الاتفاقية المتعلقة بالجريمة الإلكترونية

البروتوكول حول التمييز العنصري وكراهية الأجانب

البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية

www.coe.int/cybercrime

تقارير تفسيرية ومذكرات توجيهية

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

الاتفاقية المتعلقة بالجريمة الإلكترونية

البروتوكول حول التمييز العنصري وكراهية الأجانب

البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية

تقارير تفسيرية ومذكرات توجيهية

مجلس أوروبا

إعادة إنتاج النصوص الموجودة في هذا النشر مصرح بها شريطة أن يتم الإشارة إلى العنوان الكامل والمصدر، وهو مجلس أوروبا. إذا كانت تستخدم لأغراض تجارية أو مترجمة إلى إحدى اللغات غير الرسمية لمجلس أوروبا، فيرجى الاتصال عبر البريد الإلكتروني publishing@coe.int.

الغلاف والتصميم: قسم إنتاج الوثائق والمطبوعات (DPDP)، مجلس أوروبا

© مجلس أوروبا، نونبر 2023

مطبوع في مجلس أوروبا

قائمة المحتويات

الاتفاقية المتعلقة بالجريمة الإلكترونية سلسلة المعاهدات الأوروبية رقم 185	**5**
التقرير التوضيحي لاتفاقية مكافحة جرائم الإنترنت	33
البروتوكول الأول الإضافي المتعلق بتجريم الأفعال ذات الطابع العنصري والكراهية تجاه الأجانب المرتكبة عبر أنظمة الحاسوب (ETSرقم 189) ستراسبورغ، 28 يناير 2003	**121**
التقرير التوضيحي للبروتوكول الإضافي الأول	129
البروتوكول الإضافي الثاني بشأن تعزيز التعاون وكشف الأدلة الإلكترونية (ETSرقم 224)، ستراسبورغ، 12 ماي 2022	**141**
التقرير التوضيحي للبروتوكول الإضافي الثاني	169
بخصوص المذكرات التوجيهية	**261**
المذكرة التوجيهية #1 بشأن مفهوم "نظام الكمبيوتر"	262
المذكرة التوجيهية #2 بشأن أحكام اتفاقية بودابست التي تشمل شبكات البناء والتشغيل والنقل "بوتنت" (botnets)	265
المذكرة التوجيهية #5 بشأن هجمات حجب الخدمة الموزعة (DDOS)	269
المذكرة التوجيهية #4 بشأن انتحال الشخصية والتصيد المرتبطين بالاحتيال	272
المذكرة التوجيهية #6 بشأن الهجمات على البنية التحتية للمعلومات الحيوية	277
المذكرة التوجيهية #7 بشأن الأشكال الجديدة للبرمجيات الخبيثة	280
المذكرة التوجيهية #3 بشأن النفاذ العابر للحدود إلى البيانات (المادة 32)	284
المذكرة التوجيهية #8 بشأن البريد الإلكتروني غير المرغوب فيه (Spam)	290
المذكرة التوجيهية #10 بشأن أوامر إبراز البيانات للحصول على معلومات عن المشترك (المادة 18 من اتفاقية بودابست)	293
المذكرة التوجيهية #11 بشأن الإرهاب	302
المذكرة التوجيهية# 9 للجنة اتفاقية مكافحة الجريمة الإلكترونية بعض جوانب التدخل في الانتخابات بواسطة أنظمة الكمبيوتر المشمولة باتفاقية بودابست	307
المذكرة التوجيهية رقم 12 للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية جوانب برامج الفدية التي تغطيها اتفاقية بودابست	312
المذكرة التوجيهية رقم 13 للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية نطاق الصلاحيات الإجرائية وأحكام التعاون الدولي الواردة في اتفاقية بودابست	321
مذكرة توجيهية رقم 14 صادرة عن اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية المعلومات التلقائية (المادة 26 من الاتفاقية المتعلقة بالجريمة الإلكترونية)	330

الاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة المعاهدات الأوروبية – رقم 185)

الديباجة

إن الدول الأعضاء في مجلس أوروبا وغيرها من الدول الأخرى الموقعة على هذه الاتفاقية؛

إذ تأخذ في الاعتبار أن هدف مجلس أوروبا هو تحقيق وحدة أكبر بين أعضائه؛

واعترافاً منها بقيمة تعزيز التعاون مع الدول الأخرى الأطراف في هذه الاتفاقية؛

واقتناعاً منها بالحاجة إلى إتباع سياسة جنائية مشتركة، كمسألة ذات أولوية، بهدف حماية المجتمع من الجريمة الإلكترونية، من خلال تبني تشريع ملائم ودعم التعاون الدولي، من بين أمور أخرى؛

وإدراكاً منها بعمق التغييرات التي أحدثتها الرقمنة والالتقائية
والعولمة المتواصلة لشبكات الكومبيوتر؛

وإذ يساورها القلق بشأن مخاطر إمكانية استخدام شبكات الكومبيوتر
والمعلومات الإلكترونية أيضا لارتكاب جرائم جنائية، وأن الأدلة المتعلقة
بمثل هذه الجرائم يمكن تخزينها ونقلها عبر هذه الشبكات؛

واعترافاً منها بالحاجة إلى التعاون بين الدول والقطاع الخاص في مجال مكافحة الجريمة الإلكترونية، والحاجة إلى حماية المصالح المشروعة عند استخدام وتطوير تكنولوجيا المعلومات؛

وإيماناً منها بأن المكافحة الفعالة للجريمة الإلكترونية تستلزم تعزيز التعاون
الدولي في المسائل الجنائية وتسريع وتيرته وتوظيفه بشكل جيد؛

واقتناعاً منها بأن هذه الاتفاقية ضرورية لردع الأعمال الموجهة ضد سرية وسلامة وتوافر نظم الكومبيوتر، والشبكات والبيانات بالإضافة إلى إساءة استخدام هذه النظم والشبكات والبيانات، وذلك بالتنصيص على تجريم سلوكيات من هذا القبيل، كما هو مبين في هذه الاتفاقية واعتماد الصلاحيات الكافية من أجل مكافحة فعالة لمثل هذه الجرائم الجنائية من خلال تيسير كشفها، والتحقيق بشأنها، ومقاضاتها على المستويين الوطني والدولي على حد سواء، وكذلك عن طريق توفير ترتيبات من أجل تحقيق تعاون دولي سريع وموثوق؛

وحرصاً منها على ضرورة تأمين التوازن الملائم بين المصالح المتصلة بإنفاذ القانون من جهة واحترام حقوق الإنسان الأساسية كما هو منصوص عليه في اتفاقية مجلس أوروبا لعام 1950 بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966 المتعلق بالحقوق المدنية والسياسية، وغيرها من المعاهدات الدولية بشأن حقوق الإنسان السارية والتي تؤكد حق كل فرد في التعبير عن رأيه دون أي تدخل، وكذلك الحق في حرية التعبير، بما في ذلك حرية البحث عن مختلف أنواع المعلومات والأفكار وتلقيها ونقلها بغض النظر عن الحدود، علاوة على الحقوق المتعلقة باحترام الخصوصية؛

وحرصاً منها كذلك على الحق في حماية البيانات الشخصية، الذي تخوله على سبيل المثال اتفاقية مجلس أوروبا لعام 1981 بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية؛

وإذ تأخذ في الاعتبار اتفاقية الأمم المتحدة لعام 1989 بشأن حقوق الطفل، واتفاقية منظمة العمل الدولية لعام 1999 بشأن أسوأ صور عمل الأطفال؛

وإذ تأخذ بعين الاعتبار اتفاقيات مجلس أوروبا القائمة بشأن التعاون في المجال الجنائي، وكذلك المعاهدات المماثلة القائمة بين الدول الأعضاء في مجلس أوروبا وغيرها من الدول، وتؤكد على أن الاتفاقية الحالية ترمي إلى استكمال تلك الاتفاقيات بغية تعزيز فعالية التحقيقات والإجراءات الجنائية المتعلقة بالجرائم ذات الصلة بنظم وبيانات الكومبيوتر، والتمكين من جمع الأدلة في الجرائم الجنائية ذات الطابع الإلكتروني؛

وإذ ترحب بالتطورات الأخيرة التي تعزز التفاهم والتعاون الدوليين في مجال مكافحة الجريمة الإلكترونية، بما في ذلك الإجراء الذي اتخذته منظمة الأمم المتحدة، ومنظمة التعاون والتنمية الاقتصادية والاتحاد الأوروبي ومجموعة الثمانية؛

وإذ تذكر بتوصيات لجنة الوزراء رقم 10/85 بشأن التطبيق العملي للاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اعتراض الاتصالات السلكية واللاسلكية، والتوصية رقم 2/88 بشأن القرصنة في مجال حقوق التأليف والنشر والحقوق المجاورة، والتوصية رقم 15/87 التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، والتوصية رقم 4/95 بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات مع إشارة خاصة إلى الخدمات الهاتفية، بالإضافة إلى التوصية رقم 9/89 بشأن الجرائم ذات الصلة بالكمبيوتر التي توفر مبادئ توجيهية للهيئات التشريعية الوطنية بشأن تعريف بعض جرائم الكومبيوتر، والتوصية رقم 13/95 بشأن المشاكل التي يطرحها قانون الإجراءات الجنائية علاقة بتكنولوجيا المعلومات؛

ومراعاة للقرار رقم 1 الذي تبناه وزراء العدل الأوروبيون في مؤتمرهم الواحد والعشرين (براغ، في 10 و11 يونيو/حزيران 1997) والذي أوصى لجنة الوزراء بدعم الجهود التي تبذلها اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) في مجال الجريمة الإلكترونية بغية تقريب أحكام القوانين الجنائية

الوطنية من بعضها البعض، وتمكين استخدام الوسائل الفعالة لإجراء التحقيقات في مثل هذه الجرائم، بالإضافة إلى القرار رقم 3 المعتمد خلال المؤتمر الثاني لوزراء العدل الأوروبيين (لندن، 8 و9 يونيو/حزيران 2000) والذي شجع الأطراف المتفاوضة على مواصلة جهودهم بغرض إيجاد حلول ملائمة لتمكين أكبر عدد ممكن من الدول أن تصبح أطرافاً في الاتفاقية، وأقر بالحاجة إلى نظام سريع وفعال للتعاون الدولي يأخذ بعين الاعتبار وكما يجب الشروط الخاصة بمكافحة الجريمة الإلكترونية؛

وبالنظر لخطة العمل التي اعتمدها رؤساء الدول والحكومات الأعضاء في مجلس أوروبا بمناسبة انعقاد القمة الثانية (ستراسبورغ، 10 و11 أكتوبر/تشرين الأول 1997) بغية إيجاد ردود مشتركة لتطور تكنولوجيات المعلومات الحديثة وفقاً لمعايير وقيم مجلس أوروبا؛

اتفقت على ما يلي:

الباب الأول – استخدام المصطلحات

المادة 1 – التعريفات

لأغراض هذه الاتفاقية:

أ. يُقصد بـ "منظومة الكومبيوتر" أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقا لبرنامج، بالمعالجة الآلية للبيانات؛

ب. يُقصد بـ " بيانات الكومبيوتر " أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معينة؛

ج. يُقصد بـ"مُقدم الخدمة"

1) أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوتر، و

2) أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة.

د. يُقصد بـ"بيانات حركة الاتصالات" 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.

الباب الثاني: التدابير الواجب اتخاذها على الصعيد الوطني

القسم الأول: القانون الجنائي الموضوعي

الفصل الأول: الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكومبيوتر

المادة 2 – النفاذ غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كومبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنية الحصول على بيانات الكومبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر.

المادة 3 – الاعتراض غير المشروع

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كومبيوتر يحمل هذه البيانات. ويجوز للدولة الطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنيَّة غير صادقة أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر.

المادة 4 – التدخل في البيانات

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.
2. يجوز لدولة طرف أن تحتفظ بحقها في أن تستلزم أن تتسبب الأفعال المشار إليها في الفقرة 1 في ضرر جسيم.

المادة 5 – التدخل في النظام

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكومبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها.

المادة 6 – إساءة استخدام الأجهزة

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

أ. عملية إنتاج، بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأي طرق أخرى:

1. جهاز، بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛

2. كلمة سر خاصة بكومبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5؛ و

ب. حيازة إحدى المواد المشار إليها في الفقرة أ (1) أو (2) أعلاه، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5. ويجوز للدولة الطرف أن تشترط بموجب القانون أن تكون حيازة عدد من هذه المواد سابقة لإلحاق المسؤولية الجنائية.

2. لا يجوز تُفسير هذه المادة على أنها تفرض مسؤولية جنائية طالما أن عملية الإنتاج، البيع ، الشراء بغرض الاستخدام، الاستيراد، التوزيع، الإتاحة بطرق أخرى أو الحيازة المشار إليها بالفقرة 1 من هذه المادة ليس الغرض منها ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 2 إلى 5 من هذه الاتفاقية، بل بالأحرى للاستخدام المرخص لغرض اختبار أو حماية نظام الكمبيوتر.

3. يجوز لكل دولة طرف الاحتفاظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، شريطة ألا يكون هذا التحفظ متعلقاً بعمليات بيع، توزيع أو إتاحة هذه المواد المشار إليها في الفقرة -1 أ (2) من هذه المادة.

الفصل الثاني: الجرائم ذات الصلة بالكومبيوتر

المادة 7 – التزوير المرتبط بالكومبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق: إدخال، تغيير، حذف أو إتلاف بيانات كومبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية، بغض النظر عما إذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا. ويجوز للدولة الطرف أن تشترط وجود نية الاحتيال، أو نية غير صادقة مشابهة، سابقة لإلحاق المسؤولية الجنائية.

المادة 8 – الاحتيال المرتبط بالكومبيوتر

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق:

أ. أي إدخال، تغيير، حذف أو إتلاف لبيانات الكومبيوتر؛

ب. أي تدخل في وظيفة نظام الكومبيوتر، بنية الاحتيال أو نية سيئة، للحصول بدون وجه حق، على منفعة اقتصادية ذاتية أو لفائدة شخص آخر.

الفصل الثالث: الجرائم ذات الصلة بالمحتوى

المادة 9 – الجرائم ذات الصلة بمواد إباحية عن الأطفال

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

أ. إنتاج مواد إباحية عن الأطفال بغرض توزيعها عبر نظام الكومبيوتر؛

ب. عرض مواد إباحية عن الأطفال أو إتاحتها عبر نظام الكومبيوتر؛

ج. توزيع مواد إباحية عن الأطفال أو نقلها عبر نظام الكومبيوتر؛

د. الحصول على مواد إباحية عن الأطفال عبر نظام الكومبيوتر لصالح الشخص ذاته أو لفائدة الغير؛

هـ. حيازة مواد إباحية عن الأطفال داخل نظام الكومبيوتر أو على دعامة لتخزين بيانات الكومبيوتر.

2. لغرض الفقرة 1 أعلاه، تشمل عبارة " مواد إباحية عن الأطفال " المواد الإباحية التي تعرض بشكل مرئي:

أ. قاصر وهو يمارس سلوكا جنسيا واضحا؛

ب. شخص يبدو قاصرا وهو يمارس سلوكا جنسيا واضحا؛

ج. صور واقعية تظهر قاصرا وهو يمارس سلوكا جنسيا واضحا.

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

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

الفصل الرابع: الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

المادة 10 – الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني: انتهاك حقوق النشر والتأليف، وفقا لتعريفها بموجب القانون الخاص بتلك الدولة الطرف، وتبعاً لالتزاماتها بموجب وثيقة باريس المؤرخة في 24 يوليو/ تموز 1971 والمنقحة لاتفاقية برن لحماية المصنفات الأدبية والفنية، والاتفاق الخاص بجوانب حقوق الملكية الفكرية المتصلة بالتجارة، ومعاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية باستثناء أي حقوق معنوية مخولة بموجب هذه الاتفاقيات، عندما تُرتكب هذه الأفعال عمداً على نطاق تجاري وبواسطة نظام الكومبيوتر.

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

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

الفصل الخامس: المسؤولية الإضافية والعقوبات

المادة 11 – المحاولة، والمساعدة والتحريض

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: المساعدة أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 10 من هذه الاتفاقية، وذلك بنِية ارتكاب جريمة من هذا القبيل.

2. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً: محاولة ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من 3 إلى 5، 7، 8 و9. 1 (أ) و(ج) من هذه الاتفاقية.

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

المادة 12 – مسؤولية الشركات

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

أ. سلطة تمثيل الشخص الاعتباري؛

ب. سلطة اتخاذ القرارات نيابة عن الشخص الاعتباري؛

ج. سلطة ممارسة الرقابة لدى الشخص الاعتباري.

2. بالإضافة إلى الحالات المنصوص عليها مسبقا في الفقرة 1 من هذه المادة، تعتمد كل دولة طرف التدابير الضرورية لضمان مساءلة الشخص الاعتباري في حال ساعد عدم الإشراف أو الرقابة من قبل الشخص الطبيعي المشار إليه في الفقرة 1 في ارتكاب جريمة منصوص عليها وفقا لهذه الاتفاقية لفائدة الشخص الاعتباري من قبل شخص طبيعي يعمل تحت سلطته.

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

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

المادة 13 – العقوبات والتدابير

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير للتأكد من أن الجرائم المنصوص عليها في المواد من 2 إلى 11 مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية.

2. تضمن كل دولة طرف مساءلة الأشخاص الاعتباريين وفقا للمادة 12 وإخضاعهم لعقوبات أو تدابير فعالة، متناسبة ورادعة، سواء كانت عقوبات أو تدابير جنائية أو غير جنائية، بما في ذلك العقوبات المالية.

القسم الثاني: القانون الإجرائي

الفصل الأول: أحكام مشتركة

المادة 14 – نطاق الأحكام الإجرائية

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار السلطات والإجراءات المنصوص عليها في هذا القسم لأغراض التحقيقات والدعاوى الجنائية المحددة.

2. باستثناء ما هو منصوص عليه تحديدا خلاف ذلك في المادة 21، تطبق كل دولة طرف السلطات والإجراءات المشار إليها في الفقرة 1 من هذه المادة على:

   أ. الجرائم الجنائية المقررة في المواد من 2 إلى 11 من هذه الاتفاقية؛

   ب. الجرائم الجنائية الأخرى التي يتم ارتكابها بواسطة نظام الكومبيوتر؛ و

   ج. جمع الأدلة الخاصة بجريمة جنائية بشكل إلكتروني.

3. أ. يجوز لكل دولة طرف أن تحتفظ بالحق في تطبيق الإجراءات المشار إليها بالمادة 20 فقط على الجرائم أو أصناف الجرائم المحددة في التحفظ، شريطة ألا يكون نطاق هذه الجرائم أو أصناف الجرائم مقيدا بشكل أكبر من نطاق الجرائم التي تطبق عليها الإجراءات المشار إليها في المادة 21. ويتعين على كل دولة طرف النظر في تقييد هذا التحفظ بشكل يمكِّن من تطبيق التدبير المشار إليه في المادة 20 على أوسع نطاق.

   ب. في حال تعذر على دولة طرف، بسبب قيود موجودة في تشريعاته السارية وقت التصديق على هذه الاتفاقية، تطبيق التدابير المشار إليها في المادتين 20 و21 على الاتصالات المنقولة داخل نظام الكومبيوتر لمزود الخدمة، عندما يكون ذلك النظام:

      1. مشغلا لفائدة مجموعة مغلقة من المستخدمين، و

      2. لا يستخدم شبكات الاتصالات العمومية، وغير متصل بأي نظام كومبيوتر آخر، سواء كان عاما أو خاصا،

      فإنه يجوز لتلك الدولة الطرف الاحتفاظ بالحق في عدم تطبيق هذه التدابير على تلك الاتصالات. ويتعين على كل دولة طرف النظر في تقييد هذا التحفظ بشكل يمكِّن من تطبيق التدبير المشار إليه في المادة 20 على أوسع نطاق.

المادة 15 – الشروط والضمانات

1. تسعى كل دولة طرف إلى ضمان خضوع وضع وتنفيذ وتطبيق السلطات والإجراءات المنصوص عليها في هذا القسم، للضمانات والشروط المنصوص عليها في قانونها الوطني، الذي ينبغي أن يوفر الحماية الملائمة لحقوق الإنسان والحريات، بما

في ذلك الحقوق الناشئة عن الالتزامات التي تعهدت بها بموجب اتفاقية مجلس أوروبا لعام 1950 الخاصة بحماية حقوق الإنسان والحريات الأساسية ، والعهد الدولي للأمم المتحدة لعام 1966 الخاص بالحقوق المدنية والسياسية، وغيرها من الصكوك الدولية ذات الصلة بحقوق الإنسان، وأن يدمج مبدأ التناسب.

2. تشمل هذه الشروط والضمانات، حسب الاقتضاء بالنظر لطبيعة الإجراءات أو السلطات المعنية، الإشراف القضائي أو بواسطة أي هيئة مستقلة أخرى، والأسس المبررة للتطبيق، وحدود نطاق تلك الإجراءات أو السلطات ومدتها، من بين أمور أخرى.

3. بقدر ما يتفق مع المصلحة العامة، خاصة الإدارة السليمة للعدالة، يقوم كل طرف بتدارس تأثير السلطات والإجراءات الواردة في هذا القسم على حقوق الأغيار ومسؤولياتهم ومصالحهم المشروعة.

الفصل الثاني: التعجيل في حفظ بيانات الكومبيوتر المخزنة

المادة 16 – التعجيل في حفظ بيانات الكومبيوتر المخزنة

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من الأمر أو الحصول على الحفظ المعجل لبيانات كومبيوتر محددة، بما في ذلك بيانات الحركة المُخزنة بواسطة نظام الكومبيوتر، خاصة في حال وجود أسس للاعتقاد أن تلك البيانات معرضة بشكل خاص للضياع أو التعديل.

2. في حال تفعيل دولة طرف للفقرة 1 أعلاه عبر توجيه أمر إلى شخص من أجل حفظ بيانات كومبيوتر محددة ومخزنة توجد بحوزته أو تحت سيطرته، تعتمد الدولة الطرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام ذلك الشخص بحفظ بيانات الكومبيوتر المعنية والإبقاء على سلامتها لأطول مدة زمنية ضرورية على ألا تتجاوز تسعين يوماً، من أجل تمكين السلطات المختصة من التماس الكشف عنها. ويجوز للدولة الطرف التنصيص على تجديد هذا الأمر لاحقا.

3. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام القيِّم على حفظ بيانات الكومبيوتر أو أي شخص آخر عهدت له هذه المهمة، بالحفاظ على سرية هذه الإجراءات طيلة الفترة الزمنية المنصوص عليها في قانونها الوطني.

4. تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 14 و15.

المادة 17 – التعجيل في حفظ بيانات الكومبيوتر والكشف الجزئي عن بيانات الحركة

1. تعتمد كل دولة طرف، فيما يتعلق ببيانات الحركة الواجب حفظها بموجب المادة 16، ما يلزم من تدابير تشريعية وغيرها من التدابير بغية:

أ. ضمان توفر إمكانية التعجيل في حفظ بيانات الحركة بصرف النظر عن مشاركة مزود خدمة واحد أو أكثر في عملية نقل هذا الاتصال؛ و

ب. ضمان تعجيل الكشف للسلطة المختصة لدى الدولة الطرف، أو الشخص الذي تعينه تلك السلطة، عن القدر الكافي من بيانات الحركة من أجل تمكين الدولة الطرف من تحديد مزود الخدمة والمسار الذي تم من خلاله نقل الاتصال.

2. تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 14 و15.

الفصل الثالث: الأمر بإبراز البيانات

المادة 18 – الأمر بإبراز البيانات

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة إصدار أمر إلى:

أ. أي شخص داخل أراضيها بتقديم بيانات كمبيوتر محددة بحوزة ذلك الشخص أو تحت سيطرته، ومخزنة على نظام الكومبيوتر أو على أي دعامة أخرى لتخزين بيانات الكمبيوتر.

ب. أي مزود خدمة يعرض خدماته داخل أراضي الدولة الطرف بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته.

2. تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 14 و15.

3. لغرض هذه المادة، يقصد بعبارة "معلومات عن المشترك" أي معلومات مدرجة في شكل بيانات الكومبيوتر أو في أي شكل آخر يحفظها مزود الخدمة والتي تتعلق بالمشتركين في الخدمات التي يزودها بخلاف بيانات الحركة أو المضمون والتي بموجبها يمكن تحديد:

أ. نوع خدمة الاتصال المستخدمة والشروط الفنية المرتبطة بها ومدة الخدمة؛

ب. هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه وغيره من أرقام الولوج، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق أو ترتيبات الخدمة؛

ج. أي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصال والمتاحة بموجب اتفاق أو ترتيبات الخدمة.

الفصل الرابع: البحث عن بيانات الكومبيوتر المخزنة ومصادرتها

المادة 19 – البحث عن بيانات الكومبيوتر المخزنة ومصادرتها

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير بغية تمكين سلطاتها المختصة من البحث عن أو النفاذ إلى:

أ. أي نظام كومبيوتر أو أي جزء منه وبيانات الكمبيوتر المخزنة فيه؛ و

ب. أي دعامة تخزين بيانات الكمبيوتر يمكن أن تكون بيانات كمبيوتر مخزنة داخلها على أراضي تلك الدولة الطرف.

2. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان أنه في حال إنجاز سلطاتها لعلميات البحث أو النفاذ إلى نظام كومبيوتر أو إلى جزء منه، وفقاً للفقرة 1(أ) وتوفر أسس لديها للاعتقاد بأن البيانات المطلوبة مخزنة داخل نظام كومبيوتر آخر أو على جزء منه على أراضي الدولة الطرف، وأنه يمكن النفاذ إلى تلك البيانات أو أنها متاحة قانونياً على النظام الأصلي، ينبغي أن تتمكن السلطات من تعجيل توسيع نطاق البحث أو النفاذ إلى النظام الآخر.

3. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من مصادرة أو تأمين بيانات الكومبيوتر التي تم النفاذ إليها طبقاً للفقرتين 1 أو 2. وتشمل هذه الإجراءات سلطة:

أ. مصادرة أو تأمين نظام الكومبيوتر أو جزء منه أو دعامة تخزين بيانات الكمبيوتر؛

ب. إجراء نسخة من هذه البيانات الحاسوبية والاحتفاظ بها؛

ج. الحفاظ على سلامة بيانات الكومبيوتر المخزنة ذات الصلة؛

د. جعل تلك البيانات الحاسوبية غير قابلة للنفاذ على نظام الكومبيوتر الذي تم الولوج إليه أو إزالتها.

4. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من أمر أي شخص لديه معرفة بتشغيل نظام الكومبيوتر أو التدابير المطبقة لحماية البيانات الحاسوبية الموجودة عليه، بتقديم، في حدود المعقول، المعلومات اللازمة لتمكين إجراء التدابير المشار إليها في الفقرتين 1 و2.

5. تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 14 و15.

الفصل الخامس: جمع بيانات الكومبيوتر في الوقت الحقيقي

المادة 20 – جمع بيانات الكومبيوتر في الوقت الحقيقي

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من:

أ. جمع أو تسجيل من خلال تطبيق وسائل فنية، على أراضيها؛ و

ب. إجبار مزود الخدمة، في نطاق قدرته الفنية القائمة على:

1. جمع أو تسجيل من خلال تطبيق وسائل فنية، عل ؛ أو أراضي الدولة الطرف؛ أو

2. التعاون مع السلطات المختصة ودعمها في جمع أو تسجيل بيانات الحركة، في الوقت الحقيقي، ذات الصلة باتصالات محددة على أراضيها والتي تم نقلها بواسطة نظام الكمبيوتر.

2. في حال تعذر على الدولة الطرف، بسبب المبادئ القائمة في نظامها القانوني الوطني تبني التدابير المشار إليها في الفقرة 1(أ)، ، يجوز لها بدلاً من ذلك اعتماد تدابير تشريعية وغيرها من التدابير الضرورية لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات الحركة المرتبطة باتصالات محددة تم نقلها على أراضيها، من خلال تطبيق وسائل فنية على تلك الأراضي.

3. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام مزود الخدمة بالحفاظ على سرية تنفيذ أي من السلطات المنصوص عليها في هذه المادة وعلى أي معلومات مرتبطة بها.

4. تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 14 و15.

المادة 21 – اعتراض بيانات المحتوى

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير، فيما يتعلق بنطاق الجرائم الجسيمة التي يحددها القانون الوطني، لتمكين سلطاتها المختصة من:

أ. جمع أو تسجيل من خلال تطبيق وسائل فنية على أراضيها؛ و

ب. إجبار مزود الخدمة، في نطاق قدرته الفنية القائمة، على:

1. جمع أو تسجيل من خلال تطبيق وسائل فنية على أراضيها؛ أو

2. التعاون مع السلطات المختصة ودعمها في جمع أو تسجيل بيانات المحتوى، في الوقت الحقيقي، ذات الصلة باتصالات محددة على أراضيها والتي تم نقلها بواسطة نظام الكمبيوتر.

2. في حال تعذر على الدولة الطرف تبني الإجراءات المشار إليها في الفقرة 1(أ)، بسبب المبادئ القائمة في نظامها القانوني الوطني، يجوز لها بدلاً من ذلك أن تعتمد ما يلزم من تدابير تشريعية وغيرها من التدابير لضمان الجمع أو التسجيل في الوقت الحقيقي لبيانات المحتوى المرتبطة باتصالات معينة تم نقلها في أقاليمها عبر تطبيق وسائل فنية في تلك الأقاليم.

3. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام مزود الخدمة بالمحافظة على سرية تنفيذ أي من السلطات المنصوص عليها هذه المادة وأي معلومات متصلة بها.

4. تخضع السلطات والإجراءات المشار إليها في هذه المادة لأحكام المادتين 14 و15.

القسم الثالث: الولاية القضائية

المادة 22 – الولاية القضائية

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار الولاية القضائية على أي جريمة تنص عليها المواد من 2 إلى 11 من هذه الاتفاقية، عندما تُرتكب الجريمة:
   أ. داخل أقاليمها؛ أو
   ب. على متن سفينة ترفع علم تلك الدولة الطرف؛ أو
   ج. على متن طائرة مسجلة بموجب قوانين تلك الدولة الطرف؛ أو
   د. من قبل أحد مواطنيها، إذا كانت الجريمة مُعاقبا عليها بموجب القانون الجنائي في مكان ارتكابها أو في حال ارتكاب الجريمة خارج الولاية القضائية الإقليمية لأي دولة.
2. يجوز لكل دولة طرف الاحتفاظ بالحق في عدم التطبيق أو التطبيق فقط في حالات أو ظروف معينة قواعد الولاية القضائية المنصوص عليها في الفقرات من 1(ب) إلى 1(د) من هذه المادة أو أي جزء منها.
3. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإقرار الولاية القضائية على الجرائم المشار إليها في الفقرة 1 من المادة 24 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم متواجدا داخل أقاليمها ولا تقوم بتسليمه إلى دولة طرف أخرى على أساس جنسيته فقط، وذلك بعد التوصل بطلب التسليم.
4. لا تستبعد هذه الاتفاقية ممارسة أي دولة طرف لولاية جنائية يقرها قانونها الوطني.
5. في حال مطالبة أكثر من دولة طرف بالولاية القضائية على جريمة تقرها هذه الاتفاقية، تقوم الدول الأطراف المهنية، عند الاقتضاء، بالتشاور بغرض تحديد الولاية القضائية الأنسب للمقاضاة.

الباب الثالث: التعاون الدولي

القسم الأول: المبادئ العامة

الفصل الأول: المبادئ العامة ذات الصلة بالتعاون الدولي

المادة 23 – المبادئ العامة ذات الصلة بالتعاون الدولي

تتعاون الدول الأطراف فيما بينها، وفقاً لأحكام هذا الباب ومن خلال تطبيق الصكوك الدولية ذات الصلة والخاصة بالتعاون الدولي في المسائل الجنائية وبالترتيبات المتفق عليها بمقتضى

التشريعات الموحدة أو ذات الصلة بالمعاملة بالمثل والقوانين الوطنية، على أوسع نطاق ممكن لأغراض إجراءات التحقيقات أو المتابعات التي تتعلق بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر، أو من أجل جمع أدلة بشأن جريمة جنائية في شكل إلكتروني.

الفصل الثاني: المبادئ ذات الصلة بتسليم المجرمين

المادة 24 – تسليم المجرمين

1. أ) تطبق هذه المادة على تسليم المجرمين بين الدول الأطراف بالنسبة للجرائم المنصوص عليها في المواد من 2 إلى 11 من هذه الاتفاقية، شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد.

ب) في حال كانت هناك تقرير تطبيق عقوبة دنيا مختلفة بموجب ترتيبات متفق عليها على أساس تشريع موحد أو ذي الصلة بالمعاملة بالمثل أو بموجب معاهدة تسليم المجرمين، بما في ذلك الاتفاقية الأوروبية بشأن تسليم المجرمين (سلسة المعاهدات الأوربية رقم 24)، واجبة التطبيق بين طرفين أو أكثر، تُطبق العقوبة الدنيا المنصوص عليها بموجب تلك الترتيبات أو المعاهدة.

2. تعتبر الجرائم الجنائية الواردة في الفقرة 1 من هذه المادة مدرجة كجرائم يجب فيها التسليم في أي معاهدة بشأن تسليم المجرمين قائمة بين الأطراف، وتتعهد الدول الأطراف بتضمين هذه الجرائم على أنها جرائم يجب فيها تسليم المجرمين في أي معاهدة بشأن تسليم المجرمين يتم إبرامها فيما بينهم.

3. في حالة تلقت دولة طرف تخضع تسليم المجرمين لشرط وجود معاهدة ذات الصلة طلباً بالتسليم من طرف دولة طرف أخرى لا تربطها بها معاهدة لتسليم المجرمين، يجوز لتلك الدولة الطرف اعتبار هذه الاتفاقية بمثابة الأساس القانوني لعملية التسليم فيما يتعلق بأي من الجرائم الجنائية المشار إليها في الفقرة 1 من هذه المادة.

4. تعترف الدول الأطراف التي لا تشترط وجود معاهدة لتسليم المجرمين بالجرائم الجنائية المشار إليها في الفقرة 1 من هذه المادة على أنها جرائم يجب فيها تسليم المجرمين فيما بينها.

5. يخضع تسليم المجرمين للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها التسليم أو معاهدات تسليم المجرمين واجبة التطبيق، بما في ذلك الأسباب التي تستند إليها الدولة الطرف المطالبة بالتسليم لرفض التسليم.

6. في حال رفض التسليم بشأن إحدى الجرائم المشار إليها في الفقرة 1 من هذه المادة، على أساس جنسية الشخص المطلوب فقط أو لأن الدولة الطرف المطلوب منها التسليم

تعتبر أنها ذات الولاية القضائية على تلك الجريمة، تقوم الدولة الطرف المطلوب منها التسليم، بناء على طلب الدولة الطرف مقدمة الطلب، بإحالة القضية على سلطاتها المختصة بغرض المقاضاة ثم بإبلاغ الطرف الطالب بالنتيجة النهائية في الوقت المناسب. وتتخذ تلك السلطات قرارها وتُجري التحقيقات والمتابعات بنفس الطريقة المطبقة على أي جريمة أخرى ذات طابع مشابه بموجب القانون تلك الدولة الطرف.

7. أ) تخبر كل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، الأمين العام لمجلس أوروبا باسم وعنوان كل سلطة مسؤولة عن إصدار أو تلقي طلبات التسليم، أو أوامر الاعتقال الاحترازي في حال عدم وجود معاهدة تسليم المجرمين.

ب) يقوم الأمين العام لمجلس أوروبا بإنشاء سجل خاص بالسلطات التي يعينها الأطراف وبتحيينه. ويتعين على كل دولة طرف التأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت.

الفصل الثالث: المبادئ العامة ذات الصلة بالمساعدة المتبادلة

المادة 25 – المبادئ العامة ذات الصلة بالمساعدة المتبادلة

1. توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن لأغراض التحقيقات أو المتابعات المتعلقة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر أو بجمع أدلة جريمة جنائية في شكل إلكتروني.

2. تعتمد أيضا كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتنفيذ الالتزامات الواردة في المواد من 27 إلى 35.

3. يجوز لكل دولة طرف، في الظروف العاجلة، المطالبة بالمساعدة المتبادلة أو بوثائق عن طريق وسائل الاتصال العاجلة، بما في ذلك الفاكس أو البريد الإلكتروني، بقدر ما توفره تلك الوسائل من مستويات ملائمة للأمن والتحقق من صحة البيانات (بما في ذلك استخدام التشفير عند الضرورة) مع التأكيد الرسمي بتطبيق تلك الوسائل عندما تطالب بذلك الدولة الطرف المطلوب منه تقديم المساعدة. وتقبل الدولة الطرف المطلوب منها تقديم المساعدة وتستجيب للطلب بأي من وسائل الاتصال العاجلة.

4. باستثناء ما تنص عليه تحديدا خلاف ذلك مواد هذا الباب، تخضع المساعدة المتبادلة للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها المساعدة، أو معاهدات المساعدة المتبادلة الجاري بها العمل بما في ذلك الأسس التي ترتكز إليها الدولة الطرف المطلوب منها المساعدة لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها

المساعدة ممارسة الحق في رفض المساعدة المتبادلة فيما يتعلق بالجرائم المشار إليها في المواد من 2 إلى 11 فقط على أساس أن الطلب يتعلق بجريمة تعتبرها جريمة مالية.

5. متى كان مسموحاً للدولة الطرف المطلوب منها المساعدة، طبقاً لأحكام هذا الباب، بتقديم المساعدة المتبادلة في حال وجود جريمة مزدوجة، يُعتبر هذا الشرط مستوفياً بغض النظر عما إذا كانت قوانينها تدرج الجريمة داخل التصنيف ذاته أو تطلق على الجريمة نفس المصطلح للطرف مقدم الطلب، طالما أن السلوك الذي يحدد الجريمة المطلوب تقديم المساعدة بشأنها يشكل جريمة جنائية بموجب قوانينها.

المادة 26 – المعلومات التلقائية

1. يجوز لدولة طرف، في حدود قانونها الوطني ودون طلب مسبق، أن ترسل إلى طرف آخر معلومات يتم الحصول عليها في إطار التحقيقات التي تنجزها في حال إذا ما ارتأت أن الإفصاح عن هذه المعلومات قد يساعد الطرف المتلقي لهذه المعلومات في الشروع أو القيام بتحقيقات أو متابعات بشأن جرائم جنائية مقررة طبقا لهذه الاتفاقية أو أن ذلك قد يؤدى إلى تقديم طلب للتعاون من جانب تلك الدولة الطرف بموجب هذا الباب.

2. يجوز للطرف الذي يقدم هذه المعلومات، قبل تقديمها، أن يطلب الحفاظ على سرية تلك المعلومات أو استخدامها فقط وفقاً لشروط مُعينة. وإذا لم يكن بإمكان الدولة الطرف المتلقية لهذه المعلومات الامتثال لهذا الطلب، وجب عليها إشعار الطرف المقدم للمعلومات بذلك، والذي يقرر عندئذ إذا ما كان يتعين عليه مع ذلك تقديم تلك المعلومات. في حال قبول الدولة الطرف المتلقية بالمعلومات الخاضعة للشروط، وجب عليها الالتزام بها.

الفصل الرابع: الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

المادة 27 – الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق

1. في حالة عدم وجود أي معاهدة أو ترتيب بشأن المساعدة المتبادلة على أساس تشريع موحد ومتعلق بمبدأ المعاملة بالمثل بين الدولة الطرف المقدمة للطلب والدولة الطرف المطلوب منها، تطبق أحكام الفقرات من 2 إلى 9 من هذه المادة. ولا تطبق أحكام هذه المادة في حال وجود معاهدة أو ترتيب أو تشريع من هذا القبيل، ما لم توافق الأطراف المعنية على تطبيق أي أو كل البنود الباقية من هذه المادة بدلا منها.

2. أ) تقوم كل دولة طرف بتعيين سلطة أو سلطات مركزية مسؤولة عن إرسال طلبات المساعدة المتبادلة والرد عليها، أو تنفيذها أو إحالتها على الجهات المختصة من أجل تنفيذها؛

ب) تتواصل السلطات المركزية مع بعضها البعض بشكل مباشر؛

ج) تخبر كل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، الأمين العام لمجلس أوروبا بأسماء وعناوين السلطات المعينة طبقاً لهذه الفقرة؛

د) يقوم الأمين العام لمجلس أوروبا بإنشاء سجل خاص بالسلطات المركزية التي تعينها الدول الأطراف وبتحيينه. ويتعين على كل دولة طرف التأكد من صحة البيانات التي يتم حفظها في هذا السجل طوال الوقت.

3. يتم تنفيذ الطلبات الخاصة بالمساعدة المتبادلة بموجب هذه المادة وفقاً للإجراءات التي يحددها الطرف مقدم الطلب، فيما عدا ما يتعارض مع القانون الدولة الطرف المطلوب منها المساعدة.

4. يجوز للدولة الطرف المطلوب منها المساعدة، علاوة على أسس الرفض الواردة في الفقرة 4 من المادة 25، أن ترفض تقديم المساعدة في حال:

أ. كان الطلب يتعلق بجريمة تعتبرها الدولة الطرف المطلوب منها المساعدة جريمة سياسية أو جريمة لها علاقة بجريمة سياسية، أو

ب. ارتأت تلك الدولة أن تنفيذ الطلب من المحتمل أن يمس بسيادتها، أمنها، نظامه العام، أو بمصالح أساسية أخرى.

5. يجوز للدولة الطرف المطلوب منها تقديم المساعدة تأجيل البث في الطلب إذا كان من شأن ذلك إلحاق الضرر بتحقيقات أو متابعات جنائية تنجزها سلطاتها.

6. قبل رفض أو تأجيل تقديم المساعدة، تقوم الدولة الطرف المطلوب منها تقديم المساعدة، عند الاقتضاء وبعد التشاور مع الدولة الطرف مقدمة الطلب، بالنظر في إمكانية تنفيذ الطلب جزئياً أو إخضاعه للشروط التي تراها ضرورية.

7. تخبر الدولة الطرف المطلوب منها تقديم المساعدة على الفور الدولة الطرف مقدمة الطلب بنتيجة تنفيذ الطلب الخاص بالمساعدة. ويتوجب شرح الأسباب أي رفض أو تأجيل للطلب. علاوة على ذلك، تخبر الدولة الطرف المطلوب منها المساعدة الطرف مقدم الطلب بالأسباب التي تجعل تنفيذ الطلب مستحيلا أو التي من المحتمل أن تؤخره بشكل هام.

8. يجوز للدولة الطرف مقدمة الطلب أن تطلب من الطرف المطلوب منه المساعدة الحفاظ على سرية أي طلب يتم تقديمه بموجب هذا الباب علاوة على موضوع الطلب، إلا في حدود ما هو ضروري لتنفيذه. وفي حالة تعذر على الدولة الطرف المطلوب منها المساعدة الامتثال للطلب الخاص بالسرية، وجب عليها فورا إخبار الطرف مقدم الطلب الذي يقرر عندئذ ما إذا كان يتعين مع ذلك تنفيذ الطلب.

9. أ) في الحالات الطارئة، يجوز للسلطات القضائية بالدولة الطرف مقدمة الطلب أن ترسل مباشرة الطلبات الخاصة بالمساعدة المتبادلة أو المراسلات المتعلقة بذلك إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة. وفي مثل هذه الحالات، يتم إرسال نسخة في الوقت نفسه إلى السلطة المركزية في الدولة الطرف المطلوب منها المساعدة عن طريق نظيرتها في الدولة الطرف مقدمة الطلب.

ب) يجوز تقديم أي طلب أو مراسلة بموجب هذه الفقرة من خلال المنظمة الدولية للشرطة الجنائية (الإنتربول).

ج) في حال تقديم طلب وفقاً للفقرة الفرعية (أ) من هذه المادة وعدم اختصاص السلطة للتعامل مع الطلب، وجب على تلك السلطة إحالة الطلب على السلطة الوطنية المختصة وإخبار الدولة الطرف مقدمة الطلب فور إنجاز الإحالة.

د) يجوز للسلطات المختصة بالدولة الطرف مقدمة الطلب أن ترسل مباشرة الطلبات أو المراسلات بموجب هذه الفقرة والتي لا تتضمن أي إجراء إلزامي إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة.

هـ) يجوز لكل دولة طرف، وقت التوقيع أو عند إيداع صك التصديق أو القبول، الموافقة أو الانضمام، إخبار الأمين العام لمجلس أوروبا أن الطلبات المقدمة بموجب هذه الفقرة يجب أن ترسل، من أجل الفعالية، إلى سلطتها المركزية.

المادة 28 – السرية والقيود على الاستخدام

1. في حال عدم وجود أي معاهدة أو ترتيب بشأن المساعدة المتبادلة على أساس تشريع موحد أو المعاملة بالمثل بين الدولة الطرف مقدمة الطلب والدولة الطرف المطلوب منها المساعدة، تطبق أحكام هذه المادة. ولا تطبق أحكام هذه المادة في حال وجود معاهدة، ترتيب أو تشريع من هذا القبيل، ما لم تتفق الأطراف المعنية على تطبيق أي من البنود المتبقية من هذه المادة أو كلها بدلا منها.

2. يجوز للدولة الطرف المطلوب منها المساعدة تقييد توفير المعلومات أو المواد في إطار تلبية الطلب المقدم بشرط:

أ. الحفاظ على سريتها في حال تعذر إمكانية الاستجابة لطلب المساعدة القانونية المتبادلة في غياب شرط من هذا القبيل، أو

ب. عدم استخدامها في تحقيقات أو إجراءات غير تلك المشار إليها في الطلب.

3. في حال تعذر على الدولة الطرف مقدمة الطلب الامتثال لأحد الشرطين المشار إليهما في الفقرة 2، وجب عليها فورا إخبار الطرف الآخر، الذي يقرر عندئذ إذا كان يتعين، مع ذلك، تقديم المعلومات. وفي حال قبول الدولة الطرف مقدمة الطلب لهذا الشرط، وجب عليها الالتزام به.

4. يجوز لأي دولة طرف تقدم معلومات أو مواد وفقاً لأحد الشروط المشار إليها في الفقرة 2 أن تطلب من الطرف الآخر توضيح استخدام تلك المعلومات أو المواد علاقة بذلك الشرط.

القسم الثاني: أحكام خاصة

الفصل الأول: المساعدة المتبادلة بشأن التدابير المؤقتة

المادة 29 – التعجيل في حفظ بيانات الكومبيوتر المخزنة

1. يجوز لأي دولة طرف أن تطالب دولة طرفا أخرى أن تأمر أو تحصل بطريقة أخرى على التعجيل في حفظ بيانات مُخزنة بواسطة نظام كومبيوتر، يوجد على أراضي الدولة الطرف الأخرى، والتي تنوي أن تقدم بشأنها طلبا بالمساعدة المتبادلة من أجل البحث عن بيانات، النفاذ إليها، مصادرتها، تأمينها أو كشفها.
2. يجب أن يحدد طلب الحفظ الذي يتم تقديمه بموجب الفقرة 1 ما يلي:
   أ. الجهة التي تطلب الحفظ؛
   ب. الجريمة موضوع التحقيقات أو الإجراءات الجنائية وملخص موجز عن الوقائع المتعلقة بها؛
   ج. بيانات الكومبيوتر المخزنة المطلوب حفظها وعلاقتها بالجريمة؛
   د. أي معلومات متاحة تكشف عن القيِّم على بيانات الكومبيوتر المخزنة أو عن مكان وجود نظام الكومبيوتر؛
   هـ. الضرورة الموجبة للحفظ؛ و
   و. أن تلك الدولة تنوي تقديم طلب المساعدة المتبادلة من أجل البحث عن بيانات الكمبيوتر المخزنة، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها.
3. عند استلام الطلب من الطرف الآخر، يقوم الطرف المطلوب منه المساعدة باتخاذ كافة الإجراءات الملائمة وذلك لتعجيل حفظ البيانات المحددة وفقاً للقانون الوطني. ولأغراض الاستجابة للطلب، لا يجوز تقييد توفير هذا الحفظ بشرط ازدواجية التجريم.
4. يجوز لأي دولة طرف تقيد الاستجابة لطلب المساعدة المتبادلة بشرط ازدواجية التجريم من أجل البحث عن بيانات الكمبيوتر المخزنة، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها، بالنسبة لجرائم غير تلك المنصوص عليها وفقاً للمواد من 2 إلى 11 من هذه الاتفاقية، أن تحتفظ بالحق في رفض طلب الحفظ بموجب هذه المادة في الحالات التي يتوافر لديها فيها أسباب للاعتقاد بأنه يتعذر، في وقت الكشف أو الإفصاح عن هذه المعلومات، استيفاء الشرط الخاص بازدواجية التجريم.

5. بالإضافة إلى ذلك، يجوز رفض طلب الحفظ فقط إذا:

أ. كان الطلب يتعلق بجريمة تعتبر الدولة الطرف المطلوب منها المساعدة أنها تشكل جريمة سياسية أو جريمة مرتبطة بجريمة سياسية، أو

ب. اعتبرت الدولة الطرف المطلوب منها المساعدة أن تنفيذ الطلب من شأنه إلحاق الضرر بسيادتها، أمنها، نظامها العام أو مصالحها الأساسية الأخرى.

6. في حال اعتقاد الدولة الطرف المطلوب منها المساعدة أن الحفظ لن يضمن توافر البيانات مستقبلاً أو أنه سيهدد السرية أو يلحق الضرر بالتحقيقات التي تنجزها الدولة الطرف مقدمة الطلب، وجب عليها فوراً إخبار الدولة الطرف مقدمة الطلب التي يحدد عندئذ إذا ما كان ينبغي، مع ذلك، تنفيذ الطلب.

7. يكون أي حفظ يتم تفعيله استجابة للطلب المشار إليه في الفقرة 1 لفترة لا تقل عن ستين يوماً بغية تمكين الدولة الطرف مقدمة الطلب من تقديم طلب للبحث في بيانات، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها. بعد تلقي طلب من هذا القبيل، يجب مواصلة حفظ البيانات في انتظار صدور قرار بشأن ذلك الطلب.

المادة 30 – تعجيل الكشف عن بيانات الحركة المحفوظة

1. في حال اكتشفت الدولة الطرف المطلوب منها المساعدة، أثناء تنفيذ طلب مقدم وفقاً للمادة 29 بحفظ بيانات الحركة المتعلقة باتصال محدد، أن أحد مزودي الخدمة في دولة أخرى مشترك في نقل الاتصال، تقوم الدولة الطرف المطلوب منها المساعدة على الفور بالكشف عن القدر الكافي من بيانات الحركة لتحديد هوية مزود الخدمة والمسار الذي تم من خلاله ذلك الاتصال.

2. يجوز حجب بيانات الحركة بموجب الفقرة 1 فقط إذا:

أ. كان الطلب يتعلق بجريمة تعتبر الدولة الطرف المطلوب منها المساعدة أنها تشكل جريمة سياسية أو أنها متصلة بجريمة سياسية، أو

ب. اعتبرت الدولة الطرف المطلوب منها المساعدة أن تنفيذ الطلب من شأنه إلحاق الضرر بسيادتها، أمنها، نظامها العام أو مصالحها الأساسية الأخرى.

الفصل الثاني: المساعدة المتبادلة ذات الصلة بسلطات التحقيقات

المادة 31 – المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكومبيوتر المخزنة

1. يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث في بيانات، النفاذ إليها، مصادرتها، تأمينها أو الكشف عنها عندما تكون تلك البيانات

مخزنة بواسطة نظام كومبيوتر يوجد داخل أراضي الدولة الطرف المطلوب منها المساعدة، بما في ذلك البيانات التي تم حفظها وفقاً للمادة 29.

2. تستجيب الدولة الطرف المطلوب منها المساعدة للطلب من خلال تطبيق الصكوك والترتيبات والقوانين الدولية المشار إليها في المادة 23، وطبقاً للأحكام الأخرى ذات الصلة الواردة في هذا الباب.

3. تتم الاستجابة للطلب بشكل معجل عندما:

أ. توجد أسباب للاعتقاد بأن البيانات ذات الصلة مُعَرضة بصفة خاصة للضياع أو التعديل؛ أو

ب. تكون الصكوك والترتيبات والقوانين المشار إليها في الفقرة 2 تنص على التعجيل في التعاون.

المادة 32 – النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم

يجوز لدولة طرف، دون ترخيص من دولة طرف أخرى:

أ. النفاذ إلى بيانات كومبيوتر مُخزنة متاحة للعموم (مصدر مفتوح) بغض النظر عن مكان تواجد البيانات جغرافياً؛ أو

ب. النفاذ إلى بيانات كومبيوتر مُخزنة موجودة لدى دولة طرف أخرى أو تلقيها، من خلال نظام كومبيوتر داخل أقاليمها، في حال حصول تلك الدولة الطرف على الموافقة القانونية والطوعية للشخص الذي يتوفر على السلطة القانونية للكشف عن البيانات لتلك الدولة الطرف عبر نظام الكومبيوتر المذكور.

المادة 33 – المساعدة المتبادلة ذات الصلة بجمع بيانات الحركة في الوقت الحقيقي

1. تقدم الدول الأطراف المساعدة المتبادلة لبعضها البعض لجمع بيانات الحركة في الوقت الحقيقي المرتبطة باتصالات محددة في أقاليمها والتي يتم نقلها بواسطة نظام كومبيوتر. وطبقاً لأحكام الفقرة 2، تخضع هذه المساعدة للشروط والإجراءات المنصوص عليها بموجب القانون الوطني.

2. توفر كل دولة طرف مساعدة من هذا القبيل على الأقل فيما يتعلق بالجرائم الجنائية التي يكون فيها جمع بيانات الحركة في الوقت الحقيقي متاحاً في قضية محلية مماثلة.

المادة 34 – المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى

توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض لجمع بيانات المحتوى في الوقت الحقيقي أو تسجيلها فيما يتعلق باتصالات محددة يتم نقلها بواسطة نظام كومبيوتر بقدر ما تسمح به المعاهدات والقوانين الوطنية واجبة التطبيق.

الفصل الثالث: شبكة على مدار الساعة و7 أيام في الأسبوع

المادة 35 – شبكة على مدار الساعة و7 أيام في الأسبوع

1. تعين كل دولة طرف نقطة اتصال متاحة على مدار الساعة وسبعة أيام في الأسبوع بغية ضمان توفير المساعدة الفورية لأغراض التحقيقات أو الإجراءات الخاصة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر أو من أجل جمع الأدلة الخاصة بجريمة جنائية في شكل إلكتروني. وتشمل هذه المساعدة تسهيل، أو إذا كان قانونها الوطني وممارستها يسمح بذلك، تنفيذ التدابير التالية بشكل مباشر:
   أ. توفير المشورة الفنية؛
   ب. حفظ البيانات طبقاً للمادتين 29 و30؛
   ج. جمع الأدلة وتوفير المعلومات القانونية وتحديد موقع المشتبه بهم.
2. (أ) يجب أن تتوفر نقطة الاتصال للدولة الطرف على القدرة على إجراء اتصالات مع مثيلتها في دولة طرف أخرى على وجه السرعة.
   (ب) إذا كانت نقطة الاتصال التي تعينها دولة طرف ليست جزءاً من السلطة أو السلطات المسؤولة عن المساعدة المتبادلة الدولية أو عن تسليم المجرمين، وجب على نقطة الاتصال أن تضمن أنها قادرة على التنسيق مع تلك السلطة أو السلطات على وجه السرعة.
3. تضمن كل دولة طرف توفير طاقم حاصل على التدريب والمعدات الضروريين من أجل تسهيل تشغيل الشبكة.

