجرائم ذات الصلة بالكمبيوتر، ومع ذلك، قد تكون هنالك خيارات أخرى ملائمة لطرف معين، بالنظر إلى هيكله الحكومي ونظامها القانوني. وحيث يتعين على نقطة الاتصال ٧/٢٤ تقديم المشورة الفنية لوقف هجوم أو تتبعه، علاوة على واجبات التعاون الدولي من قبيل تحديد مكان المشتبه بهم، فلا يمكن تلخيص الحلول في إجابة واحدة صحيحة، علما أنه من المتوقع أن تتطور بنية

الشبكة مع مرور الوقت. وينبغي عند تعيين نقطة الاتصال الوطنية، إيلاء الاعتبار الواجب للحاجة إلى التواصل مع نقاط الاتصال في لغات أخرى.

٣٠١.تنص الفقرة ٢ على أن من بين المهام الحاسمة التي يتعين أن تضطلع بها نقطة الاتصال ٧/٢٤ ثمة القدرة على تيسير التنفيذ السريع لتلك المهام التي لا تضطلع بها مباشرة بنفسها. على سبيل المثال، إذا كانت نقطة الاتصال ٧/٢٤ للطرف جزءا من وحدة الشرطة، وجب أن تكون لديها القدرة على التعجيل بالتنسيق مع العناصر الأخرى ذات الصلة داخل الحكومة، من قبيل السلطة المركزية لتسليم المجرمين أو المساعدة المتبادلة، بغية تمكين اتخاذ الإجراءات المناسبة في أي ساعة من النهار أو الليل. وبالإضافة إلى ذلك، تقتضي الفقرة ٢ أن يكون لدى كل نقطة اتصال ٧/٢٤ لدى طرف القدرة على إجراء اتصالات عاجلة بأعضاء آخرين في الشبكة.

٣٠٢.تقتضي الفقرة ٣ أن تتوفر كل نقطة اتصال في الشبكة على المعدات المناسبة، حيث تعتبر أجهزة الهاتف والفاكس والكمبيوتر الحديثة ضرورية لاشتغال الشبكة بشكل سلس، كما ستكون هنالك حاجة إلى إدراج أشكال أخرى من معدات الاتصال والتحليل كجزء من النظام مع تقدم التكنولوجيا. وتقتضي الفقرة ٣ أيضا بأن يكون الموظفون المشاركون في فريق الطرف المعني بالشبكة مدربين بالشكل اللازم في مجال الجريمة المرتكبة على الكمبيوتر والجريمة ذات الصلة بالكمبيوتر وطرق التصدي لها بفعالية.

الفصل الرابع – الأحكام الختامية

٣٠٣.مع بعض الاستثناءات، تستند الأحكام الواردة في هذا الفصل، في معظمها، إلى "البنود الختامية النموذجية للاتفاقيات والاتفاقات المبرمة داخل مجلس أوروبا" والتي وافقت عليها لجنة الوزراء في الجلسة ٣١٥ خلال اجتماع النواب المنعقد في فبراير/شباط ١٩٨٠. وبما أن معظم المواد من ٣٦ إلى ٤٨ إما تستخدم اللغة الموحدة في البنود النموذجية أو تستند إلى ممارسة طويلة الأمد في مجال وضع المعاهدات في مجلس أوروبا، فإنها لا تدعو إلى تعليقات محددة. ومع ذلك، فإن بعض التعديلات في البنود النموذجية المعيارية أو بعض الأحكام الجديدة، تقتضي بعض التوضيح. ويلاحظ في هذا السياق، أن البنود النموذجية اعتمدت كمجموعة غير ملزمة من الأحكام. وكما وردت الإشارة في تقديم البنود النموذجية فإن "الغرض من هذه البنود الختامية النموذجية يتلخص في تسهيل مهمة لجان الخبراء وتجنب الاختلافات النصية التي لا يكون لها أي مبرر حقيقي. ولا يعتبر النموذج بأي حال من الأحوال ملزما ويمكن تكييف بنود مختلفة لتناسب حالات معينة ".