الباب الرابع: الأحكام الختامية

المادة 36 – التوقيع ودخول حيز النفاذ

1. تفتتح هذه الاتفاقية للتوقيع من قبل الدول الأعضاء بمجلس أوروبا والدول غير الأعضاء التي شاركت في صياغتها.
2. تخضع هذه الاتفاقية للتصديق، القبول أو الموافقة. وتودع وثائق التصديق، القبول أو الموافقة لدى الأمين العام لمجلس أوروبا.

3. تدخل هذه الاتفاقية حيز التنفيذ في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ تعبير خمس دول، من بينها ثلاث دول على الأقل من أعضاء مجلس أوروبا، عن موافقتها على الالتزام بالاتفاقية طبقاً لأحكام الفقرتين 1 و2.

4. تدخل هذه الاتفاقية حيز التنفيذ، بالنسبة لأي دولة توقع عليها وتعرب بعدها عن موافقتها على الالتزام بها، في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ التعبير عن موافقتها على الالتزام بالاتفاقية طبقاً لأحكام الفقرتين 1 و2.

المادة 37 – الانضمام إلى الاتفاقية

1. بعد دخول الاتفاقية حيز التنفيذ، يجوز للجنة وزراء مجلس أوروبا، بعد التشاور مع الدول المتعاقدة في الاتفاقية والحصول على موافقتها بالإجماع، توجيه الدعوة لأي دولة غير عضو في المجلس ولم تشارك في صياغة الاتفاقية للانضمام إلى هذه الاتفاقية. ويتم اتخاذ القرار بالأغلبية المنصوص عليها في المادة -20 د من النظام الأساسي لمجلس أوروبا وعن طريق تصويت الدول المتعاقدة في الاتفاقية بالإجماع المخول لها المشاركة في لجنة الوزراء.

2. تدخل الاتفاقية حيز التنفيذ – بالنسبة لأي دولة تنضم للاتفاقية بموجب الفقرة 1 أعلاه – في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ إيداع وثيقة الانضمام لدى الأمين العام لمجلس أوروبا.

المادة 38 – التطبيق الإقليمي

1. يجوز لأي دولة، وقت التوقيع على الاتفاقية أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، تحديد الإقليم أو الأقاليم التي تطبق عليها هذه الاتفاقية.

2. يجوز لأي دولة، في أي تاريخ لاحق، وبموجب إعلان موجه إلى الأمين العام لمجلس أوروبا، توسيع نطاق تطبيق هذه الاتفاقية على أي إقليم يتم تحديده في الإعلان. وتدخل الاتفاقية حيز التنفيذ بالنسبة لهذا الإقليم في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ استلام الإعلان من قبل الأمين العام لمجلس أوروبا.

3. يجوز سحب أي إعلان تم تقديمه بموجب الفقرتين السابقتين، بالنسبة لأي إقليم محدد في مثل هذا الإعلان، بموجب إشعار موجه إلى الأمين العام لمجلس أوروبا. ويدخل سحب الإعلان حيز النفاذ في اليوم الأول من الشهر الموالي لانتهاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام لمجلس أوروبا لهذا الإشعار.

المادة 39 – الآثار المترتبة على الاتفاقية

1. يتلخص الغرض من هذه الاتفاقية في استكمال المعاهدات أو الترتيبات ثنائية أو متعددة الأطراف فيما بين الأطراف، بما في ذلك أحكام:

- الاتفاقية الأوروبية بشأن تسليم المجرمين، التي فتحت للتوقيع بباريس في 13 ديسمبر/كانون الأول 1957 (سلسلة المعاهدات الأوروبية رقم 24)؛
- الاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية، التي فتحت للتوقيع بستراسبورغ في 20 أبريل/نيسان 1959 (سلسلة المعاهدات الأوروبية رقم 30)؛
- البروتوكول الإضافي للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية، التي فتحت للتوقيع بستراسبورغ في 17 مارس/آذار 1978 (سلسلة المعاهدات الأوروبية رقم 99).

2. في حال إبرام طرفين أو أكثر لاتفاقية أو معاهدة بشأن المسائل التي تتناولها هذه الاتفاقية، أو إقامة علاقات بشأن مثل هذه المسائل بشكل آخر، أو عزمهم القيام بذلك في المستقبل، تكون تلك الدول مخولة لتطبيق تلك الاتفاقية أو المعاهدة أو تنظيم علاقاتها بناء عليها. ومع ذلك، يجب على الدول الأطراف، في حال إقامة علاقات فيما يتعلق بالمسائل التي تتناولها هذه الاتفاقية بخلاف ما تنظمه هذه الاتفاقية، أن تنظم تلك العلاقات بطريقة تتفق مع أهداف الاتفاقية ومبادئها.

3. لا يؤثر أي شيء ورد بهذه الاتفاقية على حقوق أي دولة طرف، قيودها، التزاماتها ومسئولياتها.

المادة 40 – الإعلانات

يجوز لأي دولة، بموجب إعلان خطي يوجه إلى الأمين العام لمجلس أوروبا، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، أن تعلن أنها تستفيد من إمكانية طلب عناصر إضافية كما هو منصوص عليه بموجب المواد 2، 3 و6 - الفقرة 1(ب)، والمادة 7، والمادة 9 - الفقرة 3، والمادة 27 - الفقرة 9 (هـ).

المادة 41 – البند الاتحادي

1. يجوز للدولة الاتحادية الاحتفاظ بالحق في الاضطلاع بالالتزامات بموجب الباب الثاني من هذه الاتفاقية بما يتفق ومبادئها الأساسية التي تنظم العلاقة بين حكومتها المركزية والدول المؤسسة أو غيرها من الكيانات الإقليمية الأخرى المماثلة شريطة أن تظل قادرة على التعاون بموجب الباب الثالث.

2. لا يجوز للدولة الاتحادية، عند التحفظ بموجب الفقرة 1، تطبيق بنود هذا التحفظ لاستبعاد أو تقليص التزاماتها بشكل جوهري للتنصيص على التدابير المذكورة في الباب الثاني. وبشكل عام، يجب عليها توفير قدرة فعالة وواسعة في تنفيذ القانون فيما يتعلق بتلك التدابير.

3. بالنسبة لأحكام هذه الاتفاقية، التي يصبح تطبيقها بموجب الولاية القضائية للدول المؤسسة أو غيرها من الكيانات الإقليمية الأخرى المماثلة غير الملزمة بالنظام الدستوري للاتحاد من أجل اتخاذ تدابير تشريعية، تقوم الحكومة

الفيدرالية بإخبار السلطات المختصة في تلك الدول بالأحكام المذكورة إلى جانب رأيها المفضل، لتشجيعها على اتخاذ الإجراءات الملائمة لتفعيلها.

المادة 42 – التحفظات

يجوز لأي دولة، بموجب إشعار خطي موجه إلى الأمين العام لمجلس أوروبا، وقت التوقيع أو عند إيداع صك التصديق، القبول، الموافقة أو الانضمام، أن تعلن أنها تستفيد من التحفظ أو التحفظات المنصوص عليها في المادة 4 – الفقرة 2، والمادة 6 – الفقرة 3، والمادة 9 – الفقرة 4، والمادة 10 – الفقرة 3، والمادة 11 – الفقرة 3، والمادة 14 – الفقرة 3، والمادة 22 – الفقرة 2، والمادة 29 – الفقرة 4، والمادة 41 – الفقرة 1. ولا يجوز تقديم أية تحفظات أخرى.

المادة 43 – وضع التحفظات وسحبها

1. يجوز لأي دولة طرف تقدمت بتحفظ طبقاً للمادة 42 أن تسحب ذلك التحفظ كلياً أو جزئياً وذلك عن طريق إشعار خطي موجه إلى الأمين العام لمجلس أوروبا. ويدخل سحب التحفظ حيز التنفيذ في تاريخ استلام الإشعار من قبل الأمين العام لمجلس أوروبا. وفي حال أشار الإشعار إلى تاريخ محدد لدخول سحب التحفظ حيز النفاذ، وكان ذلك التاريخ لاحقاً لتاريخ استلام الإشعار من قبل الأمين العام، يبدأ العمل بسحب التحفظ في ذلك التاريخ اللاحق.
2. يجوز لأي دولة طرف تقدمت بتحفظ كما هو مشار إليه في المادة 42 سحب هذا التحفظ، كلياً أو جزئياً، بمجرد ما تسمح الظروف بذلك.
3. يجوز للأمين العام لمجلس أوروبا أن يستفسر، بشكل دوري، الدول الأطراف التي استخدمت تحفظا أو أكثر من تحفظ طبقاً للمادة 42 عن احتمالات سحب ذلك التحفظ (أو تلك التحفظات).

المادة 44 – التعديلات

1. يجوز لأي دولة طرف اقتراح تعديلات على هذه الاتفاقية، ويقوم الأمين العام لمجلس أوروبا بإرسالها إلى الدول الأعضاء بمجلس أوروبا، والدول غير الأعضاء التي شاركت في صياغة الاتفاقية، وكذلك إلى أي دولة انضمت إليها، أو تم توجيه الدعوة إليها للانضمام إلى هذه الاتفاقية وفقاً لأحكام المادة 37.
2. يرسل أي تعديل مقترح من قبل دولة طرف إلى اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، التي تعرض رأيها في هذا التعديل المقترح على لجنة الوزراء.
3. تنظر لجنة الوزراء في التعديل المقترح والرأي الذي تحيله عليها اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، ويجوز لها، بعد التشاور مع الدول الأطراف غير الأعضاء في هذه الاتفاقية، تبني التعديل.

4. يرسل نص أي تعديل تتبناه لجنة الوزراء طبقاً للفقرة 3 من هذه المادة إلى الدول الأطراف للموافقة عليه.

5. يدخل أي تعديل يتم إقراره طبقاً للفقرة 3 من هذه المادة حيز التنفيذ في اليوم الثلاثين بعد إخبار جميع الدول الأطراف الأمين العام لمجلس أوروبا بقبولها بذلك التعديل.

المادة 45 – تسوية النزاعات

1. يتم إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) على علم بما يتعلق بتفسير وتطبيق هذه الاتفاقية.

2. في حال حدوث نزاع بين دول أطراف بشأن تفسير أو تطبيق هذه الاتفاقية، يتعين عليها السعي إلى تسوية للنزاع عبر التفاوض أو أي وسيلة سلمية أخرى من اختيارهم، بما في ذلك إحالة النزاع على اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) أو إلى هيئة تحكيم والتي تكون قرارتها ملزمة بالنسبة للأطراف، أو إلى محكمة العدل الدولية حسبما تتفق عليه الأطراف المعنيين.

المادة 46 – مشاورات الأطراف

1. تقوم الدول الأطراف، عند الاقتضاء، بالتشاور فيما بينها بشكل دوري بغية تيسير:

أ. الاستخدام والتنفيذ الفعال لهذه الاتفاقية، بما في ذلك تحديد أي مشاكل ذات الصلة، علاوة على آثار أي إعلان أو تحفظ يتم تقديمهما بموجب هذه الاتفاقية؛

ب. تبادل المعلومات بشأن التطورات القانونية، السياسية أو التكنولوجية ذات الصلة بالجريمة الإلكترونية وجمع الأدلة في شكل إلكتروني؛

ج. دراسة الإضافات أو التعديلات الممكنة للاتفاقية.

2. يتم إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) على علم، بشكل دوري، بنتائج المشاورات المشار إليها في الفقرة 1.

3. تقوم اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، عند الاقتضاء، بتيسير المشاورات المشار إليها في الفقرة 1 واتخاذ التدابير اللازمة لمساعدة الدول الأطراف في جهودها لاستكمال أو تعديل الاتفاقية. وتقوم اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، على الأكثر بعد ثلاث سنوات من دخول هذه الاتفاقية حيز التنفيذ، بالتعاون مع الدول الأطراف لإجراء مراجعة لكافة أحكام الاتفاقية، وعند الضرورة، تقدم توصيات بالتعديلات الملائمة.

4. بخلاف ما يتكفل به مجلس أوروبا، تلتزم الدول الأطراف بالنفقات الناجمة عن تنفيذ أحكام الفقرة 1 بالطريقة التي تحددها.

5. تساعد الأمانة العامة لمجلس أوروبا الدول الأطراف في تنفيذ مهامها طبقاً لهذه المادة.

المادة 47 – الانسحاب

1. يجوز لأي دولة طرف، في أي وقت، الانسحاب من هذه الاتفاقية عن طريق إشعار موجه إلى الأمين العام لمجلس أوروبا.
2. ويدخل هذا الانسحاب حيز التنفيذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام للإشعار.

المادة 48 – الإبلاغ

يقوم الأمين العام لمجلس أوروبا بإبلاغ الدول الأعضاء في مجلس أوروبا والدول غير الأعضاء التي شاركت في صياغة هذه الاتفاقية، علاوة على أي دولة انضمت إليها أو دعيت للانضمام إلى هذه الاتفاقية بـما يلي:

أ. أي توقيع؛

ب. إيداع أي صك للتصديق، القبول، الموافقة أو الانضمام؛

ج. أي تاريخ لدخول هذه الاتفاقية حيز التنفيذ طبقاً للمادتين 36 و37؛

د. أي إعلان يتم تقديمه بموجب المادة 40 أو أي تحفظ يتم تقديمه طبقاً للمادة 42؛

هـ. أي إجراء، إخطار أو تواصل آخر يتعلق بهذه الاتفاقية.

وإثباتا لذلك، قام الموقعون أدناه، المفوضون بذلك حسب الأصول، بالتوقيع على هذه الاتفاقية.

حرر في بودابست - في الثالث والعشرين من شهر نوفمبر/تشرين الثاني 2001، باللغتين الإنجليزية والفرنسية وكلا النصين متساويين في الحجية، وذلك في نسخة واحدة تودع في محفوظات مجلس أوروبا. ويرسل الأمين العام لمجلس أوروبا نسخا مصدقا عليها إلى كل دولة عضو في مجلس أوروبا، وإلى الدول غير الأعضاء التي شاركت في صياغة هذه الاتفاقية وإلى أي دولة دعيت للانضمام إليها.

التقرير التفسيري

أولا – تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (8 نوفمبر/تشرين الثاني 2001) وفتح باب التوقيع على الاتفاقية في بودابست، في 23 نوفمبر/تشرين الثاني 2001، 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

1. 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.

2. 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.

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

4. 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.

5. 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.

6. 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

7. قررت اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، في قرارها رقم CDPC/103/211196 الصادر في نوفمبر/تشرين الثاني 1996، إنشاء لجنة خبراء للتعامل مع الجريمة الإلكترونية. واستندت اللجنة في قرارها على الأساس المنطقي التالي:

8. "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.

9. 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 89 (9) 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".

10. 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 (89) 9[2] بشأن القانون الموضوعي وفي التوصية رقم (95) 13[3] بشأن مشاكل القانون الإجرائي المتصلة بتكنولوجيا المعلومات.

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

أ. "على ضوء التوصيتين رقم (89) 9 بشأن الجرائم المتصلة بالكمبيوتر ورقم (95) 13 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

---

1. إعمال التوصية رقم 9 (89) بشأن الجرائم المتصلة بالكمبيوتر، تقرير أعده الأستاذ الدكتور ه. كاسبرسين (وثيقة. اللجنة الأوروبية المعنية بمشاكل الإجرام (97) 5 أند ولجنة الخبراء المتعلقة بالفضاء الإلكتروني (5 (97) (PC-CY، صفحة 106).
2. انظر الجريمة المتصلة بالكمبيوتر، تقرير اللجنة الأوروبية المعنية بمشاكل الإجرام، الصفحة 86.
3. انظر مشاكل قانون الإجراءات الجنائية المتصلة بتكنولوجيا المعلومات، التوصية رقم (95) 13، المبدأ رقم 17.

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 ".

12. 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 4 فبراير/شباط (1997). وقد بدأت هذه اللجنة المعروفة بالاختصار الانجليزي (PC-CY) أعمالها في أبريل/نيسان 1997 وأجرت مفاوضات بشأن مسودة اتفاقية دولية حول الجريمة الإلكترونية. وفي إطار بنودها المرجعية الأصلية، كان من المقرر أن تنهي اللجنة عملها بحلول 31 ديسمبر/كانون الأول 1999. 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 31 ديسمبر/كانون الأول 2000 بموجب القرار رقمCM/Del/Dec(99)679 الصادر عن نواب الوزراء. وقد أعرب وزراء العدل الأوروبيون مرتين عن تأييدهم للمفاوضات: بموجب القرار رقم 1 المعتمد خلال مؤتمرهم الحادي والعشرين (براغ، يونيو/حزيران 1997)، 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 3، المعتمد خلال المؤتمر الثالث والعشرين لوزراء العدل الأوروبيين (لندن، يونيو/حزيران 2000)، 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 1999.

13. في الفترة الممتدة ما بين أبريل/نيسان 1997 وديسمبر/كانون الأول 2000، عقدت لجنة (PC-CY) (10 اجتماعات في جلسات عامة و15 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 2000 إبداء رأيها بشأن مسودة الاتفاقية الذي اعتمدته في الجزء الثاني من دورتها العامة في أبريل/نيسان 2001.

14. في أعقاب قرار اتخذته لجنة (PC-CY)، تم الكشف عن نسخة مبكرة من مسودة الاتفاقية وصدورها في أبريل/نيسان 2000، تلتها مسودات لاحقة صدرت بعد كل جلسة عامة، بغية تمكين الدول المتفاوضة من التشاور مع كافة الأطراف المهتمة. وقد ثبتت فائدة عملية التشاور.

15. قدمت مسودة الاتفاقية المنقحة والنهائية ومذكرتها التفسيرية للموافقة عليهما إلى اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) في دورتها العامة الخمسين المنعقدة في يونيو/حزيران 2001، وبعدها، تم عرض نص مسودة الاتفاقية على لجنة الوزراء لاعتماده وفتح باب التوقيع عليه.

ثالثا. الاتفاقية

16. ترمي الاتفاقية بشكل أساسي إلى (1) مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية (2) 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 (3) وإلى إنشاء نظام سريع وفعال للتعاون الدولي.

17. بناء على ذلك، تتضمن الاتفاقية أربعة فصول: (1) استخدام المصطلحات؛ (2) التدابير الواجب اتخاذها على الصعيد المحلي – القانون الموضوعي والقانون الإجرائي؛ (3) التعاون الدولي؛ (4) الأحكام الختامية.

18. يتطرق القسم 1 من الفصل الثاني (مسائل القانون الموضوعي) إلى أحكام التجريم والأحكام الأخرى ذات الصلة في مجال الجريمة الإلكترونية أو الجريمة المتصلة بالكمبيوتر: يحدد أولا 9 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.

19. يحدد القسم 2 من الفصل الثاني (المسائل المتعلقة بالقانون الإجرائي) – الذي يتجاوز نطاقه الجرائم المحددة في القسم 1 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.

20. يتضمن الفصل الثالث الأحكام المتعلقة بالمساعدة المتبادلة التقليدية والمتصلة بالجريمة الإلكترونية، فضلا عن قواعد تسليم المجرمين. ويتناول هذا الفصل المساعدة المتبادلة التقليدية في حالتين: 1) غياب الأساس القانوني (معاهدة، تشريع متبادل، وما إلى ذلك) بين الأطراف – وفي هذه الحالة تنطبق أحكامه – 2) 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 24 ساعة طوال أيام الأسبوع بغية ضمان المساعدة السريعة بين الاطراف.

21. 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 1

22. استوعب القائمون على الصياغة أن الأطراف لن تكون ملزمة، بموجب هذه الاتفاقية، باستنساخ المفاهيم الأربعة المحددة في المادة 1حرفيا في قوانينها الداخلية، شريطة أن تغطي هذه القوانين تلك المفاهيم بطريقة تتفق مع مبادئ الاتفاقية و توفر إطارا مطابقا لتنفيذها.

المادة 1 (أ) – نظام الكمبيوتر

23. 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 المُعالج (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.

24. 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 1 (ب) – بيانات الكمبيوتر

25. 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 تُفهم 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 1 (ج) – مقدم الخدمة

26. 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 2). وبموجب الفقرة (1) 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 تقدَّم لهم هذه الخدمة من خلال شبكة الشركة.

27. بموجب الفقرة (2) من التعريف، يتضح أن مصطلح "مقدم الخدمات" يشمل أيضا الهيئات التي تخزن البيانات أو تعالجها نيابة عن الأشخاص المذكورين في الفقرة الفرعية (1). 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 (1). 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 1 (د) – بيانات الحركة

28. لأغراض هذه الاتفاقية، تشكل بيانات حركة المرور، على النحو المحدد في المادة 1 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.

29. 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.

30. 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.

31. يترك التعريف للمجالس التشريعية الوطنية القدرة على إدخال تمييز في الحماية القانونية لبيانات الحركة وفقا لحساسيتها. وفي هذا السياق، تلزم المادة 15 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

32. يتضمن الفصل الثاني (من المادة 2 إلى المادة 22) ثلاثة أقسام: القانون الجنائي الموضوعي (المواد من 2 إلى 13)، والقانون الإجرائي (المواد من 14 إلى 21) والولاية القضائية (المادة 22).

القسم 1 – القانون الجنائي الموضوعي

33. يتلخص الغرض من القسم 1 من الاتفاقية (المواد من 2 إلى 13) 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.

34. 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 9 (89) 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.

35. ينقسم القسم إلى خمسة أبواب. ويشمل الباب 1 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 2 إلى 4 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 2 (الغش والتزوير المتصلان بالكمبيوتر) طبقا للمقترحات الواردة في المبادئ التوجيهية لتوصية مجلس أوروبا رقم 9 (89). ويغطي الباب 3 "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 4 "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 5 أحكاما إضافية بشأن المحاولة والمساعدة والتحريض والعقوبات والتدابير، وامتثالا للصكوك الدولية الحديثة، أحكاما بشأن مسؤولية الشركات.

36. 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.

37. أدرك القائمون على صياغة الاتفاقية أن الأطراف قد تستبعد سوء السلوك البسيط أو غير الهام من تطبيق الجرائم المحددة في المواد من 2 إلى 10.

38. 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).

39. 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 8 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.

40. تسمح بعض المواد الواردة في هذا القسم بإضافة ظروف مؤهلة عند تنفيذ الاتفاقية في القانون المحلي. وفي حالات أخرى، تمنح إمكانية التحفظ (انظر المادتين 40 و42). 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.

41. 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.

42. خلال عملية الصياغة، تدارس القائمون على الصياغة استصواب تجريم سلوك غير السلوكيات المحددة في المواد من 2 إلى 11، 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

43. يتلخص الغرض من الجرائم المحددة في المواد (من 2 إلى 6) 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 2)

44. 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.

45. 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.

46. 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).

47. 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".

48. قد يؤدي تطبيق أدوات تقنية محددة إلى النفاذ بموجب المادة 2، 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 واسترجاع 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 قبِل بتطبيقه، على سبيل المثال في حالة "الكوكيز"، بعدم رفض التركيب الأولي أو عدم إزالته.

49. 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 2 موضع نزاع، لكن تتبع 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 9 (89) واقتراح الفريق العامل التابع لمنظمة التعاون والتنمية الاقتصادية في عام 1985.

50. يمكن للأطراف أن تعتمد المقاربة الواسعة وأن تجرم مجرد الاختراق طبقا للجملة الأولى من المادة 2. 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 3)

51. 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 8 من الاتفاقية الأوروبية لحقوق الإنسان الحق في خصوصية المراسلات. وتطبق الجريمة المنصوص عليها في المادة 3 هذا المبدأ على جميع أشكال نقل البيانات الإلكترونية، سواء عن طريق الهاتف أو الفاكس أو البريد الإلكتروني أو نقل الملفات.

52. اقتُبس نص الحكم أساسا من جريمة "الالتقاط غير المرخص" الواردة في التوصية 9 (89). وتوضح هذه الاتفاقية أن الاتصالات المعنية تتعلق "بإرسال بيانات الكمبيوتر" فضلا عن الإشعاع الكهرومغناطيسي، في ظل الظروف المبينة أدناه.

53. 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.

54. 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 3 (انظر مثلا حكم المحكمة الأوروبية لحقوق الإنسان في قضية هالفورد ضد المملكة المتحدة، 25 يونيو/حزيران 1997، 20605/92).

55. 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.

56. 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 الولوج إليه بسهولة، وبالتالي يمكن اعتراضه، على سبيل المثال من قبل هواة الراديو.

57. 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 1. 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.

58. 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 3 (انظر الفقرة 54 أعلاه)، يمكن أن يوفر القانون المحلي سببا للاعتراض المشروع على هذه الاتصالات. وبموجب المادة 3، يعتبر الاعتراض في مثل هذه الظروف على أنه تم "عن حق".

59. 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 2، 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 4)

60. 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.

61. في الفقرة 1، 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.

62. 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 المشغِّل، أو

إعادة تشكيل نظام تشغيل الكمبيوتر الذي يتم عندما يقتني مشغِّل 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.

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

64. تسمح الفقرة 2 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 5)

65. يشار إلى ذلك في التوصية رقم 9 (89) 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.

66. 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.

67. 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 المشغِّل 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).

68. 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 المشغِّل، أو إعادة تشكيل نظام تشغيل الكمبيوتر الذي يتم عندما يقتني مشغِّل 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.

69. 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.

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

إساءة استخدام الأجهزة (المادة 6)

71. 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 2 إلى 5. 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 178) والاتحاد الأوروبي (التوجيه رقم 98/84/EC الصادر عن البرلمان الأوروبي والمجلس والمؤرخ في 20 نوفمبر /تشرين الثاني 1998 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 1929 بشأن تزييف النقد.

72. تجرم الفقرة 1 (أ) 1 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 2 إلى 5 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.

73. 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.

74. تجرم الفقرة 1 (أ) 2 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.

75. تنشئ الفقرة 1 (ب) جريمة حيازة المواد المبينة في الفقرة 1 (أ) 1 أو 1 (أ) 2. ويسمح للأطراف، بموجب الجملة الأخيرة من الفقرة 1 (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.

76. 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 2 إلى 5 من الاتفاقية.

77. تبين الفقرة 2 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" .

78. نظرا لمختلف عمليات التقييم لضرورة تطبيق جريمة "إساءة استعمال الأجهزة" على جميع أنواع جرائم الكمبيوتر المختلفة الواردة في المواد من 2 إلى 5، تسمح الفقرة 3، على أساس التحفظ (انظر المادة 42)، 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 1 (أ) 2.

الباب 2 – الجرائم المتصلة بالكمبيوتر

79. تتعلق المواد من 7 إلى 10 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.

80. 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 7)

81. 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.

82. 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 تُصْدر البيانات، بصرف النظر عن صحة أو صدق محتويات البيانات. ويمكن للأطراف أن تذهب أبعد من ذلك وأن تدرج في مصطلح "أصلي" صحة البيانات.

83. 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.

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

85. 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 8)

86. 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 بِنية النقل غير المشروع للملكية.

87. بغية ضمان تغطية جميع التلاعبات المحتملة ذات الصلة، تم استكمال العناصر المكونة ل "الإدخال"، "التغيير"، "الحذف" أو "الإتلاف" الواردة في المادة 8(أ) بالفعل العام المتمثل في "التدخل في أداء برنامج أو نظام الكمبيوتر "في المادة 8 (ب). وتكتسي عناصر "الإدخال، التغيير، الحذف أو الاتلاف" نفس المعنى الوارد في المواد السابقة. وتغطي المادة 8 (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.

88. تجرَّم 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.

89. 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).

90. 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 3 – الجرائم ذات الصلة بالمحتوى

الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية (المادة 9)

91. تسعى المادة 9 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.

92. يستجيب هذا الحكم لقلق رؤساء دول وحكومات مجلس أوروبا، المعرب عنه خلال مؤتمر القمة الثاني (ستراسبورغ، 11-10 أكتوبر/تشرين الأول 1997) في خطة عملهم (البند الثالث – 4) 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).

93. يجرِّم 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.

94. تجرم الفقرة 1(أ) إنتاج المواد الإباحية المتعلقة بالأطفال لأغراض التوزيع عن طريق نظام الكمبيوتر. واعتبرت أن هذا الحكم ضروري لمكافحة الأخطار المذكورة أعلاه من مصدرها.

95. تجرم الفقرة 1(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.

96. تجرم الفقرة 1(ج) توزيع أو نقل المواد الإباحية المتعلقة بالأطفال عن طريق نظام الكمبيوتر. ويعرف "التوزيع" بأنه النشر النشط للمادة. وتُناول مسألة إرسال المواد الإباحية المتعلقة بالأطفال عن طريق نظام الكمبيوتر إلى شخص آخر في إطار جريمة "نقل" المواد الإباحية المتعلقة بالأطفال.

97. يقصد بعبارة "الشراء لحساب الشخص نفسه أو لفائدة شخص آخر" الواردة في الفقرة 1(د)، السعي بنشاط إلى الحصول على المواد الإباحية المتعلقة بالأطفال، مثلا عن طريق تحميلها.

98. تُجرِّم الفقرة 1(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.

99. يخضع مصطلح "المواد الإباحية" الوارد في الفقرة 2 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.

100. 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.

101. تغطي الأنواع الثلاثة من المواد المحددة في الفقرة 2 لأغراض ارتكاب الجرائم الواردة في الفقرة 1 صور الاعتداء الجنسي على طفل من دم ولحم (2.أ)، والصور الإباحية التي يظهر في شخص يبدو أنه قاصر وهو يمارس سلوكا جنسي واضحا (2.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 (2.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.

102. في الحالات الثلاث المشمولة بالفقرة 2، تختلف المصالح القانونية المحمية اختلافا طفيفا. وتركز الفقرة 2(أ) بصورة مباشرة على الحماية من سوء معاملة الأطفال. وتهدف الفقرتان 2(ب) و2(ج) إلى توفير الحماية من السلوك الذي، إن لم يكن يؤدي بالضرورة إلى إلحاق الضرر بـــ "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.

103. 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 بـــــ "المواد الإباحية" التي لها مزايا فنية، طبية، علمية أو ما شابه ذلك. وفيما يتعلق بالفقرة 2(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 المصوَّر ليس قاصرا بالمعنى الوارد في هذا الحكم.

104. تعرف الفقرة 3 مصطلح "القاصر" في سياق المواد الإباحية عن الأطفال بصفة عامة، باعتباره أي شخص دون سن 18 عاما، وفقا لتعريف "الطفل" في اتفاقية الأمم المتحدة لحقوق الطفل (المادة 1). وقد اعتُبر 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 3 تسمح للأطراف بأن تقضي بحدود عمرية مختلفة، شريطة ألا تقل عن 16 سنة.

105. تسرد هذه المادة أنواعا مختلفة من الأفعال غير المشروعة المتعلقة باستغلال الأطفال في المواد الإباحية التي تلزم الأطراف، كما هو الحال في المواد من 2 إلى 8، 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.

106. تسمح الفقرة 4 للأطراف بإبداء تحفظات بشأن الفقرة 1(د) و(ه) والفقرة 2(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 42.

الباب 4 – الجرائم المتعلقة بانتهاكات حق التأليف والنشر والحقوق المجاورة

الجرائم المتعلقة بانتهاكات حق التأليف والنشر والحقوق المجاورة (المادة 10)

107. 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.

108. 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 1 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 2 انتهاك الحقوق ذات الصلة عن طريق نظام الكمبيوتر.

109. يُعرَّف 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 10 بصريح العبارة، وبالتالي تستبعد الانتهاكات المتعلقة ببراءات الاختراع أو العلامات التجارية.

110. بخصوص الفقرة 1، فإن الاتفاقات المشار إليها هي قانون باريس المؤرخ 24 يوليو/ تموز 1971، 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 2، 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.

111. 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.

112. 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 6 مكرر من اتفاقية برن وفي المادة 5 من معاهدة الويبو بشأن حقوق المؤلف).

113. 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 1 و2، لأن هذا هو المصطلح المستخدم في الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (اتفاق تريبس) (المادة 61)، الذي يحكم الالتزام بتجريم انتهاكات حقوق التأليف والنشر.

114. تهدف الأحكام إلى التنصيص على عقوبات جنائية ضد الانتهاكات "على نطاق تجاري" وعن طريق نظام الكمبيوتر. وهذا يتماشى مع المادة 61 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.

115. 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.

116. تسمح الفقرة 3 للأطراف بعدم فرض المسؤولية الجنائية بموجب الفقرتين 1 و2 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 61 من الاتفاق المتعلق بجوانب حقوق الملكية الفكرية المتصلة بالتجارة (اتفاق تريبس) الذي يشكل الحد الأدنى المطلوب من شروط التجريم القائمة.

117. 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 5 – المسؤولية الإضافية والعقوبات

المحاولة والمساعدة أو التحريض (المادة 11)

118. 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.

119. تقتضي الفقرة 1 من الأطراف تجريم المساعدة أو التحريض على ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد من 2 إلى 10. 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.

120. فيما يخص الفقرة 2 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 3، 4، 5، 7، 8 و9 (1) (أ) و9 (1) (ج).

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

122. أضيفت الفقرة 3 لمعالجة الصعوبات التي قد تواجهها الأطراف من حيث الفقرة 2، بالنظر إلى المفاهيم المتباينة على نطاق واسع في مختلف التشريعات، على الرغم من الجهود المبذولة في الفقرة 2 لاستثناء بعض الجوانب من الحكم المتعلق بالمحاولة. ويجوز لأي طرف أن يعلن تحفظه بالحق في عدم تطبيق الفقرة 2 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 12)

123. تتناول المادة 12 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 12 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.

124. بموجب الفقرة 1، يلزم استيفاء أربعة شروط من أجل إلحاق المسؤولية. أولا، يجب أن ترتكب إحدى الجرائم الموصوفة في الاتفاقية. ثانيا، يجب أن تكون الجريمة قد

ارتُكبت 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 1 الأطراف بأن تكون قادرة على فرض المسؤولية على الشخص الاعتباري فقط على الجرائم التي يرتكبها هؤلاء القادة.

125. بالإضافة إلى ذلك، تلزم الفقرة 2 الأطراف بأن تكون لديها القدرة على فرض المسؤولية على شخص اعتباري عندما لا ترتكب الجريمة من قبل الشخص القائد الوارد وصفه في الفقرة 1، 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 (1) ارتكاب جريمة من قبل موظف أو وكيل الشخص الاعتباري، (2) ارتكاب الجريمة لفائدة الشخص الاعتباري؛ و(3) 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 54 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.

126. 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 2 من المادة 13، بأن تكون العقوبة أو التدبير " فعالة، متناسبة ورادعة "وأن تشمل العقوبات المالية.

127. توضح الفقرة 4 أن مسؤولية الشركات لا تستبعد المسؤولية الفردية.

العقوبات والتدابير (المادة 13)

128. ترتبط هذه المادة ارتباطا وثيقا بالمواد من 2 إلى 11 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.

129. يخضع الأشخاص الاعتباريون الذين تنشأ مسؤوليتهم وفقا للمادة 12 أيضا لعقوبات "فعالة ومتناسبة ورادعة" يمكن أن تكون جنائية، إدارية أو مدنية بطبيعتها. ويتعين على الأطراف المتعاقدة، بموجب الفقرة 2، أن تنص على إمكانية فرض عقوبات مالية على الأشخاص الاعتباريين.

130. 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. ويُترك للأطراف السلطة التقديرية لإنشاء نظام للجرائم والعقوبات الجنائية يتوافق مع أنظمتها القانونية الوطنية القائمة.

القسم الثاني – القانون الإجرائي

131. تصف المواد الواردة في هذا القسم بعض التدابير الإجرائية الواجب اتخاذها على الصعيد الوطني لأغراض التحقيق الجنائي في الجرائم المنصوص عليها في القسم 1، والجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر، وجمع الأدلة على جريمة جنائية في شكل إلكتروني. ووفقا للفقرة 3 من المادة 39، 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.

132. 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.

133. 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.

134. 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.

135. 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.

136. 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 1 و18. 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.

137. 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 ".

138. 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 1 – أحكام عامة

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

نطاق الأحكام الإجرائية (المادة 14)

140. 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".

141. مع مراعاة استثناءين، تطبق كل دولة طرف السلطات والإجراءات المنصوص عليها في هذا القسم على ما يلي: (1) الجرائم الجنائية المقررة وفقا للقسم 1 من الاتفاقية؛ (2) الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر؛ و(3) 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.

142. ثمة استثناءان لنطاق التطبيق هذا. أولا، تنص المادة 21 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.

143. وثانيا، يجوز لأي طرف أن يحتفظ بالحق في تطبيق التدابير الواردة في المادة 20 (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 21. 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.

144. 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 20 أو 21، 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 15)

145. 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 1950 والبروتوكولات الإضافية رقم 1 و4 و6 و7 و12 (سلسلة المعاهدات الأوروبية رقم 5[4] و9 و46 و114 و117 و177)، 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 1969 والميثاق الأفريقي لحقوق الإنسان وحقوق الشعوب لعام 1981) والتي هي أطراف في هذه الآليات، علاوة على العهد الدولي الخاص بالحقوق المدنية والسياسية لعام 1966. فضلا عن ذلك، ثمة أشكال مماثلة من الحماية تنص عليها قوانين معظم الدول.

146. 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 1950 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

4. تم تعديل نص الاتفاقية وفقا لأحكام البروتوكول رقم 3 (سلسلة المعاهدات الأوروبية رقم 45) الذي دخل حيز النفاذ في 21 سبتمبر/أيلول 1970، والبروتوكول رقم 5 (سلسلة المعاهدات الأوروبية رقم 55) الذي دخل حيز النفاذ في 20 ديسمبر/كانون الأول 1971، والبروتوكول رقم 8 (سلسلة المعاهدات الأوروبية رقم 118) الذي دخل حيز النفاذ في 1 يناير/كانون الثاني 1990، وشمل أيضا نص البروتوكول رقم 2 (سلسلة المعاهدات الأوروبية رقم 44) الذي يشكل، طبقا للمادة 5، الفقرة 3 منه، جزء لا يتجزأ من الاتفاقية منذ دخولها حيز النفاذ في 21 سبتمبر/أيلول 1970. وتم استبدال جميع الأحكام التي عدلت أو أضيفت بموجب هذه البروتوكولات، بالبروتوكول رقم 11 (سلسلة المعاهدات الأوروبية رقم 155) اعتبارا من تاريخ دخوله حيز النفاذ في 1 نوفمبر/تشرين الثاني 1998. ومنذ ذلك التاريخ، ألغي البروتوكول رقم 9 (سلسلة المعاهدات الأوروبية رقم 140) الذي دخل حيز النفاذ في 1 أكتوبر/تشرين الأول 1994، وفقد البروتوكول رقم 10 (سلسلة المعاهدات الأوروبية رقم 146) الغرض المتوخى منه.

الصريح الوارد في المادة 21 بشأن الالتزامات المتعلقة بتدابير الاعتراض تتعلق بمجموعة من الجرائم الخطيرة، التي يحددها القانون المحلي، يعتبر مثالا واضح على تطبيق مبدأ التناسب.

147. 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 215، 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.

148. بالنظر إلى المسائل التي نوقشت في الفقرة 3، 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.

الباب 2 – تعجيل حفظ بيانات الكمبيوتر المخزنة

149. تنطبق التدابير الواردة في المادتين 16 و17 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 5 هذه المسائل.

150. 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 16 و17 هذه المشاكل.

151. 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 يُبقي تلك البيانات المخزنة سليمة وآمنة.

152. تشير المادتان 16 و17 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 14، فإن جميع الصلاحيات والإجراءات المطلوب إنشاؤها في القسم 2 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 2). 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.

153. 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.

154. 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 EC/95/46 ، وفي السياق الخاص لقطاع الاتصالات السلكية واللاسلكية، ينفذ بموجب المبدإ التوجيهي رقم EC/97/66. 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.

155. 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 17). 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.

156. تهدف صلاحية التعجيل بحفظ بيانات الكمبيوتر إلى معالجة هذه المشاكل. ومن ثم، فإن الأطراف مطالبة بإدخال صلاحية تأمر بحفظ بيانات حاسوبية محددة كتدبير

مؤقت، بحيث يتم حفظ البيانات لفترة من الوقت طالما كان ذلك ضروريا، أقصاها 90 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 152 و160.

157. 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 16)

158. تهدف المادة 16 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.

159. 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".

160. 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 تتجلي 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.

161. 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، لعله 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 1 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 16 و17.

162. تحدد الفقرة 2 أنه عندما تُفعِّل 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 90 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 90 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 29 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 60 يوما لتمكين الطرف مقدم الطلب من تقديم طلب للبحث أو النفاذ بطريقة مماثلة، أو المصادرة أو التأمين بطريقة مماثلة أو الكشف عن البيانات."

163. تفرض الفقرة 3 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.

164. بالإضافة إلى القيود المبينة أعلاه، تخضع الصلاحيات والإجراءات المشار إليها في المادة 16 أيضا للشروط والضمانات المنصوص عليها في المادتين 14 و15.

التعجيل في حفظ بيانات الكومبيوتر والكشف الجزئي عن بيانات الحركة (المادة 17)

165. تنص هذه المادة على التزامات محددة ذات الصلة بحفظ بيانات الحركة بموجب المادة 16، 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 1.

166. 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).

167. 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.

168. تضمن المادة 17 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.

169. 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 يمكِّن 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 14 و15.

الباب 3 – أمر التقديم

أمر التقديم (المادة 18)

170. تدعو الفقرة 1 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.

171. 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.

172. 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.

173. ينبغي على الدولة الطرف، بموجب الفقرة 1(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 1(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 1(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.

174. يمكن أن تستثني الشروط والضمانات المشار إليها في الفقرة 2 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.

175. 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.

176. 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.

177. يرد تعريف "المعلومات عن المنخرط" في الفقرة 3. 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.

178. 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.

179. 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 في (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).

180. 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.

181. 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.

182. بما أن الصلاحيات والإجراءات الواردة في هذا القسم وضعت لأغراض تحقيقات أو إجراءات جنائية محددة (المادة 14)، 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.

183. 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 4 – البحث عن بيانات الكومبيوتر المخزنة ومصادرتها

البحث عن بيانات الكومبيوتر المخزنة ومصادرتها (المادة 19)

184. 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 19 من هذه الاتفاقية إلى إنشاء صلاحية معادلة خاصة بالبيانات المخزنة.

185. 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.

186. 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.

187. 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.

188. تقتضي الفقرة 1 من الأطراف أن تمكِّن 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 1 إلى "أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة"، فإن الفقرة 1 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 2 هذه الحالة التي تنطوي على روابط مع أنظمة حاسوبية أخرى عن طريق شبكات الاتصالات داخل نفس الإقليم (مثل شبكة المنطقة الواسعة أو شبكة الإنترنت).

189. على الرغم من إمكانية إجراء البحث في " دعامة تخزين بيانات الكمبيوتر التي يمكن أن تكون بيانات كمبيوتر مخزنة داخلها " (الفقرة 1 (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 1 على سلطة قانونية شاملة تغطي كلا الحالتين.

190. تنطبق المادة 19 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 19. لذلك، ينبغي على الأطراف مراجعة قوانينها فيما يتعلق بهذه المسألة لتحديد ما هو ملائم في أنظمتها القانونية المحلية.

191. 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. ويُستخدم كلا المصطلحان من أجل إقران المفاهيم التقليدية بالمصطلحات الحديثة.

192. 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.

193. تسمح الفقرة 2 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".

194. 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.

195. 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.

196. تتناول الفقرة 3 مسائل تمكين السلطات المختصة من مصادرة أو تأمين بيانات الكمبيوتر التي تم البحث فيها أو النفاذ إليها بطريقة مماثلة بموجب الفقرتين 1 أو 2. 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.

197. 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 وُجدت فيها وقت مصادرتها وحفظها من أي تغيير خلال فترة الدعاوى الجنائية. وتشير هذه العبارة إلى التحكم في البيانات أو إبعادها.

198. 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.

199. وبالتالي، تحقق مصادرة البيانات أو تأمينها بطريقة مماثلة وظيفتين: 1) جمع الأدلة، مثلا عن طريق استنساخ البيانات، أو 2) مصادرة البيانات، مثلا من خلال استنساخها وجعل نسختها الأصلية غير قابلة للنفاذ أو عن طريق إزالتها. ولا تنطوي المصادرة على الحذف النهائي للبيانات المصادرة.

200. تدرج الفقرة 4 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.

201. 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.

202. 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.

203. بموجب الفقرة 5 من هذه المادة، تخضع هذه التدابير للشروط والضمانات المنصوص عليها في القانون المحلي على أساس المادة 15 من هذه الاتفاقية. وقد تشمل هذه الشروط أحكاما تتعلق بمشاركة الشهود والخبراء وتعويضهم المالي.

204. واصل القائمون على الصياغة في إطار الفقرة 5 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 20 و21). ومن تم، تُرك 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 5 – جمع بيانات الكمبيوتر في الوقت الحقيقي

205. تنص المادتان 20 و21 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.

206. 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 1 طريقة ترابط الأجهزة أو مجموعة من الأجهزة. ومن ثم، تنطبق المادتان 20 و21 على الاتصالات المحددة المرسلة بواسطة نظام الكمبيوتر، والتي يمكن أن تشمل نقل الاتصال من خلال شبكات الاتصالات قبل استلامها بواسطة نظام كمبيوتر آخر.

207. لا تميز المادتان 20 و21 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 1 إلى الهيئات العامة والخاصة التي توفر لمستخدمي خدماتها القدرة على الاتصال عن طريق نظام كمبيوتر.

208. 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).

209. ثمة نوعان من البيانات التي يمكن جمعها: بيانات الحركة وبيانات المحتوى. وتعرف المادة 1 (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).

210. 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.

211. 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 20 و21.

212. 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 21 تحديدا، فيما يتعلق باعتراض بيانات المحتوى، على أن الأطراف مطالبة فقط بوضع التدبير "فيما يتعلق بمجموعة من الجرائم الخطيرة التي يحددها القانون المحلي".

213. من ناحية أخرى، تعتبر المادة 20 المتعلقة بجمع بيانات الحركة غير محدودة ومن حيث المبدأ تنطبق على أي جريمة جنائية تشملها الاتفاقية. غير أن الفقرة 3 من المادة 14 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.

214. 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 1 من الفصل الثاني، بغية توفير وسيلة فعالة للتحقيق في جرائم الكمبيوتر والجرائم المتصلة بالكمبيوتر.

215. تخضع الشروط والضمانات المتعلقة بالصلاحيات والإجراءات المتعلقة باعتراض بيانات المحتوى في الوقت الحقيقي وجمع بيانات الحركة في الوقت الحقيقي لأحكام المادتين 14 و15. 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)

5. الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية كلاس (Klass) وآخرين ضد ألمانيا، أ.28، 6 سبتمبر/أيلول 1978.

6. الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية كروسلين (Kruslin) ضد فرنسا، -176أ، 24 أبريل/نيسان

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 20)

216. 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 20 موضوع جمع وتسجيل بيانات الحركة في الوقت الحقيقي لأغراض تحقيقات أو إجراءات جنائية محددة.

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

218. 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

.1990

7. الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية هوفيج (Huvig) ضد فرنسا، -176ب، 24 أبريل/نيسان 1990

8. الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية مالون (Malone) ضد المملكة المتحدة، أ.82، 2 أغسطس/آب 1984.

9. الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية هالفورد (Halford) ضد المملكة المتحدة، تقارير 1997 – الجزء 3، 25 يونيو/حزيران 1997.

10. الحكم الصادر عن المحكمة الأوروبية لحقوق الإنسان، قضية لامبرت (Lambert) ضد فرنسا، تقارير 1998 – الجزء 4، 24 أغسطس/آب 1998.

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.

219. 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 "تصيُّد المعلومات بنيةٍ مبيَّتة" 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.

220. رهنا بأحكام الفقرة 2، تلزَم الأطراف، بموجب الفقرة 1(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.

221. بالإضافة إلى ذلك، فإن الأطراف ملزمة، بموجب الفقرة 1(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.

222. 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.

223. بصفة عامة، لا تعتبر الإمكانيتان المنصوص عليها لجمع بيانات الحركة في الفقرتين 1(أ) و(ب) بدائل. وباستثناء ما هو منصوص عليه في الفقرة 2، 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 (1"ب")، وجب على الطرف التوفر على إمكانية اضطلاع سلطات إنفاذ القانون بنفسها بهذه المهمة (1"أ"). وبالمثل، فإن الالتزام بموجب الفقرة 1(ب)"2" 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 1(أ) و(ب) في كل مرة، لكن تطالب المادة بتوافر هاتين الطريقتين.

224. 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 2 هذه الحالة. ففي الحالات التي لا يمكن فيها للطرف، بسبب "المبادئ الثابتة في نظامه القانوني المحلي"، أن يتبنى التدابير المشار إليها في الفقرة 1(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.

225. 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.

226. تلزم الفقرة 3 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 3 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 14 و15. وينبغي أن تفرض هذه الضمانات أو الشروط فترات زمنية معقولة بالنسبة لمدة الالتزام، نظرا للطابع السري لتدابير التحقيق.

227. 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 14 و15.

اعتراض بيانات المحتوى (المادة 21)

228. 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.

229. 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.

230. معظم عناصر هذه المادة مماثلة لتلك الواردة في المادة 20. 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".

231. كما هو مبين في التعليقات الواردة أعلاه بشأن المادة 20، 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 3: الولاية القضائية

الولاية القضائية (المادة 22)

232. تنص هذه المادة على مجموعة من المعايير التي تلزم بموجبها الأطراف المتعاقدة بإقامة ولايتها القضائية على الجرائم الجنائية المنصوص عليها في المواد من 2 إلى 11 من الاتفاقية.

233. تستند الفقرة 1 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.

234. 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 1(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 1(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.

235. تستند الفقرة 1، 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. وينفَّذ 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 1 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.

236. تستند الفقرة 1 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.

237. تسمح الفقرة 2 للأطراف بتقديم تحفظ على أسباب الولاية القضائية المنصوص عليها في الفقرة 1، 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 3، بمعنى عندما يرفض ذلك الطرف تسليم الجاني المزعوم على أساس جنسيته ويكون الجاني موجودا في إقليمه. وتعتبر الولاية القضائية المنشأة على أساس الفقرة 3 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 6 من المادة 24 من هذه الاتفاقية.

238. لا تعتبر أسس الولاية القضائية المنصوص عليها في الفقرة 1 حصرية. وتسمح الفقرة 4 من هذه المادة للأطراف بأن تنشئ، وفقا لقانونها الداخلي، أنواعا أخرى من الولاية القضائية الجنائية أيضا.

239. 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

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

القسم 1: المبادئ العامة

الباب الأول – المبادئ العامة ذات الصلة بالتعاون الدولي

المبادئ العامة ذات الصلة بالتعاون الدولي (المادة 23)

241. تحدد المادة 23 ثلاثة مبادئ عامة فيما يتعلق بالتعاون الدولي بموجب الفصل الثالث.

242. 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.

243. ثانيا، يرد النطاق العام للالتزام بالتعاون في المادة 23: ينبغي توسيع نطاق التعاون ليشمل جميع الجرائم ذات الصلة بأنظمة وبيانات الكمبيوتر (أي الجرائم المشمولة بالفقرة 2 من المادة 14، 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 24 (تسليم المجرمين) (المساعدة المتبادلة بشأن جمع بيانات الحركة في الوقت الحقيقي) و34 (المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى) تسمح للأطراف بتوفير نطاق مختلف لتطبيق هذه التدابير.

244. 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 27 أدناه)، أو والأحكام ذات الصلة في القانون المحلي والمتعلقة بالتعاون الدولي. ويعزَّز هذا المبدأ الأساسي بشكل صريح في المواد 24 (تسليم المجرمين)، و25 (المبادئ العامة المتعلقة بالمساعدة المتبادلة)، و26 (المعلومات التلقائية)، و27 (الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق)، و28 (السرية والقيود على الاستخدام) و(31) (المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكمبيوتر المخزنة) و33 (المساعدة المتبادلة ذات الصلة بجمع بيانات الحركة في الوقت الحقيقي) و34 (المساعدة المتبادلة ذات الصلة باعتراض بيانات المحتوى).

الباب الثاني – المبادئ ذات الصلة بتسليم المجرمين

المادة 24 – تسليم المجرمين (المادة 24)

245. تنص الفقرة 1 على أن الالتزام بالتسليم لا ينطبق إلا على الجرائم المقررة طبقا للمواد من 2 إلى 11 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 2 – النفاذ غير القانوني – والمادة 4 – 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 2 إلى 11 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 2 من الاتفاقية الأوروبية لتسليم المجرمين (سلسلة المعاهدات الأوروبية رقم 24). 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.

246. 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 1 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 27 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 24)، 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.

247. تنص الفقرة 2 على أن الجرائم المبينة في الفقرة 1 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 5، تكون الأطراف قادرة على توفير شروط أخرى لتسليم المجرمين.

248. بموجب الفقرة 3، 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.

249. عندما يستخدم طرف نظاما قانونيا عاما لتنفيذ التسليم بدلا من الاعتماد على معاهدات تسليم المجرمين، تقضي الفقرة 4 بأن تدرج في ذلك النظام الجرائم المبينة في الفقرة 1 ضمن الجرائم التي يتاح بشأنها التسليم.

250. تنص الفقرة 5 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 24) وبروتوكوليها الإضافيين (سلسلة المعاهدات الأوروبية 86 و98) على الأطراف في تلك الاتفاقات، ويمكن رفض التسليم على هذه الأسس (على سبيل المثال، تنص المادة 3 من الاتفاقية الأوروبية لتسليم المجرمين على رفض تسليم المجرمين إذا اعتبرت الجريمة ذات طابع سياسي، أو إذا اعتُبر أن الطلب قدم لغرض مقاضاة أو معاقبة شخص ما بسبب جملة أمور منها العرق أو الدين أو الجنسية أو الرأي السياسي).

251. تنطبق الفقرة 6 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 6، 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 6 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.

252. بغية أن يعلم كل طرف إلى من ينبغي توجيه طلباتهم بشأن الاعتقال المؤقت أو التسليم، تقتضي الفقرة 7 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 24)، 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 25)

253. ترد المبادئ العامة التي تنظم الالتزام بتقديم المساعدة المتبادلة في الفقرة 1. وينبغي توفير التعاون "على أوسع نطاق ممكن". وهكذا، وكما ورد في المادة 23 ("المبادئ العامة ذات الصلة بالتعاون الدولي")، تكون المساعدة المتبادلة من حيث المبدأ واسعة النطاق، والمعيقات التي تقيدها محدودة للغاية. ثم، وكما ورد في المادة 23، ينطبق الالتزام بالتعاون من حيث المبدأ على كل من الأفعال الإجرامية المتعلقة بأنظمة وبيانات الكمبيوتر (أي الجرائم المشمولة بالفقرة 2 من المادة 14، 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 34 و35 للأطراف بتوفير نطاق مختلف لتطبيق هذه التدابير.