التوقيع والدخول حيز النفاذ (المادة ٣٦)

٣٠٤.صيغت الفقرة ١ من المادة ٣٦ وفقا لعدة سوابق وضعت في اتفاقيات أخرى أعدت في إطار مجلس أوروبا، ومنها مثلا اتفاقية نقل الأشخاص المدانين (سلسلة المعاهدات الأوروبية رقم ١١٢) والاتفاقية المعنية بمكافحة غسل الأموال، والبحث عن عائدات الجريمة وضبطها ومصادرتها (سلسلة المعاهدات الأوروبية رقم ١٤١)، والتي تسمح بالتوقيع عليها، قبل دخولها حيز النفاذ، ليس فقط من قبل الدول الأعضاء في مجلس أوروبا، بل أيضا من لدن الدول غير الأعضاء التي تشارك في صياغتها. ويهدف هذا الحكم إلى تمكين أكبر عدد ممكن من الدول المهتمة، وليس فقط الدول الأعضاء في مجلس أوروبا، من أن تصبح أطرافا في أقرب وقت ممكن. وهنا، يقصد من هذا الحكم أن ينطبق على أربع دول غير أعضاء هي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية التي شاركت بنشاط في صياغة الاتفاقية. وبمجرد دخول الاتفاقية حيز النفاذ، وفقا للفقرة ٣، يجوز دعوة دول أخرى من غير الأعضاء التي لا يشملها هذا الحكم إلى الانضمام إلى الاتفاقية وفقا للفقرة ١ من المادة ٣٧.

٣٠٥.تحدد الفقرة ٣ من المادة ٣٦ عدد التوقيعات أو القبول أو الموافقات اللازمة لدخول الاتفاقية حيز النفاذ، في ٥. ويعتبر هذا الرقم أعلى من العتبة المعتادة (٣) في معاهدات مجلس أوروبا ويعكس الاعتقاد بأن ثمة حاجة إلى مجموعة أكبر قليلا من الدول للشروع بنجاح في التصدي للتحدي للجرائم الدولية المرتكبة عبر الكمبيوتر أو ذات الصلة بالكمبيوتر. ومع ذلك، فإن هذا العدد ليس مرتفعا لدرجة قد تؤدي إلى التأخير غير الضروري لدخول الاتفاقية حيز النفاذ. ومن بين الدول الخمس الأولى، يجب أن تكون ثلاثة دول على الأقل من الأعضاء في مجلس أوروبا، ويمكن أن تكون الدولتان الأخريان من الدول

الأربع غير الأعضاء التي شاركت في صياغة الاتفاقية. وبطبيعة الحال، من شأن هذا الحكم أيضا أن يسمح بدخول الاتفاقية حيز التنفيذ بناء على التعبير خمس دول أعضاء في مجلس أوروبا عن الموافقة بالالتزام.

الانضمام إلى الاتفاقية (المادة ٣٧)

٣٠٦. صيغت المادة ٣٧ أيضا وفقا للسوابق المنصوص عليها في اتفاقيات أخرى لمجلس أوروبا، مع تضمنها لعنصر إضافي صريح. بموجب ممارسة معمول بها منذ عهد طويل، تقرر لجنة الوزراء، بمبادرة منها أو بناء على طلب، دعوة دولة غير عضو لم تشارك في وضع اتفاقية، للانضمام إلى الاتفاقية بعد التشاور مع جميع الأطراف المتعاقدة، سواء كانت دولا أعضاء أم لا. وهذا يعني أنه إذا اعترض أي طرف متعاقد على انضمام دولة غير عضو، فإن لجنة الوزراء لا تدعوها عادة للانضمام إلى الاتفاقية. غير أنه بموجب الصياغة المعتادة، يمكن للجنة الوزراء، نظريا، أن تدعو تلك الدولة غير العضو إلى الانضمام إلى اتفاقية حتى إذا اعترضت دولة طرف غير عضو على انضمامها. وهذا يعني أن حق النقض - من الناحية النظرية - لا يمنح عادة للدول غير الأعضاء بشأن عملية توسيع معاهدات مجلس أوروبا إلى دول أخرى من غير الأعضاء. ومع ذلك، تم إدراج شرط صريح يتمثل في تشاور لجنة الوزراء مع جميع الدول المتعاقدة – وليس فقط الأعضاء في مجلس أوروبا – والحصول على موافقتها بالإجماع – قبل دعوة دولة غير عضو إلى الانضمام إلى الاتفاقية. وكما هو مبين أعلاه، فإن هذا الشرط يتفق مع الممارسة ويعترف بأن جميع الدول المتعاقدة في الاتفاقية ينبغي أن تكون قادرة على تحديد الدول غير الأعضاء التي ترغب في بناء علاقات تعاهدية معها. ومع ذلك، يتم اتخاذ القرار الرسمي بدعوة دولة غير عضو إلى الانضمام، وفقا للممارسة المعتادة، من قبل ممثلي الأطراف المتعاقدة التي يحق لها حضور اجتماعات لجنة الوزراء. ويقتضي هذا القرار أغلبية الثلثين المنصوص عليها في المادة ٢٠(د) من النظام الأساسي لمجلس أوروبا وتصويت ممثلي الأطراف المتعاقدة الذين يحق لهم حضور اجتماع اللجنة بالإجماع.