254. ستوضح أحكام أخرى من هذا الفصل أن الالتزام بتقديم المساعدة المتبادلة يتم عموما وفقا لأحكام معاهدات وقوانين وترتيبات المساعدة القانونية سارية التطبيق. وبمقتضى الفقرة 2، 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 29 إلى 35 (أحكام خاصة - الأبواب 1 و2 و3) أمرا حيويا للتعاون الفعال في المسائل الجنائية المتعلقة بالكمبيوتر.

255. لن تقتضي بعض الأطراف أي تشريع تنفيذي لتطبيق الأحكام المشار إليها في الفقرة 2، 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.

256. 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 3 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 3 ذلك من خلال: (1) 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(2) 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.

257. تنص الفقرة 4 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.

258. ومع ذلك، لا تنطبق الفقرة 4 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 2 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 24/7) 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 27 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 27 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 2 إلى 11 من الاتفاقية، على أساس أن الطرف متلقي الطلب يعتبر أن الطلب ينطوي على جريمة "مالية". وفي الأخير، تعتبر المادة 29 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.

259. الفقرة 5 هي، في الأساس، تعريف لازدواجية التجريم لأغراض المساعدة المتبادلة في إطار هذا الفصل. عندما يُسمح 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 4 من المادة 29 "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 26)

260. تستمد هذه المادة من أحكام صكوك مجلس أوروبا السابقة، مثل المادة 10 من الاتفاقية المعنية بغسل الأموال والبحث عن عائدات الجريمة وضبطها ومصادرتها (سلسلة المعاهدات الأوروبية رقم 141) والمادة 28 من اتفاقية القانون الجنائي بشأن الفساد (سلسلة المعاهدات الأوروبية رقم 173). 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 1 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.

261. تتناول الفقرة 2 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 27)

262. تلزم المادة 27 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 ذُكر 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 29 إلى 35 (أحكام خاصة - الأبواب 1 و2 و3) 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.

263. 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 30) وبروتوكولها (سلسلة المعاهدات الأوروبية رقم 99) 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 25، الفقرة 4)، 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.

264. تنص المادة 27 (الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حال عدم وجود اتفاقات دولية واجبة التطبيق)، الفقرات من 2 إلى 10، 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 27 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 4 من المادة 25 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.

265. تقتضي الفقرة 2 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.

266. 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.

267. 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 3 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.

268. تنص الفقرة 4 على إمكانية رفض طلبات المساعدة المتبادلة المقدمة بموجب هذه المادة. ويمكن رفض تقديم المساعدة بناء على الأسباب المنصوص عليها في الفقرة 4 من المادة 25 (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 23 و25)، 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.

269. تمشيا مع هذه المقاربة، كان من المفهوم أنه باستثناء الأسباب المبينة في المادة 28، 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 6 من المادة 27 والفقرة 271 من هذا التقرير).

270. تسمح الفقرة 5 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.

271. تنص الفقرة 6 على أنه يجوز، في الحالات التي يرفَض 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.

272. تلزم الفقرة 7 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.

273. 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 8 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.

274. ينبغي للسلطات المركزية المعينة وفقا للفقرة 2 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، تمكِّن 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 28)

275. 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.

276. على غرار المادة 27، لا تنطبق المادة 28 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.

277. تسمح الفقرة 2 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).

278. 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.

279. تنص الفقرة 3 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.

280. تنص الفقرة 4 على أنه يجوز أن يُطلب من الطرف مقدم الطلب تفسير الاستخدام المخصص للمعلومات أو المواد التي تلقاها بموجب الشروط المبينة في الفقرة 2، 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 2: أحكام خاصة

281. 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 29)

282. تنص هذه المادة على آلية على الصعيد الدولي مطابقة لتلك المنصوص عليها في المادة 16 من أجل الاستخدام على الصعيد الوطني. وتخول الفقرة 1 من هذه المادة للطرف أن يقدم طلبا للحصول على التعجيل بحفظ البيانات المخزنة في إقليم الطرف متلقي الطلب، وتقتضي الفقرة 3 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.

283. ولئن كان هذا التدبير أسرع بكثير من ممارسة المساعدة المتبادلة العادية، فإنه في الوقت نفسه أقل تطفلا. ولا يُطلب 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، يُسمح 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.

284. تبين الفقرة 2 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.

285. تنص الفقرة 3 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.

286. وهكذا، تتمثل القاعدة العامة في استغناء الأطراف عن أي شرط بازدواجية التجريم لأغراض الحفظ. إلا أن الفقرة 4 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 2 إلى 11، 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.

287. على خلاف ذلك، لا يجوز للطرف متلقي الطلب، بموجب الفقرة 5، 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.

288. 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 6، 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.

289. وفي الأخير، تلزم الفقرة 7 كل طرف بضمان الاحتفاظ بالبيانات المحفوظة عملا بهذه المادة، لمدة 60 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 30)

290. تنص هذه المادة على المقابل الدولي للقوة للسلطة المنصوص عليها من أجل الاستخدام المحلي في المادة 17. 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.

291. بموجب الفقرة 2، 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 29 (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.

الباب الثاني – المساعدة المتبادلة ذات الصلة بسلطات التحقيقات

المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكومبيوتر المخزنة (المادة 31)

292. 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 19 (البحث عن بيانات الكمبيوتر المخزنة ومصادرتها) حيث يجب أن يتوفر على القدرة على القيام بذلك للأغراض المحلية. وتجيز الفقرة 1 للطرف بطلب هذا النوع من المساعدة المتبادلة، وتقضي الفقرة 2 بأن يكون الطرف متلقي الطلب قادرا على تقديمه. وتطبق الفقرة 2 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 3، يجب التعجيل بالرد على هذا الطلب عندما (1) تكون هنالك أسباب تدعو إلى الاعتقاد بأن البيانات ذات الصلة معرضة بشكل خاص للإتلاف أو التعديل، أو (2) 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 32)

293. ناقش القائمون على صياغة الاتفاقية بشكل مستفيض مسألة متى يُسمح 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 32 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 3 من المادة 39 على أن الحالات الأخرى ليست لا مرخصة ولا مستبعدة.

294. تتناول المادة 32 (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 33)

295. 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 33 (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.

296. 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 2، فيما يتعلق بنطاق التدبير الداخلي المطابق، للأطراف بحصر نطاق تطبيق هذا التدبير على نطاق أضيق من الجرائم المنصوص عليها في المادة 23 (المبادئ العامة المتعلقة بالتعاون الدولي) بنفس الطريقة التي يجوز بها للأطراف أن يبدوا تحفظا بموجب المادة 14 (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 2 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 34)

297. 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 14 و15 و21 وكذلك إلى التوصية رقم (85) 10 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 و7 أيام في الأسبوع

شبكة على مدار الساعة و7 أيام في الأسبوع (المادة 35)

298. 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 بُعد 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 24 ساعة في اليوم و7 أيام في الأسبوع لضمان تقديم المساعدة الفورية في التحقيقات والإجراءات في نطاق هذا الفصل، خاصة كما هو محدد بموجب المادة 35، الفقرة 1، 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.

299. 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 1 تقديم المشورة لطرف آخر يطلب التعاون بأي شروط قانونية مسبقة مطلوبة لتوفير التعاون غير الرسمي أو الرسمي.

300. يتمتع كل طرف بحرية تحديد المكان الذي تستقر فيه نقطة الاتصال داخل بنية إنفاذ القانون. وقد ترغب بعض الأطراف في جعل مقر نقطة الاتصال 24/7 داخل سلطتها المركزية للمساعدة المتبادلة، وقد يعتبر البعض الآخر أن أفضل مكان لإيواء نقطة الاتصال هو وحدة الشرطة المتخصصة في مكافحة الجريمة المرتبكة 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 24/7 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.

301. تنص الفقرة 2 على أن من بين المهام الحاسمة التي يتعين أن تضطلع بها نقطة الاتصال 24/7 ثمة القدرة على تيسير التنفيذ السريع لتلك المهام التي لا تضطلع بها مباشرة بنفسها. على سبيل المثال، إذا كانت نقطة الاتصال 24/7 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 2 أن يكون لدى كل نقطة اتصال 24/7 لدى طرف القدرة على إجراء اتصالات عاجلة بأعضاء آخرين في الشبكة.

302. تقتضي الفقرة 3 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 3 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

303. 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 315 خلال اجتماع النواب المنعقد في فبراير/شباط 1980. وبما أن معظم المواد من 36 إلى 48 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 36)

304. صيغت الفقرة 1 من المادة 36 وفقا لعدة سوابق وضعت في اتفاقيات أخرى أعدت في إطار مجلس أوروبا، ومنها مثلا اتفاقية نقل الأشخاص المدانين (سلسلة المعاهدات الأوروبية رقم 112) والاتفاقية المعنية بمكافحة غسل الأموال، والبحث عن عائدات الجريمة وضبطها ومصادرتها (سلسلة المعاهدات الأوروبية رقم 141)، 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 3، يجوز دعوة دول أخرى من غير الأعضاء التي لا يشملها هذا الحكم إلى الانضمام إلى الاتفاقية وفقا للفقرة 1 من المادة 37.

305. تحدد الفقرة 3 من المادة 36 عدد التوقيعات أو القبول أو الموافقات اللازمة لدخول الاتفاقية حيز النفاذ، في 5. ويعتبر هذا الرقم أعلى من العتبة المعتادة (3) 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 37)

306. صيغت المادة 37 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 20(د) من النظام الأساسي لمجلس أوروبا وتصويت ممثلي الأطراف المتعاقدة الذين يحق لهم حضور اجتماع اللجنة بالإجماع.

307. يطلب من الدول الاتحادية التي تسعى إلى الانضمام إلى الاتفاقية، والتي تعتزم إصدار إعلان بموجب المادة 41، أن تقدم مسبقا مشروع الإعلان المشار إليه في الفقرة 3 من المادة 41، بحيث تتمكن الأطراف من تقييم كيفية تأثير تطبيق الحكم الاتحادي على تنفيذ الطرف المقبل للاتفاقية (انظر الفقرة 320).

الآثار المترتبة على الاتفاقية (المادة 39)

308. تتناول الفقرتان 1 و2 من المادة 39 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 156) على: (1) ألا تؤثر الاتفاقيات الجديدة على الحقوق والتعهدات المستمدة من الاتفاقيات القائمة والاتفاقيات الدولية متعددة الأطراف المتعلقة بالمسائل الخاصة؛ (2) 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(3) 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.

309. 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 1 من المادة 39 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 1957 (سلسلة المعاهدات الأوروبية رقم 24) ، والاتفاقية الأوروبية بشأن المسائل الجنائية لعام 1959 (سلسلة المعاهدات الأوروبية رقم 30) وبروتوكولها الإضافي لعام 1978 (سلسلة المعاهدات الأوروبية رقم 99). 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 30 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.

310. 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.

311. 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 3 من المادة 25) إن لم تكن هذه الإمكانية متاحة بموجب المعاهدة أو الترتيب الأصليين.

312. وتماشيا مع الطابع التكميلي للاتفاقية، ولا سيما مقاربتها الخاصة بالتعاون الدولي، تنص الفقرة 2 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 112). 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 27(1)). وفي هذه الحالات، فإن أحكام التعاون ذات الصلة المنصوص عليها في المادة 27 ستحل محل القواعد ذات الصلة في هذه الاتفاقات الأخرى. وبما أن هذه الاتفاقية تنص عموما على حد أدنى من الالتزامات، فإن الفقرة 2 من المادة 39 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.

313. 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.

314. 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 3 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 40)

315. تشير المادة 40 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 41)

316. تماشيا مع الهدف المتمثل في تمكين أكبر عدد ممكن من الدول من أن تصبح أطرافا، تسمح المادة 41 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] (1). وهنا، تعترف المادة 41 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 المؤسِّسة لدولة اتحادية. وكان هناك اتفاق بين القائمين على صياغة الاتفاقية على ألا يحدث تفعيل البند الاتحادي سوى اختلافات طفيفة على تطبيق الاتفاقية.

317. 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 41.

318. اقتصر نطاق تطبيق البند الاتحادي على أحكام الفصل الثاني (القانون الجنائي الموضوعي والقانون الإجرائي والولاية القضائية). وتبقى الدول الاتحادية التي تستفيد من هذا الحكم

11. مثلا، الاتفاقية المتعلقة بوضع اللاجئين المؤرخة في 28 يوليو/تموز 1951، المادة 34؛ الاتفاقية المتعلقة بوضع الأشخاص عديمي الجنسية، المؤرخة في 28 سبتمبر/أيلول 1954، المادة 37؛ اتفاقية الاعتراف بقرارات التحكيم الأجنبية وإنفاذها، الصادرة في 10 يونيو/حزيران 1958، المادة 11؛ اتفاقية حماية التراث الثقافي والطبيعي العالمي المؤرخة في 16 نوفمبر/تشرين الثاني 1972، المادة 34.

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.

319. فضلا عن ذلك، تنص الفقرة 2 من المادة 41 على أنه لا يجوز للدولة الاتحادية، عند إبداء تحفظ بموجب الفقرة 1 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 42)

320. تنص المادة 42 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.

321. واعترافا بأن بعض التحفظات ضرورية لبعض الأطراف لتفادي التضارب مع مبادئها الدستورية أو القانونية الأساسية، لا تفرض المادة 43 مهلة محددة لسحب التحفظات. وبدلا من ذلك، ينبغي سحبها حالما تسمح الظروف بذلك.

322. 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 44)

323. تنص المادة 44 على سابقة مستخلصة من الاتفاقية المعنية بغسل الأموال والبحث عن عائدات الجريمة وضبطها ومصادرتها (سلسلة المعاهدات الأوروبية رقم 141)، 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.

324. يمكن للأطراف نفسها أن تدرس الحاجة إلى إدخال تعديلات أو بروتوكولات بموجب إجراء التشاور المنصوص عليه في المادة 46. وفي هذا الصدد، تحاط اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) علما بذلك على أساس دوري ويُطلب منها اتخاذ التدابير اللازمة لمساعدة الأطراف في جهودها الرامية إلى تعديل الاتفاقية أو استكمالها.

325. وفقا للفقرة 5، لن يدخل أي تعديل يُعتمد حيز النفاذ إلا بعدما تبلغ جميع الأطراف الأمين العام بقبوله. ويسعى هذا الشرط إلى ضمان تطور الاتفاقية بطريقة موحدة.

تسوية النزاعات (المادة 45)

326. تنص الفقرة 1 من المادة 45 على وجوب إبقاء اللجنة الأوروبية المعنية بمشاكل الإجرام على علم بتفسير وتطبيق أحكام الاتفاقية. وتُلزم الفقرة 2 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 46)

327. تنشئ المادة 46 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 40 و42.

328. 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 14).

329. تنص الفقرة 3 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.

330. تشير الفقرة 4 إلى أنه يتعين على الأطراف نفسها أن تمول أي مشاورات تجرى وفقا للفقرة 1 من المادة 46، 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.

البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر ستراسبوغ 2003/1/28

إن الدول الأعضاء في مجلس أوروبا والدول الأخرى الأطراف في اتفاقية الجريمة الإلكترونية، التي افتتحت للتوقيع في بودابست في 23 نوفمبر/تشرين الثاني 2001، الموقعة على هذه الوثيقة؛

إذ تأخذ في الاعتبار أن هدف مجلس أوروبا هو تحقيق وحدة أكبر بين أعضائه؛

وإذ تذكر بأن كافة البشر ولدوا أحراراً ومتساوين في الكرامة والحقوق؛

وإذ تؤكد على الحاجة إلى الإعمال الفعلي لكافة حقوق الإنسان دون أي تمييز أو تفريق، طبقا لما تنص عليه الصكوك الأوروبية واتفاقيات دولية أخرى؛

واقتناعاً منها بأن الأفعال المتصلة بالتمييز العنصري وكراهية الأجانب تشكل انتهاكاً لحقوق الإنسان وتهديداً لسيادة القانون والاستقرار الديمقراطي؛

وإذ تضع في الاعتبار أن القانون الوطني والدولي في حاجة إلى توفير أجوبة قانونية ملائمة للتصدي للدعاية ذات الطابع العنصري والمعادي للأجانب التي ترتكب من خلال أنظمة الكمبيوتر؛

ووعيا منها بأن الدعاية لمثل هذه الأفعال تكون في الغالب خاضعة للتجريم في التشريعات الوطنية؛

واعتبارا لاتفاقية الجريمة الإلكترونية، التي تنص على وسائل حديثة ومرنة للتعاون الدولي، واقتناعاً منها بالحاجة إلى مواءمة النصوص القانونية الجوهرية ذات الصلة بمكافحة الدعاية التي تحض على العنصرية وكراهية الأجانب؛

وإدراكاً منها أن أنظمة الكمبيوتر تقدم وسائل غير مسبوقة لتيسير حرية التعبير والتواصل حول العالم؛

واعترافاً منها بأن حرية التعبير تشكل أحد الأسس الجوهرية للمجتمع الديمقراطي وأحد الشروط الأساسية لتقدمه وتنمية كافة البشر؛

وإذ يساورها القلق، مع ذلك، بشأن خطر إساءة استخدام أنظمة الكمبيوتر هاته لنشر الدعاية التي تحض على العنصرية وكراهية الأجانب؛

وإدراكاً منها بالحاجة إلى ضمان توازن سليم بين حرية التعبير والمناهضة الفعالة للأفعال ذات الطابع العنصري والمعادي الأجانب؛

واقراراً منها بأن هذا البروتوكول لا يرمي إلى التأثير على المبادئ القائمة ذات الصلة بحرية التعبير في الأنظمة القانونية الوطنية؛

ومراعاة للصكوك القانونية الدولية ذات الصلة في هذا المجال، وعلى وجه الخصوص اتفاقية حماية حقوق الإنسان والحريات الأساسية وبروتوكولها رقم 12 بشأن الحظر العام للتمييز، واتفاقيات مجلس أوروبا القائمة بشأن التعاون في المجال الجنائي؛ وعلى وجه الخصوص اتفاقية الجريمة الإلكترونية، والاتفاقية الدولية للأمم المتحدة للقضاء على جميع أشكال التمييز العنصري الصادرة بتاريخ 21 ديسمبر/كانون الأول 1965، والعمل المشترك للاتحاد الأوروبي بتاريخ 15 يوليو/تموز 1996 الذي تبناه المجلس بموجب المادة (K.3) من معاهدة الاتحاد الأوروبي بشأن العمل على مناهضة العنصرية وكراهية الأجانب؛

وإذ ترحب بالتطورات الحديثة التي تعزز التفاهم والتعاون الدوليين في مجال مكافحة الجريمة الإلكترونية والتمييز العنصري وكراهية الأجانب؛

وإذ تضع في الاعتبار خطة العمل التي اعتمدها رؤساء الدول والحكومات في مجلس أوروبا بمناسبة انعقاد قمتهم الثانية (ستراسبورغ، 10-11 أكتوبر/تشرين الأول 1997) للسعي إلى التوصل إلى حلول مشتركة بشأن تطورات التكنولوجيات الحديثة بناء على معايير وقيم مجلس أوروبا؛

اتفقت على ما يلي:

الفصل الأول – أحكام عامة

المادة 1 – الغرض من البروتوكول

يرمي هذا البروتوكول إلى استكمال، فيما بين الأطراف في البروتوكول، أحكام الاتفاقية المتعلقة بالجريمة الإلكترونية، التي فتحت للتوقيع في بودابست في 23 نوفمبر/تشرين الثاني 2001 (ويشار إليها في هذه الوثيقة بـ "الاتفاقية") وذلك فيما يتعلق بتجريم الأفعال ذات الطابع العنصري والمعادي للأجانب التي ترتكب من خلال أنظمة الكمبيوتر.

المادة 2 – التعريف

1. لأغراض هذا البروتوكول:

يقصد بـــ "المواد التي تتعلق بالعنصرية وكراهية الأجانب" أي مادة كتابية أو صورة أو أي عروض تقديمية أخرى لأفكار أو نظريات تدعو أو تروج أو تحث على الكراهية أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد على أساس الجنس، أو اللون، أو النسب، أو الأصل القومي أو الإثني، وكذلك الدين إذا استخدمت كذريعة لأي من هذه العوامل.

2. تفسر المصطلحات والتعابير المستخدمة في هذا البروتوكول بنفس طريقة تفسيرها بموجب الاتفاقية.

الفصل الثاني – التدابير الواجب اتخاذها على المستوى الوطني

المادة 3 – نشر المواد المتصلة بالعنصرية وكراهية الأجانب عبر أنظمة الكمبيوتر

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق: توزيع أو إتاحة بشكل أو بآخر، المواد ذات الصلة بالعنصرية وكراهية الأجانب على الجمهور عبر أنظمة الكمبيوتر.

2. يجوز لأي طرف الاحتفاظ بالحق في عدم ربط المسؤولية الجنائية بالسلوك كما هو معرف في الفقرة 1 من هذه المادة إذا كانت المواد، وفقا للتعريف الوارد في المادة 2 – الفقرة 1، تدعو أو تروج أو تحث على التمييز الذي لا يرتبط بالكراهية أو العنف، شريطة توافر سبل انتصاف فعالة أخرى.

3. يجوز لأي طرف، بغض النظر عن الفقرة 2 من هذه المادة، الاحتفاظ بالحق في عدم تطبيق الفقرة 1 على حالات التمييز التي لا يمكنه أن يوفر بشأنها سبل انتصاف فعالة على النحو المشار إليه في الفقرة 2 المذكورة، نظرا للمبادئ المقررة في نظامه القانوني الوطني فيما يتعلق بحرية التعبير.

المادة 4 – التهديد المبرر بدافع التمييز العنصري وكراهية الأجانب

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً وبغير حق: التهديد الموجه عبر نظام الكمبيوتر، بارتكاب جريمة جنائية خطيرة كما هي معرفة بموجب قانونه الوطني (أ) ضد أشخاص نظرا لانتمائهم إلى مجموعة متميزة بسبب الجنس، أو اللون، أو النسب، أو الأصل القومي أو الإثني، وكذلك الدين إذا استخدمت كذريعة لأي من هذه العوامل؛ أو (ب) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.

المادة 5 – السب المبرر بدافع التمييز العنصري وكراهية الأجانب

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم التصرف التالي في قانونها الوطني، إذا ما ارتكب عمداً و بغير حق: السب العلني الموجه، عبر نظام كمبيوتر، (أ) ضد أشخاص نظرا لانتمائهم إلى مجموعة متميزة بسبب الجنس، أو اللون، أو النسب، أو الأصل القومي أو الإثني، وكذلك الدين إذا استخدمت كذريعة لأي من هذه العوامل؛ أو (ب) ضد مجموعة من الأشخاص تتميز بأي من هذه الخصائص.

2. يجوز لأي طرف إما:

(أ) أن يطلب أن يكون للجريمة المشار إليها في الفقرة 1 من هذه المادة، الأثر عندما يتعرض الشخص أو مجموعة الأشخاص المشار إليهم في الفقرة 1 للكراهية، أو الاحتقار، أو السخرية؛ أو

(ب) أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، كلياً أو جزئياً.

المادة 6 – إنكار الإبادة الجماعية أو الجرائم ضد الإنسانية، أو التقليل الجسيم من شأنها أو الموافقة عليها أو تبريرها

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير اللازمة لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق:

توزيع أو إتاحة للجمهور بشكل أو بآخر عبر نظام كمبيوتر، مواد تنكر أفعالاً تشكل إبادة جماعية أو جرائم ضد الإنسانية أو تقلل بشكل جسيم من شأنها، أو توافق عليها، أو تبررها، كما هي معرفة في القانون الدولي، وكما أقرتها القرارات النهائية والملزمة للمحكمة العسكرية الدولية التي أنشئت بموجب اتفاقية لندن بتاريخ 8 أغسطس/آب 1945، أو قرارات أي محكمة دولية أخرى أنشئت بموجب صكوك دولية ذات الصلة ويقر باختصاصها ذلك الطرف.

2. يجوز لأى طرف إما:

(أ) أن يطلب أن يكون الإنكار أو التقليل الجسيم من الشأن، المشار إليهما في الفقرة 1 من هذه المادة، قد ارتكبا بغرض التحريض على الكراهية، أو التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد، على أساس الجنس، أو اللون، أو النسب، أو الأصل القومي أو الإثني، وكذلك الدين إذا استخدما كذريعة لأي من هذه العوامل، أو خلاف ذلك

(ب) أن يحتفظ بالحق في عدم تطبيق الفقرة 1 من هذه المادة، كلياً أو جزئياً.

المادة 7 – المساعدة والتحريض

تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير اللازمة لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: المساعدة

أو التحريض على ارتكاب أي من الجرائم المحددة بموجب
هذا البروتوكول، بنية ارتكاب مثل هذه الجرائم.

الفصل الثالث – العلاقة بين الاتفاقية وهذا البروتوكول

المادة 8 – العلاقة بين الاتفاقية وهذا البروتوكول

1. تطبق المواد 1، 12، 13، 22، 41، 44، 45 و46 من الاتفاقية، مع إدخال ما يلزم من تعديل، على هذا البروتوكول.

2. تقوم الدول الأطراف بتوسيع نطاق تطبيق التدابير المحددة في المواد 14 إلى 21، والمواد من 23 إلى 35 من الاتفاقية لتتلاءم مع المواد 2 إلى 7 من هذا البروتوكول.

الفصل الرابع – أحكام ختامية

المادة 9 – التعبير عن الموافقة على الالتزام

1. يُفتتح هذا البروتوكول للتوقيع من قبل الدول التي وقعت على الاتفاقية والتي يجوز لها أن تعرب عن موافقتها على الالتزام إما عبر:

أ. التوقيع دون تحفظ حفظ عند التصديق أو القبول أو الموافقة، أو

ب. التوقيع الخاضع للتصديق أو القبول أو الموافقة، الذي يعقبه تصديق أو قبول أو موافقة.

2. لا يجوز لأى دولة أن توقع على هذا البروتوكول دون تحفظ بالنسبة للتصديق، أو القبول أو الموافقة ، أو أن تودع وثيقة التصديق، أو القبول أو الموافقة ما لم تكن قد أودعت بالفعل، أو تقوم في آن واحد بإيداع صكوك التصديق، أو القبول أو الموافقة على الاتفاقية.

3. تُودع صكوك التصديق، أو القبول أو الموافقة لدى الأمين العام لمجلس أوروبا.

المادة 10 – الدخول حيز التنفيذ

1. يدخل هذا البروتوكول حيز التنفيذ في اليوم الأول من الشهر الموالي لانقضاء فترة ثلاثة أشهر من التاريخ الذي تعبر فيه خمس دول عن موافقتها على الالتزام بالبروتوكول طبقاً لأحكام المادة 9.

2. ويدخل البروتوكول حيز التنفيذ، بالنسبة لأي دولة تعبر لاحقاً عن موافقتها على الالتزام به، في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ توقيعها دون تحفظ بالنسبة للتصديق، أو القبول أو الموافقة، أو إيداع صكوك التصديق، أو القبول أو الموافقة الخاصة بها.

المادة 11 – الانضمام

1. بعد دخول هذا البروتوكول حيز التنفيذ، يجوز لأي دولة انضمت إلى الاتفاقية أن تنضم كذلك إلى البروتوكول.

2. ويتم الانضمام بإيداع صك الانضمام لدى الأمين العام لمجلس أوروبا ويدخل حيز النفاذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ الإيداع.

المادة 12 – التحفظات والإعلانات

1. تسري التحفظات والإعلانات التي تبديها دولة طرف على أحد أحكام الاتفاقية كذلك على هذا البروتوكول، ما لم تعلن تلك الدولة الطرف عن خلاف ذلك وقت التوقيع أو عند إيداع صك التصديق، أو القبول، الموافقة أو الانضمام.

2. يجوز لأي دولة طرف، بواسطة إشعار خطي يوجه إلى الأمين العام لمجلس أوروبا وقت التوقيع أو عند إيداع صك التصديق أو القبول أو الموافقة أو الانضمام، أن تعلن أنها ستستخدم تحفظا (أو أكثر من تحفظ) المنصوص عليه في الفقرة 2 من المادة 22، والفقرة 1 من المادة 41 من الاتفاقية، بغض النظر عن الإعمال المنجز من قبل تلك الدولة الطرف بموجب الاتفاقية، ولا تقبل أي تحفظات أخرى.

3. يجوز لأي دولة، بواسطة إشعار خطي يوجه إلى الأمين العام لمجلس أوروبا وقت التوقيع أو عند إيداع صك التصديق أو القبول أو الموافقة أو الانضمام، أن تعلن أنها ستستخدم إمكانية المطالبة بعناصر إضافية طبقا لما تنص عليه الفقرة 2 (أ) من المادة 5 والفقرة 2 (أ) من المادة 6 من هذا البروتوكول.

المادة 13 – حالة سحب التحفظات

1. يقوم الطرف الذي قدم تحفظاً طبقاً للمادة 12 أعلاه بسحب ذلك التحفظ، كلياً أو جزئياً، بمجرد أن تسمح الظروف بذلك، ويدخل سحب التحفظ حيز التنفيذ في تاريخ إيداع الإشعار الموجه إلى الأمين العام لمجلس أوروبا. وإذا أشار الإشعار أن سحب التحفظ سيدخل حيز التنفيذ في تاريخ معين وكان ذلك التاريخ لاحقاً عن التاريخ استلام الإشعار من قبل الأمين العام، يدخل سحب للتحفظ حيز التنفيذ في ذلك التاريخ اللاحق.

2. يجوز للأمين العام لمجلس أوروبا، بشكل دوري، أن يستفسر الأطراف التي استخدمت تحفظا أو أكثر من تحفظ طبقاً للمادة 12 عن احتمالات سحب ذلك التحفظ (أو تلك التحفظات).

المادة 14 – التطبيق الإقليمي

1. يجوز لأي طرف وقت التوقيع أو عند إيداع صك التصديق أو القبول أو الموافقة أو الانضمام أن يحدد الإقليم أو الأقاليم التي يشملها تطبيق هذا البروتوكول.

2. يجوز لأى طرف، في أي تاريخ لاحق، أن يوسع، عن طريق إعلان يوجه إلى الأمين العام لمجلس أوروبا، نطاق تطبيق هذا البروتوكول إلى أي إقليم آخر محدد في الإعلان. ويدخل البروتوكول حيز التنفيذ بالنسبة لهذا الإقليم في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر بعد استلام الأمين العام للإعلان.

3. يجوز سحب أي إعلان تم تقديمه بموجب الفقرتين السابقتين، فيما يتعلق بأي إقليم محدد في هذا الإعلان، من خلال إشعار يوجه إلى الأمين العام لمجلس أوروبا. ويدخل سحب الإعلان حيز التنفيذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر بعد تاريخ استلام الأمين العام لهذا الإشعار.

المادة 15 – الانسحاب

1. يجوز لأي طرف، في أي وقت، أن ينسحب من هذا البروتوكول عن طريق إشعار موجه إلى الأمين العام لمجلس أوروبا.

2. ويدخل هذا الانسحاب حيز التنفيذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام للإشعار.

المادة 16 – الإبلاغ

يقوم الأمين العام لمجلس أوروبا بإبلاغ الدول الأعضاء في مجلس أوروبا والدول غير الأعضاء التي شاركت في صياغة هذا البروتوكول، علاوة على أي دولة انضمت إليه أو دعيت للانضمام لهذا البروتوكول بـما يلي:

أ. أي توقيع؛

ب. إيداع أي صك للتصديق أو القبول، أو الموافقة أو الانضمام؛

ت. أي تاريخ لدخول هذا البروتوكول حيز التنفيذ طبقاً للمواد 9 و10 و11 منه،

ث. أي إجراء، إخطار أو تواصل آخر يتعلق بهذا البروتوكول.

وإثباتا لذلك، قام الموقعون أدناه، المفوضون بذلك حسب الأصول، بالتوقيع على هذا البروتوكول.

تم في ستراسبورغ في 28 يناير/كانون الثاني 2003، باللغتين الإنجليزية والفرنسية وكلا النصين متساويين في الحجية، وذلك في نسخة واحدة تودع في محفوظات مجلس أوروبا. ويرسل الأمين العام لمجلس أوروبا نسخا مصدقا عليها إلى كل دولة عضو في مجلس أوروبا، وإلى الدول غير الأعضاء التي شاركت في صياغة هذا البروتوكول وإلى أي دولة دعيت للانضمام إليه.

التقرير التفسيري

لا يشكل نص هذا التقرير التفسيري أداة توفر تفسيرا ذي حجية للبروتوكول، على الرغم من أنه قد يكون ذا طبيعة تسهل تطبيق الأحكام الواردة فيه. وسيفتح باب التوقيع على هذا البروتوكول في ستراسبورغ، في 28 يناير/كانون الثاني 2003، بمناسبة الجزء الأول أو دورة الجمعية البرلمانية لعام 2003.

المقدمة

1. أحرز المجتمع الدولي، منذ اعتماد الإعلان العالمي لحقوق الإنسان في عام 1948، تقدما هاما في مكافحة العنصرية والتمييز العنصري وكراهية الأجانب وما يتصل بذلك من تعصب. فضلا عن ذلك، تم سن قوانين وطنية ودولية واعتماد عدد من الصكوك الدولية لحقوق الإنسان، لا سيما الاتفاقية الدولية لنيويورك لعام 1966 بشأن القضاء على جميع أشكال التمييز العنصري، التي أبرمت في إطار احتياجات الأمم المتحدة التي ستتم الإشارة إليها (اتفاقية القضاء على التمييز العنصري "CERD"). وعلى الرغم من إحراز تقدم في هذا المجال، فإن الرغبة في عالم خال من الكراهية والتحيز العنصريين لم تتحقق إلا جزئيا.

2. لما كانت التطورات التكنولوجية والتجارية والاقتصادية تقرب شعوب العالم من بعضها البعض، فإن التمييز العنصري وكراهية الأجانب وغير ذلك من أشكال التعصب لا تزال قائمة في مجتمعاتنا. فالعولمة تنطوي على مخاطر يمكن أن تؤدي إلى الإقصاء وتعزيز عدم المساواة الذين في كثير من الأحيان ما يرتبطان بأسس عرقية وإثنية.

3. وتحديدا، يوفر ظهور شبكات اتصال دولية مثل الإنترنت لبعض الأشخاص وسائل حديثة وقوية لدعم العنصرية وكراهية الأجانب تمكِّنهم من نشر تعابير تتضمن مثل هذه الأفكار بطريقة سهلة وعلى نطاق واسع. لذلك، يعتبر التعاون الدولي أمرا حيويا من أجل التحقيق مع هؤلاء الأشخاص وملاحقتهم قضائيا. وفي هذا الإطار، تمت صياغة الاتفاقية بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية رقم 185) المشار إليها فيما يلي باسم "الاتفاقية"، لتمكين المساعدة المتبادلة بطريقة مرنة وحديثة فيما يتعلق بالجرائم ذات الصلة بالكمبيوتر بمعناها الأوسع. ويتلخص الغرض من هذا البروتوكول في شقين: أولهما، مواءمة القانون الجنائي الموضوعي لمكافحة العنصرية وكراهية الأجانب على شبكة الإنترنت، وثانيهما، تحسين التعاون الدولي في هذا المجال. ويساعد هذا النوع من المواءمة في تخفيف عبئ مكافحة هذه الجرائم على الصعيدين الوطني والدولي. ولعل الجرائم المطابقة في القوانين الوطنية قد تتعلق بحظر إساءة استخدام نظم الكمبيوتر لغرض عنصري، من قبل الدول الأطراف التي تكون قوانينها في هذا المجال محددة بشكل أقل جودة. لذلك، يمكن أيضا تعزيز تبادل الخبرات المشتركة المفيدة في التعامل التطبيقي مع هذا النوع

من القضايا. وهكذا، يصبح التعاون الدولي (بالخصوص تسليم المجرمين والمساعدة القانونية المتبادلة)، ميسرا، على سبيل المثال. فيما يتعلق بشروط ازدواجية التجريم.

4. ناقشت لجنة صياغة الاتفاقية إمكانية إدراج جرائم أخرى ذات الصلة بالمحتوى، من قبيل نشر الدعاية العنصرية عن طريق نظم الكمبيوتر. غير أن اللجنة لم تتمكن من التوصل إلى توافق في الآراء بشأن تجريم سلوك من هذا القبيل. وبينما كان هناك تأييد كبير لإدراج هذا الفعل كجريمة جنائية، أعربت بعض الوفود عن قلقها الشديد إزاء إدراج حكم من هذا القبيل على أسس حرية التعبير. وبعد أن لاحظت اللجنة مدى تعقيد المسألة، تقرر أن تحيل اللجنة على اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC) مسألة وضع بروتوكول إضافي للاتفاقية.

5. أوصت الجمعية البرلمانية، في رأيها 226 (2001) بشأن الاتفاقية، بوضع بروتوكول للاتفاقية على الفور تحت عنوان "توسيع نطاق الاتفاقية لتشمل أشكالا جديدة من الجرائم"، بهدف تحديد وتجريم نشر الدعاية العنصرية، من بين أمور أخرى.

6. ومن ثم، عهدت لجنة الوزراء إلى اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، ولا سيما لجنة الخبراء التابعة لها المعنية بتجريم الأعمال ذات الطابع العنصري والمعادي للأجانب التي ترتكب عن طريق نظم الكمبيوتر (PC-RX)، مهمة إعداد مسودة بروتوكول إضافي، كصك قانوني ملزم مفتوح لتوقيع وتصديق الدول الأطراف المتعاقدة في الاتفاقية، تتناول بصفة خاصة ما يلي:

أولا. تعريف وتحديد نطاق عناصر تجريم الأفعال ذات الطابع العنصري والمعادي للأجانب التي ترتكب عن طريق شبكات الكمبيوتر، بما في ذلك إنتاج المواد أو الرسائل ذات محتوى من هذا القبيل من خلال شبكات الكمبيوتر أو عرضها أو نشرها أو غير ذلك من أشكال توزيعها؛

ثانيا. تحديد نطاق تطبيق أحكام التعاون الموضوعي والإجرائي والدولي في اتفاقية الجريمة الإلكترونية على التحقيق والملاحقة القضائية للجرائم التي يتعين تعريفها بموجب البروتوكول الإضافي.

7. ينطوي هذا البروتوكول على توسيع نطاق الاتفاقية، بما في ذلك أحكامها الخاصة بالتعاون الموضوعي والإجرائي والدولي، بحيث تشمل أيضا جرائم الدعاية العنصرية وكراهية الأجانب. وهكذا، وبصرف النظر عن مواءمة عناصر القانون الموضوعي لهذا السلوك، يهدف البروتوكول إلى تحسين قدرة الدول الأطراف على استخدام وسائل وسبل التعاون الدولي المنصوص عليها في الاتفاقية في هذا المجال.

تعليق على مواد البروتوكول

الباب الأول – الأحكام المشتركة

المادة 1 – الغرض

8. يتلخص الغرض من هذا البروتوكول في تكملة أحكام الاتفاقية، فيما بين الأطراف في البروتوكول، بشأن تجريم الأفعال ذات الطابع العنصري والمعادي للأجانب التي ترتكب عن طريق نظم الكمبيوتر.

9. تعتبر أحكام البروتوكول ذات طابع إلزامي. ويتعين على الدول الأطراف، من أجل الامتثال لهذه الالتزامات، ألا تكتفي بسن تشريعات مناسبة، بل أن تكفل أيضا إعمالها على نحو فعال.

المادة 2 – التعريف

الفقرة 1 – "المواد التي تتعلق بالعنصرية وكراهية الأجانب"

10. تمت صياغة عدة صكوك قانونية على الصعيدين الدولي والوطني لمكافحة العنصرية أو كراهية الأجانب. وقد أخذ القائمون على صياغة هذا البروتوكول في الاعتبار بصفة خاصة (أ) الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري (CERD)، (ب) البروتوكول رقم 12 (سلسلة المعاهدات الأوروبية رقم 177) الملحق باتفاقية حماية حقوق الإنسان و الحريات الأساسية (ECHR)، (ج) الإجراء المشترك المؤرخ في 15 يوليو/تموز 1996 للاتحاد الأوروبي الذي اتخذه المجلس على أساس المادة كاف - 3 من معاهدة الاتحاد الأوروبي بشأن إجراءات مكافحة العنصرية وكراهية الأجانب، (د) المؤتمر العالمي لمكافحة العنصرية والتمييز العنصري وكراهية الأجانب وما يتصل بذلك من تعصب (ديربان، 31 أغسطس/آب - 8 سبتمبر /أيلول 2001)؛ (ه) استنتاجات المؤتمر الأوروبي لمكافحة العنصرية (ستراسبورغ، 13 أكتوبر/تشرين الأول 2000)، (و) الدراسة الشاملة الصادرة عن لجنة مجلس أوروبا لمكافحة العنصرية وكراهية الأجانب (ECRI) في أغسطس/آب 2000 (27 (2000) CRI) و (ز) اقتراح المفوضية الأوروبية بشأن القرار الإطار للمجلس بشأن مكافحة العنصرية الصادر في نوفمبر/تشرين الثاني 2001 (في إطار الاتحاد الأوروبي).

11. تعترف المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان بالحق في حرية التعبير، الذي يشمل حرية اعتناق الآراء وتلقي المعلومات والأفكار ونقلها. "لا ينحصر تطبيق المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان في المعلومات والأفكار التي تجد استحساناً أو يُنظر إليها على أنها غير ضارة أو غير مقصودة، بل تنطبق أيضاً على تلك التي تحدث أضراراً أو

اضطرابات في الدولة أو في أوساط أي شريحة من السكان"[12]. غير أن المحكمة الأوروبية لحقوق الإنسان رأت أن الإجراءات التي تتخذها الدولة لتقييد الحق في حرية التعبير مبررة على النحو الملائم بموجب القيود الواردة في الفقرة 2 من المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان، ولا سيما عندما تنتهك هذه الأفكار أو التعبيرات حقوق الآخرين. وهكذا، يحدد هذا البروتوكول، بناء على الصكوك الوطنية والدولية، النطاق الذي يعتبر فيه نشر التعبيرات والأفكار العنصرية والمعادية للأجانب انتهاكا لحقوق الآخرين.

12. يشير التعريف الوارد في المادة 2 إلى المواد المكتوبة (مثل النصوص، والكتب، والمجلات، والبيانات، والرسائل، وما إلى ذلك)، أو الصور (مثل اللوحات والصور الفوتوغرافية والرسومات، وما إلى ذلك) أو أي تمثيل آخر للأفكار أو النظريات ذات طابع عنصري ومعادي للأجانب، في شكل من هذا القبيل يمكن تخزينه ومعالجته ونقله عن طريق نظام الكمبيوتر.

13. يشير التعريف الوارد في المادة 2 من هذا البروتوكول إلى سلوك معين يمكن أن يؤدي إليه مضمون المادة، بدلا من التعبير عن مشاعر / معتقدات / نفور على النحو الوارد في المادة المعنية. ويستند التعريف إلى التعاريف والوثائق الوطنية والدولية (الأمم المتحدة والاتحاد الأوروبي) إلى أقصى حد ممكن.

14. يقتضي التعريف أن تستخدم مواد من هذا القبيل لمناصرة التمييز، العنف أو الكراهية أو الترويج لهم أو التحريض عليهم. ومصطلح "المناصرة" إلى الدعوة إلى الكراهية، التمييز أو العنف. ويشير مصطلح "الترويج" إلى التشجيع على الكراهية، التمييز أو العنف. و يحيل مصطلح "التحريض" على حث الآخرين على الكراهية، التمييز أو العنف.

15. يشير مصطلح "العنف" إلى الاستخدام غير المشروع للقوة، في حين يشير مصطلح "الكراهية" إلى البغض أو العداوة الشديدين.

16. عند تفسير مصطلح "التمييز"، ينبغي مراعاة الاتفاقية الأوروبية لحقوق الإنسان (المادة 14 والبروتوكول رقم 12)، وكذلك السوابق القضائية ذات الصلة، علاوة على المادة 1 من اتفاقية القضاء على جميع أشكال التمييز العنصري. ويكفل حظر التمييز الوارد في الاتفاقية الأوروبية لحقوق الإنسان لكل شخص يدخل في ولاية دولة طرف المساواة في التمتع بالحقوق والحريات التي تحميها الاتفاقية الأوروبية لحقوق الإنسان نفسها. وتنص المادة 14 من الاتفاقية الأوروبية لحقوق الإنسان على التزام عام للدول تابع للحقوق والحريات المنصوص عليها في الاتفاقية الأوروبية لحقوق الإنسان. وفي هذا السياق، يشير مصطلح "التمييز" المستخدم في البروتوكول إلى معاملة مختلفة غير مبررة لأشخاص أو لمجموعة من الأشخاص على أساس خصائص معينة. وفي العديد من الأحكام (من قبيل قضية اللغة

12. راجع في هذا السياق، على سبيل المثال، حكم هانديساید (Handyside) المؤرخ في 7 ديسمبر/كانون الأول 1976، السلسلة أ، عدد 24، ص.23، الفقرة 49.

البلجيكية، حكم عبد العزيز وكاباليس وبلكندالي)[13]، ذكرت المحكمة الأوروبية لحقوق الإنسان أن "اختلاف المعاملة يكون تمييزيا إذا لم يكن هناك "مبرر موضوعي ومعقول"، بمعنى إذا لم يسع إلى تحقيق "هدف مشروع" أو إذا لم تكن هناك "علاقة معقولة للتناسب بين الوسائل المستخدمة والهدف المنشود تحقيقه". وبالتالي، يجب تحديد ما إذا كانت المعاملة تمييزية أم لا على ضوء الظروف الخاصة بالقضية. ويمكن أيضا الاسترشاد لتفسير مصطلح "التمييز" في المادة 1 من اتفاقية القضاء على جميع أشكال التمييز العنصري، حيث يشير مصطلح "التمييز العنصري" إلى "أي تمييز أو استبعاد أو تقييد أو تفضيل على أساس العرق، أو الأصل القومي أو الإثني الذي يكون غرضه أو أثره إبطال أو عرقلة الاعتراف بحقوق الإنسان والحريات الأساسية أو التمتع بها أو ممارستها على قدم المساواة في الحريات السياسية، الاقتصادية، الاجتماعية أو الثقافية أو أي مجال آخر من مجالات الحياة العامة".

17. يجب أن تكون الكراهية أو التمييز أو العنف موجها ضد أي فرد أو مجموعة من الأفراد، لأنهم ينتمون إلى جماعة تتميز ب "العرق أو اللون أو النسب أو الأصل القومي أو الإثني، وكذلك الدين، إذا ما استخدمت كذريعة لأي من هذه العوامل".

18. تجدر الإشارة إلى أن هذه الأسباب لا تتطابق تماما مع الأسباب الواردة في المادة 1 من البروتوكول رقم 12 الملحق بالاتفاقية الأوروبية لحقوق الإنسان، حيث أن بعض تلك الأحكام الواردة في هذه الأخيرة غريبة عن مفهوم العنصرية أو كراهية الأجانب. كما أن الأسس الواردة في المادة 2 من هذا البروتوكول ليست مطابقة لتلك الواردة في اتفاقية القضاء على جميع أشكال التمييز العنصري، حيث أن هذه الأخيرة تتناول "التمييز العنصري" بشكل عام وليس "العنصرية" في حد ذاتها. وبصفة عامة، ينبغي تفسير هذه الأسس بمعناها في القانون والممارسة القائمين على الصعيدين الوطني والدولي. ومع ذلك، يتطلب بعضها مزيدا من التوضيح من حيث معناها الدقيق في سياق هذا البروتوكول.

19. يشير "النسب" أساسا إلى أشخاص أو مجموعات الأشخاص الذين ينحدرون من أشخاص يمكن تحديدهم بخصائص معينة (كالعرق أو اللون)، لكن ليس من الضروري أن تكون جميع هذه الخصائص موجودة. وعلى الرغم من ذلك، قد يتعرض هؤلاء الأشخاص أو مجموعات الأشخاص، بسبب نسبهم، للكراهية، التمييز أو العنف. ولا يشير "النسب" إلى الأصل الاجتماعي.

20. ينبغي تأويل مفهوم "الأصل القومي" بمعنى واقعي واسع. فقد يشير إلى تاريخ الأفراد، ليس فيما يتعلق بجنسية أو أصل أسلافهم فحسب، بل أيضا بانتماءاتهم الوطنية، بصرف النظر عما إذا كانوا لا يزالون يتمتعون بها من الناحية القانونية. وعندما يحمل الأشخاص

13. عبد العزيز، كاباليس وبلكندالي، الحكم الصادر في 28 ماي/ أيار 1985، السلسلة ألف، عدد 94، ص. 32، الفقرة 62؛ الحكم البلجيكي اللغوي، الحكم الصادر في 23 يوليو/تموز 1968، السلسلة ألف، عدد 6، ص. 34، الفقرة 10.

أكثر من جنسية واحدة أو يكونون عديمي الجنسية، فإن التفسير الواسع لهذا المفهوم يروم حمايتهم إذا ما تعرضوا للتمييز على أي من هذه الأسباب. علاوة على ذلك، قد لا يشير مفهوم "الأصل القومي" فقط إلى الانتماء إلى إحدى البلدان المعترف بها دوليا بصفتها هذه، بل أيضا إلى الأقليات أو مجموعات أخرى من الأشخاص، ذات خصائص مماثلة.

21. كثيرا ما يرد مفهوم "الدين" في الصكوك الدولية والتشريعات الوطنية. ويشير المصطلح إلى الإيمان الراسخ والمعتقدات. ولعل إدراج هذا المصطلح على هذا النحو في التعريف قد ينطوي على خطر تجاوز نطاق هذا البروتوكول. ومع ذلك، يمكن استخدام الدين كذريعة أو حجة أو بديل عن عوامل أخرى ورد ذكرها في التعريف. لذلك، ينبغي تفسير "الدين" بهذا المعنى المقيد.

الفقرة 2

22. من خلال التنصيص على تفسير المصطلحات والعبارات المستخدمة في البروتوكول بنفس الطريقة التي تفسر بها بموجب الاتفاقية، تضمن هذه المادة التفسير الموحد لكليهما. وهذا يعني أن المصطلحات والعبارات المستخدمة في هذا التقرير التفسيري يجب أن تفسر بنفس الطريقة التي تفسر بها هذه المصطلحات والعبارات في التقرير التفسيري للاتفاقية.

الباب الثاني – التدابير الواجب اتخاذها على المستوى الوطني

اعتبارات عامة

23. تتضمن الجرائم، على النحو المنصوص عليه في هذا البروتوكول، عددا من العناصر المشتركة التي اقتبست من الاتفاقية. وتوخيا للوضوح، ترد فيما يلي الفقرات ذات الصلة في التقرير التفسيري للاتفاقية.

24. لعل إحدى خصائص الجرائم المضمنة تتمثل في الطلب الصريح بأن يتم السلوك المعني "دون حق". ويعكس ذلك فكرة أن السلوك الموصوف لا يعاقب دائما في حد ذاته، بل 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 المبادئ أو المصالح الأخرى إلى استبعاد المسؤولية الجنائية (على سبيل المثال، لأغراض إنفاذ القانون أو لأغراض أكاديمية أو بحثية). ويستمد التعبير "دون حق" معناه من السياق الذي يستخدم فيه. وبالتالي، وفي غياب تقييد الطريقة التي يمكن للأطراف أن تنفذ من خلالها هذا المفهوم في قوانينها الوطنية، يجوز أن يشير هذا التعبير إلى سلوك يتم دون سلطة (سواء كانت تشريعية، تنفيذية، إدارية، قضائية، تعاقدية أو توافقية) أو سلوك لا تشمله خلاف ذلك الدفوع والأعذار والمبررات القانونية القائمة أو المبادئ ذات الصلة بموجب

القانون الوطني. لهذا، فإن البروتوكول يترك السلوك غير المتضرر الذي يتم تنفيذه بموجب سلطة حكومية شرعية (على سبيل المثال، عندما تعمل حكومة الدولة الطرف للحفاظ على النظام العام، وحماية الأمن القومي أو التحقيق في الجرائم الجنائية). وعلاوة على ذلك، لا ينبغي تجريم الأنشطة المشروعة والمشتركة ذات الصلة بتصميم الشبكات أو الممارسات التشغيلية أو التجارية المشروعة والمشتركة. ويترك للأطراف تحديد كيفية تنفيذ هذه الإعفاءات في إطار نظمها القانونية الوطنية (بموجب القانون الجنائي أو غيره من القوانين).

25. يجب أن ترتكب جميع الجرائم الواردة في البروتوكول "عمدا" لتطبيق المسؤولية الجنائية. وفي بعض الحالات، يشكل عنصر إضافي محدد ومتعمد جزءا من الجريمة. واتفق القائمون على صياغة البروتوكول، على غرار نظرائهم بشأن الاتفاقية، أن يتركوا المعنى الدقيق لمصطلح "عمدا" للتفسير وطنيا. ولا يمكن اعتبار الأشخاص مسؤولين جنائيا عن أي من الجرائم المنصوص عليها في هذا البروتوكول إذا لم تكن لديهم النية المطلوبة. ولا يكفي، على سبيل المثال، أن يتحمل مزود خدمات المسؤولية الجنائية بموجب هذا الحكم، حيث يكون مزود الخدمة هذا بمثابة قناة أو مستضيف لموقع على شبكة الإنترنت أو غرفة إخبارية تحتوي على مواد من هذا القبيل، دون أن النية المطلوبة بموجب القانون الوطني في هذه الحالة الخاصة. بالإضافة إلى ذلك، لا يشترط في مقدم الخدمة رصد السلوك لتجنب المسؤولية الجنائية.

26. وفيما يتعلق بمفهوم "نظام الكمبيوتر"، فإن هذا المفهوم هو نفسه الوارد في الاتفاقية والموضح في الفقرتين 23 و 24 من تقريرها التفسيري. ويشكل ذلك تطبيقا للمادة 2 من هذا البروتوكول (راجع أيضا شرح المادة 2 أعلاه).

المادة 3 – نشر المواد المتصلة بالعنصرية وكراهية الأجانب عبر أنظمة الكمبيوتر

27. تقتضي هذه المادة بأن تجرم الدول الأطراف توزيع مواد عنصرية ومعادية للأجانب أو إتاحتها بطرق أخرى للجمهور من خلال نظام الكمبيوتر. ولا يكون فعل التوزيع أو الإتاحة جنائيا إلا إذا كانت النية أيضا متصلة بالطابع العنصري والمعادي للأجانب لتلك المواد.

28. يشير "التوزيع" إلى النشر النشط للمواد العنصرية والمعادية للأجانب، على النحو المحدد في المادة 2 من البروتوكول، إلى الغير، في حين يشير مصطلح "إتاحة" إلى وضع مواد عنصرية ومعادية للأجانب في متناول الغير لاستخدامها. ويهدف هذا المصطلح أيضا إلى تغطية إنشاء أو تجميع وصلات تشعبية من أجل تيسير الحصول على مواد من هذا القبيل.

29. يوضح مصطلح "للجمهور" المستخدم في المادة 3 أن الاتصالات الخاصة أو التعبيرات التي يتم إيصالها أو نقلها عن طريق نظام الكمبيوتر خارجة عن نطاق هذا الحكم. وبالفعل، فإن هذه الاتصالات أو التعبيرات، على غرار الأشكال التقليدية للمراسلات، محمية بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان.

30. يجب تحديد ما إذا كان الاتصال المتعلق بالمواد العنصرية والمعادية للأجانب يعتبر اتصالا خاصا أو نشرا متاحا للجمهور، بناء على ظروف القضية. لكن ما يهم في المقام الأول هو نية المرسل أن الرسالة المعنية سيتم استقبالها فقط من قبل جهاز الاستقبال المحدد مسبقا. وبالتالي، يمكن تحديد وجود هذه النية الذاتية بناء على عدد من العوامل الموضوعية، مثل محتوى الرسالة، والتكنولوجيا المستخدمة، والتدابير الأمنية المطبقة، والسياق الذي ترسل فيه الرسالة. وعندما ترسل هذه الرسائل في الوقت نفسه إلى أكثر من متلقي واحد، يكون عدد المتلقين وطبيعة العلاقة بين المرسل والمتلقي (المتلقيين) عاملا لتحديد ما إذا كان من الممكن اعتبار هذا الاتصال خاصا.

31. يعتبر تبادل المواد العنصرية والمعادية للأجانب في غرف الدردشة، أو نشر رسائل مماثلة في مجموعات الأخبار أو منتديات المناقشة أمثلة على إتاحة هذه المواد للجمهور. وفي هذه الحالات، تكون تلك المواد هي في متناول أي شخص. وحتى عندما يتطلب النفاذ إلى تلك المواد ترخيصا بواسطة كلمة سر، تكون هذه المواد متاحة للجمهور حيثما منح هذا الترخيص لأي شخص أو لأي شخص يستوفي معايير معينة. ومن أجل تحديد ما إذا كانت الإتاحة أو التوزيع موجها للجمهور أم لا، ينبغي مراعاة طبيعة العلاقة بين الأشخاص المعنيين.

32. أدرجت الفقرتان 2 و3 لتوفير إمكانية التحفظ في ظروف محدودة للغاية. وينبغي قراءتها بالتزامن والتسلسل. لذلك، تتوفر الدولة الطرف، أولا، على إمكانية عدم ربط المسؤولية الجنائية بالسلوك الوارد في هذه المادة، حيثما كانت المواد تدعو، تروج أو تحرض على تمييز غير متصل بالكراهية أو العنف، شريطة توافر سبل انتصاف فعالة أخرى. ويمكن أن تكون سبل الانتصاف هاته إما مدنية أو إدارية، على سبيل المثال. وفي الحالات التي لا تستطيع فيها الدولة الطرف، بسبب المبادئ القائمة في نظامها القانوني بشأن حرية التعبير، التنصيص على سبل الانتصاف هذه، يجوز لها أن تحتفظ بالحق في عدم تنفيذ الالتزام المنصوص عليه في الفقرة 1 من هذه المادة، شريطة ألا يتعلق الأمر إلا بالدعوة، الترويج أو التحريض على التمييز الذي لا يرتبط بالكراهية أو العنف. ويجوز لأي دولة طرف أن تحد كذلك من نطاق التحفظ بأن تشترط أن يكون التمييز، على سبيل المثال، سبا، إهانة أو تهديدا لمجموعة من الأشخاص.

المادة 4 – التهديد المبرر بدافع التمييز العنصري وكراهية الأجانب

33. تنص معظم التشريعات على تجريم التهديد بشكل عام. واتفق القائمون على الصياغة على التأكيد في البروتوكول على أنه ينبغي، دون أي شك، تجريم التهديدات المتعلقة بدوافع عنصرية ومعادية للأجانب.

34. يمكن أن يشير مفهوم "التهديد" إلى خطر يثير الخوف لدى الأشخاص الذين يوجه إليهم التهديد، من التعرض إلى ارتكاب فعل إجرامي خطير (يؤثر على حياة الضحية

أو أقاربها، أمنهم أو سلامتهم الشخصية، أو يلحق ضررا خطير بممتلكاتهم، وما إلى ذلك). ويترك للدول الأطراف أن تقرر المقصود بالفعل الإجرامي الخطير.

35. ووفقا لهذه المادة، يجب أن يوجه التهديد إما إلى (أ) شخص بسبب انتمائه إلى مجموعة متميزة بالعرق، اللون، النسب أو الأصل القومي أو الإثني، وكذلك الديانة، إذا استخدمت كذريعة لأي من هذه العوامل، أو (ب) مجموعة من الأشخاص تتميز بأي من هذه الخصائص. ولا يوجد أي تقييد يوجب أن يكون التهديد علنًا. وتشمل هذه المادة أيضا التهديدات التي تتم عبر اتصالات خاصة.

المادة 5 – السب المبرر بدافع التمييز العنصري وكراهية الأجانب

36. تتناول المادة 5 مسألة سب شخص أو مجموعة من الأشخاص علنا لأنهم ينتمون أو يعتقد أنهم ينتمون إلى جماعة تتميز بخصائص محددة. ويشير مفهوم "السب" إلى أي تعبير هجومي، ازدرائي أو انتقامي يضر بشرف شخص أو كرامته. وينبغي أن يكون واضحا في التعبير نفسه أن الإهانة ترتبط ارتباطا مباشرا بانتماء الشخص الذي يتعرض إلى السب إلى المجموعة. وخلافا لما لحالة التهديد، لا يشمل هذا الحكم السب المعبر عنه في اتصالات خاصة.

37. تسمح الفقرة 2 (أ) للدول الأطراف بأن تشترط أن يكون للسلوك أيضا تأثير على شخص أو مجموعة من الأشخاص، ليس فقط بشكل محتمل بل أن يتعرضوا فعلا للكراهية، الازدراء أو السخرية.

38. تسمح الفقرة 2 (ب) للدول الأطراف بإدخال تحفظات تتجاوز حتى الآثار التي لا تنطبق عليها أن الفقرة 1.

المادة 6 – إنكار الإبادة الجماعية أو الجرائم ضد الإنسانية، أو التقليل الجسيم من شأنها أو الموافقة عليها أو تبريرها

39. في السنوات الأخيرة، بثت المحاكم الوطنية في قضايا مختلفة أعرب فيها أشخاص (من العموم، وسائل الإعلام، إلخ.) عن أفكار أو نظريات ترمي إلى إنكار الجرائم الخطيرة التي وقعت خاصة خلال الحرب العالمية الثانية (ولا سيما الهولوكوست) أو التقليل الجسيم من شأنها أو الموافقة عليها أو تبريرها. وغالبا ما يكون الدافع لهذه السلوكيات بحجة البحث العلمي، في حين أنها تهدف حقا إلى دعم وتعزيز الدافع السياسي الذي أدى إلى محرقة اليهود. علاوة على ذلك، ألهمت هذه السلوكيات أو حفزت وشجعت مجموعات عنصرية ومعادية للأجانب في أنشطتها، بما في ذلك من خلال نظم الكمبيوتر. ويعتبر التعبير عن مثل هذه الأفكار مهينا (لذكرى) لأولئك الأشخاص الذين وقعوا ضحايا لهذه العاقبة الوخيمة، وكذلك لأقاربهم. وفي الأخير، يهدد هذا التعبير كرامة المجتمع البشري.

40. تعالج المادة 6، التي تتوفر على بنية مشابهة للمادة 3، هذه المشكلة، حيث اتفق القائمون على الصياغة على أنه من المهم تجريم العبارات التي تنكر الأعمال التي تشكل إبادة جماعية أو جرائم ضد الإنسانية، تقلل من شأنها بشكل جسيم، توافق عليها أو تبررها، على النحو الذي يحدده القانون الدولي وتعترف به قرارات نهائية وملزمة للمحكمة العسكرية الدولية، المؤسسة بموجب اتفاق لندن المؤرخ في 8 أبريل/نيسان 1945. ويعزى ذلك إلى أن أهم تلك السلوكيات التي أدت إلى الإبادة الجماعية والجرائم ضد الإنسانية، حدثت خلال الفترة ما بين 1940 و1945. غير أن القائمين على الصياغة اعترفوا أنه منذ ذلك الحين، وقعت حالات أخرى من جرائم الإبادة الجماعية والجرائم المرتكبة ضد الإنسانية، كانت دوافعها القوية قائمة على نظريات وأفكار ذات الطبيعة العنصرية والمعادية للأجانب. لذلك، ارتأى القائمون على الصياغة أنه من الضروري عدم حصر نطاق هذا الحكم على الجرائم التي ارتكبها النظام النازي خلال الحرب العالمية الثانية والتي اعتبرتها كذلك محكمة نورمبيرغ، بل أيضا على عمليات الإبادة الجماعية والجرائم المرتكبة ضد الإنسانية التي أقامتها منظمات دولية أخرى أنشئت منذ عام 1945 بموجب الصكوك القانونية الدولية ذات الصلة (من قبيل قرارات مجلس الأمن التابع للأمم المتحدة والمعاهدات متعددة الأطراف، وما إلى ذلك). ومن بين هذه المحاكم، على سبيل المثال، المحكمتين الجنائيتين الدوليتين ليوغوسلافيا السابقة، ولرواندا، والمحكمة الجنائية الدولية الدائمة. وتسمح هذه المادة بالإشارة إلى القرارات النهائية الملزمة للمحاكم الدولية المستقبلية، طالما تعترف الدولة الطرف الموقِّعة على هذا البروتوكول باختصاص محكمة من هذا القبيل.

41. يرمي هذا الحكم إلى توضيح أن الوقائع التي ثبتت صحتها التاريخية لا يمكن إنكارها، التقليل الجسيم من شأنها، الموافقة عليها أو تبريرها من أجل دعم هذه النظريات والأفكار المقيتة.

42. أوضحت المحكمة الأوروبية لحقوق الإنسان أن رفض أو مراجعة "الوقائع التاريخية الواضحة - مثل محرقة اليهود - [...] ستستبعد من الحماية بمقتضى المادة 10 بموجب المادة 17" من الاتفاقية الأوروبية لحقوق الإنسان (راجع في هذا السياق حكم لوهيدو (Lehideux) وإيزورني (Isorni) المؤرخ في 23 سبتمبر/أيلول 1998)[14].

43. تسمح الفقرة 2 من المادة 6 للدولة الطرف إما (أ) بأن تشترط، من خلال إعلان، أن يرتكب الإنكار أو التقليل الجسيم المشار إليهما في الفقرة 1 من المادة 6 بقصد التحريض على الكراهية، التمييز أو العنف ضد أي فرد أو مجموعة من الأفراد، على أساس العرق، اللون، النسب أو الأصل القومي أو الإثني، وكذلك الديانة إذا استخدم كذريعة لأي من هذه العوامل، أو (ب) أن تستخدم التحفظ، من خلال السماح لدولة طرف بعدم تطبيق هذا الحكم كليا أو جزئيا.

14. حكم لويهيدو وإيزورني المؤرخ في 23 سبتمبر/أيلول 1998، التقارير 7-1998، الفقرة 47.

المادة 7 – المساعدة والتحريض

44. يتلخص الغرض من هذه المادة في اعتبار المساعدة والتحريض على ارتكاب أي من الجرائم المنصوص عليها في المواد من 3 إلى 6 كجرائم جنائية. وخلافا للاتفاقية، لا يتضمن البروتوكول تجريم محاولة ارتكاب الجرائم الواردة فيه، نظرا لأن كثيرا من الأعمال المجرمة لها طابع تحضيري.

45. تنشأ المسؤولية عن تقديم المساعدة أو التحريض حيثما يكون الشخص الذي يرتكب جريمة منصوص عليها في البروتوكول مدعوما بشخص آخر ينوي أيضا ارتكاب الجريمة. على سبيل المثال، على الرغم من أن نقل المواد العنصرية والمعادية للأجانب عن طريق الإنترنت يتطلب مساعدة مزودي الخدمات كقناة، لا يمكن أن يتحمل مزود الخدمة الذي لا تتوفر لديه النية الجنائية، أي مسؤولية بموجب هذا القسم. وبالتالي، لا يوجد أي واجب على مزود الخدمة لرصد المحتوى بفعالية بغية تفادي المسؤولية الجنائية بموجب هذا الحكم.

46. كما هو الحال بالنسبة لجميع الجرائم المقررة وفقا للبروتوكول، يجب أن يكون ارتكاب المساعدة أو التحريض عمدا.

الباب الثالث – العلاقة بين الاتفاقية وهذا البروتوكول

المادة 8 – العلاقة بين الاتفاقية وهذا البروتوكول

47. تتناول المادة 8 العلاقة بين الاتفاقية وهذا البروتوكول. ويتجنب هذا الحكم إدراج عدد من أحكام الاتفاقية في هذا البروتوكول، ويشير التقرير إلى أن بعض أحكام الاتفاقية تنطبق، مع مراعاة ما يقتضيه اختلاف الحال، على هذا البروتوكول (مثلا فيما يتعلق بالمسؤولية والعقوبات الثانوية، والولاية القضائية، وجزء من الأحكام الختامية). وتذكر الفقرة 2 الدول الأطراف بأن المعنى الوارد في الاتفاقية ينبغي أن ينطبق على الجرائم المنصوص عليها في البروتوكول. وتوخيا للوضوح، تم تحديد المواد ذات الصلة.

الباب الرابع – الأحكام الختامية

48. تستند الأحكام الواردة في هذا الفصل، في معظمها، إلى "الأحكام الختامية النموذجية للاتفاقيات والاتفاقات المبرمة في مجلس أوروبا" التي وافقت عليها لجنة الوزراء في الاجتماع الـ315 لنواب الوزراء في فبراير/شباط 1980. وبما أن معظم المواد من 9 إلى 16 تستخدم اللغة العادية للبنود النموذجية أو تستند إلى ممارسة طويلة العهد في مجال صياغة المعاهدات في مجلس أوروبا، فإنها لا تتطلب تعليقات خاصة. ومع ذلك، تحتاج بعض التعديلات على البنود النموذجية العادية أو بعض الأحكام الجديدة مزيدا من التوضيح.

ويلاحظ في هذا السياق أن الأحكام النموذجية اعتُمدت كمجموعة غير ملزمة من الأحكام. وكما أشارت مقدمة البنود النموذجية أن "هذه الأحكام الختامية النموذجية لا تهدف إلا إلى تسهيل مهمة لجان الخبراء وتجنب الاختلافات النصية التي لا يكون لها أي مبرر حقيقي. وهكذا، فإن النموذج ليس بأي حال من الأحوال ملزما ويمكن اعتماد بنود مختلفة لتناسب حالات معينة " (راجع أيضا في هذا السياق الفقرات 330-304 من التقرير التفسيري للاتفاقية).

49. تحدد الفقرة 2 من المادة 12 أنه يجوز للدول الأطراف أن تستفيد من التحفظ على النحو المحدد في المواد 3 و 5 و 6 من هذا البروتوكول. ولا يجوز إبداء أي تحفظ آخر.

50. يفتح باب التوقيع على هذا البروتوكول فقط للموقعين على الاتفاقية. ويدخل البروتوكول حيز النفاذ بعد ثلاثة أشهر من إعلان خمس دول أطراف في الاتفاقية عن موافقتها على الالتزام به (المادتان 10-9).

51. تسمح الاتفاقية بالتحفظات بشأن أحكام معينة يمكن أن يكون لها، من خلال شرط الربط الوارد في المادة 8 من البروتوكول، أثر على التزامات دولة طرف بموجب البروتوكول أيضا. ومع ذلك، يجوز للدولة الطرف إشعار الأمين العام بأنها لن تطبق هذا التحفظ فيما يتعلق بمحتوى البروتوكول، طبقا لما هو معبر عنه في الفقرة 2 من المادة 12 من البروتوكول.

52. إلا أنه عندما لا تستفيد دولة طرف من إمكانية التحفظ هاته بموجب الاتفاقية، قد تكون هنالك حاجة إلى تقييد التزاماتها فيما يتعلق بالجرائم المنصوص عليها في البروتوكول. وتتيح الفقرة 2 من المادة 12 للدول الأطراف إمكانية القيام بذلك فيما يتعلق بالفقرة 2 من المادة 22 والفقرة 1 من المادة 41 من الاتفاقية.

البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية [ستراسبورغ 12 مايو 2022]

الديباجة

إن الدول الأعضاء في مجلس أوروبا والدول الأخرى الأطراف في الاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة المعاهدات الأوروبية رقم 185، المشار إليها فيما بعد بـ "الاتفاقية")، التي فتح باب التوقيع عليها في بودابست بتاريخ 23 نوفمبر/تشرين الثاني 2001، والموقعة على هذه الوثيقة،

وإذ تضع في اعتبارها مدى انتشار الاتفاقية وتأثيرها في جميع مناطق العالم؛

وإذ تشير إلى أن الاتفاقية قد استُكملت بالفعل بالبروتوكول الإضافي بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر (سلسلة المعاهدات الأوروبية رقم 189)، الذي فتح باب التوقيع عليه في ستراسبورغ بتاريخ 28 يناير/كانون الثاني 2003 (يشار إليه فيما يلي باسم "البروتوكول الأول")، بالنسبة للدول الأطراف في البروتوكول المذكور؛

وإذ تأخذ بعين الاعتبار معاهدات مجلس أوروبا القائمة بشأن التعاون في المسائل الجنائية وكذلك الاتفاقات والترتيبات الأخرى بشأن التعاون في المسائل الجنائية بين الأطراف في الاتفاقية؛

وإذ تأخذ في الحسبان أيضًا اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (سلسلة المعاهدات الأوروبية رقم 108)، كما تم تعديلها بموجب بروتوكولها التعديلي (سلسلة المعاهدات الأوروبية رقم 223)، الذي فتح باب التوقيع عليه في ستراسبورغ بتاريخ 10 أكتوبر/تشرين الأول 2018، وتجوز دعوة أي دولة للانضمام إليه؛

وإذ تقر بالاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات، بما في ذلك خدمات الإنترنت، وزيادة الجريمة السيبرانية، التي تشكل تهديدًا للديمقراطية وسيادة القانون والتي تعتبرها دول كثيرة أيضًا تهديدًا لحقوق الإنسان؛

وإذ تدرك أيضاً تزايد عدد ضحايا الجرائم الإلكترونية وأهمية تحقيق العدالة لهؤلاء الضحايا؛

وإذ تشير إلى أن الحكومات تتحمل مسؤولية حماية المجتمع والأفراد من الجريمة ليس فقط خارج الإنترنت ولكن أيضًا عبر الإنترنت، بما في ذلك من خلال التحقيقات الجنائية والملاحقات القضائية الفعالة؛

وإذ تدرك أن الأدلة المتعلقة بأي جريمة جنائية يتم تخزينها بشكل متزايد في شكل إلكتروني على أنظمة الكمبيوتر في ولايات قضائية أجنبية أو متعددة أو غير معروفة، واقتناعا منها بالحاجة إلى اتخاذ تدابير إضافية للحصول على مثل هذه الأدلة بشكل قانوني ضمانا لاستجابة جنائية فعالة وتعزيزاً سيادة القانون؛

وإذ تقر بالحاجة إلى تعاون متزايد وأكثر كفاءة بين الدول والقطاع الخاص، وأنه في هذا السياق، ثمة حاجة إلى مزيد من الوضوح أو اليقين القانوني بالنسبة لمقدمي الخدمات والكيانات الأخرى فيما يتعلق بالظروف التي قد يستجيبون فيها للطلبات المباشرة من سلطات العدالة الجنائية لدى الدول الأطراف الأخرى للكشف عن البيانات الإلكترونية؛

وإذ تسعى، بالتالي، إلى زيادة تعزيز التعاون بشأن الجرائم الإلكترونية وجمع الأدلة في شكل إلكتروني عن أي جريمة جنائية لغرض تحقيقات أو إجراءات جنائية محددة من خلال أدوات إضافية تتعلق بالمساعدة المتبادلة الأكثر كفاءة وأشكال التعاون الأخرى بين السلطات المختصة؛ وإلى تعزيز التعاون في حالات الطوارئ والتعاون المباشر بين السلطات المختصة ومقدمي الخدمات والكيانات الأخرى التي تمتلك أو تتحكم في المعلومات ذات الصلة؛

واقتناعا منها بأن الظروف والضمانات الفعالة لحماية حقوق الإنسان والحريات الأساسية مفيدة للتعاون العابر للحدود الفعال لأغراض العدالة الجنائية، بما في ذلك بين القطاعين العام والخاص؛

واعترافا منها بأن جمع الأدلة الإلكترونية في إطار التحقيقات الجنائية غالبًا ما يتعلق بالبيانات الشخصية، وبأنه يتعين على العديد من الأطراف حماية الخصوصية والبيانات الشخصية من أجل الوفاء بالتزاماتها الدستورية والدولية؛

وإذ تضع في اعتبارها الحاجة إلى ضمان خضوع تدابير العدالة الجنائية الفعالة بشأن الجرائم الإلكترونية وجمع الأدلة في شكل إلكتروني لشروط وضمانات توفر الحماية الكافية لحقوق الإنسان والحريات الأساسية، بما في ذلك الحقوق المنبثقة عن الالتزامات التي تعهدت بها الدول بموجب صكوك حقوق الإنسان الدولية المعمول بها، على غرار اتفاقية عام 1950 لحماية حقوق الإنسان والحريات الأساسية لمجلس أوروبا (سلسلة المعاهدات الأوروبية رقم 5)، وعهد الأمم المتحدة الدولي الخاص بالحقوق المدنية والسياسية لعام 1966، والميثاق الأفريقي لحقوق الإنسان والشعوب لسنة 1981، والاتفاقية الأمريكية لحقوق الإنسان لعام 1969 وغيرها من المعاهدات الدولية المتعلقة بحقوق الإنسان؛

اتفقت على ما يلي:

الباب I - أحكام عامة

المادة 1 - الغرض من البروتوكول

يرمي هذا البروتوكول إلى استكمال:

أ. الاتفاقية بين الدول الأطراف في هذا البروتوكول؛

ب. البروتوكول الأول بين الدول أطراف هذا البروتوكول التي هي أيضًا أطراف في البروتوكول الأول.

المادة 2 - نطاق التطبيق

1. ما لم يتم تحديد خلاف ذلك في هذه الوثيقة، تطبق التدابير الواردة في هذا البروتوكول:

أ. بالنسبة للدول الأطراف في الاتفاقية التي هي أيضا أطراف في هذا البروتوكول، على التحقيقات أو الإجراءات الجنائية الخاصة المتعلقة بالجرائم الجنائية ذات الصلة بأنظمة الكمبيوتر والبيانات، وجمع الأدلة في شكل إلكتروني عن جريمة جنائية؛

ب. بالنسبة للدول الأطراف في البروتوكول الأول التي هي أيضا أطراف في هذا البروتوكول، على التحقيقات أو الإجراءات الجنائية الخاصة المتعلقة بالجرائم الجنائية المنصوص عليها في البروتوكول الأول.

2. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتنفيذ الالتزامات المنصوص عليها في هذا البروتوكول.

المادة 3 - التعريفات

1. تسري التعاريف الواردة في المادتين 1 و 18، الفقرة 3، من الاتفاقية على هذا البروتوكول.

2. لأغراض هذا البروتوكول، تنطبق التعاريف التالية:

أ. يقصد بـــ "السلطة المركزية" السلطة أو السلطات المعينة بموجب معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة سارية بين الأطراف المعنية، أو، في حالة عدم وجودها، السلطة أو السلطات المعينة من قبل إحدى الدول الأطراف بموجب المادة 27، الفقرة 2أ من الاتفاقية؛

ب. يقصد بـــ "السلطة المختصة" سلطة قضائية أو إدارية أو غيرها من سلطات إنفاذ القانون المخولة بموجب القانون المحلي بإصدار الأمر بتنفيذ التدابير الواردة في هذا البروتوكول أو الترخيص بها أو تتولى تنفيذها لغرض جمع أو تقديم أدلة فيما يتعلق بتحقيقات أو إجراءات جنائية خاصة؛

ج. يقصد بـ "حالة طوارئ" الوضعية التي يوجد فيها خطر كبير ووشيك على حياة أو سلامة أي شخص طبيعي؛

د. يقصد بـ "البيانات الشخصية" معلومات متعلقة بشخص طبيعي محدد أو يمكن التعرف عليه؛

هـ. يقصد بـ "الطرف المحوّل" الطرف الذي يقوم بنقل البيانات استجابة لطلب أو كجزء من فريق تحقيق مشترك أو، لأغراض القسم الثاني من الباب الثاني، طرف يوجد فوق ترابه مقدم خدمات قادر على نقل البيانات أو كيان يوفر خدمات تسجيل أسماء النطاقات.

المادة 4 - اللغة

1. يجب أن تكون الطلبات والأوامر والمعلومات المصاحبة المقدمة إلى أحد الأطراف بلغة مقبولة لدى الطرف متلقي الطلب أو الطرف المُخطر بموجب المادة 7، الفقرة 5، أو تكون مصحوبة بترجمة إلى هذه اللغة.

2. يجب أن تكون الأوامر المنصوص عليها في المادة 7 والطلبات المنصوص عليها في المادة 6 وأي معلومات مصاحبة:

أ. محررة بلغة الطرف الآخر التي يقبل بها مقدم الخدمة أو الكيان عملية محلية مماثلة؛

ب. محررة بلغة أخرى مقبولة لدى مقدم الخدمة أو الكيان؛ أو

ج. مصحوبة بترجمة إلى إحدى اللغات الواردة في الفقرتين 2. أ أو 2. ب.

الباب II - تدابير تعزيز التعاون

القسم 1 - المبادئ العامة المطبقة على الباب الثاني

المادة 5 - المبادئ العامة المطبقة على الباب الثاني

1. تتعاون الدول الأطراف بشكل متبادل وفقًا لأحكام هذا الباب إلى أقصى حد ممكن.

2. يشمل القسم 2 من هذا الباب المادتين 6 و 7. وينص على إجراءات تعزيز التعاون المباشر مع مقدمي الخدمات والكيانات الموجودة في أراضي دولة طرف أخرى. تسري مقتضيات القسم 2 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف المعنية.

3. يشمل القسم 3 من هذا الباب المادتين 8 و 9. وينص على إجراءات لتعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة. تسري مقتضيات القسم

3 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الطرف مقدم الطلب والطرف الذي يتلقاه.

4. يشمل القسم 4 من هذا الباب المادة 10. ينص على الإجراءات المتعلقة بالمساعدة المتبادلة في حالات الطوارئ. تسري مقتضيات القسم 4 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الطرف مقدم الطلب والطرف الذي يتلقاه.

5. يشمل القسم 5 من هذا الباب المادتين 11 و 12. تسري مقتضيات القسم 5 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الطرف مقدم الطلب والطرف الذي يتلقاه. ولا تسري أحكام القسم 5 في حالة وجود مثل هذه المعاهدة أو الترتيب، باستثناء ما هو منصوص عليه في المادة 12، الفقرة 7. ومع ذلك، يجوز للدول الأطراف المعنية أن تقرر بشكل متبادل تطبيق أحكام القسم 5 بدلاً من ذلك، إذا كانت المعاهدة أو الترتيب لا يحظر هذا الأمر.

6. عندما يُسمح للطرف متلقي الطلب، وفقًا لأحكام هذا البروتوكول، بجعل التعاون مشروطًا بوجود تجريم مزدوج، يعتبر هذا الشرط مستوفى، بغض النظر عما إذا كانت قوانينه تضع الجريمة ضمن نفس فئة الجرائم أو تسميها بنفس المصطلحات التي يستخدمها الطرف الطالب، إذا كان السلوك الكامن وراء الجريمة التي يتم طلب المساعدة من أجلها يعتبر جريمة جنائية بموجب قوانينه.

7. لا تقيد الأحكام الواردة في هذا الباب التعاون بين الدول الأطراف، أو بين الأطراف ومقدمي الخدمات أو الكيانات الأخرى، من خلال الاتفاقات أو الترتيبات أو الممارسات الأخرى المعمول بها أو القانون الوطني.

القسم 2 - إجراءات تعزيز التعاون المباشر مع مقدمي الخدمات وغيرهم من الكيانات في الأطراف الأخرى

المادة 6 - طلب معلومات حول تسجيل اسم نطاق

1. يجب على كل طرف أن يتبنى التدابير التشريعية وغيرها من التدابير التي قد تكون ضرورية لتمكين سلطاته المختصة، لأغراض التحقيقات أو الإجراءات الجنائية الخاصة، من إصدار طلب إلى أي كيان يقدم خدمات تسجيل أسماء النطاقات في أراضي طرف آخر للحصول على معلومات في حوزة الكيان أو تحت سيطرته من أجل تحديد مسجل اسم النطاق أو الاتصال به.

2. يجب على كل طرف اتخاذ ما قد يلزم من تدابير تشريعية وتدابير أخرى للسماح لأي كيان موجود فوق أراضيه بالكشف عن هذه المعلومات تلبية لطلب بموجب الفقرة 1، مع مراعاة الشروط المعقولة التي ينص عليها القانون المحلي.

3. يتضمن الطلب بموجب الفقرة 1 ما يلي:

أ. تاريخ إصدار الطلب وهوية وبيانات الاتصال بالسلطة المختصة التي أصدرته؛

ب. اسم النطاق الذي يتم البحث عن معلومات حوله وقائمة مفصلة بالمعلومات المطلوبة، بما في ذلك عناصر البيانات المحددة؛

ج. بيانًا يفيد بأن الطلب قد صدر وفقًا لهذا البروتوكول، وأن الحاجة إلى المعلومات ناجمة عن صلتها بتحقيق أو إجراء جنائي محدد وأن المعلومات لن تُستخدم إلا لهذا التحقيق أو الإجراء الجنائي المحدد؛

د. الأجل والطريقة التي يتم الكشف بها عن المعلومات وأي تعليمات إجرائية خاصة أخرى.

4. في حالة موافقة الكيان المعني، يجوز للطرف تقديم طلب بموجب الفقرة 1 في شكل إلكتروني. ويتطلب هذا الأمر توفير مستويات مناسبة من الأمن وإجراءات التحقق.

5. في حالة امتناع كيان مشار إليه في الفقرة 1 عن التعاون، يجوز للطرف الطالب أن يستفسر عن سبب عدم الكشف عن المعلومات المطلوبة. ويجوز للطرف الطالب أن يسعى إلى التشاور مع الطرف الذي يوجد الكيان فوق أراضيه، بهدف تحديد التدابير المتاحة للحصول على المعلومات.

6. يجب على كل طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به ، أو في أي وقت آخر ، إبلاغ الأمين العام لمجلس أوروبا بالسلطة المعينة لغرض التشاور بموجب الفقرة 5.

7. يقوم الأمين العام لمجلس أوروبا بإنشاء وتحديث سجل السلطات المعينة من قبل الدول الأطراف بموجب الفقرة 6. يجب على كل طرف الحرص دائما على صحة المعلومات الواردة في السجل المذكور.

المادة 7 - كشف المعلومات المتعلقة بالمشتركين

1. يتعين على كل دولة طرف اعتماد القدر الكافي من التدابير التشريعية وغيرها من الإجراءات التي قد تكون ضرورية للسماح لسلطاتها المختصة بإصدار أمر مباشر إلى مقدم خدمات يوجد مقره في أراضي دولة طرف أخرى من أجل الكشف عن معلومات المشترك المحددة والمخزنة في حيازة مقدم الخدمة أو تحت تحكمه، عندما تكون معلومات المشترك مطلوبة في تحقيقات أو إجراءات جنائية محددة تقوم بها سلطات الطرف المُصدر.

2. أ. يتعين على كل دولة طرف اعتماد القدر الكافي من التدابير التشريعية وغيرها من الإجراءات التي قد تكون ضرورية لمقدم الخدمة الموجود فوق أراضيها للكشف عن معلومات المشترك استجابة لأمر بموجب الفقرة 1.

ب. أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، يجوز لأي دولة طرف -فيما يتعلق بالأوامر الصادرة لمقدمي الخدمات الموجودين فوق أراضيها - إدراج التصريح التالي: "يجب أن يصدر الأمر بموجب المادة 7، الفقرة 1، من قبل، أو تحت إشراف، المدعي العام أو سلطة قضائية أخرى، أو أن يصدر بطريقة أخرى تحت إشراف مستقل".

3. يجب أن يشمل الأمر المنصوص عليه في الفقرة 1:

أ. سلطة الإصدار وتاريخه؛

ب. بيانًا بأن الأمر صدر وفقًا لأحكام هذا البروتوكول؛

ج. اسم مقدم (مقدمي) الخدمات المعني وعنوانه؛

د. الجرم (الجرائم) موضوع التحقيق أو الإجراءات الجنائية؛

هـ. السلطة التي تسعى للحصول على معلومات المشترك المحددة، إن لم تكن السلطة المصدرة؛

و. وصف تفصيلي لمعلومات المشترك المحددة المطلوبة.

4. ينبغي أن يكون الطلب بموجب الفقرة 1 مصحوبًا بالمعلومات التكميلية التالية:

أ. الأسس القانونية الوطنية التي تخول سلطة إصدار الأمر؛

ب. ملخص الأحكام القانونية والعقوبات المطبقة على الجريمة التي يتم التحقيق فيها أو موضوع المحاكمة؛

ج. معلومات الاتصال الخاصة بالسلطة التي يجب على مقدم الخدمة بعث معلومات المشترك إليها، والتي يمكنه أن يطلب منها مزيداً من المعلومات، أو أن يجيبها بطريقة أخرى؛

د. الأجل والطريقة التي يتم عبرها بعث معلومات المشترك؛

هـ. الإشارة إلى أي طلب احتفاظ بالبيانات تم تقديمه سابقا، بما في ذلك تاريخ الحفظ وأي رقم مرجعي معمول به؛

و. أي تعليمات إجرائية خاصة؛

ز. عند الاقتضاء، بيان بأن الإخطار المتزامن قد تم وفقًا للفقرة 5؛

ح. أي معلومات أخرى قد تساعد في الكشف عن معلومات المشترك.

5. أ. يجوز لأي دولة طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة المتعلق به، وفي أي وقت آخر، إخطار الأمين العام لمجلس أوروبا بأنه عند إصدار أمر بموجب الفقرة 1 لمقدم خدمات موجود فوق أراضيها، ينبغي على الطرف المعني، في كل حالة أو في ظروف معينة محددة، إخطاره فوريا بالأمر ومده بالمعلومات التكميلية ومخلص الوقائع المتعلقة بالتحقيق أو الإجراء.

ب. سواء طلب الطرف إخطاره بموجب الفقرة 5. أ أم لا، فقد يُطلب من مقدم الخدمات استشارة سلطات الطرف في ظروف محددة قبل كشف البيانات المطلوبة.

ج. يجوز للسلطات المبلغة بموجب الفقرة 5.أ أو التي يتم التشاور معها بموجب الفقرة 5.ب، دون تأخير لا داعي له، أن تطلب من مقدم الخدمة عدم الكشف عن المعلومات المطلوبة إذا:

أولا. كان كشفها سيضر بالتحقيقات أو الإجراءات الجنائية الجارية عند هذا الطرف؛ أو

ثانيا. وجب تطبيق شروط أو أسباب الرفض وفق المادة 25، الفقرة 4، والمادة 27، الفقرة 4، من الاتفاقية لأنه تم التماس معلومات المشترك عبر المساعدة المتبادلة.

د. السلطات التي تم إخطارها بموجب الفقرة 5.أ أو التي تم التشاور معها بموجب الفقرة 5.ب:

i. يجوز لـها طلب معلومات إضافية من السلطة المشار إليها في الفقرة 4. ج لأغراض تطبيق الفقرة 5.ج ولا يجوز لها كشفها لمقدم الخدمات دون موافقة تلك السلطة؛

ii. يجب عليها إبلاغ السلطة المشار إليها في الفقرة 4.ج على الفور إذا تم توجيه تعليمات إلى مزود الخدمة بعدم الكشف عن معلومات المشترك وإعطاء أسباب القيام بذلك.

هـ . تعين كل دولة طرف سلطة واحدة لتلقي الإخطار بموجب الفقرة 5. أ وتنفيذ الإجراءات الواردة في الفقرات 5.ب و 5. ج و 5. د. ويجب على الطرف، في الوقت الذي يتم فيه تقديم الإخطار إلى الأمين العام لمجلس أوروبا بموجب الفقرة 5. أ لأول مرة، إبلاغ الأمين العام بمعلومات الاتصال الخاصة بهذه السلطة.

ز. يقوم الأمين العام لمجلس أوروبا بإنشاء وتحديث سجل السلطات المعينة من قبل الأطراف وفقًا للفقرة 5. هـ وما إذا كانت تستلزم الإخطار بموجب الفقرة 5. أ وفي أي ظروف. يجب على كل طرف الحرص دائما على صحة المعلومات الواردة في السجل المذكور.

6. في حالة موافقة مقدم الخدمات، يجوز للدولة الطرف تقديم الطلب بموجب الفقرة 1 والمعلومات التكميلية بموجب الفقرة 4 في شكل إلكتروني. ويجوز لأي دولة

طرف تقديم الإخطار والمعلومات الإضافية بموجب الفقرة 5 في شكل إلكتروني. ويتطلب هذا الأمر توفير مستويات مناسبة من الأمن وإجراءات التحقق.

7. إذا أبلغ مقدم الخدمة السلطة المشار إليها في الفقرة 4.ج أنه لن يكشف عن معلومات المشترك المطلوبة، أو إذا لم يكشف عن معلومات المشترك استجابة للطلب بموجب الفقرة 1 في غضون ثلاثين يومًا من استلام الطلب أو داخل الأجل المنصوص عليه في الفقرة 4. د، مع اعتماد المدة الأطول في هذا الصدد، يجوز للسلطات المختصة للطرف المُصدر أن تسعى إلى إنفاذ الأمر فقط من خلال المادة 8 أو عبر أشكال أخرى من المساعدة المتبادلة. يجوز للأطراف أن تطلب من مقدم الخدمة تقديم سبب لرفض الكشف عن معلومات المشترك المطلوبة في الأمر.

8. يجوز لأي طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أن يعلن أن على الطرف المُصدر أن يسعى إلى الكشف عن معلومات المشترك من مقدم الخدمات قبل أن يطلبها بموجب المادة 8، ما لم يقدم الطرف المُصدر تفسيراً معقولاً لعدم القيام بذلك.

9. أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة، يجوز للطرف أن:

أ. يحتفظ بالحق في عدم تطبيق هذه المادة ؛ أو

ب. إذا كان الكشف عن أنواع معينة من أرقام الولوج بموجب هذه المادة غير متوافق مع المبادئ الأساسية لنظامها القانوني المحلي، أن تحتفظ بالحق في عدم تطبيق هذه المادة على هذه الأرقام.

القسم 3 – إجراءات تعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة

المادة 8 - تفعيل الأوامر الصادرة عن دولة طرف أخرى بشأن التقديم المعجل لمعلومات المشترك وبيانات الحركة

1. يجب على كل طرف أن يتبنى التدابير التشريعية وغيرها من التدابير الضرورية لتمكين سلطاته المختصة من إصدار أمر يتم تقديمه كجزء من الطلب الموجه لطرف آخر بغرض إجبار مقدم خدمات في إقليم الطرف المتلقي على تقديم:

أ. معلومات المشترك،

ب. بيانات الحركة

المحددة والمخزنة والموجودة في حيازة مقدم الخدمات أو تحت تحكمه، عندما تكون هذه المعلومات والبيانات ضرورية للتحقيقات أو الإجراءات الجنائية المحددة التي يقوم بها الطرف.

2. تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لإنفاذ أي أمر بموجب الفقرة 1 مقدم من الطرف الطالب.

3. يتضمن طلب الطرف الطالب الأمر المشار إليه في الفقرة 1 والمعلومات الداعمة وأية تعليمات إجرائية خاصة موجهة إلى الطرف متلقي الطلب.

أ. يجب أن يحدد الأمر:

i. السلطة المصدرة للأمر وتاريخه؛

ii. البيان الذي يؤكد صدور الأمر وفقًا لأحكام هذا البروتوكول ؛

iii. اسم مقدم (مقدمي) الخدمات المعني وعنوانه؛

vi. الجرم (الجرائم) موضوع التحقيقات أو الإجراءات الجنائية ؛

v. السلطة التي تسعى للحصول على المعلومات أو البيانات، إن لم تكن هي السلطة المصدرة؛

iv. الوصف التفصيلي للمعلومات أو البيانات المحددة المطلوبة.

ب. ينبغي أن تتضمن المعلومات الداعمة للأمر، المقدمة بغرض مساعدة الطرف المتلقي على تنفيذه والتي لا يجب كشفها لمقدم الخدمات دون موافقة الطرف الطالب، ما يلي:

i. الأسس القانونية الوطنية التي تخول للسلطة اختصاص إصدار الأمر؛

ii. مخلص الأحكام القانونية والعقوبات المطبقة على الجريمة التي يتم التحقيق فيها أو موضوع المحاكمة؛

iii. سبب اعتقاد الطرف الطالب أن مقدم الخدمة يمتلك البيانات أو يتحكم فيها؛

vi. ملخصًا للوقائع المتعلقة بالتحقيق أو الإجراء؛

v. صلة المعلومات أو البيانات بالتحقيق أو الإجراء؛

iv. العناصر التي تسمح بالاتصال بهيئة أو هيئات من أجل الحصول على المزيد من المعلومات؛

iiv. الإشارة إلى أي طلب احتفاظ بالمعلومات تم تقديمه سابقا، بما في ذلك تاريخ الحفظ وأي رقم مرجعي معمول به؛

iiiv. هل تم طلب المعلومات أو البيانات بوسائل أخرى في وقت سابق، وإذا كان الأمر كذلك، فبأي طريقة.

ج. يجوز للطرف الطالب أن يلتمس من الطرف المتلقي تنفيذ تعليمات إجرائية خاصة.

4. يجوز لأي دولة طرف أن تعلن أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة الخاص به، وفي أي وقت آخر، أن توفير المعلومات الداعمة الإضافية ضروري لتنفيذ الأوامر بموجب الفقرة 1.

5. يجب على الطرف المتلقي قبول الطلبات في شكل إلكتروني. ويتطلب هذا الأمر توفير مستويات مناسبة من الأمن وإجراءات التحقق قبل قبول الطلب.

6. أ. انطلاقاً من تاريخ استلام جميع المعلومات المحددة في الفقرتين 3 و 4، يجب على الطرف المتلقي بذل الجهود المناسبة لتبليغ مقدم الخدمات بالأمر في غضون خمسة وأربعين يومًا، إن لم يكن قبل ذلك، مع توجيه الأمر له بتوفير المعلومات المطلوبة في أجل:

i. عشرين يومًا بالنسبة لمعلومات المشترك؛

ii. خمسة وأربعين يومًا بالنسبة ببيانات حركة الاتصالات.

ب. يجب على الطرف المتلقي إرسال المعلومات أو البيانات المنتجة إلى الطرف الطالب دون تأخير لا داعي له.

7. إذا عجز الطرف المتلقي عن الامتثال للتعليمات المنصوص عليها في الفقرة 3.ج بالطريقة المطلوبة، يجب عليه إبلاغ الطرف الطالب على الفور، وإذا أمكن، تحديد الشروط التي ستمكنه من الامتثال للتعليمات، وبعد ذلك يقرر الطرف الطالب هل ينبغي تنفيذ الطلب أم لا.

8. يجوز للطرف المتلقي استعمال الأسباب المنصوص عليها في المادة 25، الفقرة 4، أو المادة 27، الفقرة 4، من الاتفاقية من أجل رفض تنفيذ طلب أو فرض شروط يراها ضرورية للسماح بتنفيذه. ويجوز للطرف المتلقي تأجيل تنفيذ طلب بناء على الأسباب المحددة بموجب الفقرة 5 من المادة 27 من الاتفاقية. يجب على الطرف المتلقي إخطار الطرف الطالب في أقرب وقت ممكن بالرفض أو الشروط أو التأجيل. يجب على الطرف المتلقي أيضًا إخطار الطرف الطالب بالظروف الأخرى التي من المحتمل أن تؤخر تنفيذ الطلب بشكل كبير. وتسري مقتضيات الفقرة 2 (ب) من المادة 28 من الاتفاقية على هذه المادة.

9. أ. إذا لم يتمكن الطرف الطالب من الامتثال لشرط يفرضه الطرف المتلقي وفق الفقرة 8، ينبغي عليه إبلاغ الطرف المتلقي على الفور. يجب على الطرف المتلقي بعد ذلك تحديد ما إذا كان ينبغي مع ذلك تقديم المعلومات أو المواد المطلوبة أم لا.

ب. إذا وافق الطرف الطالب على الشرط، يتعين عليه الالتزام به. ويجوز للطرف المتلقي الذي يقدم معلومات أو مواد تخضع لمثل هذا الشرط أن يطلب من الطرف الطالب تقديم شروحات حول استخدام هذه المعلومات أو المواد ذات العلاقة بهذا الشرط..

10. يجب على كل طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أو في أي وقت آخر، إبلاغ الأمين العام لمجلس أوروبا ببيانات الاتصال الخاصة بالسلطة المعينة وفقا للفقرة 5 من أجل:

أ. تقديم طلب بموجب هذه المادة؛

ب. تلقي أمر بموجب هذه المادة.

11. يجوز لأي دولة طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أن يعلن أنه يشترط أن يتم بعث الطلبات المشار إليها في هذه المادة من خلال السلطة أو السلطات المركزية للطرف الطالب، أو من قبل أي سلطة أخرى يتم تحديدها بشكل متبادل بين الطرفين المعنيين.

12. يقوم الأمين العام لمجلس أوروبا بإنشاء سجل السلطات المعينة من قبل الأطراف بموجب الفقرة 10 ويحرص على تحديثه. ويجب على كل دولة طرف الحرص دائما على صحة المعلومات الواردة في السجل المذكور.

13. أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة، يجوز لأي دولة طرف التحفظ على تطبيق هذه المادة على بيانات حركة الاتصالات.

المادة 9 - الكشف المعجل عن بيانات الكمبيوتر المخزنة في حالة الطوارئ

1. أ. يجب على كل طرف أن يتبنى التدابير التشريعية وغيرها من الإجراءات التي قد تكون ضرورية، في حالة الطوارئ، حتى تتمكن نقطة الاتصال التي تعمل على مدار الساعة طوال أيام الأسبوع، المنصوص عليها في المادة 35 من الاتفاقية ("نقطة الاتصال") من إرسال طلب إلى نقطة اتصال تابعة لدولة طرف أخرى أو تلقي طلب من هذه الأخيرة من أجل التمتع بمساعدة فورية في الحصول من مقدم الخدمات الموجود فوق تراب تلك الدولة الطرف على الكشف المعجل عن بيانات الكمبيوتر المحددة والمخزنة، في حوزته أو التي تخضع لتحكمه، دون طلب المساعدة القضائية المتبادلة.

ب. يجوز لأي دولة طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أن يعلن أنه لن يقوم بتنفيذ الطلبات المقدمة بموجب الفقرة 1. أ بشأن الكشف عن معلومات المشترك فقط.

2. يعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتخول، وفقاً للفقرة 1:

أ. لسلطاتها حق الحصول على بيانات من مقدم خدمات موجود على أراضيها بناءً على طلب بموجب الفقرة 1؛

ب. لمقدم الخدمات الموجود على أراضيها حق الكشف عن البيانات المطلوبة لسلطاته استجابة لطلب بموجب الفقرة 2. أ؛

ج. لسلطاتها حق تقديم البيانات المطلوبة للطرف الطالب.

3. يجب أن يشمل الأمر المقدم وفقا للفقرة 1:

أ. الجهة المختصة التي تطلب البيانات وتاريخ إصدار الطلب.

ب. بيانًا بأن الأمر صدر وفقًا لأحكام هذا البروتوكول؛

ج. اسم وعنوان مقدم (مقدمي) الخدمات الذي يمتلك البيانات المطلوبة أو الذي يتحكم فيها؛

د. الجرم (الجرائم) التي تخضع للتحقيق أو الإجراءات الجنائية وإشارة إلى المقتضيات القانونية المتعلقة بها والعقوبات السارية؛

هـ. وقائع كافية لإثبات وجود حالة طوارئ وكيفية ارتباط البيانات المطلوبة بها؛

و. وصفًا تفصيليًا للبيانات المطلوبة؛

ز. أي تعليمات إجرائية خاصة؛

ح. أي معلومات أخرى قد تساعد في الكشف عن البيانات المطلوبة.

4. يجب على الطرف المتلقي قبول الطلبات في شكل إلكتروني. يجوز للطرف قبول الطلبات الموجهة إليه شفهيا وأن يشترط تأكيد الطلب على شكل إلكتروني. ويتطلب هذا الأمر توفير مستويات مناسبة من الأمن وإجراءات التحقق قبل قبول الطلب.

5. يجوز لأي طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أن يعلن أنه يشترط على الأطراف الطالبة، بعد تنفيذ الطلب، تقديم الطلب وأي معلومات تكميلية يتم إرسالها لدعمه، في الشكل وعبر القناة التي يحددهما الطرف المتلقي والتي قد تشمل المساعدة القضائية المتبادلة.

6. يجب على الطرف المتلقي إبلاغ الطرف الطالب بقراره بشأن الطلب الموجه وفق الفقرة 1 على وجه السرعة، وعند الاقتضاء، ينبغي عليه أن يحدد الشروط التي يفرضها لتسليم البيانات وجميع أشكال التعاون الأخرى المتاحة.

7. أ. إذا لم يتمكن الطرف الطالب من الامتثال لشرط يفرضه الطرف المتلقي وفقا للفقرة 6، ينبغي عليه إبلاغ الطرف المتلقي على الفور. ويجب على الطرف

المتلقي بعد ذلك تحديد ما إذا كان ينبغي مع ذلك تقديم المعلومات أو المواد المطلوبة أم لا. إذا وافق الطرف الطالب على الشرط، يتعين عليه الالتزام به.

ب. يجوز للطرف المتلقي الذي يقدم معلومات أو مواد تخضع لمثل هذا الشرط أن يطلب من الطرف الطالب تقديم شروحات حول استخدام المعلومات أو المواد ذات العلاقة بهذا الشرط.

القسم 4 - الإجراءات المتعلقة بالمساعدة المتبادلة في حالات الطوارئ

المادة 10 - المساعدة المتبادلة في حالات الطوارئ

1. يجوز لكل دولة طرف طلب المساعدة المتبادلة على وجه السرعة عندما يرى أن هناك حالة طوارئ. ويجب أن يتضمن الطلب بموجب هذه المادة، بالإضافة إلى المحتويات الأخرى المطلوبة، وصفًا للوقائع التي تثبت وجود حالة طارئة وكيفية ارتباط المساعدة المتبادلة المطلوبة بها.

2. يجب على الطرف المتلقي قبول الطلبات في شكل إلكتروني. ويتطلب هذا الأمر توفير مستويات مناسبة من الأمن وإجراءات التحقق قبل قبول الطلب.

3. يجوز للطرف متلقي الطلب أن يطلب، على وجه السرعة، معلومات تكميلية من أجل تقييم الطلب. يجب على الطرف الطالب تقديم هذه المعلومات التكميلية على وجه السرعة.

4. بمجرد الاقتناع بوجود حالة طوارئ واستيفاء المتطلبات الأخرى للمساعدة المتبادلة، ينبغي على الطرف المتلقي الاستجابة للطلب على وجه السرعة.

5. يجب على كل دولة طرف أن تضمن تكليف شخص من سلطتها المركزية أو السلطات الأخرى المسؤولة عن الاستجابة لطلبات المساعدة المتبادلة، وأن يكون متاحاً على مدار الساعة طوال أيام الأسبوع لغرض الاستجابة للطلبات الموجهة بموجب هذه المادة.

6. يجوز للسلطة المركزية أو السلطات الأخرى المسؤولة عن المساعدة المتبادلة لدى الطرفين الطالب والمتلقي أن تقرر إمكانية بعث نتائج تنفيذ طلب المساعدة بموجب هذه المادة، أو نسخة أولية منها، إلى الطرف الطالب عبر قناة أخرى غير تلك التي استخدمت في تقليه.

7. في حالة عدم وجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول بين الطرفين الطالب والمتلقي، تسري على هذه المادة مقتضيات المادة 27، الفقرات 2 (ب) و 3 إلى 8، والفقرات 2 إلى 4 من المادة 28 من الاتفاقية.

8. في حالة وجود معاهدة أو ترتيب مماثل، يجب استكمال مقتضيات هذه المادة بأحكام هذه المعاهدة أو الترتيب ما لم يقرر الطرفان المعنيان بشكل متبادل تعويضها جزئيا أو كليا بأحكام الاتفاقية المشار إليها في الفقرة 7 من هذه المادة.

9. يحق لكل دولة طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة، أن تعلن أنه يجوز إرسال الطلبات مباشرة إلى سلطاتها القضائية، أو عبر قنوات المنظمة الدولية للشرطة الجنائية (الإنتربول)، أو عبر نقطة الاتصال المتاحة على مدار الساعة طوال أيام الأسبوع المنشأة بموجب المادة 35 من الاتفاقية. في مثل هذه الحالات، يجب إرسال نسخة في نفس الوقت إلى السلطة المركزية لدى الطرف المتلقي من خلال السلطة المركزية للطرف الطالب. إذا تم إرسال طلب مباشرة إلى سلطة قضائية لدى الطرف المتلقي، وكانت تلك السلطة غير مختصة في التعامل مع الطلب، فيجب عليها إحالته على السلطة الوطنية المختصة وإبلاغ الطرف الطالب بذلك مباشرة.

القسم 5 - الإجراءات المتعلقة بالتعاون الدولي في حالة عدم وجود اتفاقيات دولية سارية المفعول

المادة 11 - التداول بالفيديو

1. يجوز للطرف الطالب أن يلتمس أخذ أقوال شاهد أو خبير عبر التداول بالفيديو، ويجوز للطرف المتلقي أن يسمح بذلك. يتشاور الطرفان الطالب والمتلقي من أجل تسهيل حل أي مشاكل قد تنشأ بشأن تنفيذ الطلب، بما في ذلك، حسب الاقتضاء: الطرف الذي يقوم بإدارة العملية؛ والسلطات والأشخاص الذين يطلب حضورهم؛ وهل يجب أن يطلب أحد الطرفين أو كليهما من الشاهد أو الخبير أداء قسم معين أو إعطائه تحذيرات أو تعليمات؛ وطريقة استجواب الشاهد أو الخبير؛ والطريقة التي يتم بها ضمان حقوق الشاهد أو الخبير على النحو الواجب؛ ومعالجة المسائل المتصلة بالامتيازات أو الحصانة؛ ومعالجة الاعتراضات على الأسئلة أو الردود؛ وهل يقوم أحد الطرفين أو كليهما بتوفير خدمات الترجمة التحريرية والشفوية والنسخ.

2. أ. يجب على السلطات المركزية لدى الطرفين الطالب والمتلقي الاتصال ببعضها البعض مباشرة لأغراض هذه المادة. ويمكن للطرف المتلقي قبول الطلبات في شكل إلكتروني. ويتطلب هذا الأمر توفير مستويات مناسبة من الأمن وإجراءات التحقق قبل قبول الطلب.