٣٠٧. يطلب من الدول الاتحادية التي تسعى إلى الانضمام إلى الاتفاقية، والتي تعتزم إصدار إعلان بموجب المادة ٤١، أن تقدم مسبقا مشروع الإعلان المشار إليه في الفقرة ٣ من المادة ٤١، بحيث تتمكن الأطراف من تقييم كيفية تأثير تطبيق الحكم الاتحادي على تنفيذ الطرف المقبل للاتفاقية (انظر الفقرة ٣٢٠).

الآثار المترتبة على الاتفاقية (المادة ٣٩)

٣٠٨. تتناول الفقرتان ١ و٢ من المادة ٣٩ علاقة الاتفاقية بالاتفاقات أو الترتيبات الدولية الأخرى. ولا تتناول البنود النموذجية المشار إليها أعلاه موضوع طريقة ارتباط اتفاقيات مجلس أوروبا ببعضها البعض أو بمعاهدات ثنائية أو متعددة الأطراف أخرى تبرم خارج مجلس أوروبا. وتنص المقاربة المعتادة المستخدمة في اتفاقيات مجلس أوروبا في مجال القانون الجنائي (مثل الاتفاق المتعلق بالاتجار غير المشروع عن طريق البحر (سلسلة المعاهدات الأوروبية رقم ١٥٦) على: (١) ألا تؤثر الاتفاقيات الجديدة على الحقوق والتعهدات المستمدة من الاتفاقيات القائمة والاتفاقيات الدولية متعددة الأطراف المتعلقة بالمسائل الخاصة؛ (٢) أنه يجوز للأطراف في اتفاقية جديدة أن تبرم اتفاقات ثنائية أو متعددة الأطراف فيما بينها بشأن المسائل التي تتناولها الاتفاقية لأغراض تكملة أو تعزيز أحكامها أو تيسير تطبيق المبادئ المجسدة فيها؛ و(٣) أنه إذا كان طرفان أو أكثر من الأطراف في الاتفاقية الجديدة قد أبرموا بالفعل اتفاقا أو معاهدة فيما يتعلق بموضوع تتناوله الاتفاقية أو طوروا علاقاتهم فيما يتعلق بذلك الموضوع، يحق لهم التقدم تطبيق ذلك الاتفاق أو تلك المعاهدة أو تنظيم تلك العلاقات وفقا لذلك، بدلا من الاتفاقية الجديدة، شريطة أن يسهل ذلك التعاون الدولي.