ب. يجب على الطرف المتلقي إبلاغ الطرف الطالب بأسباب عدم تنفيذ الطلب أو تأخير تنفيذه، وتسري مقتضيات الفقرة 8 من المادة 27 من الاتفاقية على هذه المادة. دون المساس بأي شرط آخر قد يفرضه الطرف المتلقي وفقًا لهذه المادة، تسري الفقرات 2 إلى 4 من المادة 28 من الاتفاقية على هذه المادة.

3. يحرص الطرف المتلقي الذي يقدم المساعدة بموجب هذه المادة على ضمان حضور الشخص المطلوب شهادته أو بيانه. عند الاقتضاء، يجوز للطرف

المتلقي، في الحدود التي تسمح بها قوانينه، اتخاذ التدابير اللازمة لإجبار شاهد أو خبير على المثول لدى الطرف المتلقي في الوقت والمكان المحددين.

4. يجب اتباع الإجراءات المتعلقة بالتداول بالفيديو المحددة من قبل الطرف الطالب، إلا إذا كانت غير متوافقة مع القانون الوطني للطرف المتلقي. في حالة وجود تعارض، أو إذا لم يقم الطرف الطالب بتحديد مواصفات الإجراء، يجب على الطرف المتلقي تطبيق الإجراء المنصوص عليه في قانونه الوطني ما لم يتفق الطرفان على خلاف ذلك.

5. دون الإخلال بأي اختصاص منصوص عليه في القانون الوطني للطرف الطالب، عندما يقوم الشاهد أو الخبير خلال التداول بالفيديو:

أ. بالإدلاء عمداً ببيان كاذب رغم إلزام الطرف المتلقي له بالإدلاء بشهادته بصدق، وفقًا لقانونه الداخلي؛

ب. برفض الإدلاء بشهادته رغم أن الطرف المتلقي ألزمه بذلك وفقا لقانونه الداخلي؛ أو

ج. بارتكاب سلوك آخر محظور بموجب القانون الوطني للطرف المتلقي في سياق هذه الإجراءات؛

يخضع الشخص للعقوبة في الطرف المتلقي بنفس الطريقة كما لو كان هذا الفعل قد ارتكب في سياق إجراءاته الوطنية.

6. أ. ما لم يتفق الطرفان الطالب والمتلقي على خلاف ذلك، يتحمل الطرف المتلقي جميع التكاليف المتعلقة بتنفيذ الطلب بموجب هذه المادة، باستثناء:

أولا. أتعاب الشاهد الخبير.

ثانيا. تكاليف الترجمة التحريرية والشفوية والنسخ؛

ثالثا. التكاليف ذات الطبيعة الاستثنائية.

ب. إذا استلزم تنفيذ طلب تكاليف ذات طبيعة استثنائية، يجب على الطرفين الطالب والمتلقي التشاور مع بعضهما البعض من أجل تحديد الشروط التي يمكن وفقها تنفيذ الطلب.

7. في حالة وجود اتفاق بين الطرفين الطالب المتلقي:

أ. يمكن تطبيق أحكام هذه المادة لأغراض التداول السمعي؛

ب. يمكن استخدام تقنية التداول بالفيديو للأغراض أو لجلسات استماع، مختلفة عن تلك الموضحة في الفقرة 1، بما في ذلك لأغراض التعرف على أشخاص أو أشياء.

8. عندما يختار الطرف المتلقي السماح بسماع شخص مشتبه به أو متهم، يجوز له وضع شروط وضمانات خاصة فيما يتعلق بأخذ شهادة أو إفادة من هذا الشخص أو التنصيص على إخطارات أو تطبيق تدابير إجرائية بشأنه.

المادة -12 فرق التحقيق المشتركة والتحقيقات المشتركة

1. بالاتفاق المتبادل، يجوز للسلطات المختصة لطرفين أو أكثر إنشاء وتشغيل فريق تحقيق مشترك في أراضيها لتسهيل التحقيقات أو الإجراءات الجنائية، إذا تبين أن للتنسيق المعزز فائدة خاصة. يتم تحديد السلطات المختصة من قبل الأطراف المعنية.

2. يجب أن تكون الإجراءات والشروط التي تحكم عمل فرق التحقيق المشتركة متفقا عليها بين السلطات المختصة، مثل أغراضها وتكوينها ومهامها ومدتها وأي فترات تمديد ومقرها وتنظيمها وشروط جمع ونقل واستخدام المعلومات أو الأدلة وشروط السرية وشروط مشاركة سلطات الطرف في أنشطة التحقيق التي تجري في إقليم طرف آخر.

3. يجوز لأي طرف أن يعلن أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة، أنه ينبغي الحصول على توقيع أو موافقة سلطته المركزية على اتفاقية إنشاء الفريق.

4. يجب على تلك السلطات المختصة والمشاركة التواصل مباشرة، باستثناء أنه يجوز للأطراف أن تحدد بشكل متبادل قنوات أخرى مناسبة للاتصال عندما تتطلب الظروف الاستثنائية مزيدًا من التنسيق المركزي.

5. عندما يتعين إجراء التحقيق في أراضي أحد الأطراف المعنية، يجوز للسلطات المشاركة من هذا الطرف أن تطلب من سلطاتها القيام بذلك دون أن تضطر الأطراف الأخرى إلى تقديم طلب للمساعدة المتبادلة. يجب تنفيذ هذه الإجراءات من قبل سلطات هذا الطرف فوق أراضيه وفق الشروط نفسها السارية المفعول في القانون الداخلي على تحقيق وطني.

6. يجوز رفض أو تقييد استخدام المعلومات أو الأدلة التي تقدمها السلطات المشاركة باسم أحد الأطراف إلى السلطات المشاركة باسم الأطراف المعنية الأخرى، وذلك وفق الشروط المنصوص عليها في الاتفاق المذكور في الفقرتين 1 و2. إذا لم يحدد هذا الاتفاق شروطًا لرفض أو تقييد الاستخدام، يجوز للأطراف استخدام المعلومات أو الأدلة المقدمة:

أ. للأغراض التي تم إبرام الاتفاق من أجلها؛

ب. للكشف عن جرائم جنائية غير تلك التي تم إبرام الاتفاقية بشأنها والتحقيق فيها ومقاضاة مرتكبيها، بشرط الحصول على موافقة مسبقة من السلطات التي تقدم المعلومات أو الأدلة. ومع ذلك، لا تكون الموافقة مطلوبة عندما تتطلب المبادئ القانونية الأساسية للطرف الذي يستخدم المعلومات أو الأدلة الكشف عن المعلومات أو الأدلة لحماية حقوق شخص متهم في إطار إجراءات جنائية. في هذه الحالة، يجب على تلك السلطات إخطار السلطات التي قدمت المعلومات أو الأدلة دون تأخير لا داعي له؛ أو

ج. لمنع حدوث طارئ. في هذه الحالة، يجب على السلطات المشاركة التي تلقت المعلومات أو الأدلة إخطار السلطات المشاركة التي قدمت المعلومات أو الأدلة دون تأخير لا مبرر له، ما لم يتم الاتفاق على خلاف ذلك بشكل مشترك.

7. في حالة عدم وجود الاتفاق المذكور في الفقرتين 1 و 2، يمكن إجراء تحقيقات مشتركة وفق شروط متفق عليها بشكل مشترك على أساس كل حالة على حدة. تسري مقتضيات هذه الفقرة سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف المعنية..

الباب III - الشروط والضمانات

المادة 13 - الشروط والضمانات

وفقًا للمادة 15 من الاتفاقية، يحرص كل طرف أن يخضع وضع وتنفيذ وتطبيق الصلاحيات والإجراءات المنصوص عليها في هذا البروتوكول للشروط والضمانات المنصوص عليها في قانونه المحلي، والتي يجب أن توفر الحماية الكافية لحقوق الإنسان والحريات.

المادة 14 - حماية البيانات الشخصية

1. نطاق التطبيق

أ. باستثناء ما هو منصوص عليه في الفقرتين 1. ب و ج، يجب على كل طرف معالجة البيانات الشخصية التي يتلقاها بموجب هذا البروتوكول وفقًا للفقرات 2 إلى 15 من هذه المادة.

ب. إذا كان الطرفان المرسل والمتلقي، وقت استلام البيانات الشخصية بموجب هذا البروتوكول، ملزمين بشكل متبادل بـاتفاقية دولية تعد إطارًا شاملاً بينهما لحماية البيانات الشخصية، حيث تسري على نقل البيانات الشخصية لغرض منع الجرائم الجنائية والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها، وتضمن أن معالجة البيانات الشخصية بموجب تلك الاتفاقية تتوافق مع متطلبات تشريعات حماية البيانات في الطرفين، تسري شروط هذه الاتفاقية، بالنسبة للتدابير التي تقع في نطاقها، على البيانات الشخصية المستلمة بموجب البروتوكول بدلاً من الفقرات 2 إلى 15، ما لم يتم الاتفاق على خلاف ذلك بين الطرفين المعنيين.

ج. إذا لم يكن الطرفان المرسل والمتلقي ملزمين بشكل متبادل بموجب اتفاق على النحو الوارد في الفقرة 1.ب، يجوز لهما أن يقررا بشكل متبادل أن يتم نقل البيانات الشخصية بموجب هذا البروتوكول وفق اتفاقات أو ترتيبات أخرى بين الطرفين المعنيين، بدلا من الفقرات 2 إلى 15.

د. يجب على كل دولة طرف أن تأخذ في الاعتبار أن معالجة البيانات الشخصية وفقًا للفقرتين 1. أ و1. ب تلبي متطلبات الإطار القانوني لحماية البيانات الشخصية المعمول به في عمليات النقل الدولية للبيانات الشخصية، وأنه لا يلزم الحصول على إذن إضافي للنقل بموجب هذا الإطار القانوني. لا يجوز لأي دولة طرف أن ترفض أو تمنع نقل البيانات إلى دولة طرف أخرى بموجب هذا البروتوكول سوى لأسباب متصلة بحماية البيانات: بموجب الشروط المنصوص عليها في الفقرة 15، عندما تسري مقتضيات الفقرة 1. أ؛ أو بموجب شروط الاتفاق أو الترتيب المشار إليه في الفقرتين 1.ب أو ج، عندما تنطبق إحدى هاتين الفقرتين.

هـ . لا يوجد في هذه المادة ما يمنع أي طرف من تطبيق ضمانات أقوى على معالجة سلطاته للبيانات الشخصية المستلمة بموجب هذا البروتوكول.

2. الغرض والاستخدام

أ. يجب على الطرف الذي تلقى البيانات الشخصية معالجتها للأغراض الموضحة في المادة 2. ولا يجوز له معالجة البيانات الشخصية لغرض غير متوافق مع هذه المادة، ولا معالجتها عندما لا يسمح إطاره القانوني بذلك. لا تخل هذه المادة بقدرة الطرف المرسل على فرض شروط إضافية بموجب هذا البروتوكول في حالة معينة، ومع ذلك، لا يجب أن تتضمن هذه الشروط شروطًا عامة لحماية البيانات.

ب. يجب على الطرف المتلقي أن يضمن، بموجب إطاره القانوني المحلي، أن البيانات الشخصية المطلوبة والمعالجة ذات صلة وليست مبالغا فيها مقارنة بأغراض هذه المعالجة.

3. الجودة والسلامة

يجب على كل طرف اتخاذ خطوات معقولة لضمان الحفاظ على البيانات الشخصية بطريقة دقيقة وكاملة، والحرص على أنها محدثة بالقدر الضروري والمناسب لتتم معالجتها طبقا للقانون، مع مراعاة الأغراض التي تتم معالجتها من أجلها.

4. البيانات الحساسة

لا يجوز أن يقوم أحد الأطراف بمعالجة بيانات شخصية تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية أو غيرها من المعتقدات أو العضوية النقابية؛ وكذا البيانات الجينية والبيانات البيومترية الحساسة في ضوء المخاطر التي تنطوي عليها؛ أو البيانات الشخصية المتعلقة بالصحة أو الحياة الجنسية؛ إلا في ظل ضمانات مناسبة للوقاية من مخاطر التأثير الضار غير المبرر الناجم عن استخدام هذه البيانات، ولا سيما ضد التمييز غير القانوني.

5. آجال الاحتفاظ بالبيانات

ينبغي على كل دولة طرف الاحتفاظ بالبيانات ذات الطابع الشخصي طوال المدة الضرورية والمناسبة فقط، وذلك بالنظر إلى أغراض معالجة المعطيات المنصوص عليها في الفقرة 2. من أجل الوفاء بهذا الالتزام، يجب أن ينص إطاره القانوني المحلي على آجال محددة أو على مراجعة دورية للحاجة إلى استمرار الاحتفاظ بالبيانات.

6. القرارات الآلية

إن القرارات التي ينتج عنها تأثير سلبي كبير على المصالح ذات الصلة للفرد الذي تتعلق به البيانات الشخصية لا تستند فقط على المعالجة الآلية للبيانات الشخصية، ما لم يُسمح بذلك بموجب القانون المحلي وبضمانات مناسبة تتضمن إمكانية الحصول على تدخل بشري.

7. أمن البيانات والحوادث الأمنية

أ. يجب على كل دولة طرف الحرص على توفير التدابير التكنولوجية والمادية والتنظيمية المناسبة لحماية البيانات ذات الطابع الشخصي، ولا سيما ضد الضياع أو الوصول العرضي أو غير المصرح به أو الكشف أو التغيير أو التدمير ("الحادث الأمني").

ب. بمجرد العلم بحادثة أمنية تنطوي على تهديد كبير بوقوع ضرر مادي أو غير مادي على الأفراد أو على الطرف الآخر، يجب على الطرف المتلقي تقييم احتمالية حدوثه ونطاقه على الفور، وينبغي عليه اتخاذ الإجراءات المناسبة على الفور لتخفيف هذا الضرر. ويجب أن تشمل هذه الإجراءات إخطار السلطة المسؤول عن نقل المعطيات أو، لأغراض الباب II، القسم 2، السلطة أو السلطات المعينة وفقًا للفقرة 7. ج. ومع ذلك، قد يتضمن الإخطار قيودًا مناسبة بشأن الإرسال اللاحق للإخطار؛ وقد يتم تأخيره أو التخلي عنه عندما قد يعرض الأمن القومي للخطر، أو يجوز تأخيره عندما يعرض تدابير حماية السلامة العامة للخطر. ويجب أن تشمل هذه الإجراءات أيضًا إخطارًا الشخص المعني، ما لم يتخذ الطرف التدابير المناسبة لتجنب أي تهديد كبير. يجوز تأخير إخطار الفرد أو التخلي عن ذلك وفقًا للشروط المنصوص عليها في الفقرة 12. أ. أولا. يجوز للطرف المُخطَر أن يطلب التشاور والحصول على المعلومات الإضافية المتعلقة بالحادث والرد عليها.

ج. يجب على كل طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أو في أي وقت آخر، إبلاغ الأمين العام لمجلس أوروبا بالسلطة أو السلطات التي تستقبل الإخطار المنصوص عليه في الفقرة 7.ب، لأغراض القسم 2 من الباب II، كما يمكن تغييرها لاحقا.

8. حفظ السجلات

يحتفظ كل طرف بسجلات أو تتوفر لديه وسائل مناسبة أخرى لإثبات كيفية الوصول إلى البيانات ذات الطابع الشخصي وطريقة استخدامها والكشف عنها في حالة معينة.

9. التبادل اللاحق للبيانات بين هيئات طرف معين

أ. عندما تنقل سلطة تابعة لطرف ما بيانات ذات طابع شخصي مستلمة في الأصل بموجب هذا البروتوكول إلى سلطة أخرى تابعة لذلك الطرف، ينبغي على هذا الأخيرة أن تقوم بمعالجتها وفقا لهذه المادة، وذلك مع مراعاة الفقرة 9.ب.

ب. بصرف النظر عن الفقرة -9أ، يجوز للطرف الذي أعرب عن تحفظات وفقا للمادة 17 أن يقدم بيانات ذات طابع شخصي تلقاها إلى الولايات المكونة له أو إلى كيانات إقليمية مماثلة شريطة أن يعتمد الطرف تدابير لكي تواصل السلطات المتلقية حماية البيانات بفعالية، وذلك من خلال توفير مستوى حماية للبيانات مماثل لذلك الذي توفره هذه المادة.

ج. وفي حالة وجود مؤشرات على التنفيذ غير السليم لهذه الفقرة، يجوز للطرف المرسل أن يطلب التشاور والحصول على معلومات ذات صلة بشأن تلك المؤشرات.

10. النقل اللاحق للبيانات إلى دولة أخرى أو منظمة دولية أخرى

أ. لا يجوز للطرف المتلقي نقل البيانات الشخصية إلى دولة أخرى أو منظمة دولية أخرى إلا بإذن مسبق من السلطة المرسلة أو، لأغراض الباب II، القسم 2، السلطة أو السلطات المعينة عملا بالفقرة 10، ب.

ب. يجب على كل دولة طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أو في أي وقت آخر، إبلاغ الأمين العام لمجلس أوروبا بالسلطة أو السلطات المخولة بمنح الترخيص لأغراض القسم 2 من الباب II، كما يمكن تغييرها لاحقا.

11. الشفافية والإخطار

أ. يحرص كل طرف على الإخطار من خلال نشر إشعارات عامة، أو من خلال إخطار شخصي موجه إلى الشخص الذي تم جمع البيانات ذات الطابع الشخصي الخاصة به، فيما يتعلق بما يلي:

i. الأساس القانوني للمعالجة والغرض منها؛

ii. أي فترات حفظ أو مراجعة وفقا للفقرة 5، حسب الاقتضاء؛

iii. المتلقي أو فئات المتلقين الذين يتم الكشف لهم عن هذه البيانات؛

vi. طريقة الوصول إلى البيانات وتصحيحها والطعن فيها.

ب. يجوز للطرف إخضاع شرط الإخطار الشخصي لقيود معقولة بموجب إطاره القانوني الوطني وفقا للشروط المنصوص عليها في الفقرة 12. أ. أولا.

ج. عندما يشترط الإطار القانوني الداخلي المعمول به في الطرف المرسل توجيه إشعار شخصي إلى الشخص الذي قدمت بياناته إلى طرف آخر، يتخذ الطرف المرسل التدابير المناسبة لإبلاغ الطرف الآخر بهذا الشرط عند القيام بنقل المعطيات وكذا مده بمعلومات الاتصال المناسبة. ولا يجوز توجيه الإشعار الشخصي إذا طلب الطرف الآخر الحفاظ على سرية نقل البيانات، حيثما تنطبق الشروط التقييدية المنصوص عليها في الفقرة 12-أ-i. وبمجرد تصير هذه القيود غير سارية المفعول وأن يصبح نقل البيانات ذات الطابع الشخصي ممكنا، يتخذ الطرف الآخر التدابير لإبلاغ الطرف المرسل. وإذا لم يكن قد تم إبلاغ الطرف المرسل، يحق له تقديم طلبات إلى الطرف المتلقي ويقوم هذا الأخير بإخبار الطرف المرسل هل مازالت القيود سارية المفعول أم لا.

12. الوصول إلى البيانات وتصحيحها

أ. يكفل كل طرف لأي فرد تم استلام بياناته الشخصية بموجب هذا البروتوكول، وفقا لعمليات محددة في إطاره القانوني الوطني ودون تأخير لا مبرر له، الحق في طلب وفي ضمان:

i. الوصول إلى نسخة مكتوبة أو إلكترونية من الوثائق المحفوظة بخصوص هذا الشخص، بما يشمل بياناته الشخصية والمعلومات المتاحة التي تبين الأساس القانوني للمعالجة وأغراضها وفترات الاحتفاظ بالمعطيات ومستلميها أو فئات متلقيها ("حق الوصول")، فضلا عن المعلومات المتعلقة بالخيارات المتاحة للانتصاف؛ شريطة أن يخضع الوصول في حالة معينة إلى تطبيق قيود متناسبة مسموح بها في الإطار القانوني الداخلي، تكون هناك حاجة إليها، وقت اتخاذ القرار، لحماية حقوق الغير وحرياتهم أو تحقيق أهداف هامة ذات صلة بالمصلحة العامة، مع إيلاء الاعتبار الواجب للمصالح المشروعة للفرد المعني؛

ii. التصويب عندما تكون البيانات ذات الطابع الشخصي غير دقيقة أو تمت معالجتها بطريقة غير ملائمة، وينبغي أن يشمل التصويب، حسب ما هو مناسب ومعقول أخذا في الحسبان أسباب الطلب أو السياق الخاص للمعالجة، التصحيح أو الاستكمال أو المحو أو حجب الهوية أو تقييد المعالجة أو التجميد.

ب. إذا رفضت دولة طرف منح حق الوصول إلى البيانات أو تصويبها أو تقييدها، يجب عليها إخطار الشخص المعني عبر خطاب مكتوب، يمكن أن يكون في شكل إلكتروني، دون تأخير لا داعي له، بالقرار سواء كان رفضا أو فرضا لقيود. وينبغي على الطرف المعني الإدلاء بأسباب هذا الرفض أو التقييد وتوفير معلومات حول الخيارات المتاحة للانتصاف. يجب أن تقتصر أي نفقات يتم تكبدها للحصول على حق الوصول على ما هو معقول وغير مفرط.

13. سبل الانتصاف القضائية وغير القضائية

يجب أن يكون لدى كل طرف سبل انتصاف قضائية وغير قضائية فعالة لتوفير التعويض عن انتهاكات هذه المادة.

14. الرقابة

يجب أن يكون لكل طرف سلطة عامة واحدة أو أكثر تمارس، مجتمعة أو منفصلة، وظائف وصلاحيات الرقابة المستقلة والفعالة على التدابير المنصوص عليها في هذه المادة. يجب أن تشمل وظائف واختصاصات هذه السلطات، مجتمعة أو منفصلة، صلاحية التحقيق والتعامل مع الشكاوى والقدرة على اتخاذ الإجراءات التصحيحية.

15. التشاور والتعليق

يجوز لأي دولة طرف تعليق نقل البيانات الشخصية إلى دولة طرف أخرى إذا كان لديها دليل قوي على أن الطرف الآخر ينتهك بشكل منهجي أو مادي شروط هذه المادة أو على احتمال وقوع خرق مادي وشيك. ولا يجوز تعليق نقل البيانات قبل نهاية مهلة معقولة لا يتم التوصل خلالها إلى حل. ومع ذلك، يجوز لأي طرف أن يعلق مؤقتًا عمليات النقل في حالة حدوث خرق منهجي أو مادي يشكل خطرًا كبيرًا ووشيكًا على حياة أو سلامة شخص ذاتي أو من شأنه التسبب في ضرر كبير على سمعته أو وضعيته المالية، ويجب عليه في هذه الحالة إخطار الطرف الآخر وبدء المشاورات معه على الفور. إذا لم تؤد المشاورات إلى حل، يجوز للطرف الآخر التصرف بالمثل وتعليق عمليات النقل إذا كان لديه دليل قوي على أن التعليق من قبل الطرف الأول مخالف لشروط هذه الفقرة. ويجب على الطرف المعلق رفع التعليق بمجرد معالجة الخرق الذي كان يبرره؛ ويجب حينها رفع أي تعليق متبادل لنقل المعطيات. ويجب الاستمرار في معالجة أي بيانات ذات طابع شخصي تم نقلها قبل التعليق وفق مقتضيات هذا البروتوكول.

الباب VI- أحكام ختامية

المادة 15 - الآثار المترتبة عن البروتوكول

1. أ. تسري مقتضيات الفقرة 2 من المادة 39 من الاتفاقية على هذا البروتوكول.

ب. فيما يتعلق بالأطراف الأعضاء في الاتحاد الأوروبي، يجوز لهذه الأطراف، في علاقاتها المتبادلة، تطبيق قوانين الاتحاد الأوروبي المنظمة للقضايا التي يتناولها هذا البروتوكول.

ج. لا تؤثر الفقرة 1. ب على التطبيق الكامل لهذا البروتوكول بين الأطراف التي هي أعضاء في الاتحاد الأوروبي والأطراف الأخرى.

2. تسري مقتضيات الفقرة 3 من المادة 39 من الاتفاقية على هذا البروتوكول.

المادة 16 - التوقيع والدخول حيز التنفيذ

1. يفتح هذا البروتوكول للتوقيع من قبل الدول التي وقعت على الاتفاقية والتي يجوز لها أن تعرب عن موافقتها على الالتزام إما عبر:

   أ. التوقيع دون تحفظ عنـــد التصديق أو القبـــول أو الموافقـــة؛ أو

   ب. التوقيع الخاضع للتصديق أو القبول أو الموافقة، الذي يعقبه تصديق أو قبول أو موافقة.

2. تُودع صكوك التصديق أو القبول أو الموافقة لدى الأمين العام لمجلس أوروبا.

3. يدخل هذا البروتوكول حيز التنفيذ في اليوم الأول من الشهر الموالي لانقضاء فترة ثلاثة أشهر من التاريخ الذي تعبر فيه خمس دول عن موافقتها على الالتزام بالبروتوكول طبقاً لأحكام الفقرتين 1 و2 من هذه المادة.

4. ويدخل البروتوكول حيز التنفيذ، بالنسبة لأي دولة تعبر لاحقاً عن موافقتها على الالتزام به، في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ موافقتها على الالتزام بالبروتوكول طبقا لأحكام الفقرتين 1 و2 من هذه المادة.

المادة 17 - البند الاتحادي

1. يجوز للدولة الاتحادية الاحتفاظ بالحق في تحمل الالتزامات الناجمة عن هذا البروتوكول بما يتفق مع المبادئ الأساسية التي تحكم العلاقة بين حكومتها المركزية والولايات المكونة لها أو الكيانات الإقليمية الأخرى المماثلة، شريطة أن:

   أ. يطبق البروتوكول على الحكومة المركزية للدولة الاتحادية؛

   ب. لا يؤثر هذا التحفظ على الالتزامات بتوفير التعاون الذي تسعى إليه الأطراف الأخرى وفقًا لأحكام الباب II؛

   ج. تسري أحكام المادة 13 على الولايات المكونة للدولة الاتحادية أو الكيانات الإقليمية المماثلة الأخرى.

2. يجوز للطرف الآخر منع السلطات أو مقدمي الخدمات أو الكيانات الأخرى الموجودة في أراضيه من التعاون استجابة لطلب أو أمر مقدم مباشرة من قبل ولاية أو أي كيان إقليمي مماثل تابع لدولة اتحادية قدمت تحفظا بموجب الفقرة 1، ما لم تخطر الدولة الاتحادية الأمين العام لمجلس أوروبا بأن الولاية أو الكيان الإقليمي المماثل يطبق التزامات هذا البروتوكول الواجبة على الدولة الاتحادية. يقوم الأمين العام لمجلس أوروبا بإنشاء سجل لهذه الإخطارات، ويحرص على تحديثه.

3. لا يجوز للطرف الآخر منع السلطات أو مقدمي الخدمات أو الكيانات الموجودة في أراضيه من التعاون مع ولاية أو كيان إقليمي آخر مماثل على أساس تحفظ بموجب الفقرة 1، إذا تم تقديم أمر أو طلب عبر الحكومة المركزية أو تم إبرام اتفاقية إنشاء فريق تحقيق مشترك بموجب المادة 12 بمشاركة الحكومة المركزية. في مثل هذه الحالات، يتعين على الحكومة المركزية الوفاء بالالتزامات السارية للبروتوكول، شريطة أن تطبق، فيما يتعلق بحماية البيانات ذات الطابع الشخصي المقدمة إلى الولايات أو الكيانات الإقليمية المماثلة، أحكام المادة 14، الفقرة 9 فقط، أو، عند الاقتضاء، شروط الاتفاق أو الترتيب الوارد في المادة 14 ، الفقرة 1. ب أو 1. ج.

4. فيما يتعلق بأحكام هذا البروتوكول، التي يقع واجب تطبيقها على كاهل الولايات أو الكيانات الإقليمية المماثلة الأخرى، غير الملزمة من قبل النظام الدستوري الاتحادي باتخاذ تدابير تشريعية، يجب على الحكومة المركزية إبلاغ السلطات المختصة في ولاياتها بهذه الأحكام وتشجيعها على اتخاذ التدابير المناسبة لتطبيقها.

المادة 18 - التطبيق الإقليمي

1. يسري مفعول هذا البروتوكول على الإقليم أو الأقاليم المحددة في الإعلان الصادر عن الطرف وفقا للفقرتين 1 أو 2 من المادة 38 من الاتفاقية ما لم يتم سحب هذا الإعلان وفقا للمادة 38، الفقرة 3.

2. يجوز لأي طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع وثيقة التصديق أو القبول أو الموافقة الخاصة به، أن يعلن أن هذا البروتوكول لا ينطبق على واحد أو أكثر من الأقاليم المحددة في الإعلان الصادر عنه بموجب المادة 38، الفقرتين 1 و/أو 2 من الاتفاقية.

3. يجوز سحب أي إعلان تم تقديمه بموجب الفقرة 2 من هذه المادة، فيما يتعلق بأي إقليم محدد في هذا الإعلان، من خلال إشعار يوجه إلى الأمين العام لمجلس أوروبا. ويدخل سحب الإعلان حيز التنفيذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر بعد تاريخ استلام الأمين العام لهذا الإشعار.

المادة 19 - التحفظات والإعلانات

1. يجوز لأي دولة طرف، بواسطة إشعار خطي يوجه إلى الأمين العام لمجلس أوروبا وقت التوقيع أو عند إيداع صك التصديق أو القبول أو الموافقة أو الانضمام، أن تعلن أنها ستستخدم تحفظا (أو أكثر من تحفظ) المنصوص عليه في المادة 7، الفقرة 9. أ و9.ب والمادة 8 الفقرة 13 والمادة 17 من هذا البروتوكول. ولا تقبل أي تحفظات أخرى.

2. يجوز لأي دولة طرف، بواسطة إشعار خطي يوجه إلى الأمين العام لمجلس أوروبا وقت التوقيع أو عند إيداع صك التصديق أو القبول أو الموافقة أو

الانضمام، أن تقوم بالإعلان (الإعلانات) الواردة في المادة 7 الفقرتين 2. ب. و8، والمادة 8 الفقرة 11، والمادة 9 الفقرتين 1. ب. و5، والمادة 10 الفقرة 9. ب.، والمادة 12 الفقرة 3، والمادة 18 الفقرة 2 من هذا البروتوكول.

3. يجوز لأي دولة طرف في الاتفاقية، بواسطة إشعار خطي يوجه إلى الأمين العام لمجلس أوروبا، القيام بإصدار أي إعلان (إعلانات) أو إخطارات أو بيانات محددة في المادة 7، الفقرتين 5. أ و هـ؛ المادة 8، الفقرتين 4 و 10 (أ) و (ب)؛ المادة 14، الفقرتين 7 (ج) و 10 (ب)؛ والمادة 17، الفقرة 2، من هذا البروتوكول وفقا للشروط المحددة فيها.

المادة 20 - حالة التحفظات وسحبها

1. تقوم الدولة الطرف التي أبدت تحفظًا وفقًا للفقرة 1 من المادة 19 بسحب هذا التحفظ، كليًا أو جزئيًا، بمجرد أن تسمح الظروف بذلك. ويدخل سحب التحفظ حيز التنفيذ في تاريخ إيداع الإشعار الموجه إلى الأمين العام لمجلس أوروبا وإذا أشار الإشعار أن سحب التحفظ سيدخل حيز التنفيذ في تاريخ معين وكان ذلك التاريخ لاحقاً عن التاريخ استلام الإشعار من قبل الأمين العام، يدخل سحب للتحفظ حيز التنفيذ في ذلك التاريخ اللاحق.

2. يجوز للأمين العام لمجلس أوروبا، بشكل دوري، أن يستفسر الأطراف التي استخدمت تحفظا أو أكثر من تحفظ طبقاً للمادة 19، الفقرة 1، عن احتمالات سحب ذلك التحفظ (أو تلك التحفظات).

المادة 21 - التعديلات

1. يجوز لأي دولة طرف في هذا البروتوكول اقتراح إدخال تعديلات عليه، ويقوم الأمين العام لمجلس أوروبا بإرسالها إلى الدول الأعضاء بمجلس أوروبا والدول الأطراف الموقعة على الاتفاقية وكذلك إلى أي دولة تم توجيه الدعوة إليها للانضمام إلى الاتفاقية.

2. يرسل أي تعديل مقترح من قبل دولة طرف إلى اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، التي تعرض رأيها في هذا التعديل المقترح على لجنة الوزراء.

3. تنظر لجنة الوزراء في التعديل المقترح والرأي الذي تحيله عليها اللجنة الأوروبية المعنية بمشاكل الإجرام (CDPC)، ويجوز لها، بعد التشاور مع الدول الأطراف غير الأعضاء في هذه الاتفاقية، تبني التعديل.

4. يرسل نص أي تعديل تتبناه لجنة الوزراء طبقاً للفقرة 3 من هذه المادة إلى الدول الأطراف للموافقة عليه.

5. يدخل أي تعديل يتم إقراره طبقاً للفقرة 3 من هذه المادة حيز التنفيذ في اليوم الثلاثين بعد إخبار جميع الدول الأطراف الأمين العام لمجلس أوروبا بقبولها بذلك التعديل.

المادة 22 - تسوية النزاعات

تسري مقتضيات المادة 45 من الاتفاقية على هذا البروتوكول.

المادة 23 – هيئة مشاورات الأطراف وتقييم التنفيذ

1. تسري مقتضيات المادة 46 من الاتفاقية على هذا البروتوكول.
2. تقوم الأطراف بشكل دوري بتقييم الاستخدام والتنفيذ الفعالين لأحكام هذا البروتوكول. وتطبق المادة 2 من النظام الداخلي للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية بصيغتها المنقحة في 16 أكتوبر/تشرين الأول 2020 مع إجراء التعديلات اللازمة. تستعرض الأطراف أوليا إجراءات هذه المادة، ويجوز لها تعديل طريقة تطبيقها بالتوافق بعد خمس سنوات من بدء نفاذ هذا البروتوكول.
3. يبدأ استعراض المادة 14 بمجرد أن يعرب عشرة أطراف في الاتفاقية عن موافقتهم على الالتزام بهذا البروتوكول.

المادة 24 - الانسحاب

1. يجوز لأي دولة طرف، في أي وقت، الانسحاب من هذه الاتفاقية عن طريق إشعار موجه إلى الأمين العام لمجلس أوروبا.
2. ويدخل هذا الانسحاب حيز التنفيذ في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر من تاريخ استلام الأمين العام للإشعار.
3. يعتبر انسحاب أي دولة طرف في هذا البروتوكول من الاتفاقية انسحابا من هذا البروتوكول.
4. يجب أن تتم معالجة المعلومات أو الأدلة التي تم نقلها قبل تاريخ نفاذ الانسحاب وفقاً لأحكام هذا البروتوكول.

المادة 25 - الإبلاغ

يقوم الأمين العام لمجلس أوروبا بإبلاغ الدول الأعضاء في مجلس أوروبا والدول غير الأعضاء التي شاركت في صياغة هذه الاتفاقية، علاوة على أي دولة انضمت إليها أو دعيت للانضمام إلى هذه الاتفاقية بـما يلي:

أ. أي توقيع؛

ب. إيداع أي صك للتصديق، القبول، الموافقة أو الانضمام؛

ج. أي تاريخ لدخول هذا البروتوكول حيز التنفيذ وفقًا للفقرتين 3 و 4 من المادة 16؛

د. أي إعلانات أو تحفظات تم الإدلاء بها وفقًا للمادة 19 أو سحب التحفظات وفقًا للمادة 20؛

هـ. أي إجراء، إخطار أو تواصل آخر يتعلق بهذا البروتوكول.

وإثباتا لذلك، قام الموقعون أدناه، المفوضون بذلك حسب الأصول، بالتوقيع على هذا البروتوكول.

حرر في ستراسبوغ، في هذا اليوم 12 مايو 2022 ، باللغتين الإنجليزية والفرنسية وكلا النصين متساويين في الحجية، وذلك في نسخة واحدة تودع في محفوظات مجلس أوروبا. ويرسل الأمين العام لمجلس أوروبا نسخا مصدقا عليها إلى كل دولة عضو في مجلس أوروبا، وإلى الدول غير الأعضاء الموقعة على هذه الاتفاقية وإلى أي دولة دعيت للانضمام إليها.

التقرير التفسيري للبروتوكول الإضافي الثاني الملحق بالاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية [ستراسبورغ 12 مايو 2022]

1. تم اعتماد البروتوكول الإضافي الثاني الملحق بالاتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية ("هذا البروتوكول") من قبل لجنة وزراء مجلس أوروبا في اجتماع نواب الوزراء الـ 1417 مكرر (17 تشرين الثاني / نوفمبر 2021). تم فتح هذا البروتوكول للتوقيع في ستراسبورغ في 12 مايو 2022. كما أحاطت لجنة الوزراء علما بالتقرير التفسيري.

2. الغرض من نص هذا التقرير التفسيري هو توجيه ومساعدة الأطراف في تطبيق هذا البروتوكول، ويعكس فهم فريق صياغة هذا البروتوكول فيما يتعلق بإنفاذه.

مقدمة

خلفية

3. أصبحت الاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة المعاهدات الأوروبية رقم 185)، المشار إليها فيما يلي بـ "الاتفاقية")، منذ فتح باب التوقيع عليها في بودابست في 23 تشرين الثاني / نوفمبر 2001، صكاً ذا عضوية وتأثير في جميع مناطق العالم.

4. في عام 2003، تم استكمال الاتفاقية بالبروتوكول الإضافي الملحق بالاتفاقية المتعلقة بالجريمة الإلكترونية المتعلق بتجريم الأفعال ذات الطابع العنصري وكراهية الأجانب المرتكبة من خلال أنظمة الكمبيوتر (سلسلة المعاهدات الأوروبية رقم 189، المشار إليه فيما يلي بـ "البروتوكول الأول".)

5. لقد تطورت تكنولوجيا المعلومات والاتصالات وحوّلت المجتمعات على الصعيد العالمي بطريقة غير عادية منذ فتح باب التوقيع على الاتفاقية في عام 2001. ومع ذلك، منذ ذلك الحين، حدثت زيادة كبيرة في استغلال التكنولوجيا لأغراض إجرامية. تعتبر الجريمة الإلكترونية الآن من قبل العديد من الأطراف تهديدًا خطيرًا لحقوق الإنسان وسيادة القانون وسير عمل المجتمعات الديمقراطية. تتعدد التهديدات التي تشكلها الجرائم الإلكترونية. تشمل الأمثلة العنف الجنسي عبر الإنترنت ضد الأطفال والجرائم الأخرى ضد كرامة الأفراد وسلامتهم؛ سرقة وإساءة استخدام البيانات الشخصية التي تؤثر

على الحياة الخاصة للأفراد؛ التدخل في الانتخابات والهجمات الأخرى ضد المؤسسات الديمقراطية؛ الهجمات على الهياكل الأساسية الحيوية، مثل الهجمات الموزعة لحجب الخدمة وهجمات برامج الفدية؛ أو إساءة استخدام هذه التكنولوجيا لأغراض إرهابية. في عامي 2020 و2021، خلال جائحة فيروس كورونا (كوفيد 19)، لاحظت البلدان جرائم إلكترونية كبيرة مرتبطة بجائحة فيروس كورونا (كوفيد 19)، بما في ذلك الهجمات على المستشفيات والمرافق الطبية التي تطور لقاحات ضد الفيروس؛ إساءة استخدام أسماء النطاقات للترويج لقاحات وعلاجات وأدوية مزيفة؛ وأنواع أخرى من النشاط الاحتيالي.

6. على الرغم من تطور التكنولوجيات القائمة على البيانات والتوسع الخبيث للجريمة الالكترونية وتطورها، فإن المفاهيم المجسدة في الاتفاقية محايدة من الناحية التكنولوجية بحيث يمكن تطبيق القانون الجنائي الموضوعي على التكنولوجيات الحالية والمستقبلية المعنية، وتبقى الاتفاقية بالغة الأهمية في مكافحة الجريمة الالكترونية. تهدف الاتفاقية بشكل أساسي إلى (1) مواءمة عناصر القانون الجنائي الوطني الموضوعي للجرائم والأحكام ذات الصلة في مجال الجريمة الالكترونية؛ (2) النص على صلاحيات قانون الإجراءات الجنائية الوطني اللازمة للتحقيق والملاحقة القضائية في مثل هذه الجرائم، وكذلك الجرائم الأخرى المرتكبة عن طريق نظام الكمبيوتر أو المتعلقة باستخدام أدلة الكترونية لجرائم أخرى؛ (3) وضع نظام سريع وفعال للتعاون الدولي.

7. عند تطبيق الاتفاقية، تحترم الأطراف المسؤولية التي تقع على عاتق الحكومات لحماية الأفراد من الجرائم، سواء ارتكبت على شبكة الإنترنت أو خارجها، من خلال التحقيقات والملاحقات الجنائية الفعالة. في الواقع، ترى بعض الأطراف في الاتفاقية أنها ملزمة بالتزام دولي بتوفير وسائل الحماية من الجرائم المرتكبة عن طريق نظام الكمبيوتر (انظر ك. ي ضد فنلندا، المحكمة الأوروبية لحقوق الإنسان (قضية رقم 2872/02، الحكم/القرار المؤرخ في 2 آذار/مارس 2009)، الذي يشير إلى إجراءات وصلاحيات إجراء التحقيقات أو الدعاوى الجنائية التي يجب على الأطراف وضعها وفقًا للاتفاقية.

8. سعت الأطراف باستمرار إلى الوفاء بالتزاماتها لمكافحة الجريمة الالكترونية من خلال الاعتماد على مختلف الآليات والهيئات المنشأة بموجب الاتفاقية وعن طريق اتخاذ الخطوات اللازمة للتمكين من إجراء التحقيقات أو الدعاوى الجنائية بفعالية أكثر. بشكل ملحوظ، يتم تسهيل استخدام الاتفاقية وتنفيذها من خلال لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية المنشأة بموجب المادة 46 من الاتفاقية. علاوة على ذلك، يتم دعم الاتفاقية من خلال برامج بناء القدرات التي ينفذها مكتب برنامج مكافحة الجريمة الإلكترونية التابع لمجلس أوروبا في بوخارست، رومانيا، والذي يساعد البلدان في جميع أنحاء العالم في تنفيذ الاتفاقية. وقد ساهمت هذه العناصر الثلاثة من (1) المعايير المشتركة للاتفاقية في مجال الجريمة الإلكترونية، إلى جانب (2) آلية قوية للالتزام

المشترك المستمر للأطراف من خلال لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية و (3) التركيز على برامج بناء القدرات قد ساهم بشكل كبير في مدى انتشار تأثير الاتفاقية.

9. في عام 2012، تماشيا مع ولايتها بموجب الفقرة 1 من المادة 46 من الاتفاقية، قامت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية بتبادل "المعلومات المتعلقة بالتطورات القانونية أو السياساتية أو التكنولوجية الهامة المتعلقة بالجرائم الإلكترونية وجمع الأدلة في شكل إلكتروني" والنظر في "إمكانية الاستكمال أو التعديل المحتمل للاتفاقية"، أنشأت الفريق الفرعي المخصص بشأن الولاية القضائية والوصول إلى البيانات عبر الحدود ("الفريق عبر الحدود"). في ديسمبر 2014، أكملت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية أيضًا تقييمًا لأحكام المساعدة المتبادلة الواردة في الاتفاقية المتعلقة بالجريمة الإلكترونية واعتمدت مجموعة من التوصيات، بما في ذلك بعض التوصيات التي كان من المقرر تناولها في بروتوكول جديد للاتفاقية. أدت هذه الجهود إلى إنشاء فريق العمل المعني بوصول القضاء الجنائي إلى الأدلة المخزنة في السحابة في عام 2015، بما في ذلك من خلال المساعدة القانونية المتبادلة ("فريق الأدلة السحابية").

10. في عام 2016، خلص فريق الأدلة السحابية، من بين أمور أخرى، إلى أن "الجريمة الإلكترونية وعدد الأجهزة والخدمات والمستخدمين (بما في ذلك الأجهزة والخدمات المحمولة) مع كل هذا وصل عدد الضحايا إلى نسب بحيث لا يتم تسجيل سوى حصة ضئيلة من الجرائم الإلكترونية أو غيرها من الجرائم التي تنطوي على أدلة إلكترونية والتحقيق فيها. الغالبية العظمى من ضحايا الجرائم الإلكترونية لا يمكنهم توقع تحقيق العدالة". تتعلق التحديات الرئيسية التي حددها الفريق بـ "الحوسبة السحابية، الاختصاص الإقليمي، والولاية القضائية"، وبالتالي بالصعوبات في الحصول بكفاءة على الأدلة الإلكترونية أو الكشف عنها.

11. عند استعراض استنتاجات فريق الأدلة السحابية، خلصت الأطراف في الاتفاقية إلى أنه ليست هناك حاجة لتعديل الاتفاقية أو النص على تجريم إضافي من خلال أحكام القانون الجنائي الموضوعي. قررت الأطراف، مع ذلك، أن هناك ضرورة اتخاذ تدابير إضافية لتعزيز التعاون وقدرة سلطات القضاء الجنائي للحصول على أدلة إلكترونية من خلال بروتوكول إضافي ثان للتمكين من اتخاذ تدابير أكثر فعالية في مجال القضاء الجنائي ودعم سيادة القانون.

العمل التحضيري

12. أقرت الدورة العامة السابعة عشرة للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية (8 حزيران/يونيو 2017) الإطار المرجعي لإعداد هذا البروتوكول بناءً على اقتراح أعده فريق الأدلة السحابية التابع للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية وقررت الشروع في صياغة هذا البروتوكول بمبادرة منها بموجب المادة 46، الفقرة 1 (ج) من الاتفاقية. في

14 حزيران/يونيو 2017، أبلغ نائب الأمين العام لمجلس أوروبا لجنة الوزراء (الاجتماع الـ 1289 لنواب الوزراء) بمبادرة لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية.

13. شمل الإطار المرجعي في البداية الفترة من سبتمبر 2017 إلى ديسمبر 2019 وتم تمديده لاحقًا من قبل لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية إلى ديسمبر 2020 ومرة أخرى حتى مايو 2021.

14. بموجب هذا الإطار المرجعي، أنشأت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية هيئة عامة لصياغة البروتوكول تتألف من ممثلي الأطراف في الاتفاقية والدول والمنظمات وهيئات مجلس أوروبا التي تتمتع بصفة مراقب في لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية، كمراقبين. تمت مساعدة الهيئة العامة لصياغة البروتوكول في إعداد مسودة البروتوكول من قبل فريق صياغة البروتوكول المكون من خبراء من الأطراف في الاتفاقية. وأنشأ فريق صياغة البروتوكول بدوره عدة فرق فرعية وفرق مخصصة للعمل على أحكام محددة.

15. بين أيلول/سبتمبر 2017 وأيار/مايو 2021، عقدت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية 10 دورات عامة للصياغة و16 اجتماعًا لفريق الصياغة والعديد من اجتماعات الفرق الفرعية والمخصصة. تم إعداد جزء كبير من هذا البروتوكول أثناء جائحة كوفيد 19-. بسبب القيود المتعلقة بجائحة كوفيد 19-، بين مارس 2020 ومايو 2021، تم عقد أكثر من 65 اجتماعًا في شكل افتراضي.

16. سمحت أساليب العمل المذكورة أعلاه في الدورات العامة، وفرق الصياغة والفرق الفرعية والمخصصة للممثلين والخبراء من الأطراف بالمساهمة على نطاق واسع في صياغة هذا البروتوكول ووضع حلول مبتكرة.

17. شاركت مفوضية الاتحاد الأوروبي في هذا العمل نيابة عن الدول الأطراف في الاتفاقية التي كانت أعضاء في الاتحاد الأوروبي بموجب ولاية تفاوضية منحها مجلس الاتحاد الأوروبي في 6 حزيران / يونيو 2019.

18. بمجرد إعداد مسودة الأحكام واعتمادها مؤقتًا من قبل هيئة صياغة البروتوكول، تم نشر مسودات المواد وتمت دعوة أصحاب المصلحة إلى تقديم تعليقات.

19. عقدت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية ست جولات من المشاورات مع أصحاب المصلحة من المجتمع المدني والقطاع الخاص، ومع خبراء حماية البيانات. كان ذلك بالتزامن مع مؤتمر الأخطبوط حول التعاون ضد الجريمة الإلكترونية في ستراسبورغ في يوليو 2018؛ مع خبراء حماية البيانات في ستراسبورغ في نوفمبر 2018؛ عبر دعوة لتقديم تعليقات مكتوبة على مشاريع المواد في فبراير 2019؛ بالتزامن مع مؤتمر الأخطبوط حول التعاون ضد الجريمة الإلكترونية في ستراسبورغ في نوفمبر 2019؛ من

خلال دعوة لتقديم تعليقات مكتوبة على مسودات مواد أخرى في ديسمبر 2020؛ وفي مايو 2021 من خلال الطلبات المكتوبة والاجتماع الافتراضي الذي عقد في 6 مايو 2021.

20. كما تشاورت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية مع اللجنة الأوروبية حول مشاكل الجريمة واللجنة الاستشارية لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية التابعة لمجلس أوروبا.

21. وافقت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية في الدورة العامة 24 في 28 مايو 2021 على مشروع هذا البروتوكول وقررت تقديمه إلى لجنة الوزراء بهدف اعتماده.

الاعتبارات الموضوعية

22. من حيث الموضوع، كانت نقطة البداية للعمل على هذا البروتوكول هي نتائج تقييم لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية لأحكام المساعدة المتبادلة للاتفاقية في عام 2014 وتحليلات وتوصيات الفريق عبر الحدود التابع للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية وفريق الأدلة السحابية في 2014 و2017 على التوالي. كانت التحديات الإقليمية والولاية القضائية المتعلقة بالأدلة الإلكترونية مصدر قلق خاص، أي أن البيانات المحددة المطلوبة في تحقيق جنائي قد يتم تخزينها في ولايات قضائية متعددة أو متغيرة أو غير معروفة ("في السحابة")، وأن هناك حاجة إلى حلول من أجل الحصول على الكشف عن هذه البيانات بطريقة تتسم بالفعالية والكفاءة لغرض إجراء تحقيقات أو دعاوى جنائية محددة.

23. نظراً لتعقيد هذه التحديات، اتفق فريق صياغة هذا البروتوكول على التركيز على المسائل المحددة التالية:

- أثناء صياغة هذا البروتوكول، كانت طلبات المساعدة المتبادلة هي الطريقة الأساسية للحصول على أدلة إلكترونية حول جريمة جنائية من دول أخرى، بما في ذلك أدوات المساعدة المتبادلة الواردة في الاتفاقية. مع ذلك، فإن المساعدة المتبادلة ليست دائمًا طريقة فعالة لدراسة عدد متزايد من الطلبات للأدلة الإلكترونية غير المستقرة. لذلك، كان من الضروري تطوير آلية أكثر بساطة لإصدار أوامر أو طلبات لمقدمي الخدمات في الأطراف الأخرى لتقديم معلومات المشتركين وبيانات الحركة.
- معلومات المشترك - على سبيل المثال، لتحديد هوية مستخدم بريد إلكتروني معين أو حساب وسائل التواصل الاجتماعي أو عنوان بروتوكول إنترنت محدد مستخدم في ارتكاب جريمة - هي المعلومات الأكثر طلبًا في التحقيقات الوطنية والدولية المتعلقة بالجرائم الإلكترونية والجرائم الأخرى التي تنطوي على أدلة إلكترونية. بدون هذه المعلومات، غالبًا ما يكون من المستحيل متابعة التحقيق. الحصول على معلومات المشترك من خلال المساعدة المتبادلة في معظم القضايا غير فعال ويثقل كاهل نظام المساعدة

المتبادلة. عادة ما يحتفظ مقدمو الخدمة بمعلومات المشترك. بينما تتناول المادة 18 من الاتفاقية بالفعل بعض جوانب الحصول على معلومات المشتركين من مقدمي الخدمة (انظر المذكرة التوجيهية للجنة الاتفاقية المتعلقة بالجريمة الالكترونية بشأن المادة 18)، بما في ذلك في الأطراف الأخرى، تم اعتبار أن الأدوات التكميلية ضرورية للحصول على الكشف عن معلومات المشترك مباشرة من مقدم خدمة في طرف آخر. ستعمل هذه الأدوات على زيادة كفاءة العملية وأيضًا تخفيف الضغط على نظام المساعدة المتبادلة.

- غالبًا ما يتم البحث عن بيانات الحركة في التحقيقات الجنائية، وقد يكون الكشف المعجل عنها ضروريًا لتتبع مصدر الاتصال كنقطة انطلاق لجمع المزيد من الأدلة أو لتحديد المشتبه فيه.

- بالمثل، نظرًا لأن العديد من أشكال الجريمة عبر الإنترنت يتم تسهيلها من خلال النطاقات التي تم إنشاؤها أو استغلالها لأغراض إجرامية، فمن الضروري تحديد الشخص الذي قام بتسجيل مثل هذا النطاق. يتم الاحتفاظ بهذه المعلومات من قبل الكيانات التي تقدم خدمات تسجيل اسم النطاق، أي عادة من قبل المسجلين والسجلات. وبالتالي، هناك حاجة إلى إطار عمل فعال للحصول على هذه المعلومات من الكيانات ذات الصلة في الأطراف الأخرى.

- في حالة الطوارئ، حيث يوجد خطر كبير ووشيك على حياة أو سلامة أي شخص طبيعي، يلزم اتخاذ إجراء سريع إما من خلال توفير المساعدة المتبادلة في حالات الطوارئ أو الاستفادة من نقاط الاتصال للشبكة المنشأة بموجب الاتفاقية (المادة 35) التي تعمل على مدار الساعة طوال أيام الأسبوع.

- بالإضافة إلى ذلك، ينبغي استخدام أدوات التعاون الدولي التي أثبتت جدواها على نطاق أوسع وبين جميع الأطراف. توجد بالفعل تدابير مهمة، مثل التداول بالفيديو أو فرق التحقيق المشتركة، بموجب معاهدات مجلس أوروبا (على سبيل المثال، البروتوكول الإضافي الثاني الملحق بالاتفاقية الأوروبية للمساعدة المتبادلة في المسائل الجنائية، سلسلة المعاهدات الأوروبية رقم 182) أو غيرها من الاتفاقيات الثنائية والاتفاقات المتعددة الأطراف. ومع ذلك، فإن هذه الآليات ليست متاحة عالميًا بين الأطراف في الاتفاقية، ويهدف هذا البروتوكول إلى سد هذه الفجوة.