٣٠٩. بما أن الاتفاقية تهدف عموما إلى تكملة الاتفاقات والترتيبات ثنائية ومتعددة الأطراف بين الأطراف وليس إلى الحلول مكانها، لم يعتبر القائمون على الصياغة أن الإشارة المحدودة إلى "المسائل الخاصة" مفيدة بشكل خاص، وساورهم القلق بشأن الارتباك المحتمل الذي قد تسفر عنه تلك الإشارة. وبدلا من ذلك، تشير الفقرة ١ من المادة ٣٩ ببساطة إلى أن هذه الاتفاقية تكمل المعاهدات أو الترتيبات الأخرى المعمول بها بين الأطراف، وتذكر على وجه الخصوص ثلاث معاهدات من معاهدات مجلس أوروبا على سبيل المثال لا الحصر: الاتفاقية الأوروبية بشأن تسليم المجرمين لعام ١٩٥٧ (سلسلة المعاهدات الأوروبية رقم ٢٤) ، والاتفاقية الأوروبية بشأن المسائل الجنائية لعام ١٩٥٩ (سلسلة المعاهدات الأوروبية رقم ٣٠) وبروتوكولها الإضافي لعام ١٩٧٨ (سلسلة المعاهدات الأوروبية رقم ٩٩). ومن ثم، ينبغي للأطراف في الاتفاقية المعنية بالجريمة الإلكترونية، مبدئيا، أن تطبق هذه الاتفاقات أو الترتيبات فيما يتعلق بالمسائل العامة. أما في يخص المسائل الخاصة التي تتناولها هذه الاتفاقية فقط، تنص قاعدة التفسير "القانون الخاص يبطل القانون العام" (*lex specialis*

derogat legi generali) على أنه ينبغي للأطراف أن تعطي الأسبقية للقواعد الواردة في الاتفاقية. ومن الأمثلة على ذلك، المادة ٣٠ التي تنص على التعجيل بالكشف عن بيانات الحركة المحفوظة عند الاقتضاء بغية تحديد مسار اتصال محدد. وفي هذا المجال الخاص، ينبغي للاتفاقية، بوصفها قاعدة التخصيص (*lex specialis*)، أن توفر قاعدة الملاذ الأول على الأحكام الواردة في اتفاقات المساعدة المتبادلة الأعم.

٣١٠.وبالمثل، اعتبر القائمون على الصياغة أن الصيغة اللغوية التي تجعل تطبيق الاتفاقات القائمة أو المقبلة متوقفا على ما إذا كانت "تعزز" أو "تسهل" التعاون من شأنها أن تطرح إشكاليات، لأنه من المفترض، في إطار المقاربة المشار إليها في الفصل المتعلق بالتعاون الدولي، أن تطبق الأطراف الاتفاقات والترتيبات الدولية ذات الصلة.

٣١١.عندما يكون هنالك معاهدة أو ترتيب قائمان للمساعدة المتبادلة كأساس للتعاون، فإن هذه الاتفاقية تكمل فقط القواعد القائمة، عند الاقتضاء، على سبيل المثال، تنص هذه الاتفاقية على نقل طلبات المساعدة المتبادلة عن طريق وسائل الاتصال المعجلة (انظر الفقرة ٣ من المادة ٢٥) إن لم تكن هذه الإمكانية متاحة بموجب المعاهدة أو الترتيب الأصليين.

٣١٢.وتماشيا مع الطابع التكميلي للاتفاقية، ولا سيما مقاربتها الخاصة بالتعاون الدولي، تنص الفقرة ٢ على أن للأطراف الحرية أيضا في تطبيق الاتفاقات القائمة أو تلك التي ستدخل حيز النفاذ في المستقبل. وتوجد سابقة لهذا التعبير في الاتفاقية المعنية بنقل الأشخاص المدانين (سلسلة المعاهدات الأوروبية رقم ١١٢). وبالتأكيد، يتوقع في سياق التعاون الدولي، أن يؤدي تطبيق اتفاقات دولية أخرى (التي يوفر العديد منها صيغا فعالة منذ زمن طويل للمساعدة الدولية) إلى النهوض بالتعاون في الواقع. وتماشيا مع بنود هذه الاتفاقية، يجوز للأطراف أيضا أن توافق على تطبيق أحكام التعاون الدولي بدلا من اتفاقات أخرى من هذا القبيل (انظر المادة ٢٧(١)). وفي هذه الحالات، فإن أحكام التعاون ذات الصلة المنصوص عليها في المادة ٢٧ ستحل محل القواعد ذات الصلة في هذه الاتفاقات الأخرى. وبما أن هذه الاتفاقية تنص عموما على حد أدنى من الالتزامات، فإن الفقرة ٢ من المادة ٣٩ تعترف بأن للأطراف حرية التعهد بالتزامات أكثر تحديدا بالإضافة إلى الالتزامات المنصوص عليها في الاتفاقية عند تطوير علاقاتها بشأن المسائل التي تتناولها. إلا أن هذه الحرية ليست حقا مطلقا: يجب على الأطراف أن تحترم أهداف ومبادئ الاتفاقية عند القيام بذلك، وبالتالي لا يمكنها أن تقبل التزامات من شأنها أن تعطل غرضها.