- تنص الاتفاقية على جمع وتبادل المعلومات والأدلة من أجل إجراء تحقيقات أو دعاوى جنائية محددة. أقر فريق الصياغة بأن إنشاء وتنفيذ وتطبيق السلطات والإجراءات المتعلقة بالتحقيقات والملاحقات القضائية يجب أن تخضع دائمًا لشروط وضمانات تضمن الحماية الكافية لحقوق الإنسان والحريات الأساسية. ولذلك كان من الضروري إدراج مادة بشأن الشروط والضمانات، على غرار المادة 15 من الاتفاقية. علاوة على ذلك،

وإدراكًا لمتطلبات العديد من الأطراف لحماية الخصوصية والبيانات الشخصية من أجل الوفاء بالتزاماتها الدستورية والدولية، قرر فريق الصياغة توفير ضمانات خاصة لحماية البيانات في هذا البروتوكول. إن ضمانات حماية البيانات هذه تكمّل التزامات العديد من الأطراف في الاتفاقية، والتي هي أيضًا أطراف في اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (سلسلة المعاهدات الأوروبية رقم 108). تم فتح البروتوكول المعدّل لتلك الاتفاقية (سلسلة معاهدات مجلس أوروبا رقم 223) للتوقيع أثناء صياغة هذا البروتوكول في أكتوبر 2018. وتجدر الإشارة أيضاً إلى أن عملية صياغة هذا البروتوكول شملت الأطراف التي لم تكن تخضع آنذاك لصكوك مجلس أوروبا المتعلقة بحماية البيانات أو لقواعد الاتحاد الأوروبي لحماية البيانات. وبناء على ذلك، بُذلت جهود كبيرة لضمان وضع بروتوكول متوازن يعكس النظم القانونية العديدة للدول التي يحتمل أن تكون أطرافا في هذا البروتوكول مع احترام أهمية ضمان حماية الخصوصية والبيانات الشخصية على النحو الذي تقتضيه دساتير الأطراف الأخرى في الاتفاقية والتزاماتها الدولية.

24. أخذ فريق الصياغة أيضًا في الاعتبار تدابير أخرى لم يتم الإبقاء عليها في هذا البروتوكول، بعد مناقشة مستفيضة. كان اثنان من هذه الأحكام، وهما "التحقيقات السرية عن طريق نظام الكمبيوتر" و "توسيع نطاق عمليات البحث"، موضع اهتمام كبير لدى الأطراف، ولكن تبين أنهما يتطلبان مزيداً من العمل والوقت والمشاورات مع أصحاب المصلحة، وبالتالي لم يكن النظر فيهما ممكنا في الإطار الزمني المحدد لإعداد هذا البروتوكول. واقترح فريق الصياغة أن تتم متابعتهما في شكل مختلف وربما في صك قانوني منفصل.

25. بشكل عام، اعتقد فريق الصياغة أن أحكام هذا البروتوكول ستضيف قيمة كبيرة من منظور عملي ومن منظور السياسة. سيعمل هذا البروتوكول على تحسين قدرة الأطراف بشكل كبير على تعزيز التعاون بين الأطراف وبين مقدمي الخدمات والكيانات الأخرى، والحصول على الكشف عن الأدلة الإلكترونية لغرض إجراء تحقيقات أو دعاوى جنائية محددة. بالتالي، فإن هذا البروتوكول، مثل الاتفاقية، يهدف إلى زيادة قدرة سلطات إنفاذ القانون على مكافحة الجريمة الإلكترونية والجرائم الأخرى، مع الاحترام الكامل لحقوق الإنسان والحريات الأساسية، ويشدد على أهمية وقيمة شبكة الإنترنت القائمة على التدفق الحرّ للمعلومات.

هذا البروتوكول

26. كما هو منصوص عليه في الديباجة، يهدف هذا البروتوكول إلى زيادة تعزيز التعاون بشأن الجريمة الالكترونية وقدرة سلطات القضاء الجنائي على جمع الأدلة في شكل إلكتروني لجريمة جنائية لغرض إجراء تحقيقات أو دعاوى جنائية محددة من خلال أدوات إضافية تتعلق بمساعدة متبادلة أكثر كفاءة وأشكال أخرى من التعاون بين السلطات المختصة؛ التعاون في حالات الطوارئ (أي في الحالات التي يوجد فيها خطر كبير ووشيك على حياة أو

سلامة أي شخص طبيعي)؛ والتعاون المباشر بين السلطات المختصة ومقدمي الخدمات والكيانات الأخرى التي تمتلك أو تسيطر على المعلومات ذات الصلة. وبالتالي، فإن الغرض من هذا البروتوكول هو استكمال الاتفاقية، بين الأطراف فيها، والبروتوكول الأول.

27. ينقسم هذا البروتوكول إلى أربعة فصول: أولاً- "الأحكام المشتركة"؛ ثانيًا- "تدابير لتعزيز التعاون"؛ ثالثا- "الشروط والضمانات"؛ ورابعا- "الأحكام الختامية".

28. تتناول الأحكام المشتركة للفصل الأول الغرض من هذا البروتوكول ونطاقه. كما هو الحال بالنسبة للاتفاقية، يتعلق هذا البروتوكول بإجراء تحقيقات أو دعاوى جنائية محددة، ليس فقط فيما يتعلق بجريمة الكترونية ولكن أيضًا أيَ جريمة جنائية تنطوي على أدلة في شكل إلكتروني يشار إليها أيضًا باسم "الأدلة الإلكترونية" أو "الأدلة الرقمية". يضع هذا الفصل أيضًا تعريفات للاتفاقية المنطبقة على هذا البروتوكول ويحتوي على تعريفات إضافية للمصطلحات المستخدمة بشكل متكرر في هذا البروتوكول. علاوة على ذلك، وبالنظر إلى أن المتطلبات اللغوية للمساعدة المتبادلة وغيرها من أشكال التعاون كثيرا ما تعيق كفاءة الإجراءات، تمت إضافة مادة بشأن "اللغة" للسماح باتباع نهج أكثر واقعية في هذا الصدد.

29. يحتوي الفصل الثاني على المواد الأساسية الجوهرية لهذا البروتوكول، التي تصف مختلف طرق التعاون المتاحة للأطراف. تنطبق مبادئ مختلفة على كل نوع من أنواع التعاون. لهذا السبب، كان من الضروري تقسيم هذا الفصل إلى أقسام تحتوي على (1) مبادئ عامة تنطبق على الفصل الثاني، (2) إجراءات تعزز التعاون المباشر مع مقدمي الخدمات والكيانات في الأطراف الأخرى، (3) إجراءات تعزز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة، (4) الإجراءات المتعلقة بالمساعدة المتبادلة في حالات الطوارئ (5) والإجراءات المتعلقة بالتعاون الدولي في حالة عدم وجود اتفاقيات دولية سارية المفعول.

30. ينص الفصل الثالث على الشروط والضمانات. وهي تتطلب أن تطبق الأطراف شروطًا وضمانات مماثلة للمادة 15 من الاتفاقية أيضًا على صلاحيات وإجراءات هذا البروتوكول. بالإضافة إلى ذلك، يتضمن هذا الفصل مجموعة مفصلة من الضمانات لحماية البيانات الشخصية.

31. تتشابه معظم الأحكام الختامية للفصل الرابع مع الأحكام الختامية الموحدة لمعاهدات مجلس أوروبا أو تجعل أحكام الاتفاقية قابلة للتطبيق على هذا البروتوكول. ومع ذلك، تختلف المادة 15 بشأن "آثار هذا البروتوكول" والمادة 17 بشأن "البند الاتحادي" والمادة 23 بشأن "هيئة مشاورات الأطراف وتقييم التنفيذ" بدرجات متفاوتة عن الأحكام المماثلة في الاتفاقية. لا تجعل هذه المادة الأخيرة المادة 46 من الاتفاقية قابلة للتطبيق فحسب، بل تنص أيضاً على أن تقوم الأطراف دورياً بتقييم الاستخدام والتنفيذ الفعالين لأحكام هذا البروتوكول.

تعليق على مواد هذا البروتوكول

الفصل الأول - الأحكام المشتركة

المادة 1 – الغرض

32. الغرض من هذا البروتوكول هو استكمال (1) الاتفاقية بين الأطراف في هذا البروتوكول، و (2) البروتوكول الأول بين الأطراف فيه التي هي أيضاً أطراف في هذا البروتوكول.

المادة 2 – نطاق التطبيق

33. النطاق العام لتطبيق هذا البروتوكول هو نفس نطاق تطبيق الاتفاقية: يجب تطبيق تدابير هذا البروتوكول، بين الأطراف في هذا البروتوكول، على إجراء تحقيقات أو دعاوى جنائية محددة تتعلق بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات (أي الجرائم المشمولة بالمادة 14 من الاتفاقية، الفقرتان 2 (أ) و (ب))، وكذلك جمع الأدلة في شكل إلكتروني لجريمة جنائية (المادة 14 من الاتفاقية، الفقرة 2 (ج)). كما هو موضح في الفقرتين 141 و243 من التقرير التفسيري للاتفاقية، فإن هذا يعني أنه إما في حالة ارتكاب الجريمة باستخدام نظام كمبيوتر، أو عندما لا تُرتكب الجريمة باستخدام نظام كمبيوتر (على سبيل المثال جريمة قتل) من المفترض أن تكون الأدلة الإلكترونية والصلاحيات والإجراءات وتدابير التعاون التي أنشأها هذا البروتوكول متاحة.

34. تنص الفقرة 1 (ب) على أنه فيما بين الأطراف في البروتوكول الأول التي هي أطراف أيضًا في هذا البروتوكول، ينطبق هذا البروتوكول أيضًا على إجراء تحقيقات أو دعاوى جنائية محددة تتعلق بالجرائم الجنائية المحددة بموجب البروتوكول الأول. لا تتعهد الأطراف في هذا البروتوكول التي ليست أطرافاً في البروتوكول الأول بأي التزام بتطبيق أحكام هذا البروتوكول على تلك الجرائم.

35. بموجب الفقرة 2، يتعين على كل طرف أن يكون لديه أساس قانوني لتنفيذ الالتزامات المنصوص عليها في هذا البروتوكول إذا كانت معاهداته أو قوانينه أو ترتيباته لا تتضمن بالفعل مثل هذه الأحكام. هذا لا يغير صراحة الأحكام التي تخضع لسلطة تقديرية إلى أحكام إلزامية، وبعض الأحكام تسمح بالإعلانات أو التحفظات. قد لا تشترط بعض الأطراف أي تشريع تنفيذي من أجل تطبيق أحكام هذا البروتوكول.

المادة 3 – التعاريف

36. تتضمن الفقرة 1 التعاريف الواردة في المادة 1 ("نظام الكمبيوتر" و "بيانات الكمبيوتر" و "مقدم الخدمة" و "بيانات الحركة") والفقرة 3 من المادة 18 ("معلومات المشترك")

من الاتفاقية في هذا البروتوكول. أدرج فريق الصياغة هذه التعريفات من الاتفاقية لأن هذه المصطلحات مستخدمة في منطوق النص والتقرير التفسيري لهذا البروتوكول. كان فريق الصياغة يهدف أيضا أن التفسيرات الواردة في التقرير التفسيري للاتفاقية وفي المذكرات التوجيهية (التي اعتمدتها لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية) المتعلقة بهذه المصطلحات تنطبق بالمثل على هذا البروتوكول.

37. تهدف تعاريف الجرائم والمصطلحات الأخرى الواردة في نص الاتفاقية إلى تطبيقها لأغراض التعاون بين الأطراف في هذا البروتوكول، وتعاريف الجرائم والمصطلحات الأخرى الواردة في نص البروتوكول الأول تهدف إلى تطبيق لأغراض التعاون بين الأطراف في البروتوكول الأول. على سبيل المثال، تنص الفقرة 1 من المادة 2 على أن "يتم تطبيق التدابير المبينة في هذا البروتوكول ... فيما بين الأطراف في الاتفاقية التي هي أطراف في هذا البروتوكول، في إجراء تحقيقات أو دعاوى جنائية محددة تتعلق بأفعال إجرامية تتصل بأنظمة الكمبيوتر والبيانات". لذلك، عند التعاون بموجب هذا البروتوكول فيما يتعلق بالجرائم المتعلقة باستغلال الأطفال في المواد الإباحية، ينطبق تعريف "استغلال الأطفال في المواد الإباحية" في المادة 9، الفقرة 2، من الاتفاقية، وتعريف "القاصر" في المادة 9، الفقرة 3، من الاتفاقية. وبالمثل، بين الأطراف في البروتوكول الأول التي هي أطراف في هذا البروتوكول، ينطبق تعريف "المواد التي تحض على العنصرية وكره الأجانب" في المادة 2 من البروتوكول الأول. لا تتعهد الأطراف في هذا البروتوكول التي ليست أطرافاً في البروتوكول الأول بأي التزام بتطبيق المصطلحات أو التعاريف المنصوص عليها في البروتوكول الأول.

38. تتضمن الفقرة 2 من المادة 3 تعاريف إضافية تنطبق على هذا البروتوكول والتعاون بموجب هذا البروتوكول. تُعرِّف الفقرة 2 (أ) "السلطة المركزية" على أنها "السلطة أو السلطات المعينة بموجب معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف المعنية، أو في حالة عدم وجودها، السلطة أو السلطات المعينة من قبل أحد الأطراف بموجب المادة 27، الفقرة 2 (أ)، من الاتفاقية". يستخدم هذا البروتوكول السلطات المركزية في العديد من المواد من أجل إتاحة التعاون من خلال قناة تستخدمها الأطراف بالفعل وتعرفها. لذلك، يتعين على الأطراف التي لديها معاهدات أو ترتيبات للمساعدة المتبادلة على أساس تشريع موحد أو متبادل استخدام السلطات المركزية المعينة بموجب تلك المعاهدات أو الترتيبات. في حالة عدم وجود معاهدة أو ترتيب من هذا القبيل بين الأطراف المعنية، يتعين على هذه الأطراف استخدام نفس قناة السلطة المركزية التي يستخدمونها حاليًا بموجب المادة 27، الفقرة 2 (أ) من الاتفاقية. على الرغم من أنه لا تستخدم جميع معاهدات أو ترتيبات المساعدة المتبادلة على أساس تشريع موحد أو متبادل مصطلح "السلطة المركزية"، فإن فريق الصياغة كان يهدف أن يشير المصطلح إلى سلطات التنسيق المعينة في مثل هذه المعاهدات أو الترتيبات، بغض النظر عن تسميتها.

39. ما لم يرد نص محدد في هذا البروتوكول، فإن إشراك الأطراف في قنوات السلطة المركزية هذه لأغراض هذا البروتوكول لا يعني انطباق أحكام أخرى من معاهدات أو ترتيبات المساعدة المتبادلة تلك.

40. صياغة تعريف "السلطة المختصة" بموجب الفقرة 2 (ب) مستوحى من الفقرة 138 من التقرير التفسيري للاتفاقية. وبما أن هذا المصطلح كثيرا ما يستخدم في هذا البروتوكول، فقد وضع التعريف في نص المنطوق تيسيرا للاطلاع عليه.

41. تُعرِّف الفقرة 2 (ج) "الطوارئ" على أنها "حالة تنطوي خطر كبير ووشيك على حياة أو سلامة أي شخص طبيعي". يستخدم هذا المصطلح في المواد 9 و10 و12. ويهدف تعريف "الطوارئ" في هذا البروتوكول إلى فرض عتبة أعلى بكثير من "الظروف العاجلة" بموجب المادة 25، الفقرة 3، من الاتفاقية. تمت صياغة هذا التعريف أيضًا للسماح للأطراف بالنظر في السياقات المختلفة التي يُستخدم فيها المصطلح في هذا البروتوكول مع مراعاة قوانين الأطراف وسياساتها المنطبقة.

42. يشمل تعريف حالة الطوارئ الحالات التي يكون فيها الخطر جسيمًا ووشيكًا، بمعنى أنه لا يشمل الحالات التي يكون فيها الخطر على حياة أو سلامة الشخص قد مضى بالفعل أو يكون ضئيلًا، أو التي قد يكون فيها خطر غير وشيك في المستقبل. سبب هذه المتطلبات المهمة والوشيكة هو أن المادتين 9 و10 تضعان التزامات عمل كثيفة على كل من الأطراف مقدمة الطلب والأطراف متلقية الطلب بالاستجابة بطريقة سريعة للغاية في حالات الطوارئ، مما يتطلب بالتالي إعطاء طلبات الطوارئ أولوية أعلى من القضايا الهامة الأخرى وإن كانت أقل إلحاحا إلى حد ما، حتى لو تم تقديمها مسبقًا. قد تشمل القضايا التي تنطوي على "خطر كبير ووشيك على حياة أو سلامة أي شخص طبيعي"، على سبيل المثال، حالات الرهائن التي يوجد فيها خطر حقيقي يتمثل في وقوع خسارة وشيكة في الأرواح أو إصابة خطيرة أو ضرر مماثل آخر للضحية؛ الاعتداء الجنسي المستمر على الطفل؛ سيناريوهات مباشرة بعد الهجوم الإرهابي حيث تسعى السلطات إلى تحديد الجهة التي اتصل بها المهاجمون لتحديد ما إذا كانت الهجمات الأخرى وشيكة؛ والأخطار التي تهدد أمن الهياكل الأساسية الحيوية التي تنطوي على خطر كبير ووشيك على حياة شخص طبيعي أو سلامته.

43. كما هو موضح في المادة 10، الفقرة 4، من هذا البروتوكول وفي الفقرة 154 من هذا التقرير التفسيري، الذي يتعلق بالمادة 9، فإن الطرف متلقي الطلب بموجب هذه المواد سيحدد ما إذا كانت هناك "حالة طوارئ"، بتطبيق التعريف الوارد في هذه المادة.

44. تُعرِّف الفقرة 2 (د) "البيانات الشخصية" على أنها "معلومات تتعلق بشخص طبيعي محدد الهوية أو يمكن تحديد هويته". يُقصد بـ "الشخص الطبيعي الذي يمكن تحديد هويته" الإشارة إلى الشخص الذي يمكن تحديد هويته، بشكل مباشر أو غير مباشر، بالرجوع،

على وجه الخصوص، إلى رقم التعريف أو إلى عامل أو أكثر خاص بهويته البدنية أو الفسيولوجية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية. يتوافق تعريف "البيانات الشخصية" بموجب هذا البروتوكول مع ذلك الوارد في الصكوك الدولية الأخرى، مثل اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، بصيغتها المعدلة ببروتوكولها الإضافي، المبادئ التوجيهية التي تحكم حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود لمنظمة التعاون الاقتصادي والتنمية لعام 2013، ولائحة الاتحاد الأوروبي العامة لحماية البيانات والأمر التوجيهي لإنفاذ قانون حماية البيانات، واتفاقية الاتحاد الأفريقي بشأن الأمن الالكتروني وحماية البيانات الشخصية ("اتفاقية مالابو").

45. لا يعتبر الفرد "قابلاً لتحديد هويته" إذا كان التعرف عليه يتطلب وقتًا أو جهدًا أو موارد غير معقولة. في حين أن بعض المعلومات قد تكون فريدة من نوعها بالنسبة لفرد معين، وبالتالي تنشئ رابطًا لهذا الشخص في حد ذاته، إلا أن المعلومات الأخرى قد تسمح بتحديد الهوية فقط عند دمجها مع معلومات شخصية أو معلومات تعريفية إضافية. وفقًا لذلك، إذا كان تحديد هوية الفرد على أساس الصلة بهذه المعلومات الإضافية يتطلب وقتًا أو جهدًا أو موارد غير معقولة، فإن المعلومات المعنية لا تشكل بيانات شخصية. يتوقف تحديد هوية شخص طبيعي أو إمكانية التعرف عليه، بصورة مباشرة أو غير مباشرة، على الظروف الخاصة في سياقها المحدد (وقد يتغير مع مرور الوقت مع التطورات التكنولوجية أو غيرها من التطورات).

46. لا تنطبق متطلبات حماية البيانات المنصوص عليها في هذا البروتوكول على البيانات التي ليست "بيانات شخصية"، مثل المعلومات مجهولة المصدر التي لا يمكن إعادة تحديدها بدون وقت أو جهد أو موارد غير معقولة.

المادة 4 - اللغة

47. تنص المادة 4 على إطار للغات التي يمكن استخدامها عند مخاطبة الأطراف ومقدمي الخدمات أو الكيانات الأخرى عملاً بهذا البروتوكول. وحتى عندما تكون الأطراف قادرة عمليًا على العمل بلغات غير لغاتها الرسمية، فقد لا ينص القانون الوطني أو المعاهدات على هذه الإمكانية. الهدف من هذه المادة هو توفير مرونة إضافية بموجب هذا البروتوكول.

48. إن الترجمات غير الدقيقة أو باهظة التكلفة لطلبات المساعدة المتبادلة المتعلقة بالأدلة الإلكترونية هي تذمر مزمن يتطلب اهتماما عاجلا. يؤدي هذا العائق إلى إضعاف العمليات المشروعة للحصول على البيانات وحماية السلامة العامة. وتنطبق نفس الاعتبارات خارج نطاق المساعدة المتبادلة التقليدية، مثلاً عندما يحيل أحد الأطراف أمراً مباشرة إلى مقدم خدمة في إقليم طرف آخر بموجب المادة 7، أو يطلب تنفيذ أمر بموجب المادة 8. في حين أنه من المتوقع أن تتحسن قدرات الترجمة الآلية، إلا أنها غير كافية حاليًا. ولهذه الأسباب، تكررت الإشارة إلى مشكلة الترجمة في المقترحات المتعلقة بالمواد التي ستدرج في هذا البروتوكول.

49. تعتبر الترجمة من وإلى اللغات الأقل شيوعا مشكلة خاصة لأن هذه الترجمات قد تؤخر الطلب إلى حد كبير أو قد يستحيل الحصول عليه فعليا. كما أنها قد تكون مضللة بشكل خطير، ويمكن لنوعيتها الرديئة أن تضيع وقت الطرفين. غير أن تكلفة وصعوبة الترجمات تقع بشكل غير متناسب على عاتق الأطراف مقدمة الطلب التي تتحدث لغات أقل شيوعاً.

50. بسبب هذا العبء غير المتناسب، طلب عدد من الأطراف غير الناطقة بالإنجليزية أن تكون اللغة الإنجليزية إلزامية في هذا البروتوكول. وأشاروا إلى أن اللغة الإنجليزية هي لغة شائعة الاستخدام من قبل مقدمي الخدمات الرئيسيين. علاوة على ذلك، نظرًا لأن البيانات يتم نقلها وتخزينها على نطاق أوسع في العالم واشتراك المزيد من البلدان في مساعدة بعضها البعض، فقد تصبح الترجمة أكثر إرهاقًا وغير عملية. على سبيل المثال، قد يستخدم طرفان لغات أقل شيوعًا، ويكونان بعيدين جغرافيًا وليس بينهما اتصال يذكر. إذا احتاج الطرف "أ" فجأة إلى مساعدة الطرف "ب"، فقد يتعذر عليه العثور على مترجم للغة الطرف "ب"، أو قد تكون الترجمة النهائية أقل وضوحًا من اللغة الإنجليزية غير الأصلية. وشدد فريق الصياغة بشكل خاص على ضرورة بذل كل الجهود، للإسراع في تقديم المساعدة، من أجل قبول الطلبات الطارئة بموجب هذا البروتوكول، على وجه الخصوص، باللغة الانجليزية أو بلغة مشتركة بدلا من اشتراط ترجمتها إلى اللغة الرسمية للطرف متلقي الطلب.

51. خلص فريق صياغة هذا البروتوكول إلى أنه لا ينبغي إلزام اللغة الإنجليزية في هذا البروتوكول. لدى بعض الأطراف متطلبات لغة رسمية تمنع هذا الإلزام؛ تشترك العديد من الأطراف في لغة ولا تحتاج إلى اللغة الإنجليزية؛ وفي بعض الأطراف، يقل احتمال أن يكون المسؤولون خارج العواصم قادرين على قراءة اللغة الإنجليزية ولكنهم غالبًا ما يشاركون في تنفيذ الطلبات.

52. هكذا، تمت صياغة الفقرة 1 بعبارة "لغة مقبولة للطرف متلقي الطلب أو الطرف الذي تم إشعاره بموجب المادة 7". يجوز لهذا الطرف تحديد اللغات المقبولة - على سبيل المثال اللغات التي يتم التحدث بها على نطاق واسع مثل الإنجليزية أو الإسبانية أو الفرنسية - حتى عندما لا يتم النص عليها في قانونه الوطني أو معاهداته.

53. كما هو وارد في الفقرة 1، تشير عبارة "[الطلبات] والأوامر والمعلومات المرفقة" إلى:

- بموجب المادة 8، الطلب (الفقرة 3)، الأمر (الفقرة 3 (أ))، المعلومات الداعمة (الفقرة 3 (ب)) وأي تعليمات إجرائية خاصة (الفقرة 3 (ج))؛
- بالنسبة للأطراف التي تطلب الإشعار بموجب المادة 7، الفقرة 5، الأمر (الفقرة 3)، والمعلومات التكميلية (الفقرة 4) وملخص الوقائع (الفقرة 5 (أ))؛
- بموجب المادة 9، الطلب (الفقرة 3).

"الطلبات" تشير أيضًا إلى محتويات الطلبات بموجب المواد 10 و11 و12 والتي تتضمن الوثائق التي تشكل جزءًا من الطلب.

54. عملياً، قد تكون بعض البلدان مستعدة لقبول الطلبات والأوامر بلغة غير اللغة المحددة في القانون الوطني أو في المعاهدات. هكذا، مرة واحدة في السنة، سوف تشارك لجنة الاتفاقية المتعلقة بالجريمة الالكترونية في استطلاع غير رسمي للغات المقبولة للطلبات والأوامر. يجوز للأطراف تغيير معلوماتهم في أي وقت وسيتم إبلاغ جميع الأطراف بأي تغيير من هذا القبيل. قد يصرحون بأنهم يقبلون لغات محددة فقط لأشكال معينة من المساعدة. ستكون نتائج هذا الاستطلاع واضحة لجميع الأطراف في الاتفاقية، وليس فقط الأطراف في هذا البروتوكول.

55. يوضح هذا الحكم العملي الأهمية القصوى لتسريع التعاون. يوفر أساسًا تعاهديًا للطرف لقبول لغات إضافية لأغراض هذا البروتوكول.

56. في كثير من الحالات، أبرمت الأطراف معاهدات للمساعدة المتبادلة تحدد اللغة أو اللغات التي يجب أن تقدم بها الطلبات بموجب تلك المعاهدات. لا تتعارض هذه المادة مع شروط تلك المعاهدات أو الاتفاقات الأخرى بين الأطراف. علاوة على ذلك، من المتوقع، لأغراض هذا البروتوكول، أن تتضمن "اللغة المقبولة للطرف متلقي الطلب أو الطرف الذي تم إشعاره بموجب المادة 7" أي لغة أو لغات تحددها تلك المعاهدات أو الاتفاقات. لذلك، ينبغي للطرف مقدم الطلب أن يطبق اللغة المحددة في معاهدات المساعدة المتبادلة أو الاتفاقات الأخرى على الطلبات والإشعارات التي تتم بموجب هذا البروتوكول، ما لم يذكر الطرف متلقي الطلب أو الذي تم إشعاره أنه مستعد أيضًا لقبول مثل هذه الطلبات أو الإشعار بلغات أخرى.

57. سوف ينعكس استعداد أي طرف لقبول لغات أخرى من خلال إشارته إلى لجنة الاتفاقية المتعلقة بالجريمة الالكترونية بأنه يعتزم قبول بعض أو كل أنواع الطلبات أو الإشعار بالأوامر بموجب هذا البروتوكول بلغة أخرى.

58. تحدد الفقرة 2 اللغة (أو اللغات) التي يجب أن يستخدمها الطرف المُصدر لتقديم الطلبات أو الأوامر والمعلومات المرفقة لمقدمي الخدمات أو الكيانات التي تقدم خدمات تسجيل اسم النطاق في إقليم طرف آخر وفقًا للمادتين 7 و6 على التوالي. يهدف هذا الحكم لضمان التعاون السريع وزيادة اليقين دون فرض عبء إضافي على مقدمي الخدمات أو الكيانات عندما يتلقون أوامر أو طلبات للكشف عن البيانات. يشير الخيار الأول، المنصوص عليه في الفقرة 2 (أ)، إلى أنه يمكن تقديم الأمر أو الطلب بلغة يقبل بها مقدم الخدمة أو الكيان عادةً أوامر وطنية أو طلبات من سلطاته في إطار إجراء تحقيقات أو دعاوى جنائية محددة ("دعاوى وطنية مماثلة"). بالنسبة للأطراف التي لديها لغة رسمية واحدة أو أكثر، قد يشمل ذلك إحدى تلك اللغات. يشير الخيار الثاني، المنصوص عليه في الفقرة 2 (ب)، إلى أنه إذا

وافق مقدم الخدمة أو الكيان على تلقي أوامر أو طلبات بلغة أخرى، على سبيل المثال لغة مقره الرئيسي، فيمكن تقديم هذه الطلبات والمعلومات المرفقة بتلك اللغة. كخيار ثالث، تنص الفقرة 2 (ج) على أنه في حالة عدم إصدار الأمر أو الطلب والمعلومات المرفقة بإحدى لغات الخيارين الأولين، يجب أن تكون مصحوبة بترجمة إلى إحدى هاتين اللغتين.

59. على النحو الوارد في الفقرة 2، تشير عبارة "[الأوامر] بموجب المادة 7 والطلبات بموجب المادة 6 وأي معلومات مرفقة" إلى:

- الطلب بموجب المادة 6 (الفقرة 3)؛ و
- بموجب المادة 7، الترتيب (الفقرة 3) والمعلومات التكميلية (الفقرة 4).

60. عندما يطلب أحد الأطراف إشعارًا وفقًا للمادة 7، يجب أن يكون الطرف مقدم الطلب مستعدًا لإرسال الأمر وأي معلومات مرفقة بلغة مقبولة للطرف الذي يطلب الإشعار، على الرغم من قبول مقدم الخدمة للغات أخرى.

61. ستسعى لجنة الاتفاقية المتعلقة بالجريمة الالكترونية أيضًا بشكل غير رسمي إلى جمع معلومات عن اللغات التي يتم بها تقديم الطلبات والأوامر والمعلومات المرفقة لمقدمي الخدمات والكيانات التي تقدم خدمات تسجيل اسم النطاق وفقًا للفقرة 2 من المادة 4، وتوعية الأطراف منها كجزء من الاستطلاع المبين في الفقرة 54 من التقرير التفسيري أعلاه.

الفصل الثاني - تدابير لتعزيز التعاون

القسم 1 - المبادئ العامة المطبقة على الفصل الثاني

المادة 5 - المبادئ العامة المطبقة على الفصل الثاني

62. توضح الفقرة 1 من المادة 5، كما هو وارد في المادة 23 والفقرة 25 من المادة 1 من الاتفاقية، يجب أن تتعاون الأطراف، وفقاً لأحكام الفصل الثاني، "إلى أقصى حد ممكن". يقتضي هذا المبدأ من الأطراف أن تقدم تعاوناً واسع النطاق وأن تقلل إلى أدنى حد العوائق التي تحول دون التدفق السلس والسريع للمعلومات والأدلة على الصعيد الدولي.

63. تنظم الفقرات من 2 إلى 5 تدابير التعاون السبعة لهذا البروتوكول في أربعة أقسام مختلفة تتبع القسم الأول المتعلق بالمبادئ العامة. وتنقسم هذه الأقسام إلى أنواع التعاون المطلوب: فالقسم 2 يغطي التعاون المباشر مع الكيانات الخاصة؛ ويتضمن القسم 3 أشكال التعاون الدولي المعزز بين السلطات للكشف عن البيانات المخزنة؛ وينص القسم 4 على المساعدة المتبادلة في حالات الطوارئ؛ وتختتم المادة 5 بأحكام التعاون الدولي التي تطبق في حالة عدم وجود معاهدة أو ترتيب على أساس تشريعات موحدة

أو متبادلة بين الأطراف المعنية. يتم تنظيم هذه الأقسام أيضًا تقريبًا في سلسلة من أشكال المساعدة الاستقصائية التي غالبًا ما يتم السعي إليها في وقت مبكر من التحقيق - للحصول على الكشف عن تسجيل اسم النطاق ومعلومات المشترك - إلى طلبات بيانات الحركة ثم بيانات المحتوى، يليها التداول بالفيديو وفرق التحقيق المشتركة، وهي أشكال من المساعدة كثيرا ما يتم طلبها في المراحل اللاحقة من التحقيق.

64. يوضح هذا القسم المتعلق بالمبادئ العامة مدى تأثر أو عدم تأثر كل تدبير بوجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل بين الأطراف المعنية، أي الطرف مقدم الطلب والطرف متلقي الطلب للتعاون بين الحكومات، والطرف الذي يسعى للحصول على المعلومات والطرف الذي يقع على إقليمه الكيان الخاص الذي يمتلك أو يتحكم في هذه المعلومات من أجل التعاون المباشر بموجب المادتين 6 و7. "ترتيب على أساس تشريع موحد أو متبادل" يُقصد به الإشارة إلى ترتيبات "مثل نظام التعاون الذي تم تطويره بين بلدان الشمال الأوروبي، والذي تم قبوله أيضًا بموجب الاتفاقية الأوروبية للمساعدة المتبادلة في المسائل الجنائية (المادة 25، الفقرة 4) وبين أعضاء الكومنولث" (انظر التقرير التفسيري، الفقرة 263، للاتفاقية). تنطبق التدابير الواردة في الأقسام من 2 إلى 4 من هذا الفصل سواء كانت الأطراف المعنية ملزمة بشكل متبادل أم لا باتفاق أو ترتيب مساعدة متبادلة ساري المفعول على أساس تشريع موحد أو متبادل. تنطبق أحكام التعاون الدولي الواردة في القسم 5 فقط في حالة عدم وجود مثل هذه الاتفاقات أو الترتيبات، ما لم ينص على خلاف ذلك.

65. كما هو موضح في الفقرة 2 من هذه المادة، يتكون القسم 2 من هذا الفصل من المادة 6، بعنوان "طلب معلومات تسجيل اسم النطاق"، والمادة 7، بعنوان "الكشف عن معلومات المشترك". هذه هي ما يسمى بمواد "التعاون المباشر"، والتي تسمح للسلطات المختصة للطرف بالتعامل مباشرة مع الكيانات الخاصة - أي مع الكيانات التي تقدم خدمات تسجيل اسم النطاق في المادة 6 ومع مقدمي الخدمات في المادة 7 - من أجل أغراض إجراء تحقيقات أو دعاوى جنائية محددة. ينطبق القسم 2 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الطرف الذي يسعى للحصول على المعلومات والطرف الذي يوجد على أراضيه الكيان الخاص الذي يمتلك هذه المعلومات أو يتحكم فيها.

66. كما هو موضح في الفقرة 3 من هذه المادة، يتكون القسم 3 من هذا الفصل من المادة 8، بعنوان "تنفيذ أوامر من طرف آخر للتعجيل بتقديم معلومات المشترك وبيانات الحركة"، والمادة 9، بعنوان "الكشف المعجل عن بيانات الكمبيوتر المخزنة في حالات الطوارئ". هذه تدابير "تعزز التعاون الدولي بين السلطات"، أي أنها تنص على التعاون بين السلطات المختصة، ولكنها ذات طبيعة مختلفة عن التعاون الدولي التقليدي. ينطبق

القسم 3 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف مقدمة الطلب والأطراف متلقية الطلب.

67. كما هو موضح في الفقرة 4 من هذه المادة، يتكون القسم 4 من هذا الفصل من المادة 10، بعنوان "المساعدة المتبادلة في حالات الطوارئ". على الرغم من أن المساعدة المتبادلة في حالات الطوارئ هي أحد أحكام المساعدة المتبادلة، إلا أنها أداة تعاون مهمة لحالات الطوارئ التي لم يتم النص عليها صراحة في العديد من معاهدات المساعدة المتبادلة. لذلك، قرر فريق الصياغة أن هذا القسم يجب أن ينطبق سواء كان هناك اتفاق أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف المعنية. فيما يتعلق بالإجراءات التي تحكم المساعدة المتبادلة في حالات الطوارئ، هناك احتمالان. عندما تكون الأطراف المعنية ملزمة بشكل متبادل باتفاق أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول، يتم استكمال القسم 4 بأحكام تلك الاتفاقية ما لم تقرر الأطراف المعنية بشكل متبادل تطبيق أحكام معينة من الاتفاقية بدلاً منها (انظر المادة 10، الفقرة 8، من هذا البروتوكول). عندما لا تكون الأطراف المعنية ملزمة بشكل متبادل بمثل هذا الاتفاق أو الترتيب، تطبق الأطراف إجراءات معينة منصوص عليها في المادتين 27 و28 من الاتفاقية، فيما يتعلق بالمساعدة المتبادلة في حالة عدم وجود معاهدة (انظر المادة 10، الفقرة 7، من هذا البروتوكول).

68. كما هو موضح في الفقرة 5 من هذه المادة، يتكون القسم 5 من هذا الفصل من المادة 11، بعنوان "التداول بالفيديو"، والمادة 12، بعنوان "فرق التحقيق المشتركة والتحقيقات المشتركة". هذه الأحكام هي تدابير للتعاون الدولي، لا تنطبق إلا في حالة عدم وجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف مقدمة الطلب والأطراف متلقية الطلب. لا تنطبق هذه التدابير في حالة وجود مثل هذه المعاهدة أو الترتيب، باستثناء أن المادة 12، الفقرة 7، تنطبق سواء كانت هذه المعاهدة أو الترتيب موجود أم لا. ومع ذلك، يجوز للأطراف المعنية أن تقرر بشكل متبادل تطبيق أحكام القسم 5 بدلاً من مثل هذه المعاهدة أو الترتيب القائم ما لم يكن ذلك محظورًا بموجب شروط المعاهدة أو الترتيب.

69. صياغة الفقرة 6 مستوحاة من الفقرة 5 من المادة 25 من الاتفاقية، والفقرة 259 من التقرير التفسيري للاتفاقية صالحة هنا أيضا: "عندما يُسمح للطرف متلقي الطلب أن يشترط التجريم المزدوج كشرط لتقديم المساعدة...يعتبر التجريم المزدوج موجودا إذا كان السلوك الكامن وراء الجريمة التي يتم طلب المساعدة من أجلها يعد أيضًا جريمة جنائية بموجب قوانين الطرف متلقي الطلب، حتى إذا كانت قوانينه تضع الجريمة ضمن فئة مختلفة من الجرائم أو تستخدم مصطلحات مختلفة في تسمية الجريمة. وكان يُعتقد أن هذا الحكم ضروري لضمان عدم اعتماد الأطراف متلقية الطلب اختبارًا شديد الصرامة عند تطبيق التجريم المزدوج.

بالنظر إلى الاختلافات في النظم القانونية الوطنية، لا بد أن تظهر اختلافات في المصطلحات وتصنيف السلوك الإجرامي. إذا كان السلوك يشكل انتهاكًا جنائيًا بموجب كلا النظامين، فإن مثل هذه الاختلافات الفنية لا ينبغي أن تعرقل المساعدة. وبدلاً من ذلك، في المسائل التي ينطبق فيها معيار التجريم المزدوج، ينبغي تطبيقه بطريقة مرنة تسهل منح المساعدة".

70. تنص الفقرة 7 على أن "الأحكام الواردة في هذا الفصل لا تقيد التعاون بين الأطراف، أو بين الأطراف ومقدمي الخدمات أو الكيانات الأخرى، من خلال الاتفاقات أو الترتيبات أو الممارسات أو القوانين الوطنية الأخرى المطبقة". وهذا يعني أن البروتوكول لا يلغي أو يقيد أي تعاون بين الأطراف أو بين الأطراف والكيانات الخاصة المتاح بوسائل أخرى - سواء من خلال الاتفاقات أو الترتيبات سارية المفعول أو القانون الوطني أو حتى الممارسات غير الرسمية. كان فريق الصياغة يعتزم توسيع، وليس تقييد، الأدوات المتاحة في مجموعة أدوات ممارس إنفاذ القانون للحصول على معلومات أو أدلة لإجراء تحقيقات أو دعاوى جنائية محددة. أدرك فريق الصياغة أنه في حالات معينة، قد تكون الآليات القائمة، مثل المساعدة المتبادلة، هي الأفضل للممارس لاستخدامها. مع ذلك، في حالات أخرى، قد تكون الأدوات التي ينشئها هذا البروتوكول أكثر كفاءة أو أفضل. على سبيل المثال، إذا احتاجت السلطة المختصة إلى بيانات المحتوى على أساس غير طارئ، فمن المحتمل أن تختار استخدام طلب المساعدة المتبادلة التقليدي بموجب معاهدة ثنائية أو بموجب المادة 27 من الاتفاقية، حسب الاقتضاء، لأن البروتوكول لا يحتوي على أحكام للحصول على بيانات المحتوى على أساس غير طارئ. ولكن إذا احتاجت إلى معلومات المشترك، فقد تختار استخدام المادة 7 من البروتوكول لإصدار أمر مباشرة إلى مزود الخدمة.

71. أخيرًا، يسمح عدد من أحكام الفصل الثاني وغيرها من أحكام هذا البروتوكول بفرض قيود أو شروط على الاستخدام، مثل السرية. عندما يخضع استلام الأدلة أو المعلومات المطلوبة، وفقًا لأحكام هذا البروتوكول، لقيد أو شرط الاستخدام هذا، أقر المفاوضون بالاستثناءات وهي ضمنية في النص. أولاً، كتدبير لحماية حقوق الإنسان والحريات وفقًا للمادة 13، بموجب المبادئ القانونية الأساسية للعديد من الدول، إذا اعتبرت المواد المقدمة للطرف المتلقي تؤدي إلى تبرئة الشخص المتهم، فيجب الكشف عنها لـلدفاع أو السلطة القضائية. لا يخل هذا المبدأ بنص المادة 12، الفقرة 6 (ب)، والتقرير التفسيري، الفقرة 215، التي يمكن تطبيقها عندما تكون الأطراف قد أنشأت فريق تحقيق مشترك. وقد اعتبر فريق الصياغة أنه في مثل هذه الحالات، يقوم الطرف المتلقي بإخطار الطرف الناقل قبل الكشف، وإذا طلب ذلك، يتشاور مع الطرف الناقل. ثانيًا، عندما يتم فرض قيود على الاستخدام فيما يتعلق بالمواد الواردة بموجب هذا البروتوكول والمتوقع استخدامها في المحاكمة، فإن المحاكمة (بما في ذلك الكشف خلال الإجراءات القضائية السابقة للمحاكمة) تكون عادةً محاكمة علنية. بمجرد نشرها للجمهور في المحاكمة، تنتقل المواد إلى المجال

العام. في هذه الحالات، لا يمكن ضمان سرية التحقيق أو الإجراء الذي تم البحث عن المواد من أجله. تشبه هذه الاستثناءات تلك المتعلقة بتطبيق الفقرة 2 من المادة 28 من الاتفاقية كما هو موضح في الفقرة 278 من التقرير التفسيري للاتفاقية. أخيرًا، يمكن استخدام المواد لغرض آخر عندما يتم الحصول على الموافقة المسبقة للطرف الناقل.

القسم 2 – إجراءات تعزز التعاون المباشر مع مقدمي الخدمات والكيانات في الأطراف الأخرى

المادة 6 – طلب معلومات تسجيل اسم النطاق

72. تنص المادة 6 على إجراء ينص على التعاون المباشر بين سلطات أحد الأطراف وكيان يقدم خدمات تسجيل اسم النطاق على إقليم طرف آخر للحصول على معلومات حول تسجيلات اسم نطاق الإنترنت. على غرار المادة 7، يستند الإجراء إلى استنتاجات فريق الأدلة السحابية التابعة للجنة اتفاقية الجرائم الإلكترونية، والتي تقر بأهمية الوصول عبر الحدود في الوقت المناسب إلى الأدلة الإلكترونية في تحقيقات أو دعاوى جنائية محددة، في ضوء التحديات التي تطرحها الإجراءات الحالية للحصول على الأدلة الإلكترونية.

73. يقر الإجراء أيضًا بالنموذج الحالي لإدارة الإنترنت الذي يعتمد على تطوير سياسات أصحاب المصلحة المتعددين القائمة على توافق الآراء. تستند هذه السياسات عادة على القانون التعاقدي. يهدف الإجراء المنصوص عليه في هذه المادة إلى استكمال تلك السياسات لأغراض هذا البروتوكول، أي لغرض تحقيقات أو دعاوى جنائية محددة. غالبًا ما يكون الحصول على بيانات تسجيل اسم النطاق أمرًا لا غنى عنه، كخطوة أولى للعديد من التحقيقات الجنائية ولتحديد مكان توجيه طلبات التعاون الدولي.

74. يسهّل الجناة أشكالاً عديدة من الجرائم الالكترونية بإنشاء النطاقات واستغلالها لأغراض خبيثة وغير مشروعة. على سبيل المثال، يمكن استخدام اسم النطاق كمنصة لنشر البرامج الضارة وشبكات البوتات والتصيد الاحتيالي والأنشطة المماثلة والاحتيال وتوزيع مواد الاعتداء على الأطفال ولأغراض إجرامية أخرى. وبالتالي، فإن الوصول إلى المعلومات الخاصة بالشخص الطبيعي أو الاعتباري الذي قام بتسجيل النطاق ("أمناء السجلات") أمر بالغ الأهمية لتحديد المشتبه به في تحقيق أو دعوى جنائية محددة. في حين كانت بيانات تسجيل اسم النطاق متاحة للجمهور تاريخياً، فإن الوصول إلى بعض المعلومات مقيد الآن، مما يؤثر على السلطات القضائية وسلطات إنفاذ القانون في مهام السياسة العامة الخاصة بهم.

75. تحتفظ الكيانات التي تقدم خدمات تسجيل أسماء النطاق بمعلومات عن تسجيل أسماء النطاق. وتشمل هذه المنظمات التي تبيع أسماء النطاق للجمهور ("المسجِلين") وكذلك مشغلي السجلات الإقليميين أو الوطنيين الذين يحتفظون

بقواعد بيانات موثوقة ("السجلات") لجميع أسماء النطاق المسجلة لنطاق رفيع المستوى والتي تقبل طلبات التسجيل. وفي حالات معينة، يمكن أن تكون هذه المعلومات بيانات شخصية ويمكن حمايتها بموجب قوانين حماية البيانات في الطرف الذي يوجد فيه الكيان المعني الذي يقدم خدمات تسجيل أسماء النطاق (المسجِل أو السجل) أو الذي يوجد فيه الشخص الذي تتعلق به البيانات.

76. الهدف من المادة 6 هو توفير إطار عمل يتسم بالفعالية والكفاءة للحصول على معلومات لتحديد أو الاتصال بمسجل اسم النطاق. يعتمد شكل التنفيذ على الاعتبارات القانونية والسياساتية لكل من الأطراف. تهدف هذه المادة إلى استكمال سياسات وممارسات حوكمة الإنترنت الحالية والمستقبلية.

الفقرة 1

77. بموجب الفقرة 1، يجب على كل طرف أن يتبنى التدابير اللازمة لتخويل سلطاته المختصة صلاحية إصدار طلبات مباشرة إلى كيان يقدم خدمات تسجيل اسم النطاق على إقليم طرف آخر، أي دون إلزام السلطات في الإقليم الذي يوجد فيه الكيان بالعمل كوسيط. تعطي الفقرة 1 للأطراف المرونة فيما يتعلق بالشكل الذي يتم تقديم الطلبات به، لأن الشكل يعتمد على الاعتبارات القانونية والسياسية للأطراف. يمكن لأي طرف استخدام الإجراءات المتاحة بموجب قانونه الوطني، بما في ذلك إصدار أمر؛ ومع ذلك، لأغراض المادة 6، يتم التعامل مع هذا الأمر على أنه طلب غير ملزم. وبالتالي، فإن شكل الطلب أو الآثار التي يحدثها بموجب القانون الوطني للطرف مقدم الطالب لن يؤثر على الطابع الطوعي للتعاون الدولي بموجب هذه المادة، وإذا لم يكشف الكيان عن المعلومات المطلوبة، فستكون الفقرة 5 قابلة للتطبيق.

78. إن الصياغة الواردة في الفقرة 1 من المادة 6 واسعة بما يكفي للإقرار بإمكانية إصدار مثل هذا الطلب ويمكن الحصول على المعلومات عبر واجهة أو بوابة أو أداة تقنية أخرى توفرها المنظمات. على سبيل المثال، قد توفر إحدى المؤسسات واجهة أو أداة بحث لتسهيل أو تسريع الكشف عن معلومات تسجيل اسم النطاق بعد الطلب. ومع ذلك، بدلاً من تكييف هذه المادة مع أي بوابة أو واجهة معينة، تستخدم هذه المادة مصطلحات محايدة من الناحية التكنولوجية للسماح بالتكيف مع التكنولوجيا المتطورة.

79. على النحو المنصوص عليه في المادة 2، لا يجوز إصدار طلب بموجب الفقرة 1 إلا لأغراض إجراء تحقيقات أو دعاوى جنائية محددة. تم تعريف مصطلح "السلطة المختصة" في المادة 3، الفقرة 2 (ب)، ويشير إلى "سلطة قضائية أو إدارية أو غيرها من سلطات إنفاذ القانون المخولة بموجب القانون الوطني أن تأمر بتنفيذ التدابير بموجب هذا البروتوكول أو تفوضها أو تتعهد بها". يشير "الكيان الذي يقدم خدمات تسجيل اسم النطاق" حاليًا إلى المسجِلين والسجلات. لأخذ الوضع الحالي في الاعتبار وفي نفس الوقت السماح

بالتكيف مع نماذج الأعمال وقد تتغير بنية الإنترنت بمرور الوقت، تستخدم هذه المادة المصطلح الأكثر عمومية "الكيان الذي يقدم خدمات تسجيل اسم النطاق".

80. بينما يتم تخزين المعلومات الخاصة بتحديد هوية أو الاتصال بمسجل اسم النطاق في كثير من الأحيان من قبل الكيانات التي تقدم خدمات تسجيل اسم النطاق العامة على الصعيد العالمي، على سبيل المثال "نطاقات المستوى الأعلى العامة"، أقرت الأطراف بأن خدمات تسجيل اسم النطاق الأكثر تحديدًا تتعلق بالكيانات الوطنية أو الإقليمية ("نطاقات المستوى الأعلى لرمز البلد") يكمن تسجيلها أيضا بواسطة أشخاص أو كيانات في دول أخرى ويمكن أيضًا استخدامها من قبل الجناة. لذلك، لا تقتصر المادة 6 على الكيانات التي تقدم "نطاقات المستوى الأعلى العامة"، حيث يمكن استخدام كلا النوعين من خدمات تسجيل اسم النطاق - أو الأنواع المستقبلية من هذه الخدمات - لارتكاب الجرائم الإلكترونية.

81. تشير عبارة "معلومات لتحديد هوية أو الاتصال بمسجل اسم النطاق" إلى المعلومات التي كانت متاحة سابقًا للجمهور من خلال ما يسمى بأدوات بحث (هو إيز WHOIS)، مثل الاسم والعنوان الفعلي وعنوان البريد الإلكتروني ورقم هاتف المسجل. قد تعتبر بعض الأطراف هذه المعلومات مجموعة فرعية من معلومات المشترك على النحو المحدد في المادة 18، الفقرة 3، من الاتفاقية. معلومات تسجيل اسم النطاق هي معلومات أساسية لا تسمح باستخلاص استنتاجات دقيقة فيما يتعلق بالحياة الخاصة والعادات اليومية للأفراد. لذلك، قد يكون الكشف عنها أقل تدخلاً من الكشف عن فئات أخرى من البيانات.

الفقرة 2

82. تتطلب الفقرة 2 من كل طرف اعتماد تدابير للسماح للكيانات الموجودة على إقليمه والتي تقدم خدمات تسجيل اسم النطاق بالكشف عن هذه المعلومات استجابة لطلب بموجب الفقرة 1، مع مراعاة الشروط المعقولة التي ينص عليها القانون الوطني، والتي قد تتضمن في بعض الأطراف شروط حماية البيانات. في الوقت نفسه، تحد المادة 14 من القدرة على رفض عمليات نقل البيانات بموجب قواعد حماية البيانات لعمليات النقل الدولية، وتم إدراج العوامل الواردة في الفقرة 83 لتسهيل المعالجة بموجب قواعد حماية البيانات. يجب أن تسهل هذه الإجراءات الكشف عن البيانات المطلوبة بطريقة سريعة وفعالة إلى أقصى حد ممكن.

83. لا تطالب هذه المادة الأطراف بسن تشريع يلزم هذه الكيانات بالاستجابة لطلب من سلطة طرف آخر. بالتالي، قد يحتاج الكيان الذي يقدم خدمات تسجيل اسم النطاق إلى تحديد ما إذا كان سيتم الكشف عن المعلومات المطلوبة. يساعد هذا البروتوكول في هذا القرار من خلال توفير الضمانات التي من شأنها تسهيل قدرة الكيانات على الاستجابة دون صعوبة للطلبات المقدمة بموجب هذه المادة، مثل:

- ينص هذا البروتوكول أو يقتضي من الأطراف تقديم أساس قانوني للطلبات؛
- تتطلب هذه المادة أن يأتي الطلب من سلطة مختصة (المادة 6، الفقرتان 1 و3 أ، والفقرتان 79 و84 من هذا التقرير التفسيري)؛
- ينص هذا البروتوكول على تقديم طلب لأغراض تحقيقات أو إجراءات جنائية محددة (المادة 2)؛
- تتطلب هذه المادة أن يتضمن الطلب بيانًا يفيد بأن الحاجة إلى المعلومات تنشأ بسبب صلتها بتحقيق أو إجراء جنائي محدد وأن المعلومات لن تُستخدم إلا لأغراض هذا التحقيق أو الدعوى الجنائية المحددة (المادة 6، الفقرة 3 (ج))؛
- ينص هذا البروتوكول على ضمانات لمعالجة البيانات الشخصية التي تم الكشف عنها ونقلها وفقًا لمثل هذه الطلبات من خلال المادة 14؛
- المعلومات التي سيتم الكشف عنها محدودة ولن تسمح باستخلاص استنتاجات دقيقة فيما يتعلق بالحياة الخاصة للأفراد؛
- قد يُتوقع أو يُطلب من الكيانات التعاون بموجب ترتيبات تعاقدية مع شركة الإنترنت للأسماء والأرقام المخصصة (ICANN).