٣١٣.علاوة على ذلك، اتفق القائمون على الصياغة أيضا على أنه يجوز للأطراف، عند تحديد العلاقة بين الاتفاقية واتفاقات دولية أخرى، أن تبحث عن توجيهات إضافية للأحكام ذات الصلة الواردة في اتفاقية فيينا لقانون المعاهدات.

٣١٤.ولئن كانت الاتفاقية توفر مستوى من التناغم ثمة حاجة ماسة إليه، فإنها لا ترمي إلى معالجة جميع المسائل المعلقة المتصلة بالجرائم المرتكبة عبر الكمبيوتر أو المتصلة بالكمبيوتر. لذلك، أضيفت الفقرة ٣ لتوضيح أن الاتفاقية تؤثر فقط على ما تتناوله. ولا تؤثر على الحقوق والقيود والالتزامات والمسؤوليات الأخرى التي يمكن أن تكون متاحة دون أن تتناولها الاتفاقية. ويمكن أن نجد سابقة "الشرط التحفظي" في اتفاقات دولية أخرى (مثل اتفاقية الأمم المتحدة لقمع تمويل الإرهاب).

الإعلانات (المادة ٤٠)

٣١٥.تشير المادة ٤٠ إلى مواد معينة، معظمها ذات الصلة بالجرائم التي تحددها الاتفاقية في قسم القانون الموضوعي، حيث يسمح للأطراف بإدراج بعض العناصر الإضافية الخاصة تعدل نطاق الأحكام. وتهدف هذه العناصر الإضافية إلى استيعاب بعض الاختلافات المفاهيمية أو القانونية التي تكون مبررة في معاهدة عالمية النطاق أكثر مما قد تكون في سياق مجلس أوروبا الصرف. وتعتبر الإعلانات تفسيرات مقبولة لأحكام الاتفاقية وينبغي التمييز بينها وبين التحفظات التي تسمح للطرف باستبعاد أو تعديل الأثر القانوني لبعض الالتزامات المنصوص عليها في الاتفاقية. ولما كان من المهم أن تعرف الأطراف في الاتفاقية أي عناصر إضافية، إن وجدت، أرفقتها أطراف أخرى، فإن إعلانها إلى الأمين العام لمجلس أوروبا إلزامي وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام. ويكتسي هذا الإشعار أهمية خاصة فيما يتعلق بتعريف الجرائم، حيث يتعين على الأطراف أن استيفاء شرط ازدواجية التجريم عند تطبيق بعض السلطات الإجرائية. ولم يتم اعتبار أن وضع حد عددي أمر ضروري بالنسبة للإعلانات.

البند الاتحادي (المادة ٤١)

٣١٦.تماشيا مع الهدف المتمثل في تمكين أكبر عدد ممكن من الدول من أن تصبح أطرافا، تسمح المادة ٤١ بتحفظ يهدف إلى مواجهة الصعوبات التي قد تتعرض لها الدول الاتحادية نتيجة لتوزيعها المميز للسلطة بين سلطات مركزية وإقليمية. وتوجد سوابق خارج مجال القانون الجنائي للإعلانات الاتحادية أو التحفظات على اتفاقات دولية أخرى[11] (١). وهنا، تعترف المادة ٤١ بأن اختلافات طفيفة في التغطية قد تحدث نتيجة للقانون المحلي والممارسة المحلية القائمين لدى الطرف الذي يكون دولة اتحادية. ويجب أن تستند هذه الاختلافات إلى دستوره أو مبادئ أساسية أخرى تتعلق بتقسيم السلطات في مسائل العدالة الجنائية بين الحكومة المركزية والولايات أو الكيانات الإقليمية المؤسسة لدولة اتحادية. وكان هناك اتفاق بين القائمين على صياغة الاتفاقية على ألا يحدث تفعيل البند الاتحادي سوى اختلافات طفيفة على تطبيق الاتفاقية.

٣١٧.على سبيل المثال، ينظم التشريع الجنائي الفيدرالي في الولايات المتحدة، بموجب دستورها ومبادئها الفيدرالية الأساسية، السلوك القائم على تداعياته على التجارة فيما بين الولايات أو على التجارة الخارجية، بينما تنظم عادة المسائل ذات أهمية دنيا أو محلية صرفة من قبل الولايات المؤسسة . ومع ذلك، تنص هذه المقاربة الفيدرالية على تغطية واسعة للسلوك غير القانوني الذي تشمله هذه الاتفاقية بموجب القانون الجنائي الاتحادي الأمريكي، لكنها تعترف بأن الولايات المؤسسة ستواصل تنظيم السلوك الذي لا يكون له سوى أثر طفيف أو طابع محلي محض. وفي بعض الحالات، وفي إطار فئة السلوك الضيقة التي ينظمها قانون الولاية وليس القانون الاتحادي، لا يجوز للولاية المؤسسة أن تنص على تدبير من شأنه أن يدخل في نطاق هذه الاتفاقية. فعلى سبيل المثال، قد لا يعتبر الهجوم على جهاز كمبيوتر شخصي مستقل أو شبكة من الحواسيب المترابطة داخل مبنى واحد بمثابة جريمة جنائية إذا نص على ذلك قانون الولاية التي وقع فيها الهجوم؛ بينما يشكل الهجوم جريمة جنائية اتحادية إذا تم النفاذ إلى الكمبيوتر عن طريق الإنترنت، لأن استخدام الإنترنت يحدث التأثير على التجارة بين الولايات أو التجارة الخارجية اللازم للاستناد إلى القانون الاتحادي. ويكون تنفيذ هذه الاتفاقية من خلال القانون الاتحادي للولايات المتحدة، أو من خلال قانون دولة اتحادية أخرى في ظروف مماثلة، مطابقا لمتطلبات المادة ٤١.

٣١٨.اقتصر نطاق تطبيق البند الاتحادي على أحكام الفصل الثاني (القانون الجنائي الموضوعي والقانون الإجرائي والولاية القضائية). وتبقى الدول الاتحادية التي تستفيد من هذا الحكم ملزمة بالتعاون مع الأطراف الأخرى بموجب الفصل الثالث، حتى في الحالات التي لا تجرم فيها الولاية المؤسسة أو أي كيان إقليمي مماثل آخر يوجد فيه المجرم في حالة فرار أو توجد فيه الأدلة هذا السلوك أو لا تتوفر لديها الإجراءات المطلوبة بموجب الاتفاقية.

٣١٩.فضلا عن ذلك، تنص الفقرة ٢ من المادة ٤١ على أنه لا يجوز للدولة الاتحادية، عند إبداء تحفظ بموجب الفقرة ١ من هذه المادة، أن تطبق شروط هذا التحفظ لاستبعاد التزاماتها المنصوص عليها في الفصل الثاني أو تقليصها بشكل هام. عموما، ينبغي أن تنص على قدرة واسعة وفعالة على إنفاذ القانون فيما يتعلق بتلك التدابير. وبخصوص الأحكام التي يدخل تنفيذها في نطاق الولاية التشريعية للولايات المؤسسة أو الكيانات الإقليمية المماثلة الأخرى، تحيل الحكومة الاتحادية الأحكام إلى سلطات هذه الكيانات بتأييد إيجابي، وتشجعها على اتخاذ الإجراءات المناسبة لتفعيلها.