الفقرة 3

84. تحدد الفقرة 3 من هذه المادة المعلومات التي يجب أن تُقدم، كحد أدنى، من قبل سلطة تصدر طلباً عملاً بالفقرة 1 من هذه المادة. هذه المعلومات ذات صلة خاصة بتنفيذ الطلب من قبل الكيان الذي يقدم خدمات تسجيل اسم النطاق. يجب أن يتضمن الطلب ما يلي:

أ. تاريخ الطلب وهوية وتفاصيل الاتصال بالسلطة المختصة التي أصدرت الطلب (الفقرة 3 (أ)) (انظر الفقرة 79 من التقرير التفسيري)؛

ب. اسم النطاق الذي يتم البحث عن المعلومات حوله وقائمة مفصلة بالمعلومات المطلوبة، بما في ذلك عناصر البيانات المعينة مثل الاسم أو العنوان الفعلي أو عنوان البريد الإلكتروني أو رقم هاتف المسجِل (الفقرة 3 (ب))؛

ت. بيان بأن الطلب قد صدر بموجب هذا البروتوكول؛ من خلال الإدلاء بهذا البيان، يعتبر الطرف أن الطلب يتوافق مع أحكام هذا البروتوكول (الفقرة 3 (ج)). يؤكد الطرف مقدم الطلب أيضًا في هذا البيان أن المعلومات "[لازمة]"بسبب صلتها بتحقيق أو دعوى جنائية محددة وأن المعلومات سوف تستخدم فقط لهذا التحقيق أو الدعوى الجنائية المحددة. بالنسبة للبلدان الأوروبية، المعلومات "[لازمة]" - أي ضرورية ومتناسبة - لإجراء تحقيق أو دعوى جنائية، يجب أن تكون مستمدة من مبادئ اتفاقية مجلس أوروبا لعام 1950 لحماية حقوق الإنسان والحريات الأساسية، اجتهاداتها القضائية السارية والتشريعات

والاجتهادات القضائية الوطنية. وتنص هذه المصادر على أن السلطة أو الإجراء يجب أن يتناسب مع طبيعة الجريمة وظروفها (انظر الفقرة 146 من التقرير التفسيري للاتفاقية المتعلقة بالجريمة الإلكترونية). ستطبق الأطراف الأخرى المبادئ ذات الصلة في قانونها، مثل المبادئ ذات الصلة (أي أن الأدلة المطلوبة في الطلب يجب أن تكون ذات صلة بالتحقيق أو المحاكمة). يجب على الأطراف تجنب الطلبات العامة للكشف عن معلومات اسم النطاق ما لم تكن هناك حاجة إليها لتحقيق أو دعوى جنائية محددة؛

ث. الزمن والطريقة التي يتم بها الكشف عن المعلومات وأي تعليمات إجرائية خاصة أخرى (الفقرة 3 (د)). تهدف "التعليمات الإجرائية الخاصة" إلى إدراج أي طلب للسرية، بما في ذلك طلب عدم الكشف عن الطلب للمسجِل أو لأطراف ثالثة أخرى. إذا كانت السرية مطلوبة لتجنب الكشف المبكر عن المسألة، فيجب الإشارة إلى ذلك في الطلب. في بعض الأطراف، سيتم الحفاظ على سرية الطلب من خلال تطبيق القانون، بينما في الأطراف الأخرى ليس هذا هو الحال بالضرورة. لذلك، عند الحاجة إلى السرية، يتم تشجيع الأطراف على مراجعة المعلومات المتاحة للجمهور وطلب التوجيه من الأطراف الأخرى فيما يتعلق بالقانون الساري، وكذلك سياسات الكيانات التي تقدم خدمات تسجيل اسم النطاق فيما يتعلق بمعلومات المشترك / المسجل، قبل تقديم الطلب بموجب الفقرة 1 للكيان. بالإضافة إلى ذلك، قد تتضمن التعليمات الإجرائية الخاصة مواصفات قناة الإرسال الأكثر ملاءمة لاحتياجات السلطة.

85. لا تتضمن الفقرة 3 مطلبًا بإدراج بيان بالوقائع في الطلب، بالنظر إلى أن هذه المعلومات سرية في معظم التحقيقات الجنائية ولا يجوز الكشف عنها لطرف خاص. مع ذلك، قد يحتاج الكيان الذي يتلقى طلبًا بموجب هذه المادة إلى معلومات إضافية معينة من شأنها أن تسمح له بالتوصل إلى قرار إيجابي بشأن الطلب. لذلك، قد يسعى الكيان إلى الحصول على معلومات أخرى حيث لا يمكنه تنفيذ الطلب بطريقة أخرى.

الفقرة 4

86. الهدف من الفقرة 4 هو تشجيع استخدام الوسائل الإلكترونية عندما يوافق الكيان الذي يقدم خدمات تسجيل اسم النطاق، حيث أن الوسائل الإلكترونية هي دائمًا أكثر وسائل الاتصال كفاءةً وأسرعها. بناءً على ذلك، إذا وافق الكيان الذي يقدم خدمات تسجيل اسم النطاق، يجوز للطرف تقديم طلب إلى الكيان في شكل إلكتروني، على سبيل المثال باستخدام البريد الإلكتروني أو البوابات الإلكترونية أو وسائل أخرى. في حين أنه من المفترض أن الكيانات تفضل تلقي الطلبات في مثل هذه الصيغة، فليس من الضروري استخدام هذه الصيغة فقط. كما هو منصوص عليه في مواد أخرى من هذا البروتوكول تسمح بأوامر أو طلبات في شكل إلكتروني (مثل المواد 7 و8 وغيرها)، قد تكون هناك حاجة إلى مستويات مناسبة من الأمن وإمكانية التحقق من الهوية. يجوز للأطراف والكيانات أن تقرر بنفسها ما

إذا كانت القنوات أو الوسائل آمنة للإرسال وإمكانية التحقق من الهوية متاحة، أو ما إذا كانت الحماية الأمنية الخاصة (بما في ذلك التشفير) قد تكون ضرورية في قضية حساسة معينة.

الفقرة 5

87. بينما يتعلق هذا الحكم "بالطلبات" وليس "الأوامر" الإلزامية للكشف عن بيانات تسجيل اسم النطاق، فمن المتوقع أن يكون الكيان متلقي الطلب قادرًا على الكشف عن المعلومات المطلوبة وفقًا لهذا الحكم عندما تكون الشروط المطبقة مستوفاة. إذا لم يكشف الكيان عن المعلومات المطلوبة، فيمكن النظر في آليات أخرى للحصول على المعلومات، اعتمادًا على الظروف. لذلك، تنص الفقرة 5 على التشاور بين الأطراف المعنية من أجل الحصول على معلومات إضافية وتحديد الآليات المتاحة، على سبيل المثال لتحسين التعاون في المستقبل. من أجل تسهيل المشاورات، تنص الفقرة 5 أيضًا على أنه يجوز للطرف مقدم الطلب أن يسعى للحصول على مزيد من المعلومات من الكيان. يتم تشجيع الكيانات على شرح أسباب عدم الكشف عن البيانات المطلوبة استجابة لمثل هذا الطلب.

الفقرة 6

88. تتطلب الفقرة 6، أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة، أو في أي وقت آخر، أن تعين الأطراف سلطة لغرض التشاور بموجب الفقرة 5. سيساعد توفير جهة الاتصال في الطرف الذي يقع فيه الكيان، الطرف مقدم الطلب في التحديد السريع للإجراءات المتاحة للحصول على البيانات المطلوبة، إذا رفض الكيان تنفيذ طلب مباشر تم إجراؤه بموجب المادة 6.

الفقرة 7

89. الفقرة 7 لا تحتاج إلى شرح وتنص على أن يقوم الأمين العام لمجلس أوروبا بإنشاء والاحتفاظ بسجل للسلطات المعينة بموجب الفقرة 6 وأن يضمن كل طرف صحة التفاصيل التي قدمها للسجل في كل الأوقات.

المادة 7 – الكشف عن معلومات المشترك

90. تنص المادة 7 على إجراء ينص على التعاون المباشر بين سلطات أحد الأطراف ومقدم الخدمة على إقليم طرف آخر للحصول على معلومات المشترك. يستند الإجراء إلى الاستنتاجات التي توصل إليها فريق الأدلة السحابية والمذكرة التوجيهية للجنة الاتفاقية المعنية بالجريمة الالكترونية بشأن المادة 18 من الاتفاقية، والتي تقر بأهمية الوصول عبر الحدود في الوقت المناسب إلى الأدلة الإلكترونية في تحقيقات أو دعاوى جنائية محددة، في ضوء التحديات التي تطرحها الإجراءات الحالية للحصول على الأدلة الإلكترونية من مقدمي الخدمات في البلدان الأخرى.

91. يتطلب عدد متزايد من التحقيقات أو الدعاوى الجنائية في الوقت الحاضر الوصول إلى الأدلة الإلكترونية من مقدمي الخدمات في البلدان الأخرى. حتى بالنسبة للجرائم ذات الطابع الوطني بالكامل - أي عندما تكون الجريمة والضحية والجاني جميعًا في نفس بلد سلطة التحقيق - قد يكون الدليل الإلكتروني محتفظًا به من قبل مقدم خدمة على إقليم بلد آخر. في كثير من الحالات، قد يُطلب من السلطات التي تحقق في جريمة استخدام إجراءات التعاون الدولي، مثل المساعدة المتبادلة، والتي لا تكون دائمًا قادرة على تقديم المساعدة بسرعة أو بشكل فعال بما يكفي لاحتياجات التحقيق أو الدعوى بسبب استمرار زيادة حجم طلبات البحث عن أدلة إلكترونية.

92. المعلومات المتعلقة بالمشتركين هي أكثر المعلومات المطلوبة في التحقيقات الجنائية المتعلقة بالجرائم الالكترونية وأنواع الجرائم الأخرى التي تتطلب أدلة إلكترونية بشأنها. فهي توفر هوية مشترك معين في خدمة ما وعنوانه ومعلومات مماثلة محددة في المادة 18، الفقرة 3، من الاتفاقية. لا يسمح باستنتاجات دقيقة بشأن الحياة الخاصة والعادات اليومية للأفراد المعنيين، مما يعني أن الكشف عنها قد يكون بدرجة أقل من التطفل مقارنة بالكشف عن فئات أخرى من البيانات.

93. تُعرَّف معلومات المشترك في الفقرة 3 من المادة 18 من الاتفاقية (مدرجة في الفقرة 1 من المادة 3 من هذا البروتوكول) على أنها "أي معلومات واردة في شكل بيانات كمبيوتر أو أي شكل آخر تحتفظ به خدمة ما، تتعلق بالمشتركين في خدماته بخلاف بيانات الحركة أو المحتوى والتي يمكن من خلالها إنشاء: أ) نوع خدمة الاتصال المستخدمة والأحكام التقنية المتخذة بشأنها ومدة الخدمة؛ ب) هوية المشترك، العنوان البريدي أو الجغرافي، الهاتف ورقم الوصول الآخر، معلومات الفواتير والدفع، المتاحة على أساس اتفاقية أو ترتيب الخدمة؛ ج) أي معلومات أخرى على موقع تركيب معدات الاتصالات، متاحة على أساس اتفاقية أو ترتيب الخدمة" (انظر أيضًا التقرير التفسيري للاتفاقية، الفقرات من 177 إلى 183). قد تتضمن المعلومات المطلوبة لغرض تحديد مشترك في خدمة معينة معلومات عنوان بروتوكول الإنترنت على سبيل المثال، عنوان بروتوكول الإنترنت المستخدم أثناء إنشاء الحساب، أو أحدث عنوان بروتوكول الإنترنت لتسجيل الدخول أو عنوان بروتوكول الإنترنت المستخدم أثناء زمن محدد. في بعض الأطراف، يتم التعامل مع هذه المعلومات على أنها بيانات حركة لأسباب مختلفة، بما في ذلك اعتبارها ذات صلة بإرسال اتصال ما. بناءً على ذلك، تنص الفقرة 9 (ب) من المادة 7 على تحفظ لبعض الأطراف.

94. في حين أن المادة 18 من الاتفاقية تتناول بالفعل بعض جوانب الحاجة إلى الوصول السريع والفعال إلى الأدلة الإلكترونية من مقدمي الخدمات، فإنها لا توفر في حد ذاتها حلاً كاملاً لهذا التحدي، حيث تنطبق هذه المادة في نطاق محدود بدرجة أكبر على مجموعة من الظروف. على وجه التحديد، تنطبق المادة 18 من الاتفاقية عندما يكون مقدم الخدمة

"في إقليم" الطرف مُصدر الطلب (انظر المادة 18، الفقرة 1 (أ)، من الاتفاقية) أو "يعرض خدماته" في الطرف مُصدر الطلب (انظر المادة 18، الفقرة 1 (ب) من الاتفاقية). بالنظر إلى قيود المادة 18 والتحديات التي تواجه المساعدة المتبادلة، فقد اعتبر أنه من المهم إنشاء آلية تكميلية من شأنها أن تتيح وصولاً أكثر فعالية عبر الحدود إلى المعلومات اللازمة لتحقيقات أو دعاوى جنائية محددة. وفقًا لذلك، يتجاوز نطاق المادة 7 من هذا البروتوكول نطاق المادة 18 من الاتفاقية من خلال السماح لأحد الأطراف بإصدار أوامر معينة لمقدمي الخدمات في إقليم طرف آخر. أقرت الأطراف أنه على الرغم من أن مثل هذه الأوامر المباشرة من سلطات أحد الأطراف إلى مقدمي الخدمات الموجودين في طرف آخر مرغوب فيها للوصول السريع والفعال إلى المعلومات، يجب ألا يُسمح للطرف باستخدام جميع آليات الإنفاذ المتاحة بموجب قانونه الوطني لإنفاذ هذه الأوامر. لهذا السبب، فإن تنفيذ هذه الأوامر في الحالات التي لا يكشف فيها مقدم الخدمة عن معلومات المشترك المحددة يكون محدودًا على النحو المنصوص عليه في الفقرة 7 من المادة 7. ينص هذا الإجراء على ضمانات تأخذ في الاعتبار المتطلبات الفريدة الناشئة عن مباشرة التعاون بين سلطات أحد الأطراف مع مقدمي الخدمات الموجودين في طرف آخر.

95. كما هو مبين في الفقرة 7 من المادة 5، لا تخل هذه المادة بقدرة الأطراف على تنفيذ الأوامر الصادرة بموجب المادة 18 أو غير ذلك على النحو الذي تسمح به الاتفاقية، كما أنها لا تخل بالتعاون (بما في ذلك التعاون التلقائي) بين الأطراف، أو بين الأطراف ومقدمي الخدمات، من خلال الاتفاقات أو الترتيبات أو الممارسات الأخرى سارية المفعول أو القانون الوطني.

الفقرة 1

96. تتطلب الفقرة 1 من الأطراف تزويد السلطات المختصة بالصلاحيات اللازمة لإصدار أمر إلى مزود الخدمة على أراضي طرف آخر للحصول على الكشف عن معلومات المشترك. لا يجوز إصدار الأمر إلا لمعلومات المشترك المحددة والمخزنة.

97. تتضمن الفقرة 1 أيضًا اشتراط إصدار الأوامر وتقديمها فقط في سياق "تحقيقات أو دعاوى جنائية محددة" للطرف مُصدر الطلب، حيث تُستخدم هذه العبارة في المادة 2 من هذا البروتوكول. كتقييد إضافي، يجوز أيضًا إصدار الأوامر فقط للحصول على المعلومات "اللازمة" لهذا التحقيق أو الدعوى. بالنسبة للبلدان الأوروبية، المعلومات اللازمة - أي الضرورية والمتناسبة – لإجراء تحقيق أو دعوى جنائية ينبغي أن تكون مستمدة من مبادئ اتفاقية مجلس أوروبا لعام 1950 لحماية حقوق الإنسان والحريات الأساسية، واجتهاداتها القضائية السارية، التشريع والاجتهادات القضائية الوطنية. تنص هذه المصادر على أن السلطة أو الإجراء يجب أن يتناسب مع طبيعة الجريمة وظروفها (انظر الفقرة 146 من التقرير التفسيري للاتفاقية). ستطبق الأطراف الأخرى المبادئ ذات

الصلة في قانونها، مثل المبادئ ذات الصلة (أي أن الأدلة المطلوبة بموجب أمر ما يجب أن تكون ذات صلة بالتحقيق أو المقاضاة) وتجنب الأوامر العامة بشكل مفرط للكشف عن معلومات المشترك. يعيد هذا التقييد التأكيد على المبدأ المنصوص عليه بالفعل في المادة 2 من هذا البروتوكول والفقرة 1 من المادة 7، الذي يقصر التدبير على التحقيقات أو الدعاوى الجنائية المحددة، وهو أنه لا يجوز استخدام الأحكام لإصدار كميات كبيرة أو ضخمة من البيانات (انظر أيضًا الفقرة 182 من التقرير التفسيري للاتفاقية).

98. يشير مصطلح "السلطة المختصة"، كما هو معرّف في الفقرة 2 (ب) من المادة 3، إلى سلطة قضائية أو إدارية أو سلطة أخرى معنية بإنفاذ القانون مخولة بموجب القانون الوطني سلطة إصدار الأوامر أو الإذن أو الاضطلاع بتنفيذ التدابير المنصوص عليها في هذا البروتوكول. تم توقع نفس الأسلوب لأغراض إجراء التعاون المباشر في هذه المادة. ووفقًا لذلك، فإن النظام القانوني الوطني للطرف سيحكم السلطة التي تعتبر السلطة المختصة لإصدار الأمر. في حين أن الطرف مُصدر الطلب يحدد أي من سلطاته يمكنه إصدار الأمر، فإن المادة 7 توفر ضمانة في الفقرة 5 حيث يجوز للطرف متلقي الطلب أن يطلب من السلطة المعينة مراجعة الأوامر الصادرة بموجب هذه المادة وأن تكون لديها القدرة على وقف التعاون المباشر، كما هو موضح أدناه.

99. في المادة 7، يتطلب مصطلح "مقدم خدمة في إقليم طرف آخر" أن يكون مقدم الخدمة موجودًا فعليًا في الطرف الآخر. بموجب هذه المادة، فإن مجرد حقيقة أن مقدم الخدمة، على سبيل المثال، قد أقام علاقة تعاقدية مع شركة في أحد الأطراف، ولكن مقدم الخدمة نفسه غير موجود فعليًا في ذلك الطرف، لن يشكل مقدم الخدمة "على إقليم" ذلك الطرف. تتطلب الفقرة 1، بالإضافة إلى ذلك، أن تكون البيانات في حوزة مقدم الخدمة أو تحت سيطرته.

الفقرة 2

100. في الفقرة 2 من المادة 7، يتعين على الأطراف اعتماد أي تدابير ضرورية لمقدمي الخدمات على أقاليمها للاستجابة لأمر صادر عن سلطة مختصة في طرف آخر عملاً بالفقرة 1. وبالنظر إلى الاختلافات في النظم القانونية الوطنية، فإن الأطراف قد تنفذ تدابير مختلفة لوضع إجراء للتعاون المباشر ليتم بطريقة تتسم بالفعالية والكفاءة. قد يتراوح هذا من إزالة العقبات القانونية لمقدمي الخدمات للاستجابة لأمر ما إلى توفير أساس إيجابي، وإلزام مقدمي الخدمة بالاستجابة لأمر من سلطة طرف آخر بطريقة تتسم بالفعالية والكفاءة. يجب على كل طرف التأكد من أن مقدمي الخدمة يمكنهم الامتثال بشكل قانوني للأوامر المنصوص عليها في المادة 7 بطريقة توفر اليقين القانوني بحيث لا يتحمل مقدمو الخدمة المسؤولية القانونية عن حقيقة امتثالهم بحسن نية لأمر صادر بموجب الفقرة 1، الذي صرح أحد الأطراف (بموجب المادة 7، الفقرة 3 (ب)) أنه صادر وفقا لهذا البروتوكول. لا يستبعد هذا المسؤولية لأسباب

أخرى غير الامتثال للأمر، على سبيل المثال، عدم اتباع أي مطلب قانوني ساري المفعول بأن يحافظ مقدم الخدمة على مستويات مناسبة من أمن المعلومات المخزنة. يعتمد شكل التنفيذ على الاعتبارات القانونية والسياساتية الخاصة بكل طرف. بالنسبة للأطراف التي لديها متطلبات حماية البيانات، قد يشمل ذلك توفير أساس واضح لمعالجة البيانات الشخصية. في ضوء المتطلبات الإضافية بموجب قوانين حماية البيانات للسماح بعمليات النقل الدولية النهائية لمعلومات المشترك المستجيبة، يعكس هذا البروتوكول المصلحة العامة الأساسية لتدبير التعاون المباشر هذا ويتضمن الضمانات المطلوبة لهذا الغرض في المادة 14.

101. كما هو موضح أعلاه، فإن النظام القانوني الوطني للطرف سيحكم السلطة التي تعتبر السلطة المختصة لإصدار الأمر. ورأت بعض الأطراف أنه من الضروري وجود ضمانة إضافية لمزيد من المراجعة لشرعية الأمر (انظر، على سبيل المثال، الفقرة 98 أعلاه) في ضوء الطبيعة المباشرة للتعاون. في حين أن الطرف المُصدر يقرر أي من سلطاته يمكنها إصدار الأمر، فإن الفقرة 2 (ب) تسمح للأطراف بإصدار إعلان ينص على أنه "يجب أن يصدر الأمر بموجب المادة 7، الفقرة 1، من قبل، أو تحت إشراف: المدعي العام أو سلطة قضائية أخرى، أو يصدر تحت إشراف مستقل بطريقة أخرى". يجب على الطرف الذي يستخدم هذا الإعلان أن يقبل أمرًا من قبل أو تحت إشراف أي من هذه السلطات التي تم تعدادها.

الفقرة 3

102. تحدد الفقرة 3 من المادة 7 المعلومات التي يجب أن يتم تقديمها، كحد أدنى، من قبل سلطة تصدر أمرًا وفقًا للفقرة 1 من هذه المادة، على الرغم من أن الطرف المُصدر قد يختار تضمين معلومات إضافية في الأمر نفسه للمساعدة في المعالجة أو لأن قانونه الوطني يتطلب معلومات إضافية. المعلومات المحددة في الفقرة 3 ذات صلة خاصة بتنفيذ الأمر من قبل مقدم الخدمة، فضلاً عن المشاركة المحتملة لسلطة الطرف الذي يوجد فيه مقدم الخدمة، وفقًا للفقرة 5. سيحتاج الأمر إلى إدراج اسم سلطة الإصدار وتاريخ إصدار الأمر، والمعلومات التي تحدد مقدم الخدمة، والجريمة التي تخضع للتحقيق أو الدعوى الجنائية، والسلطة التي تطلب معلومات المشترك، ووصفًا تفصيليًا لمعلومات المشترك المحددة المطلوبة. يجب أن يحتوي الأمر أيضًا على بيان يفيد بأن الأمر قد صدر وفقًا لهذا البروتوكول. بالإدلاء بهذا البيان، يعتبر الطرف أن الترتيب متوافق مع أحكام هذا البروتوكول.

103. فيما يتعلق بالفرق بين الفقرة 3 (أ) (سلطة الإصدار) و3 (ج) (السلطة التي تسعى للحصول على معلومات المشترك)، في بعض الأطراف، تختلف سلطة الإصدار والسلطة التي تطلب البيانات. على سبيل المثال، قد يكون المحققون أو المدعون هي السلطات التي تسعى للحصول على البيانات، بينما يصدر القاضي الأمر. في مثل هذه الحالات، يجب تحديد كل من السلطة التي تطلب البيانات والسلطة التي أصدرت الأمر.

104. لا يلزم تقديم بيان بالوقائع، مع مراعاة أن هذه المعلومات سرية في معظم التحقيقات الجنائية ولا يجوز كشفها لطرف خاص.

الفقرة 4

105. بينما تحدد الفقرة 3 الحد الأدنى من المعلومات المطلوبة للأوامر الصادرة عملاً بالفقرة 1، لا يمكن تنفيذ هذه الأوامر في كثير من الأحيان إلا إذا تم تزويد مقدم الخدمة (وحسب الاقتضاء، السلطة المعينة للطرف المتلقي بموجب الفقرة 5) بمعلومات تكميلية. لذلك، تنص الفقرة 4 من المادة 7 على أن تقدم سلطة الإصدار معلومات تكميلية حول الأسس القانونية الوطنية التي تخول السلطة لإصدار الأمر؛ والإشارة إلى الأحكام القانونية والعقوبات المطبقة على الجريمة التي يتم التحقيق فيها أو مقاضاة مرتكبيها؛ ومعلومات الاتصال الخاصة بالسلطة التي يجب على مقدم الخدمة إعادة معلومات المشترك إليها أو طلب مزيد من المعلومات أو الاستجابة بطريقة أخرى؛ الزمن والطريقة التي يتم بها إعادة معلومات المشترك؛ ما إذا كان قد تم السعي بالفعل للحفاظ على البيانات، بما في ذلك تاريخ الحفظ وأي رقم مرجعي قابل للتطبيق؛ أي تعليمات إجرائية خاصة (على سبيل المثال طلبات السرية أو التحقق من الهوية)؛ أو بيان، عند الاقتضاء، بأن إشعارا متزامنا قد تم وفقًا للفقرة 5؛ وأي معلومات أخرى قد تساعد في الكشف عن معلومات المشترك. لا تحتاج معلومات الاتصال إلى تحديد الفرد ولكن فقط المكتب. يمكن تقديم هذه المعلومات التكميلية بشكل منفصل ولكن يمكن أيضًا إدراجها في الأمر نفسه إذا كان ذلك مسموحًا به بموجب قانون الطرف المُصدر. يجب إرسال كل من الطلب والمعلومات التكميلية مباشرة إلى مقدم الخدمة.

106. تشمل التعليمات الإجرائية الخاصة، على وجه الخصوص، أيَ طلب للسرية، بما في ذلك طلب عدم الكشف عن الأمر للمشترك أو لأطراف ثالثة أخرى، باستثناء أن التعليمات الإجرائية الخاصة قد لا تمنع مقدم الخدمة من التشاور مع السلطات ليتم إشعارها بموجب الفقرة 5 (أ) أو التشاور معها بموجب الفقرة 5 (ب) إذا كانت السرية مطلوبة لتجنب الكشف المبكر عن المسألة، فيجب الإشارة إلى ذلك في الطلب. في بعض الأطراف، سيتم الحفاظ على سرية الأمر من خلال تطبيق القانون، بينما في الأطراف الأخرى ليس هذا هو الحال بالضرورة. لذلك، من أجل تجنب مخاطر الكشف المبكر عن التحقيق، يتم تشجيع الأطراف على أن تكون على دراية بالقانون الواجب التطبيق وسياسات مقدم الخدمة فيما يتعلق بإشعار المشترك، قبل تقديم الطلب بموجب الفقرة 1 إلى مقدم الخدمة. بالإضافة إلى ذلك، قد تتضمن التعليمات الإجرائية الخاصة مواصفات قناة الإرسال الأنسب لاحتياجات السلطة. قد يطلب مقدم الخدمة أيضًا معلومات إضافية تتعلق بالحساب أو معلومات أخرى لمساعدته في توفير استجابة سريعة وكاملة. يجب ألا يمنع طلب السرية مقدمي الخدمة من الإبلاغ عن الشفافية بشأن الأرقام الإجمالية المجهولة المصدر للطلبات الواردة بموجب المادة 7.

الفقرة 5

107. بموجب الفقرة 5 (أ)، يجوز لأحد الأطراف إشعار الأمين العام لمجلس أوروبا أنه عند إصدار أمر بموجب الفقرة 1 لمقدم خدمة على إقليمه، فإنه سيتطلب إشعارًا متزامنًا إما في كل حالة (أي، لجميع الطلبات المرسلة إلى مقدمي الخدمة على إقليمه) أو في ظروف محددة.

108. بموجب الفقرة 5 (ب)، يجوز لأحد الأطراف أيضًا، بموجب قانونه الوطني، أن يطلب من مقدم الخدمة الذي يتلقى أمرًا من أحد الأطراف آخر للتشاور معه في ظروف محددة. قد لا يطلب أحد الأطراف التشاور بشأن جميع الأوامر، الأمر الذي من شأنه أن يضيف خطوة إضافية قد تتسبب في تأخير كبير، ولكن فقط في ظروف محددة وأكثر محدودية. يجب أن تقتصر متطلبات التشاور على الظروف التي تزداد فيها احتمالية الحاجة إلى فرض شرط أو التذرع بأسباب الرفض، أو القلق بشأن المساس المحتمل بالتحقيقات أو الدعاوى الجنائية للطرف الناقل.

109. تعتبر إجراءات الإشعار والتشاور تقديرية بالكامل. الطرف غير ملزم بطلب أي من الإجراءين.

110. يجوز للأطراف التي تم إشعارها بموجب الفقرة 5 (أ) أو التي تم التشاور معها بموجب الفقرة 5 (ب) أن تطلب من مقدم الخدمة عدم الكشف عن المعلومات على الأسس المنصوص عليها في الفقرة 5 (ج) والتي يرد وصفها بمزيد من التفصيل في الفقرة 141 من التقرير التفسيري للمادة 8. ولهذا السبب، فإن قدرة الطرف على أن يتم إشعارها أو التشاور معها توفر ضمانة إضافية. مع ذلك، فإن التعاون من حيث المبدأ يجب أن يكون واسع النطاق ومعيقاته محدودة للغاية. بناءً على ذلك، وكما هو موضح في الفقرتين 242 و253 من التقرير التفسيري للاتفاقية، فإن تحديد الطرف الذي ينبغي إشعاره أو الذي ينبغي التشاور معه بشأن الشروط وحالات الرفض التي ستطبق بموجب المادة 25، الفقرة 4، والفقرة 4 من المادة 27 من الاتفاقية يجب أيضًا أن تكون محدودة بما يتماشى مع أهداف المادة 7 من البروتوكول لإزالة العوائق وتوفير إجراءات أكثر كفاءة وسرعة للوصول عبر الحدود إلى الأدلة الإلكترونية لأغراض التحقيقات الجنائية.

111. بموجب الفقرة 5 (د)، يجوز للأطراف التي تصدر إعلانًا بموجب الفقرة 5 (أ) أو التي تشترط التشاور بموجب الفقرة 5 (ب) الاتصال وطلب معلومات إضافية من السلطة المعينة بموجب الفقرة 4 (ج) لتحديد ما إذا كان هناك أساسًا بموجب الفقرة 5 (ج) لإصدار تعليمات لمقدم الخدمة بعدم الامتثال للأمر. الهدف من العملية أن تكون سريعة بقدر ما تسمح به الظروف. يجب على الطرف الذي تم إشعاره أو التشاور معه جمع المعلومات اللازمة واتخاذ قراره بموجب الفقرة 5 (ج) "دون تأخير غير مبرر". عند الضرورة، لإتمام التعاون، قد يوفر الإجراء المنصوص عليه في الفقرة 5 (د) أيضًا فرصة لتوضيح جوانب سرية المعلومات المطلوبة، بالإضافة إلى أي تقييد للاستخدام المقصود من قبل السلطة التي تطلب البيانات.

يجب على هذا الطرف أيضًا إشعار سلطة الطرف المُصدر على الفور في حالة ما إذا قرر إصدار تعليمات لمقدم الخدمة بعدم الامتثال، وكذلك تقديم أسباب القيام بذلك.

112. يجوز للطرف الذي يشرط إشعاراً أو تشاورا أن يفرض على مقدم الخدمة فترة انتظار قبل أن يقدم مقدم الخدمة معلومات المشترك استجابةً للأمر، من أجل السماح بالإشعار أو التشاور وأي طلب متابعة من قبل الطرف للحصول على معلومات إضافية.

113. عملاً بالفقرة 5 (ه)، يجب على الطرف الذي يشترط إشعارا أو تشاورا أن يعين سلطة واحدة، وعندما يكون الإشعار مطلوبًا بموجب الفقرة 5 (أ)، أن يزود الأمين العام لمجلس أوروبا بمعلومات اتصال كافية.

114. يجوز لأي طرف أن يغير شرط الإشعار أو التشاور الخاص به في أي وقت، رهناً بتحديده لأي عوامل ذات صلة به، مثل، على سبيل المثال، ما إذا كان يرغب في الانتقال من نظام إشعار إلى نظام تشاور أو ما إذا كان لقد طور مستوى راحة كافياً بالتعاون المباشر بحيث يمكنه مراجعة أو إزالة شرط الإشعار أو التشاور السابق. ويمكنه أن يقرر بنفس القدر، نتيجة للخبرة التي اكتسبتها مع آلية التعاون المباشر، أنه يرغب في إنشاء نظام إشعار أو تشاور.

115. بموجب الفقرة 5 (و)، يتعين على الأمين العام لمجلس أوروبا أن يُنشئ ويحتفظ بسجل بمتطلبات إشعار الأطراف بموجب الفقرتين 5 (أ) و5 (ه). يعد وجود سجل يجري تحديثه باستمرار ومتاح للجمهور أمرًا بالغ الأهمية لضمان أن تكون سلطات الطرف المُصدر ومقدمي الخدمات على دراية بمتطلبات الإشعار الخاصة بكل طرف، والتي، كما هو مذكور أعلاه، يمكن أن تتغير في أي وقت. نظرًا لأنه يجوز لكل طرف إجراء مثل هذا التغيير وفقًا لسلطته التقديرية، فإن كل طرف يقوم بإجراء أي تغيير أو يلاحظ أي عدم دقة فيما يتعلق بتفاصيله في السجل مطلوب منه إشعار الأمين العام على الفور من أجل التأكد من أن الآخرين على دراية بالمتطلبات الحالية ويمكنهم قم بتطبيقها بشكل صحيح.

الفقرة 6

116. توضح الفقرة 6 أن إشعار طرف آخر وتقديم معلومات إضافية باستخدام الوسائل الإلكترونية، بما في ذلك استخدام البريد الإلكتروني والبوابات الإلكترونية، أمر مسموح به. في حالة قبول مقدم الخدمة، يجوز للطرف تقديم طلب بموجب الفقرة 1 ومعلومات تكميلية بموجب الفقرة 4 في شكل إلكتروني. والهدف من ذلك هو تشجيع استخدام الوسائل الإلكترونية إذا كان ذلك مقبولاً من قبل مقدم الخدمة، حيث إنها دائمًا ما تكون أكثر وسائل الاتصال فعاليةً وأسرعها. قد تتضمن طرق التحقق من الهوية مجموعة متنوعة من الوسائل أو مجموعة منها تسمح بتحديد هوية السلطة مقدمة الطلب بشكل آمن. قد تشمل هذه الوسائل، على سبيل المثال، الحصول على تأكيد التحقق من صحة الهوية عبر سلطة معروفة في الطرف المُصدر (على سبيل المثال من المرسل أو سلطة مركزية

أو معينة)، والاتصالات اللاحقة بين سلطة الإصدار والطرف المتلقي، واستخدام وسيلة إلكترونية رسمية- عنوان البريد الإلكتروني أو طرق التحقق التكنولوجي المستقبلية التي يمكن استخدامها بسهولة من قبل السلطات المرسلة. ويرد نص مماثل في الفقرة 2 من المادة 10، وترد مزيد من الإرشادات فيما يتعلق بمتطلبات الأمن في الفقرة 174 من التقرير التفسيري. كما تحتوي المادة 6، الفقرة 4، والمادة 8، الفقرة 5، من البروتوكول على نص مماثل.

الفقرة 7

117. تنص الفقرة 7 على أنه في حالة عدم امتثال مقدم الخدمة لأمر صادر بموجب المادة 7، يجوز للطرف المُصدر أن يسعى فقط إلى التنفيذ وفقًا للمادة 8 أو أي شكل آخر من أشكال المساعدة المتبادلة. لا يجوز للأطراف التي تتصرف بموجب هذه المادة أن تسعى إلى الإنفاذ من جانب واحد.

118. لتنفيذ الأمر عن طريق المادة 8، يفكر هذا البروتوكول في إجراء مبسط لتحويل أمر بموجب هذه المادة إلى أمر بموجب المادة 8 لتسهيل قدرة الطرف المُصدر على الحصول على معلومات المشترك.

119. من أجل تجنب ازدواجية الجهود، يجب على الطرف المُصدر أن يمنح مقدم الخدمة 30 يومًا أو الإطار الزمني المنصوص عليه في الفقرة 4 (د)، أي الفترة الزمنية الأطول، حتى تتم عملية الإشعار والتشاور ولمقدم الخدمة للكشف عن المعلومات أو الإشارة إلى رفض القيام بذلك. فقط بعد انتهاء تلك الفترة الزمنية، أو إذا أشار المزود إلى رفضه الامتثال قبل انتهاء تلك الفترة الزمنية، يجوز للطرف المُصدر أن يسعى إلى التنفيذ وفقًا للمادة 8 أو أشكال أخرى من المساعدة المتبادلة. من أجل السماح للسلطات بتقييم ما إذا كانت ستسعى إلى التنفيذ بموجب الفقرة 7، يتم تشجيع مقدمي الخدمات على شرح أسباب عدم تقديم البيانات المطلوبة. على سبيل المثال، قد يوضح مقدم الخدمة أن البيانات لم تعد متاحة.

120. إذا أبلغت السلطة التي تم إشعارها بموجب الفقرة 5 (أ) أو تم التشاور معها بموجب الفقرة 5 (ب) الطرف المُصدر أن مقدم الخدمة قد تلقى تعليمات بعدم الكشف عن المعلومات المطلوبة، يجوز للطرف المُصدر مع ذلك أن يسعى إلى تنفيذ الأمر عن طريق المادة 8 أو شكل آخر من أشكال المساعدة المتبادلة. مع ذلك، هناك خطر من أن مثل هذا الطلب الإضافي قد يتم رفضه بالمثل. يُنصح الطرف المُصدر بالتشاور مسبقًا مع السلطة المعينة بموجب الفقرتين 5 (أ) أو 5 (ب) من أجل معالجة أي أوجه قصور في الطلب الأصلي وتجنب تقديم أوامر بموجب المادة 8 أو عبر أي آلية مساعدة متبادلة أخرى التي يمكن رفضها.

الفقرة 8

121. بموجب الفقرة 8، يجوز لطرف أن يعلن أن طرفًا آخر يجب أن يطلب الكشف عن معلومات المشترك من مقدم الخدمة قبل أن يطلبها بموجب المادة 8 ما لم يقدم الطرف

المُصدر تفسيراً معقولاً لعدم قيامه بذلك. على سبيل المثال، يجوز لطرف أن يصدر مثل هذا الإعلان لأنه يرى أن الإجراءات بموجب هذه المادة يجب أن تمكن الأطراف الأخرى من الحصول على بيانات المشترك بشكل أسرع مما هو منصوص عليه في المادة 8، نتيجة لذلك، يمكن أن يقلل عدد الحالات التي يلزم فيها الاحتجاج بالمادة 8. عندئذ لا يتم استخدام إجراءات المادة 8 بعد ذلك إلا عندما تفشل الجهود المبذولة للبحث عن معلومات المشترك مباشرة من مقدم الخدمة، عندما يكون لدى الطرف المُصدر تفسير معقول لعدم استخدام هذه المادة أولاً أو عندما يتحفظ الطرف المُصدر على عدم تطبيق هذه المادة. على سبيل المثال، قد يبرهن الطرف المُصدر على ذلك عندما لا يقدم مقدم الخدمة بشكل روتيني معلومات عن المشترك استجابةً للأوامر المستلمة مباشرة من هذا الطرف. أو، كمثال آخر، إذا طلب الطرف المصدر من خلال أمر واحد معلومات عن المشترك وبيانات الحركة من طرف آخر يطبق المادة 8 على كلتا فئتي البيانات، فلن يحتاج الطرف المصدر أولاً إلى طلب معلومات المشترك بشكل منفصل.

الفقرة 9

122. بموجب الفقرة 9 (أ)، لا يلزم الطرف الذي يتحفظ على هذه المادة باتخاذ تدابير بموجب الفقرة 2 لمقدمي الخدمات على أراضيه للكشف عن معلومات المشتركين استجابة لأوامر صادرة عن أطراف أخرى. لا يُسمح للطرف الذي يتحفظ على هذه المادة بإصدار أوامر بموجب الفقرة 1 لمقدمي الخدمات على أقاليم مناطق الأطراف الأخرى.

123. تنص الفقرة 9 (ب) على أنه - للأسباب الموضحة في الفقرة 93 أعلاه - إذا كان الكشف عن أنواع معينة من أرقام الوصول بموجب هذه المادة يتعارض مع المبادئ الأساسية لنظامه القانوني الوطني، يجوز للطرف أن يتحفظ على عدم تطبيق هذه المادة على هذه الأرقام. لا يُسمح للطرف الذي يقوم بمثل هذا التحفظ بإصدار أوامر بمثل هذه الأرقام بموجب الفقرة 1 لمقدمي الخدمات على أقاليم مناطق الأطراف الأخرى.

القسم 3 - إجراءات تعزيز التعاون الدولي بين السلطات للكشف عن بيانات الكمبيوتر المخزنة

المادة 8 - تنفيذ أوامر من طرف آخر للتقديم العاجل لمعلومات المشترك وبيانات الحركة

124. الغرض من المادة 8 هو أن يكون للطرف مقدم الطلب القدرة على إصدار أمر يتم تقديمه كجزء من طلب إلى طرف آخر وأن يكون للطرف متلقي الطلب القدرة على تنفيذ هذا الأمر عن طريق إجبار مقدم الخدمة على إقليمه لتقديم معلومات المشترك أو بيانات الحركة الموجودة في حوزة مقدم الخدمة أو تحت سيطرته.

125. تنشئ هذه المادة آلية تكمل أحكام المساعدة المتبادلة الواردة في الاتفاقية. وهي معدّة لتكون أكثر تبسيطًا من المساعدة المتبادلة في الوقت الراهن، من حيث أن المعلومات التي يجب على الطرف مقدم الطلب تقديمها محدودة بشكل أكبر وعملية الحصول على البيانات أسرع. تكمل هذه المادة عمليات المساعدة المتبادلة الأخرى بموجب الاتفاقية، أو غيرها من الاتفاقات المتعددة الأطراف أو الثنائية، التي يظل الطرف حراً في الاحتجاج بها، وبالتالي لا تخل بها. في الواقع، في الحالات التي يرغب فيها الطرف مقدم الطلب في الحصول على بيانات الحركة من أحد الأطراف الذي تحفظ على هذا الجانب من المادة 8، يمكن للطرف مقدم الطلب استخدام إجراء آخر للمساعدة المتبادلة. حيث، كما هو الحال في كثير من الأحيان، يتم طلب معلومات المشترك وبيانات الحركة وبيانات المحتوى المخزنة في نفس الوقت، فقد يكون من الأكثر كفاءة البحث عن جميع أشكال البيانات الثلاثة لنفس الحساب عبر طلب مساعدة متبادل تقليدي واحد، بدلاً من للبحث عن بعض أنواع البيانات عبر الطريقة التي توفرها هذه المادة وغيرها من خلال طلب مساعدة متبادلة منفصل.

الفقرة 1

126. تتطلب الفقرة 1 أن يكون الطرف مقدم الطلب قادرًا على إصدار أمر للحصول على معلومات المشترك أو بيانات الحركة من مقدم خدمة على إقليم طرف آخر. "الأمر" المشار إليه في المادة 8 هو أي إجراء قانوني يهدف إلى إجبار مقدم الخدمة على تقديم معلومات المشترك أو بيانات الحركة. على سبيل المثال، يمكن تنفيذه من خلال أمر تقديم أو أمر استدعاء أو أي آلية أخرى مصرح بها في القانون والتي يمكن إصدارها لغرض إلزام تقديم معلومات المشترك أو بيانات الحركة.

127. على النحو المحدد في الفقرة 2 (ب) من المادة 3، تشير عبارة "السلطة المختصة" في الفقرة 1 من هذه المادة إلى "سلطة قضائية أو إدارية أو غيرها من سلطات إنفاذ القانون المخولة بموجب القانون الوطني أن تأمر أو تصرح أو تتعهد بتنفيذ التدابير بموجب هذا البروتوكول لغرض جمع أو تقديم الأدلة فيما يتعلق بتحقيقات أو دعاوى جنائية محددة". وتجدر الإشارة إلى أن السلطات المختصة بإصدار أمر بموجب الفقرة 1 قد لا تكون بالضرورة هي نفسها السلطات المعينة لتقديم الأمر ليتم تنفيذه وفقًا للفقرة 10 (أ) من المادة 8، كما هو موضح بمزيد من التفصيل أدناه.

128. المادة 8، مصطلح "مقدم الخدمة على إقليم طرف آخر" يتطلب أن يكون مقدم الخدمة موجودًا فعليًا في الطرف الآخر. بموجب هذه المادة، فإن مجرد قيام مقدم الخدمة، على سبيل المثال، بإقامة علاقة تعاقدية مع شركة في أحد الأطراف، ولكن مقدم الخدمة نفسه غير موجود فعليًا في ذلك الطرف، لن يعتبر مقدم الخدمة "موجود على إقليم " ذلك الطرف. تقتضي الفقرة 1، بالإضافة إلى ذلك، أن تكون البيانات في حوزة مقدم الخدمة أو تحت سيطرته.

الفقرة 2

129. الفقرة 2 تتطلب من الطرف متلقي الطلب أن يتبنى التدابير اللازمة لتنفيذ أمر صادر بموجب الفقرة 1 على إقليمه، مع مراعاة الضمانات الموضحة أدناه. "إنفاذ" يعني أن الطرف متلقي الطلب سيلزم مقدم الخدمة بتقديم معلومات المشترك وبيانات الحركة باستخدام آلية من اختيار الطرف متلقي الطلب، بشرط أن تجعل الآلية الأمر قابلاً للتنفيذ بموجب القانون الوطني للطرف متلقي الطلب وتفي بمتطلبات هذه المادة. على سبيل المثال، يجوز للطرف متلقي الطلب أن ينفذ أمر الطرف مقدم الطلب بقبوله على أنه معادل للأوامر الوطنية، أو بتأييده لمنحه نفس تأثير الأمر الوطني أو بإصدار أمر التقديم الخاص به. ستخضع أيَ آلية من هذا القبيل لشروط قانون الطرف متلقي الطلب، لأن إجراءات الطرف متلقي الطلب ستتحكم فيها. لذلك، يمكن للطرف متلقي الطلب ضمان استيفاء قانونه، بما في ذلك المتطلبات الدستورية وحقوق الإنسان، خاصة فيما يتعلق بأي ضمانات إضافية بما في ذلك تلك اللازمة لتقديم بيانات الحركة.

130. بينما يمكن الامتثال لهذه المادة بعدة طرق، قد يرغب أحد الأطراف في إعداد عملياته الداخلية مع توخي المرونة في دراسة الطلبات الواردة من مختلف السلطات المختصة. تم التفاوض على الفقرة 3 (ب) لضمان تقديم معلومات كافية للطرف متلقي الطلب لضمان إمكانية إجراء استعراض كامل إذا لزم الأمر، حيث أشارت بعض الأطراف إلى أنها ستصدر أمرها الخاص كوسيلة لتنفيذ أمر الطرف مقدم الطلب.

الفقرة 3

131. لبدء عملية تنفيذ الأمر من طرف الطرف متلقي الطلب، يجب على الطرف مقدم الطلب إرسال الأمر والمعلومات الداعمة. تصف الفقرة 3 ما يجب على الطرف مقدم الطلب تقديمه للطرف متلقي الطلب حتى يتمكن الطرف متلقي الطلب من تنفيذ الأمر وإجبار مقدم الخدمة على إقليم ذلك الطرف على التقديم. تصف الفقرة 3 (أ) المعلومات التي سيتم تضمينها في الأمر نفسه وتتضمن معلومات أساسية لتنفيذه. المعلومات الواردة في الفقرة 3 (ب)، والمخصصة لاستخدام الطرف متلقي الطلب فقط وليس لمشاركتها مع مقدم الخدمة إلا بموافقة الطرف مقدم الطلب، هي المعلومات الداعمة التي تحدد الأسس القانونية الوطنية والأساس الدولي لهذا الأمر في هذا البروتوكول، وتوفر معلومات للطرف متلقي الطلب لتقييم الأسباب المحتملة للشروط أو الرفض بموجب الفقرة 8. ينبغي للأطراف، أثناء تقديم طلب بموجب المادة 8، أن توضح ما إذا كانت هناك أي معلومات بموجب الفقرة 3 (ب) يمكن مشاركتها مع مقدم الخدمة. بموجب الفقرة 3 (ج)، يجب أن يتضمن الطلب أيضًا جميع التعليمات الخاصة، بما في ذلك، على سبيل المثال، طلبات الترخيص أو سرية الطلب (على غرار المادة 27، الفقرة 8، من الاتفاقية)، أثناء الإرسال لضمان المعالجة الصحيحة للطلب.

132. يجب أن يحدد أمر الحصول على معلومات المشترك أو بيانات الحركة الموصوف في الفقرة 3 (أ)، في ظاهره ما يلي: (i) السلطة التي أصدرت الأمر وتاريخ إصدار الأمر؛ (ii) بيان بأنه يجري إصداره عملاً بهذا البروتوكول؛ (iii) اسم وعنوان مقدم (أو مقدمي) الخدمة المطلوب تقديمه؛ (iv) الجريمة (أو الجرائم) التي تخضع للتحقيقات أو الدعاوى الجنائية؛ (v) السلطة التي تطلب البيانات، إن لم تكن سلطة الإصدار؛ و (vi) وصفًا تفصيليًا للبيانات المحددة المطلوبة (أي هوية المشترك، أو العنوان البريدي أو الجغرافي، أو رقم الهاتف أو رقم الوصول الآخر، والمعلومات الخاصة بالفواتير والدفع المتاحة على أساس اتفاق أو ترتيب الخدمة (انظر المادة 3 من هذا البروتوكول التي تتضمن الفقرة 3 من المادة 18 من الاتفاقية والفقرة 93 أعلاه من التقرير التفسيري)؛ وفيما يتعلق ببيانات الحركة، بيانات الكمبيوتر المتعلقة بالاتصال عن طريق نظام الكمبيوتر، التي تم إنشاؤها بواسطة نظام الكمبيوتر الذي يشكل جزءًا من سلسلة الاتصالات، التي تشير إلى مصدر الاتصال، أو وجهته، أو مساره ، أو زمنه، أو تاريخه، أو حجمه، أو مدته أو نوع الخدمة الأساسية (انظر المادة 3، الفقرة 1 من هذا البروتوكول التي تتضمن المادة 1، الفقرة (د)، من الاتفاقية). فيما يتعلق بالفقرة 3 (أ) (v)، إذا كانت سلطة الإصدار مختلفة عن السلطة التي تطلب البيانات، فإن الحكم يتطلب تحديد كليهما. على سبيل المثال، قد تطلب سلطة التحقيق أو المقاضاة البيانات، بينما يتم إصدار الأمر من طرف القاضي. توضح هذه المعلومات شرعية الأمر وتوفر تعليمات واضحة لتنفيذه.

133. تهدف المعلومات الداعمة الموصوفة في الفقرة 3 (ب) إلى تزويد الطرف متلقي الطلب بالمعلومات التي قد يحتاجها لتنفيذ أمر الطرف مقدم الطلب. يمكن أيضًا تسهيل ذلك من خلال استمارة يسهل ملؤها، مما قد يضيف مزيدًا من الكفاءة إلى العملية. يُدرج في قائمة المعلومات الداعمة ما يلي:

- تشير الفقرة 3 (ب) (i) إلى الأساس القانوني الذي يمنح سلطة الإصدار صلاحية إصدار الأمر للإجبار على التقديم. بعبارة أخرى، هذا هو القانون ذي الصلة الذي يخول السلطة المختصة إصدار الأمر الموصوف في الفقرة 1.

- تشير الفقرة 3 (ب) (ii) إلى النص القانوني المتعلق بالجريمة المشار إليها في الأمر الوارد في الفقرة 3 (أ) (iv) وما يرتبط بها من مجموعة العقوبات. إن إدراج هذين العنصرين مهم للطرف متلقي الطلب لتقييم ما إذا كان الطلب يقع في نطاق التزاماته أم لا.

- تشير الفقرة 3 (ب) (iii) إلى أي معلومات يمكن للطرف مقدم الطلب تقديمها والتي أدت به إلى استنتاج أن مقدمي الخدمة موضوع الطلب يمتلكون أو يتحكمون في المعلومات أو البيانات المطلوبة. هذه المعلومات هي المفتاح لبدء العملية في الطرف متلقي الطلب. غالبًا ما يكون تحديد مقدم الخدمة الوطني والاعتقاد بأنه يمتلك المعلومات أو البيانات المطلوبة أو يتحكم فيها شرطًا أساسيًا لبدء تطبيقات أوامر التقديم.

- تشير الفقرة 3 (ب) (iv) إلى ملخص موجز للوقائع المتعلقة بالتحقيق أو الدعوى. تعتبر هذه المعلومات أيضًا عاملاً رئيسيًا للطرف متلقي الطلب لتحديد ما إذا كان يجب تنفيذ أمر بموجب هذه المادة على إقليمه أم لا.

- تشير الفقرة 3 (ب) (v) إلى بيان يتعلق بعلاقة المعلومات أو البيانات بالتحقيق أو الدعوى. يهدف هذا البيان إلى مساعدة الطرف متلقي الطلب في تقرير ما إذا كانت متطلبات الفقرة 1 من هذه المادة قد تم استيفاؤها أم لا، أي أن المعلومات أو البيانات "مطلوبة للتحقيقات أو الدعاوى الجنائية المحددة الخاصة بهذا الطرف".

- تشير الفقرة 33 (ب) (vi) إلى معلومات الاتصال الخاصة بسلطة أو سلطات في حالة طلب السلطة المختصة في الطرف متلقي الطلب معلومات إضافية لتنفيذ الأمر.

- تشير الفقرة 3 (ب) (vii) إلى المعلومات المتعلقة بما إذا كان قد تم السعي بالفعل إلى الحفاظ على المعلومات أو البيانات. هذه معلومات مهمة للطرف متلقي الطلب، لا سيما فيما يتعلق ببيانات الحركة ويجب أن تتضمن، على سبيل المثال، الأرقام المرجعية وتاريخ الحفظ، لأن هذه المعلومات قد تسمح للطرف متلقي الطلب بمطابقة الطلب الحالي مع طلب حفظ سابق، وبالتالي تيسير الكشف عن المعلومات أو البيانات المحفوظة أصلاً. وبغية الحد من خطر حذف المعلومات أو البيانات، تشجع الأطراف على السعي إلى حفظ المعلومات أو البيانات المطلوبة في أقرب وقت ممكن وقبل الشروع في تقديم طلب بموجب هذه المادة، والسعي إلى تمديد عمليات الحفظ في الوقت المناسب.

- الفقرة 3 (ب) (viii) تشير إلى المعلومات المتعلقة بما إذا كان قد تم بالفعل السعي إلى الحصول على البيانات بوسائل أخرى، وإذا كان الأمر كذلك، فبأي طريقة. يتناول هذا الحكم في المقام الأول ما إذا كان الطرف مقدم الطلب قد سعى بالفعل للحصول على معلومات المشترك أو بيانات الحركة مباشرة من مقدم الخدمة.

134. لا يجوز الكشف عن المعلومات التي سيتم تقديمها بموجب الفقرة 3 (ب) لمقدم الخدمة دون موافقة الطرف مقدم الطلب. على وجه الخصوص، يتم تقديم ملخص الوقائع والبيان المتعلق بأهمية المعلومات أو البيانات للتحقيق أو الدعوى إلى الطرف متلقي الطلب لغرض تحديد ما إذا كان هناك سبب لفرض أحكام أو شروط أو للرفض، ولكنه غالبًا ما يخضع لسرية التحقيق.

135. بموجب الفقرة 3 (ج)، يجوز للطرف مقدم الطلب أن يطلب تعليمات إجرائية خاصة، بما في ذلك طلبات عدم الكشف عن الأمر للمشترك أو استمارات التحقق من الهوية التي يتعين استكمالها للأدلة. يجب أن تكون هذه المعلومات معروفة في البداية، لأن التعليمات الخاصة قد تتطلب عمليات إضافية داخل الطرف المطلوب.