التحفظات (المادة ٤٢)

٣٢٠.تنص المادة ٤٢ على عدد من إمكانيات التحفظ. وتنشأ هذه المقاربة من أن الاتفاقية تغطي مجالا من مجالات القانون الجنائي وقانون الإجراءات الجنائية يعتبر جديدا نسبيا بالنسبة إلى العديد من الدول. وبالإضافة إلى ذلك، فإن الطابع العالمي للاتفاقية، التي ستكون مفتوحة للدول الأعضاء وغير الأعضاء في مجلس أوروبا، تجعل من الضروري التوفر على إمكانيات التحفظ هاته. وتهدف إمكانيات التحفظ هذه إلى تمكين أكبر عدد من الدول من أن تصبح أطرافا في الاتفاقية، مع السماح لتلك الدول بالاحتفاظ بمقاربة ومفاهيم معينة تتفق مع قوانينها المحلية. وفي الوقت نفسه، سعى القائمون على الصياغة إلى تقييد إمكانيات إبداء تحفظات من أجل ضمان التطبيق الموحد للاتفاقية من قبل الأطراف إلى أقصى حد ممكن. وبالتالي، لا يجوز إبداء تحفظات أخرى عن تلك التي تم سردها. وبالإضافة إلى ذلك، لا يجوز إجراء التحفظات إلا من جانب طرف عند التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام.

---

[11] مثلا، الاتفاقية المتعلقة بوضع اللاجئين المؤرخة في ٢٨ يوليو/تموز ١٩٥١، المادة ٣٤؛ الاتفاقية المتعلقة بوضع الأشخاص عديمي الجنسية، المؤرخة في ٢٨ سبتمبر/أيلول ١٩٥٤، المادة ٣٧؛ اتفاقية الاعتراف بقرارات التحكيم الأجنبية وإنفاذها، الصادرة في ١٠ يونيو/حزيران ١٩٥٨، المادة ١١؛ اتفاقية حماية التراث الثقافي والطبيعي العالمي المؤرخة في ١٦ نوفمبر/تشرين الثاني ١٩٧٢، المادة ٣٤.

٣٢١.واعترافا بأن بعض التحفظات ضرورية لبعض الأطراف لتفادي التضارب مع مبادئها الدستورية أو القانونية الأساسية، لا تفرض المادة ٤٣ مهلة محددة لسحب التحفظات. وبدلا من ذلك، ينبغي سحبها حالما تسمح الظروف بذلك.

٣٢٢.للحفاظ على بعض الضغوط على الأطراف ودفعها على الأقل إلى النظر في سحب تحفظاتها، تأذن الاتفاقية للأمين العام لمجلس أوروبا بأن يستفسر دوريا عن احتمالات السحب. وتعتبر إمكانية الاستفسار هذه ممارسة قائمة بموجب العديد من صكوك مجلس أوروبا. وهكذا، تتاح للأطراف فرصة للإشارة إلى ما إذا كانت لا تزال بحاجة إلى الإبقاء على تحفظاتها فيما يتعلق ببعض الأحكام وأن تسحب، بعد ذلك، تلك التي لم تعد ضرورية، على أمل أن تتمكن الأطراف مع مرور الوقت من رفع أكبر قدر ممكن من تحفظاتها من أجل تعزيز التنفيذ الموحد للاتفاقية.

التعديلات (المادة ٤٤)

٣٢٣.تنص المادة ٤٤ على سابقة مستخلصة من الاتفاقية المعنية بغسل الأموال والبحث عن عائدات الجريمة وضبطها ومصادرتها (سلسلة المعاهدات الأوروبية رقم ١٤١)، حيث تم تضمينها باعتبارها ابتكارا مرتبطا باتفاقيات القانون الجنائي التي تم إعدادها في إطار مجلس أوروبا. ووضع إجراء التعديل كتدبير لإدخال تغييرات طفيفة نسبيا ذات طابع إجرائي وتقني، في معظم الأحيان. ورأى القائمون على الصياغة أنه يمكن إدخال تغييرات رئيسية على الاتفاقية في شكل بروتوكولات إضافية.

٣٢٤.يمكن للأطراف نفسها أن تدرس الحاجة إلى إدخال تعديلات أو بروتوكولات بموجب إجراء التشاور المنصوص عليه في المادة ٤٦. وفي هذا الصدد، تحاط اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) علما بذلك على أساس دوري ويطلب منها اتخاذ التدابير اللازمة لمساعدة الأطراف في جهودها الرامية إلى تعديل الاتفاقية أو استكمالها.

٣٢٥.وفقا للفقرة ٥، لن يدخل أي تعديل يعتمد حيز النفاذ إلا بعدما تبلغ جميع الأطراف الأمين العام بقبوله. ويسعى هذا الشرط إلى ضمان تطور الاتفاقية بطريقة موحدة.

تسوية النزاعات (المادة ٤٥)

٣٢٦.تنص الفقرة ١ من المادة ٤٥ على وجوب إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام على علم بتفسير وتطبيق أحكام الاتفاقية. وتلزم الفقرة ٢ الأطراف بالسعي إلى تسوية سلمية لأي نزاع يتعلق بتفسير الاتفاقية أو بتطبيقها. وينبغي أن تتفق الأطراف المعنية على أي إجراء لحل النزاعات. ويقترح هذا الحكم ثلاث آليات ممكنة لتسوية المنازعات: اللجنة الأوروبية المعنية بمشاكل الإجرام في حد ذاتها، وهيئة تحكيم أو محكمة العدل الدولية.

مشاورات الأطراف (المادة ٤٦)

٣٢٧.تنشئ المادة ٤٦ إطارا للأطراف للتشاور بشأن تنفيذ الاتفاقية وأثر التطورات القانونية أو السياسية أو التكنولوجية الهامة المتعلقة بموضوع الجريمة المرتكبة على الكمبيوتر أو ذات الصلة بالكمبيوتر وجمع الأدلة في شكل إلكتروني، وإمكانية تكملة الاتفاقية أو تعديلها. وينبغي أن تعكف المشاورات بصفة خاصة على المسائل الناشئة عن استخدام الاتفاقية وتنفيذها، بما في ذلك آثار الإعلانات والتحفظات التي تم إبداؤها بموجب المادتين ٤٠ و٤٢.

٣٢٨.يتسم هذا الإجراء بالمرونة ويترك للأطراف تقرير كيفية وموعد عقد المشاورات إذا رغبت في ذلك. وارتأى القائمون على صياغة الاتفاقية أن هذا الإجراء ضروري لضمان مشاركة جميع الأطراف في الاتفاقية، بما في ذلك الدول غير الأعضاء في مجلس أوروبا – على قدم المساواة – في أي آلية للمتابعة، مع الحفاظ على اختصاصات اللجنة الأوروبية المعنية بمشاكل الإجرام، التي لا ينبغي إبقاؤها على علم منتظم بالمشاورات الجارية بين الأطراف فحسب، بل ينبغي لها أيضا تيسير تلك المشاورات واتخاذ التدابير اللازمة لمساعدة الأطراف في جهودها الرامية إلى استكمال الاتفاقية أو تعديلها. وبالنظر إلى الاحتياجات في مجال الوقاية والمتابعة الفعالة للجرائم الإلكترونية وقضايا الخصوصية المرتبطة بها، فإن الأثر المحتمل على أنشطة التجارية وغيرها من العوامل ذات الصلة، بالإضافة إلى آراء الأطراف المهتمة، بما في ذلك سلطات إنفاذ القانون والمنظمات غير الحكومية والقطاع الخاص، قد تكون مفيدة لهذه المشاورات (انظر أيضا الفقرة ١٤).

٣٢٩.تنص الفقرة ٣ على استعراض تفعيل الاتفاقية بعد مرور ثلاث سنوات على دخولها حيز النفاذ. ويجوز آنذاك التوصية بإدخال التعديلات المناسبة. ويتعين على اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، أن تنجز هذا الاستعراض بمساعدة الأطراف.

٣٣٠.تشير الفقرة ٤ إلى أنه يتعين على الأطراف نفسها أن تمول أي مشاورات تجرى وفقا للفقرة ١ من المادة ٤٦، باستثناء الحالات التي يأخذها مجلس أوروبا على عاتقه. ومع ذلك، تدعم أمانة مجلس أوروبا الأطراف في جهودها بموجب هذه الاتفاقية، باستثناء اللجنة الأوروبية المعنية بمشاكل الإجرام.