136. لتنفيذ الأمر وزيادة تسهيل تقديم المعلومات أو البيانات، يجوز للطرف متلقي الطلب أن يزود مقدم الخدمة بمعلومات إضافية، مثل طريقة التقديم، ولمن يجب أن تقدم البيانات في الطرف متلقي الطلب.

الفقرة 4

137. عملاً بالفقرة 4، قد يلزم تقديم معلومات إضافية للطرف متلقي الطلب حتى ينفذ الأمر. على سبيل المثال، بموجب القانون الوطني لبعض الأطراف، قد يتطلب تقديم بيانات الحركة مزيدًا من المعلومات نظرًا لوجود متطلبات إضافية في قوانينهم للحصول على هذه البيانات. بالإضافة إلى ذلك، يجوز للطرف متلقي الطلب أن يطلب توضيحات بشأن المعلومات المقدمة عملاً بالفقرة 3 (ب) وكمثال آخر، قد تطلب بعض الأطراف معلومات إضافية في حالة عدم إصدار الأمر أو مراجعته من قبل المدعي العام أو أي سلطة قضائية أو إدارية مستقلة للطرف مقدم الطلب. عند إصدار مثل هذا الإعلان، يجب أن تكون الأطراف دقيقة قدر الإمكان فيما يتعلق بنوع المعلومات الإضافية المطلوبة.

الفقرة 5

138. تتطلب الفقرة 5 من الطرف متلقي الطلب قبول الطلبات في شكل إلكتروني. قد يتطلب استخدام وسائل آمنة وقابلة للتحقق من الهوية للاتصالات الإلكترونية لتسهيل نقل المعلومات أو البيانات والوثائق، بما في ذلك إرسال الطلبات والمعلومات الداعمة. كما تنص المواد من 6 إلى 11 على وسائل الاتصال هذه.

الفقرة 6

139. بموجب الفقرة 6، ينبغي للطرف متلقي الطلب أن يتخذ خطوات معقولة على وجه السرعة للشروع في تنفيذ الطلب. يجب أن يبذل جهودًا معقولة لدراسة الطلبات وتقديم مقدم الخدمة في غضون خمسة وأربعين يومًا بعد تلقي الطرف متلقي الطلب جميع الوثائق والمعلومات اللازمة. يجب على الطرف متلقي الطلب أن يأمر مقدم الخدمة بتقديم معلومات المشترك في غضون عشرين يومًا وبيانات الحركة في غضون خمسة وأربعين يومًا. بينما يجب على الطرف متلقي الطلب أن يسعى إلى إلزام التقديم بأسرع ما يمكن، هناك العديد من العوامل التي قد تؤخر التقديم، مثل اعتراض مقدمي الخدمة أو عدم الاستجابة للطلبات أو عدم الوفاء بتاريخ التقديم، بالإضافة إلى حجم الطلبات التي قد يُطلب من الطرف متلقي الطلب دراستها. بسبب ذلك، تقرر مطالبة الأطراف متلقية الطلبات لبذل جهود معقولة لاستكمال العمليات التي تخضع لسيطرتها فقط.

الفقرة 7

140. أقرت الأطراف بأن بعض التعليمات الإجرائية الخاصة من الطرف مقدم الطلب قد تسبب أيضًا تأخيرًا في دراسة الطلبات، إذا كانت التعليمات تتطلب عمليات وطنية إضافية

من أجل تنفيذ التعليمات الإجرائية الخاصة. يجوز للطرف متلقي الطلب أيضًا أن يطلب معلومات إضافية من الطرف مقدم الطلب من أجل دعم أي طلبات لأوامر تكميلية، مثل أوامر السرية (أوامر عدم الكشف). بعض التعليمات الإجرائية قد لا تكون متاحة بموجب قانون الطرف متلقي الطلب، وفي هذه الحالة تنص الفقرة 7 على أنه يتعين عليه إبلاغ الطرف مقدم الطلب على الفور وتحديد أي شروط يمكنه بموجبها الامتثال، مما يمنح الطرف مقدم الطلب القدرة على تحديد ما إذا كان يرغب في متابعة الطلب أم لا.

الفقرة 8

141. بموجب الفقرة 8، يجوز للطرف متلقي الطلب أن يرفض تنفيذ طلب إذا كانت أسباب الرفض المنصوص عليها في المادة 25، الفقرة 4، أو المادة 27، الفقرة 4، من الاتفاقية موجودة. على سبيل المثال، تماشيا مع الفقرة 257 من التقرير التفسيري للاتفاقية، ينص ذلك على أن هذا الحكم يخضع لأسباب الرفض في معاهدات المساعدة المتبادلة والقوانين الوطنية السارية ويوفر "ضمانات لحقوق الأشخاص الموجودين في الطرف متلقي الطلب"، وتماشيا مع الفقرة 268 من ذلك التقرير التفسيري، يجوز رفض المساعدة على أساس "المساس بسيادة الدولة أو الأمن أو النظام العام أو المصالح الأساسية الأخرى". كما يجوز له أيضا فرض الشروط اللازمة للسماح بتنفيذ الطلب، مثل السرية. بالإضافة إلى ذلك، يجوز للطرف متلقي الطلب تأجيل تنفيذ الطلب بموجب الفقرة 5 من المادة 27 من الاتفاقية. يجب على الطرف متلقي الطلب إشعار الطرف مقدم الطلب بقرار رفض الطلب أو شروطه أو تأجيله. بالإضافة إلى ذلك، يجوز للأطراف تطبيق قيود على الاستخدام وفقًا لبنود المادة 28، الفقرة 2 (ب)، من الاتفاقية.

142. من أجل تعزيز مبدأ توفير أكبر قدر من التعاون (انظر المادة 5، الفقرة 1)، ينبغي أن تكون أسباب الرفض التي وضعها الطرف متلقي الطلب محدودة وأن تمارس بتحفظ. وتجدر الإشارة إلى أن الفقرة 253 من التقرير التفسيري للاتفاقية تنص على أن "المساعدة المتبادلة من حيث المبدأ يجب أن تكون واسعة النطاق وأن العوائق التي تعترضها محدودة للغاية". وفقًا لذلك، يجب أيضًا تقييد الشروط وحالات الرفض بما يتماشى مع أهداف هذه المادة لإزالة العوائق التي تحول دون مشاركة معلومات المشتركين وبيانات الحركة عبر الحدود، ولتوفير إجراءات أكثر كفاءة وسرعة من المساعدة المتبادلة التقليدية.

الفقرة 9

143. بموجب الفقرة 9، "[أ] في حالة عدم تمكن الطرف مقدم الطلب من الامتثال لشرط يفرضه الطرف متلقي الطلب بموجب الفقرة 8، يجب عليه إبلاغ الطرف متلقي الطلب على الفور. يجب على الطرف متلقي الطلب بعد ذلك تحديد ما إذا كان ينبغي مع ذلك تقديم المعلومات أو المواد. (ب) إذا قبل الطرف مقدم الطلب الشرط، فإنه يلتزم به. يجوز للطرف

متلقي الطلب الذي يقدم معلومات أو مواد تخضع لمثل هذا الشرط أن يطلب من الطرف مقدم الطلب أن يشرح، فيما يتعلق بهذا الشرط، استخدام هذه المعلومات أو المواد".

الفقرة 10

144. الغرض من الفقرة 10 هو التأكد من أن الأطراف، أثناء التوقيع، أو عند إيداع وثائق التصديق أو القبول أو الموافقة الخاصة بهم، تحدد السلطات لتقديم الطلبات وتلقيها بموجب المادة 8. لا يتعين على الأطراف إعطاء اسم وعنوان فرد معين ولكن قد يحدد مكتبًا أو وحدة يتم اعتبارها مختصة لأغراض إرسال واستلام الطلبات بموجب هذه المادة.

الفقرة 11

145. تسمح الفقرة 11 للطرف أن يعلن أنه يتطلب أن يتم إرسال الأوامر المقدمة إليه بموجب هذه المادة من قبل السلطة المركزية للطرف مقدم الطلب، أو سلطة أخرى إذا تم تحديدها بشكل متبادل بين الطرفين. يتم تشجيع الأطراف على توفير أكبر قدر ممكن من المرونة لتقديم الطلبات.

الفقرة 12

146. تتطلب الفقرة 12 من الأمين العام لمجلس أوروبا إنشاء وتحديث سجل للسلطات المعينة من قبل الأطراف بموجب الفقرة 10 وأن يضمن كل طرف دقة التفاصيل الموجودة في السجل. ستساعد هذه المعلومات الأطراف المطلوبة على التحقق من صحة الطلبات.

الفقرة 13

147. بموجب الفقرة 13، لا يُطلب من الطرف الذي يتحفظ على عدم تطبيق هذه المادة على بيانات الحركة تنفيذ أوامر بيانات الحركة من طرف آخر. لا يُسمح للطرف الذي يتحفظ على هذه المادة بتقديم أوامر للحصول على بيانات الحركة إلى الأطراف الأخرى بموجب الفقرة 1.

المادة 9 - الكشف المعجل عن بيانات الكمبيوتر المخزنة في حالات الطوارئ

148. بالإضافة إلى الأشكال الأخرى من التعاون المعجل المنصوص عليها في هذا البروتوكول، كان فريق الصياغة يدرك ضرورة تسهيل قدرة الأطراف، في حالات الطوارئ، للحصول على وجه السرعة على بيانات كمبيوتر محددة مخزنة في حوزة أو سيطرة مقدم خدمة على إقليم طرف آخر لاستخدامها في تحقيقات أو دعاوى جنائية محددة. كما هو مذكور في الفقرتين 42 و172 من هذا التقرير التفسيري، قد تنشأ الحاجة إلى أقصى قدر من التعاون السريع في مجموعة متنوعة من حالات الطوارئ، كما هو الحال في أعقاب هجوم إرهابي مباشرة، وهو هجوم فدية قد يشل نظام المستشفى، أو عند التحقيق في حسابات البريد الإلكتروني التي يستخدمها الخاطفون لإصدار مطالب والتواصل مع أسرة الضحية.

149. بموجب الاتفاقية، في حالات الطوارئ، تقدم الأطراف طلبات المساعدة المتبادلة للحصول على البيانات، وبموجب المادة 35، الفقرة 1 (ج) من الاتفاقية، فإن شبكة تعمل على مدار الساعة طوال أيام الأسبوع متاحة لتسهيل تنفيذ هذه الطلبات. بالإضافة إلى ذلك، تسمح الأنظمة القانونية في عدد قليل من البلدان للسلطات المختصة في البلدان الأخرى بطلب الكشف الطارئ عن البيانات عبر شبكة تعمل على مدار الساعة طوال أيام الأسبوع دون إرسال طلب مساعدة متبادلة.

150. كما هو مبين في المادة 5، الفقرة 7، لا تخل هذه المادة بالتعاون (بما في ذلك التعاون التلقائي) بين الأطراف، أو بين الأطراف ومقدمي الخدمات، من خلال الاتفاقات أو الترتيبات أو الممارسات الأخرى سارية المفعول أو القانون الوطني. لذلك، بموجب هذا البروتوكول، تظل جميع الآليات المذكورة أعلاه متاحة للسلطات المختصة التي تسعى للحصول على البيانات في حالة الطوارئ. يتمثل ابتكار هذا البروتوكول في صياغة مادتين تلزمان جميع الأطراف بتوفير قنوات محددة، على الأقل، للتعاون السريع في حالات الطوارئ: المادة 9 والمادة 10.

151. تسمح هذه المادة للأطراف بالتعاون للحصول على بيانات الكمبيوتر في حالات الطوارئ باستخدام الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع التي أنشأتها المادة 35 من الاتفاقية كقناة. الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع مناسبة بشكل خاص للتعامل مع الطلبات المستعجلة وذات الأولوية العالية على النحو المتصور في هذه المادة. الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع مزودة بنقاط اتصال تتواصل، في الممارسة العملية، بسرعة ودون الحاجة إلى ترجمات مكتوبة وتكون في وضع يمكنها من تنفيذ الطلبات الواردة من الأطراف الأخرى، سواء باللجوء مباشرة إلى مقدمي الخدمة على أقاليمها، لطلب المساعدة من السلطات المختصة الأخرى أو اللجوء إلى السلطات القضائية، إذا كان ذلك مطلوبًا بموجب القانون الوطني للطرف. يمكن لنقاط الاتصال هذه أيضًا تقديم المشورة للأطراف مقدمة الطلبات بشأن الأسئلة التي قد تكون لديهم فيما يتعلق بمقدمي الخدمات وجمع الأدلة الإلكترونية، على سبيل المثال من خلال شرح القانون الوطني الذي يجب الامتثال به للحصول على الأدلة. يعزز هذا الاتصال المتبادل فهم الطرف مقدم الطلب للقانون الوطني في الطرف متلقي الطلب ويسهل الحصول على الأدلة المطلوبة بشكل أكثر سلاسة.

152. قد يكون لاستخدام القناة المحددة في هذه المادة مزايا على قناة المساعدة المتبادلة في حالات الطوارئ المنصوص عليها في المادة 10. على سبيل المثال، تتمتع هذه القناة بميزة عدم الحاجة إلى إعداد طلب مساعدة متبادلة مسبقًا. قد تكون هناك حاجة إلى وقت طويل لإعداد طلب مسبق للمساعدة المتبادلة، وترجمته وتمريره عبر القنوات الوطنية إلى السلطة المركزية للطرف مقدم الطلب للمساعدة المتبادلة، الأمر الذي لن يكون مطلوبا بموجب المادة 9. بالإضافة إلى ذلك، بمجرد استلام الطلب من قبل الطرف متلقي الطلب، إذا كان يجب الحصول على معلومات تكميلية قبل أن يتمكن من منح المساعدة، فمن

المرجح أن يؤدي الوقت الإضافي الذي قد يكون ضروريًا لطلب المساعدة المتبادلة إلى تأخير تنفيذ الطلب. في سياق المساعدة المتبادلة، غالبًا ما تطلب الأطراف متلقية الطلب تقديم المعلومات التكميلية بشكل مكتوب وأكثر تفصيلاً، بينما تعمل القناة على مدار الساعة طوال أيام الأسبوع باستخدام تبادل المعلومات في الوقت الفعلي. من ناحية أخرى، تقدم قناة المساعدة المتبادلة في حالات الطوارئ مزايا في حالات معينة. على سبيل المثال، (1) قد يضيع وقت قليل أو قد لا يضيع وقت باستخدام تلك القناة إذا كانت هناك علاقات عمل وثيقة بشكل خاص بين السلطات المركزية المعنية؛ (2) يمكن استخدام المساعدة المتبادلة في حالات الطوارئ للحصول على أشكال إضافية من التعاون تتجاوز بيانات الكمبيوتر التي يحتفظ بها مقدمو الخدمات؛ و(3) قد يكون من الأسهل توثيق الأدلة التي يتم الحصول عليها من خلال المساعدة المتبادلة. الأمر متروك للأطراف، بناءً على خبرتهم المتراكمة والظروف القانونية والوقائعية المحددة القائمة، لتقرير أفضل قناة لاستخدامها في حالة معينة.

الفقرة 1

153. بموجب الفقرة 1 (أ)، يجب على كل طرف أن يعتمد تدابير حسب الضرورة لضمان أن تكون نقطة الاتصال الخاصة به للشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع قادرة على إرسال الطلبات في حالة الطوارئ إلى نقطة الاتصال في طرف آخر، وطلب المساعدة الفورية للحصول على الكشف المعجل عن بيانات الكمبيوتر المحددة والمخزنة التي يحتفظ بها مقدمو الخدمات على أقاليم ذلك الطرف وتلقي الطلبات من نقاط الاتصال في الأطراف الأخرى للحصول على مثل هذه البيانات التي يحتفظ بها مقدمو الخدمات على أقاليمها. كما هو منصوص عليه في المادة 2، يجب تقديم الطلب وفقًا لتحقيق أو دعوى جنائية محدد.

154. يجب أن تتمتع نقاط الاتصال التي تعمل على مدار الساعة طوال أيام الأسبوع بالقدرة على إرسال واستقبال مثل هذه الطلبات في حالات الطوارئ دون الحاجة إلى إعداد وإرسال طلب المساعدة المتبادلة مسبقًا، على النحو المبين في الفقرة 152 من التقرير التفسيري أعلاه، مع مراعاة ما يلي: إمكانية إصدار إعلان بموجب المادة 9، الفقرة 5. مصطلح "الطوارئ" معرّف في المادة 3. بموجب المادة 9، يجب على الطرف متلقي الطلب تحديد ما إذا كانت "حالة الطوارئ" قائمة فيما يتعلق بطلب باستخدام المعلومات الواردة في الفقرة 3.

155. على عكس المواد الأخرى في هذا البروتوكول، مثل المادة 7، التي لا يجوز استخدامها إلا للحصول على "معلومات المشترك المحددة والمخزنة"، تستخدم هذه المادة المصطلح الأوسع "بيانات الكمبيوتر المخزنة المحددة". نطاق هذا المصطلح واسع ولكنه ليس عشوائيًا: فهو يشمل أي بيانات كمبيوتر "محددة" على النحو المحدد في المادة 1 (ب) من الاتفاقية، والتي تم تضمينها في المادة 3، الفقرة 1، من هذا البروتوكول. يقر استخدام هذا المصطلح الأوسع بأهمية الحصول على المحتوى المخزن وبيانات

الحركة، وليس فقط معلومات المشترك، في حالات الطوارئ، دون الحاجة إلى تقديم طلب للمساعدة المتبادلة كشرط مسبق. البيانات المعنية مخزنة أو بيانات موجودة ولا تشمل البيانات التي لم تظهر بعد، مثل بيانات الحركة أو بيانات المحتوى المتعلقة بالاتصالات المستقبلية (انظر الفقرة 170 من التقرير التفسيري للاتفاقية).

156. يتيح هذا الحكم مرونة للطرف مقدم الطلب لتحديد أي من سلطاته ينبغي أن يقدم الطلب، مثل سلطاته المختصة التي تجري التحقيق أو نقطة الاتصال التي تعمل على مدار الساعة طوال أيام الأسبوع، وفقًا للقانون الوطني. تعمل نقطة اتصال الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع في الطرف مقدم الطلب كقناة لإرسال الطلب إلى نقطة الاتصال التي تعمل على مدار الساعة طوال أيام الأسبوع في الطرف الآخر.

157. بموجب الفقرة 1 (ب)، يجوز للطرف أن يعلن أنه لن ينفذ طلبًا بموجب المادة 9 فقط للحصول على معلومات المشترك، على النحو المحدد في المادة 3.18 من الاتفاقية، المدرجة في المادة 3، الفقرة 1، من هذا البروتوكول. بالنسبة لبعض الأطراف، فإن تلقي الطلبات بموجب هذه المادة للحصول على معلومات المشترك فقط قد يؤدي إلى زيادة العبء على نقاط اتصال الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع عن طريق تحويل الموارد والطاقة بعيدًا عن طلبات المحتوى أو بيانات الحركة. في مثل هذه الحالات، يجوز للأطراف التي تسعى فقط للحصول على معلومات المشترك استخدام المادتين 7 أو 8، والتي تسهل الكشف المعجل عن هذه المعلومات. لا يمنع هذا الإعلان الأطراف الأخرى من تضمين طلب للحصول على معلومات المشترك عندما تقوم أيضًا بإصدار طلب بموجب هذه المادة لبيانات المحتوى و / أو بيانات الحركة.

الفقرة 2

158. تقتضي الفقرة 2 أن يتخذ كل طرف التدابير اللازمة لضمان تمكين سلطاته بموجب قانونه الوطني من طلب والحصول على البيانات المطلوبة بموجب الفقرة 1 من مقدمي الخدمات على إقليمه، والاستجابة لمثل هذه الطلبات دون أن يكون لدى الطرف مقدم الطلب لتقديم طلب للمساعدة المتبادلة، رهنا بإمكانية إصدار إعلان وفقا للفقرة 5.

159. بالنظر إلى الاختلاف في القوانين الوطنية، فإن الفقرة 2 تم إعدادها لتوفير المرونة للأطراف في بناء أنظمتها للاستجابة للطلبات بموجب الفقرة 1. مع ذلك، تُشجع الأطراف على تطوير آليات للامتثال لهذه المادة تشدد على السرعة والكفاءة، التي يتم تكييفها مع مقتضيات حالة الطوارئ والتي توفر أساسًا قانونيًا واسعًا للكشف عن البيانات للأطراف الأخرى في حالات الطوارئ.

160. يحق للطرف متلقي الطلب تقرير ما يلي: (1) ما إذا كانت متطلبات استخدام هذه المادة قد تم الوفاء بها؛ (2) ما إذا كانت آلية أخرى مناسبة لأغراض مساعدة الطرف مقدم الطلب؛

(3) السلطة المناسبة لتنفيذ طلب تتلقاه نقطة اتصال الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع. في حين أن نقطة اتصال الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع في بعض الأطراف قد يكون لديها بالفعل الصلاحية المطلوبة لتنفيذ الطلب بنفسها، فقد تطلب الأطراف الأخرى أن تقوم نقطة الاتصال الخاصة بهم بإرسال الطلب إلى سلطة أو سلطات أخرى لطلب الكشف عن البيانات من مقدم الخدمة. في بعض الأطراف، قد يتطلب ذلك الحصول على أمر قضائي لطلب الكشف عن البيانات. يتمتع الطرف المطلوب منه أيضًا بسلطة تقديرية لتحديد القناة لإرسال البيانات المستجيبة إلى الطرف مقدم الطلب - سواء من خلال نقطة اتصال تعمل على مدار الساعة طوال أيام الأسبوع أو من خلال سلطة أخرى.

الفقرة 3

161. تحدد الفقرة 3 المعلومات التي يتعين تقديمها في الطلب عملاً بالفقرة 1. المعلومات المحددة في الفقرة 3 هي لتسهيل مراجعة، وعند الاقتضاء، تنفيذ الطلب من قبل السلطة المختصة للطرف متلقي الطلب.

162. فيما يتعلق بالفقرة 3 (أ)، يجب على الطرف مقدم الطلب أن يحدد السلطة المختصة التي تُطلب البيانات نيابة عنها.

163. فيما يتعلق بالفقرة 3 (ب)، يجب على الطرف مقدم الطلب أن يعلن أن الطلب قد صدر عملاً بهذا البروتوكول. سيوفر هذا تأكيدًا على أن الطلب يتم وفقًا لهذا البروتوكول وأن أيَ بيانات يتم تلقيها نتيجة لذلك سيتم التعامل معها بطريقة تتفق مع متطلبات هذا البروتوكول. سيؤدي هذا أيضًا إلى تمييز الطلب عن طلبات الكشف عن حالات الطوارئ الأخرى التي قد تتلقاها نقطة اتصال الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع.

164. بموجب الفقرة 3 (ج)، يجب على الطرف مقدم الطلب أن يقدم وقائع كافية تثبت وجود حالة طوارئ، على النحو المحدد في المادة 3، وكيف أن البيانات التي يسعى الطلب للحصول عليها تتعلق بتلك الحالة الطارئة. إذا طلب الطرف متلقي الطلب توضيحات بشأن الطلب أو طلب معلومات إضافية لاتخاذ إجراء بشأن الطلب، فيجب عليه التشاور مع نقطة اتصال شبكة الطرف الطالب التي تعمل على مدار الساعة طوال أيام الأسبوع.

165. بموجب الفقرة 3 (ز)، يجب أن يحدد الطلب أي تعليمات إجرائية خاصة. وتشمل هذه، على وجه الخصوص، طلبات عدم الكشف عن الطلب للمشتركين والأطراف الثالثة الأخرى أو استمارات التحقق من الهوية التي يتعين إكمالها للبيانات المطلوبة. بموجب هذه الفقرة، يتم إتاحة هذه التعليمات الإجرائية في البداية، حيث قد تتطلب التعليمات الخاصة عمليات إضافية داخل الطرف متلقي الطلب. في بعض الأطراف، قد يتم الحفاظ على السرية من خلال إعمال القانون بينما، في أطراف أخرى، ليس هذا هو الحال بالضرورة. لذلك، من أجل تجنب مخاطر الكشف المبكر عن التحقيق، يتم تشجيع الأطراف على التواصل فيما يتعلق

بالحاجة وأي صعوبات قد تنشأ في الحفاظ على السرية، بما في ذلك أي قانون ساري المفعول، بالإضافة إلى سياسات مقدم الخدمة فيما يتعلق بالإشعار. بما أن طلبات التحقق من الهوية للبيانات المستجيبة يمكن أن تؤدي في كثير من الأحيان إلى تأخير الهدف الرئيسي المتمثل في الكشف المعجل عن البيانات المطلوبة، ينبغي لسلطات الطرف متلقي الطلب، بالتشاور مع سلطات الطرف مقدم الطلب، تحديد متى وبأي طريقة ينبغي تأكيد إتاحة التحقق من الهوية.

166. بالإضافة إلى ذلك، قد يطلب الطرف أو مقدم الخدمة معلومات إضافية لتحديد موقع بيانات الكمبيوتر المخزنة التي يطلبها الطرف مقدم الطلب والكشف عنها.

الفقرة 4

167. تقتضي الفقرة 4 من الطرف متلقي الطلب قبول الطلبات في شكل إلكتروني. يتم تشجيع الأطراف على استخدام وسائل الاتصال السريعة لتسهيل نقل المعلومات أو البيانات والوثائق، بما في ذلك إرسال الطلبات. تستند هذه الفقرة إلى الفقرة 5 من المادة 8 ولكن تم تعديلها لإضافة أنه يجوز للطرف قبول الطلبات شفهياً، وهي طريقة اتصال تستخدمها الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع.

الفقرة 5

168. تسمح الفقرة 5 للطرف بإصدار إعلان يفرض على الأطراف الأخرى التي تطلب بيانات منه عملاً بهذه المادة، بعد تنفيذ الطلب وإرسال البيانات، أن تقدم الطلب وأي معلومات تكميلية يتم إرسالها دعماً له. بتنسيق محدد وعبر قناة محددة. على سبيل المثال، قد يعلن أحد الأطراف أنه في ظروف معينة، سوف يطلب من الطرف مقدم الطلب تقديم طلب مساعدة متبادلة لاحقًا من أجل التوثيق الرسمي لطلب عاجل والقرار المسبق لتقديم البيانات استجابة لهذا الطلب. بالنسبة لبعض الأطراف، فإن مثل هذا الإجراء سيكون مطلوبًا بموجب قانونها الوطني، بينما أشارت الأطراف الأخرى إلى أنه ليس لديها مثل هذه المتطلبات ولا تحتاج إلى استخدام هذا الخيار للقيام بإعلان.

الفقرة 6

169. تشير هذه المادة إلى "الطلبات" التي لا تقتضي من الأطراف متلقية الطلب تقديم البيانات المطلوبة إلى الأطراف مقدمة الطلب. لذلك، يقر فريق الصياغة بأنه ستكون هناك حالات لن تقدم فيها الأطراف متلقية الطلب البيانات المطلوبة إلى الطرف مقدمة الطلب بموجب هذه المادة. يجوز للطرف متلقي الطلب أن يقرر، في حالة معينة، أن تكون المساعدة المتبادلة في حالات الطوارئ بموجب المادة 10 أو أي وسيلة أخرى للتعاون هي الأنسب. نتيجة لذلك، تنص الفقرة 6 على أنه عندما يقرر الطرف متلقي الطلب أنه لن يقدم البيانات المطلوبة لطرف قدم طلبًا عملاً بالفقرة 1 من هذه المادة، يجب على الطرف متلقي الطلب إبلاغ

الطرف مقدم الطلب بقراره بشأن على أساس عاجل، وعند الاقتضاء، يجب تحديد أي شروط بموجبها ستتاح البيانات وتشرح أي أشكال أخرى من التعاون قد تكون متاحة، في محاولة لتحقيق الهدف المشترك للأطراف المتمثل في تسريع الكشف عن البيانات في حالات الطوارئ.

الفقرة 7

170. تصف الفقرة 7 الإجراءات المطبقة عندما تكون الدولة متلقية الطلب قد حددت شروطا لمنح التعاون بموجب الفقرة 6. وبموجب الفقرة 7 (أ)، عندما يكون الطرف مقدم الطلب غير قادر على الامتثال لشروط محددة، يجب أن يوجه انتباه الطرف متلقي الطلب إلى ذلك على وجه السرعة، يتعين على الطرف متلقي الطلب اتخاذ قرار بشأن ما إذا كان لا يزال من الممكن منح المساعدة. على النقيض من ذلك، إذا قبل الطرف مقدم الطلب شرطا محددا، فإنه يلتزم به. بموجب الفقرة 7 (ب)، يجوز للطرف متلقي الطلب الذي قدم معلومات أو مواد خاضعة لشرط بموجب الفقرة 6، من أجل التأكد مما إذا كان هذا الشرط قد تم الامتثال له، أن يطلب من الطرف مقدم الطلب تفسير استخدامه للمعلومات أو المواد المتاحة، ولكن كان واضحا أن الطرف مقدم الطلب قد لا يدعو إلى مساءلة تشكل عبئا كبيرا (انظر التقرير التفسيري، الفقرتين 279 و280، من الاتفاقية (.

القسم 4 - الإجراءات المتعلقة بالمساعدة المتبادلة في حالات الطوارئ

المادة 10 - المساعدة المتبادلة في حالات الطوارئ

171. تهدف المادة 10 من هذا البروتوكول إلى توفير إجراء عاجل لطلبات المساعدة المتبادلة المقدمة في حالات الطوارئ. تم تعريف حالة الطوارئ في المادة 3، الفقرة 2 (ج)، وتم شرحها في الفقرتين ذات الصلة 41 و42 من هذا التقرير التفسيري.

172. لأن المادة 10 من هذا البروتوكول تقتصر على حالات الطوارئ التي تبرر مثل هذا الإجراء العاجل، فهي تختلف عن الفقرة 3 من المادة 25 من الاتفاقية، التي يجوز فيها تقديم طلبات المساعدة المتبادلة بوسائل اتصالات عاجلة في الظروف العاجلة. التي لا ترقى إلى مستوى الطوارئ على النحو المحدد. وبعبارة أخرى، فإن المادة 25، الفقرة 3، أوسع نطاقًا من المادة 10 من هذا البروتوكول، من حيث أنها تغطي الحالات غير المشمولة في المادة 10، مثل المخاطر المستمرة ولكن غير الوشيكة على حياة أو سلامة الأشخاص، والتدمير المحتمل الأدلة التي قد تنجم عن التأخير، أو اقتراب موعد المحاكمة بسرعة، أو أنواع أخرى من حالات الطوارئ. في حين أن الآلية الواردة في المادة 25، الفقرة 3، تنص على طريقة أسرع لنقل الطلبات والاستجابة لها، فإن الالتزامات في حالة الطوارئ بموجب المادة 10 من هذا البروتوكول أكبر بكثير؛ أي عندما يكون هناك خطر كبير ووشيك على حياة أو سلامة شخص طبيعي، يجب تسريع العملية (انظر الفقرة 42 من هذا التقرير التفسيري للحصول على أمثلة لحالات الطوارئ).

الفقرة 1

173. بموجب الفقرة 1، عند تقديم طلب طارئ، يجب على الطرف مقدم الطلب أن يخلص إلى أن حالة الطوارئ بالمعنى المقصود في المادة 3، الفقرة 2 (ج)، قائمة وأن يدرج في طلبه وصفًا للوقائع التي تثبت ذلك، موضحًا الطريقة التي تكون فيها المساعدة المطلوبة ضرورية للاستجابة لحالة الطوارئ، بالإضافة إلى المعلومات الأخرى المطلوب تضمينها في الطلب بموجب المعاهدة المعمول بها أو القانون الوطني للطرف متلقي الطلب. في هذا الصدد، تجدر الإشارة إلى أنه بموجب المادة 25، الفقرة 4، من الاتفاقية، فإن تنفيذ طلبات المساعدة المتبادلة بشكل عام "يجب أن يخضع للشروط المنصوص عليها في قانون الطرف متلقي الطلب أو معاهدات المساعدة المتبادلة سارية المفعول، بما في ذلك الأسباب التي يجوز للطرف متلقي الطلب بناءً عليها رفض التعاون". وقد فهم فريق الصياغة أن هذا ينطبق أيضًا على طلبات المساعدة المتبادلة الطارئة بموجب هذا البروتوكول.

الفقرة 2

174. تتطلب الفقرة 2 من الطرف متلقي الطلب قبول طلب المساعدة المتبادلة في شكل إلكتروني. قبل قبول الطلب، يجوز للطرف متلقي الطلب أن يجعل قبول الطلب مشروطًا بامتثال الطرف مقدم الطلب للمستويات المناسبة من الأمن والتحقق من الهوية. فيما يتعلق بمتطلبات الأمن الواردة في هذه الفقرة، يجوز للأطراف أن يقرروا فيما بينهم ما إذا كانت هناك حاجة إلى تدابير حماية أمنية خاصة (بما في ذلك التشفير) التي قد تكون ضرورية في قضية حساسة بشكل خاص.

الفقرة 3

175. عندما يطلب الطرف متلقي الطلب معلومات إضافية للتوصل إلى نتيجة مفادها أن هناك حالة طوارئ بالمعنى المقصود في المادة 3، الفقرة 2 (ج)، و / أو أنه قد تم الوفاء بالمتطلبات الأخرى للمساعدة المتبادلة، فإن ذلك مطلوب بموجب الفقرة 3 للحصول على معلومات إضافية على وجه السرعة. وبالمثل، تتطلب الفقرة 3 من الطرف مقدم الطلب تقديم المعلومات التكميلية بنفس الطريقة المعجلة. لذلك ينبغي على كلا الطرفين أن يبذل قصارى جهده لتجنب ضياع الوقت الذي يمكن أن يساهم دون قصد في نتيجة مأساوية.

الفقرة 4

176. بموجب الفقرة 4، بمجرد تقديم المعلومات اللازمة للتمكين من تنفيذ الطلب، يتعين على الطرف متلقي الطلب الاستجابة للطلب على نفس الأساس المعجل. وهذا يعني عمومًا الإسراع في الحصول على أوامر قضائية تجبر مقدم الخدمة على تقديم بيانات تُعد دليلاً على الجريمة وخدمة سريعة مماثلة للأمر على مقدم الخدمة. ومع ذلك، لا ينبغي أن تُنسب التأخيرات التي تسببها أوقات استجابة مقدم الخدمة لمثل هذه الأوامر إلى سلطات الطرف متلقي الطلب.

الفقرة 5

177. بموجب الفقرة 5، يجب على جميع الأطراف أن تضمن أن أعضاء سلطتها المركزية أو السلطات الأخرى المسؤولة عن الاستجابة لطلبات المساعدة المتبادلة متاحون على مدار الساعة طوال أيام في الأسبوع، في حالة الحاجة إلى طلبات المساعدة المتبادلة الطارئة خارج ساعات العمل العادية. وتجدر الإشارة في هذا الصدد إلى أن الشبكة التي تعمل على مدار الساعة طوال أيام في الأسبوع بموجب المادة 35 من الاتفاقية متاحة للتنسيق مع السلطات المسؤولة عن المساعدة المتبادلة. لا يتطلب الالتزام الوارد في هذه الفقرة أن تكون السلطة المركزية أو السلطات الأخرى المسؤولة عن الاستجابة لطلبات المساعدة المتبادلة مزودة بالموظفين وتعمل في جميع الأوقات. بدلاً من ذلك، يجب أن تنفذ هذه السلطة إجراءات لضمان إمكانية الاتصال بالموظفين من أجل مراجعة طلبات الطوارئ خارج ساعات العمل العادية. ستسعى لجنة الاتفاقية المتعلقة بالجريمة الالكترونية بشكل غير رسمي للاحتفاظ بفهرس لهذه السلطات.

الفقرة 6

178. تنص الفقرة 6 على أساس للسلطات المركزية أو السلطات الأخرى المسؤولة عن المساعدة المتبادلة لكي تحدد بشكل متبادل قناة بديلة لإرسال المعلومات أو الأدلة المستجيبة، مهما كانت طريقة الإرسال أو السلطات التي يتم نقلها فيما بينها. بالتالي، بدلاً من إرسال المعلومات أو الأدلة المستجيبة مرة أخرى عبر قناة السلطة المركزية المستخدمة عادةً لنقل المعلومات أو الأدلة المقدمة في تنفيذ طلب الطرف مقدم الطلب، قد يقرر الطرفان بشكل متبادل استخدام قناة مختلفة لتسريع الإرسال، والحفاظ على سلامة الأدلة أو لأي سبب آخر. على سبيل المثال، في حالات الطوارئ، قد تقرر السلطات نقل الأدلة مباشرة إلى سلطة التحقيق أو المقاضاة في الطرف مقدم الطلب الذي سيستخدم الأدلة، وليس من خلال سلسلة السلطات التي تنتقل من خلالها هذه الأدلة بشكل طبيعي. قد يجوز للسلطات أيضًا، على سبيل المثال، أن تقرر التعامل الخاص مع الأدلة المادية لكي تتمكن من استبعاد الطعون في الإجراءات القضائية اللاحقة التي تفيد بأنه قد تم تغيير الأدلة أو إفسادها، أو قد تقرر بشكل متبادل بشأن معالجة خاصة لنقل الأدلة الحساسة.

الفقرة 7

179. فيما يتعلق بالإجراءات التي تحكم هذه المادة، هناك احتمالان، على النحو المبين في الفقرتين 7 و8. تنص الفقرة 7 من المادة 10 على أنه عندما لا تكون الأطراف المعنية ملزمة بشكل متبادل باتفاق أو ترتيب ساري المفعول بشأن المساعدة المتبادلة على أساس تشريع موحد أو متبادل، تطبق الأطراف إجراءات معينة منصوص عليها في فقرات محددة من المادتين 27 و28 من الاتفاقية (التي تحكم المساعدة المتبادلة في حالة عدم وجود معاهدة).

الفقرة 8

180. تنص الفقرة 8 على أنه عندما تكون الأطراف المعنية ملزمة بشكل متبادل بمثل هذا الاتفاق أو الترتيب، فإن المادة 10 تكملها أحكام ذلك الاتفاق أو الترتيب ما لم تقرر الأطراف المعنية بشكل متبادل تطبيق أي من أحكام الاتفاقية المشار إليها أو جميعها الواردة في الفقرة 7، بدلاً منها.

الفقرة 9

181. أخيراً، تنص الفقرة 9 على إمكانية إصدار إعلان يمكن للأطراف في هذا البروتوكول بموجبه تقديم الطلبات مباشرة بين المدعين العامين أو السلطات القضائية الأخرى. في بعض الأطراف، تكون هذه السلطة القضائية المباشرة لقنوات السلطة القضائية راسخة بشكل جيد ويمكن أن توفر وسيلة فعالة لزيادة تسريع تقديم الطلبات وتنفيذها. إن إرسال طلب الطوارئ من خلال نقطة الاتصال الخاصة بالطرف التي تعمل على مدار الساعة طوال أيام الأسبوع أو من خلال المنظمة الدولية للشرطة الجنائية (الإنتربول) مفيد ليس فقط لتقليل أي تأخير ولكن أيضًا لزيادة معايير الأمان والتحقق من الهوية. مع ذلك، في بعض الأطراف، قد يؤدي إرسال طلب مباشرة إلى سلطة قضائية في الطرف متلقي الطلب دون مشاركة وموافقة سلطته المركزية إلى نتائج عكسية، دون توجيه و / أو موافقة من سلطته المركزية، قد لا تكون السلطة مخولة للعمل بشكل مستقل، أو قد لا تكون على دراية بالإجراء المناسب. لذلك، يجب أن يعلن الطرف أنه يمكن إرسال الطلبات عبر قنوات السلطة غير المركزية هذه.

القسم 5 - الإجراءات المتعلقة بالتعاون الدولي في حالة عدم وجود اتفاقات دولية سارية المفعول

182. كما هو منصوص عليه في المادة 5، الفقرة 5، ينطبق هذا القسم المتعلق بالمادتين 11 و12 "في حالة عدم وجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف مقدمة الطلب والأطراف متلقية الطلب. لا تنطبق أحكام القسم 5 في حالة وجود مثل هذه المعاهدة أو الترتيب، باستثناء ما هو منصوص عليه في المادة 12، الفقرة 7. مع ذلك، يجوز للأطراف المعنية أن تقرر بشكل متبادل تطبيق أحكام القسم 5 بدلاً منها، إذا كانت المعاهدة أو الترتيب لا يحظره". وهذا يتبع نهج المادة 27 من الاتفاقية.

183. بين بعض الأطراف في هذا البروتوكول، تم تنظيم مواضيع المادتين 11 و12 بالفعل من خلال شروط معاهدات المساعدة المتبادلة (على سبيل المثال البروتوكول الإضافي الثاني للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية (سلسلة المعاهدات الأوروبية رقم 182) أو اتفاقية المساعدة القانونية المتبادلة

بين الاتحاد الأوروبي والولايات المتحدة الأمريكية. قد توفر معاهدات المساعدة المتبادلة مثل سلسلة المعاهدات الأوروبية رقم 182 مزيدًا من التفاصيل فيما يتعلق بالظروف والشروط والإجراءات التي قد يتم بموجبها هذا التعاون.

184. على الرغم من أن فريق الصياغة أخذ بعين الاعتبار هذه المعاهدات، فإن المادتين 11 و12 من هذا البروتوكول تحتويان على مصطلحات تختلف عن الأحكام المماثلة في معاهدات المساعدة المتبادلة الأخرى.

185. بينما سيستمر تطبيق شروط سلسلة المعاهدات الأوروبية رقم 182 بين الأطراف فيها، فقد اعتبر من المناسب تنظيم هاتين المادتين في هذا البروتوكول بطريقة تختلف في بعض النواحي للأسباب التالية:

– تختلف عضوية سلسلة المعاهدات الأوروبية رقم 182 عن عضوية اتفاقية الاتفاقية المتعلقة بالجريمة الالكترونية، وبالتالي فإن أحكامها غير متاحة للتعاون بين جميع الأطراف في الاتفاقية المتعلقة بالجريمة الالكترونية. تم التفاوض على سلسلة المعاهدات الأوروبية رقم 182 لتلبية احتياجات الدول الأعضاء في مجلس أوروبا بدلاً من المتطلبات والأنظمة والاحتياجات القانونية لجميع الأطراف في الاتفاقية المتعلقة بالجريمة الالكترونية، على الرغم، مبدئيا، من أن الاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية (سلسلة المعاهدات الأوروبية رقم 30) وبروتوكولاتها مفتوحة للانضمام من قبل الدول غير الأعضاء في مجلس أوروبا بناءً على دعوة من لجنة الوزراء.

– أحكام المساعدة المتبادلة في هذا البروتوكول لها نطاق مادي محدد من حيث أنها تنطبق على "التحقيقات أو الإجراءات الجنائية المحددة المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، وعلى جمع الأدلة في شكل إلكتروني للجريمة الجنائية" (المادة 2). نظرًا للمشاكل الخاصة لهذا النوع من التحقيقات أو الدعاوى - مثل عدم استقرار البيانات، والأسئلة المتعلقة بالاختصاص الإقليمي والولاية القضائية، وحجم الطلبات - قد لا تكون الأحكام المماثلة لـسلسلة المعاهدات الأوروبية رقم 182 قابلة للتطبيق دائمًا بنفس الطريقة.

– أقر فريق الصياغة بأن "الاتفاقية تنطبق على الأطراف من مختلف الأنظمة القانونية والثقافات، وليس من الممكن تحديد الشروط والضمانات المطبقة لكل سلطة أو إجراء" (انظر الفقرة 145 من التقرير التفسيري لـلاتفاقية). بدلاً من ذلك، يُطلب من الأطراف ضمان أنها توفر "حماية كافية لحقوق الإنسان والحريات" وتطبيق "معايير مشتركة [و] الحد الأدنى من الضمانات التي يجب على الأطراف الالتزام بها"، بما في ذلك "الضمانات الناشئة وفقًا للالتزامات التي تعهد بها أحد الأطراف بموجب صكوك حقوق الإنسان الدولية المنطبقة"(انظر الفقرة 145 من التقرير التفسيري للاتفاقية). انظر المادة 13 من هذا

البروتوكول (التي تدمج المادة 15 من الاتفاقية). لذلك، على عكس أحكام سلسلة المعاهدات الأوروبية رقم 182 - على سبيل المثال المادة 9 بشأن "جلسات الاستماع عن طريق التداول بالفيديو" - التي تنص على إجراءات وضمانات محددة يجب اتباعها من قبل الأطراف في سلسلة المعاهدات الأوروبية رقم 182، تسمح الأحكام المقابلة في هذا البروتوكول بالمزيد من المرونة في التنفيذ من قبل الأطراف. على سبيل المثال، يجب أن تكون الإجراءات والشروط التي تحكم عمل فرق التحقيق المشتركة على النحو المتفق عليه بين السلطات المختصة للأطراف (انظر المادة 12، الفقرة 2)، وفيما يتعلق بالتداول بالفيديو، قد يطلب الطرف متلقي الطلب شروطا وضمانات خاصة عندما السماح بالاستماع إلى المشتبه به أو المتهم عن طريق التداول بالفيديو (انظر المادة 11، الفقرة 8). وبالقدر المنصوص عليه في هذه المواد، قد تقرر الأطراف أيضًا عدم التعاون إذا لم يتم الوفاء بمتطلباتها من حيث الشروط والضمانات.

186. تنطبق المادتان 11 و12 من هذا البروتوكول فقط في حالة عدم وجود معاهدات أو ترتيبات أخرى للمساعدة المتبادلة على أساس تشريع موحد أو متبادل - ما لم تقرر الأطراف المعنية بشكل متبادل تطبيق أي من أحكامها أو جميعها بدلاً منها، إذا كانت المعاهدة أو الترتيب لا يحظر ذلك. مع ذلك، تنطبق الفقرة 7 من المادة 12 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة أم لا على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف المعنية.

المادة 11 - التداول بالفيديو

187. تتناول المادة 11 في المقام الأول استخدام تكنولوجيا التداول بالفيديو لأخذ الشهادات أو الأقوال. يمكن النص على هذا الشكل من التعاون في معاهدات المساعدة المتبادلة الثنائية والمتعددة الأطراف القائمة، على سبيل المثال، سلسلة المعاهدات الأوروبية رقم 182. في المبادئ العامة المطبقة على هذا القسم (المادة 5، الفقرة 5)، المادة 11، مثل المادة 12 في هذا البروتوكول، "تنطبق في حالة عدم وجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول بين الطرف مقدم الطلب والطرف متلقي الطلب. لا تنطبق أحكام القسم 5 في حالة وجود مثل هذه المعاهدة أو الترتيب، باستثناء ما هو منصوص عليه في المادة 12، الفقرة 7. مع ذلك، يجوز للأطراف المعنية أن تقرر بشكل متبادل تطبيق أحكام القسم 5 بدلاً منها، إذا كانت المعاهدة أو الترتيب لا يحظره".

الفقرة 1

188. تسمح الفقرة 1 بأخذ شهادة وأقوال من شاهد أو خبير عن طريق التداول بالفيديو. تمنح هذه الفقرة الطرف متلقي الطلب حرية التصرف فيما إذا كان سيقبل طلب المساعدة المتبادلة أم لا أو أن يضع شروطًا لتقديم المساعدة. على سبيل المثال، يجوز لطرف أن يرفض المساعدة أو يؤجلها للأسباب المنصوص عليها في المادة

27، الفقرات 4 إلى 5 من الاتفاقية. بدلاً من ذلك، عندما يكون تقديم المساعدة بطريقة مختلفة أكثر فعالية، مثل استمارة مكتوبة لتوثيق السجلات الرسمية أو التجارية، يجوز للطرف متلقي الطلب أن يختار تقديم المساعدة بهذه الطريقة.

189. في نفس الوقت، من المتوقع أن يكون لدى الأطراف في هذا البروتوكول القدرة التقنية الأساسية لتقديم المساعدة عبر التداول بالفيديو.

190. إن التداول بالفيديو لأخذ شهادة أو أقوال يمكن أن يثير العديد من القضايا، التي قد تشمل مشاكل قانونية ولوجستية وتقنية. من أجل أن يتم التداول بالفيديو بسلاسة، فإن التنسيق المسبق ضروري. قد تكون هناك حاجة إلى تنسيق إضافي عندما يحدد الطرف متلقي الطلب الشروط كمتطلبات مسبقة للقيام بالتداول بالفيديو. لذلك، تتطلب الفقرة 1 أيضًا من الأطراف مقدمة الطلب والأطراف متلقية الطلب التشاور عند الحاجة لتسهيل حل أي من هذه القضايا التي قد تنشأ. على سبيل المثال، كما هو موضح بمزيد من التفصيل أدناه، قد يحتاج التداول بالفيديو إلى اتباع إجراء معين حتى يتم قبول النتيجة كدليل في الطرف مقدم الطلب. وعلى العكس من ذلك، قد يحتاج الطرف متلقي الطلب إلى تطبيق متطلباته القانونية الخاصة في بعض النواحي (على سبيل المثال، أداء الشاهد اليمين أو تقديم المشورة بشأن حقوقه). علاوة على ذلك، يجوز للطرف متلقي الطلب أن يطلب من مسؤوله (أو مسؤوليه) أن يكون حاضرًا في التداول بالفيديو في بعض الحالات أو جميعها، سواء لغرض قيادة الإجراء، أو لضمان احترام حقوق الشخص الذي تم أخذ شهادته أو أقواله. في هذا الصدد، قد تكشف المشاورات أن بعض الأطراف متلقية الطلب تطلب أن يكون مسؤولها المشارك قادرًا على التدخل أو مقاطعة أو إيقاف جلسة الاستماع في حالة وجود مخاوف بشأن الامتثال لقانونه، بينما قد تسمح الأطراف الأخرى بالتداول بالفيديو دون مشاركة مسؤوليها في بعض الظروف. وكمثال آخر، قد تسعى الأطراف متلقية الطلب للحصول على ضمانات خاصة فيما يتعلق بالشهود الذين تكون سلامتهم معرضة للخطر، والأطفال الشهود، وما شابه ذلك. يجب مناقشة هذه الأمور واتخاذ قرار بشأنها مقدمًا. في بعض الحالات، قد تتعارض رغبة الطرف متلقي الطلب في إجراء واحد مع قوانين الطرف مقدم الطلب لتسهيل استخدام الشهادة أو الأقوال في المحاكمة. في مثل هذه الحالات، يجب على الأطراف بذل قصارى جهدهم لمحاولة إيجاد حلول مبتكرة تلبي احتياجات كلا الجانبين. بالإضافة إلى ذلك، يتعين على الأطراف التشاور مسبقًا لتسهيل حل المشاكل، مثل كيفية التعامل مع الاعتراضات أو دعاوى الامتياز أو الحصانة التي يثيرها الشخص أو مستشاره القانوني، أو استخدام الوثائق أو الأدلة الأخرى، أثناء التداول بالفيديو. أيضًا، قد تكون هناك حاجة إلى إجراءات معينة بسبب الشروط المفروضة من أجل القيام بالتداول بالفيديو.

ينبغي أيضًا مناقشة المسائل اللوجستية، مثل ما إذا كان ينبغي للطرف مقدم الطلب أن تنص على تفسير وتسجيل للشهادة أو الأقوال من جانبه في التداول

بالفيديو أو من جانب الطرف متلقي الطلب، بالإضافة إلى التنسيق التقني لبدء والحفاظ على الإرسال وإتاحة قنوات اتصال بديلة في حالة انقطاع الإرسال.

الفقرة 2

191. تتناول الفقرة 2 عدداً من الآليات الإجرائية وذات الصلة التي تحكم هذا الشكل من التعاون (بالإضافة إلى الإجراءات والمتطلبات المطبقة الأخرى المنصوص عليها في الفقرات المتبقية من هذه المادة)، والتي تم أخذها أو تكييفها من الاتفاقية. تنقسم الفقرة 2 إلى فقرتين فرعيتين.

192. بما أن التداول بالفيديو هو شكل من أشكال المساعدة المتبادلة، فإن الفقرة 2 (أ) تنص على أن السلطات المركزية للأطراف مقدمة الطلب والأطراف متلقية الطلب تتواصل مباشرة مع بعضها البعض لأغراض تطبيق هذه المادة. نظرًا لأن هذه المادة لا تنطبق إلا في حالة عدم وجود اتفاق أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل، فإن "السلطة المركزية" تعني هنا السلطة أو السلطات المعينة بموجب المادة 27، الفقرة 2 (أ)، من الاتفاقية (انظر المادة 3 الفقرة 2 (أ) من هذا البروتوكول والفقرة 38 من التقرير التفسيري).

193. تنص الفقرة 2 (أ) من هذه المادة أيضًا على أنه يجوز للطرف متلقي الطلب أن يقبل طلبًا لإجراء التداول بالفيديو في شكل إلكتروني، وقد يتطلب مستويات مناسبة من الأمن والتحقق من الهوية قبل قبول الطلب.

194. تقتضي الفقرة 2 (ب) (على غرار الفقرة 7 من المادة 27 من الاتفاقية) أن يقوم الطرف متلقي الطلب بإبلاغ الطرف مقدم الطلب بأسباب عدم تنفيذ الطلب أو تأخير تنفيذ الطلب. كما هو مذكور في الفقرة 192 أعلاه، يجب أن تتم هذه الاتصالات عبر قنوات السلطة المركزية. أخيرًا، تنص الفقرة 2 (ب) على أن المادة 27، الفقرة 8 (تتناول سرية طلب المساعدة المتبادلة في حالة عدم وجود معاهدة)، والفقرات 2 إلى 4 من المادة 28 (تتناول سرية الاستجابة وقيود الاستخدام في حالة عدم وجود معاهدة)، من الاتفاقية تنطبق على مادة التداول بالفيديو.

الفقرة 3

195. بما أن التداول بالفيديو قد يتطلب تواجد مسؤولين قضائيين ومساعدين في الطرف مقدم الطلب للمشاركة في أخذ الشهادة أو الأقوال في الطرف متلقي الطلب، فإن العديد من المناطق الزمنية بعيدة، فمن الأهمية أن يظهر الشخص الذي سيتم الاستماع إليه في الوقت والمكان المحددين. بموجب الفقرة 3، عندما يقدم الطرف متلقي الطلب المساعدة بموجب هذه المادة، يجب أن يسعى للحصول على حضور الشخص المطلوب شهادته أو أقواله. قد تعتمد أفضل طريقة للقيام بذلك على ظروف القضية والقانون الوطني للطرف متلقي الطلب وما إذا كان هناك، على سبيل المثال، ثقة في أن الشخص سيظهر في الوقت المحدد طواعية. في المقابل، من أجل ضمان ظهور الشخص، قد يكون من

المستحسن أن يصدر الطرف متلقي الطلب أمرًا أو استدعاءً يجبر الشخص على الحضور، وهذه الفقرة تخوله القيام بذلك، وفقًا للضمانات المنصوص عليها في قانونه الوطني.

الفقرة 4

196. يرد الإجراء المتعلق بالتداول بالفيديو في الفقرة 4. والهدف الرئيسي هو الإدلاء بالشهادة أو الأقوال إلى الطرف مقدم الطلب في شكل يسمح باستخدامها كدليل لأغراض تحقيقاته وإجراءاته. لهذا السبب، يجب تطبيق الإجراءات التي يطلبها الطرف مقدم الطلب، ما لم يكن القيام بذلك غير متوافق مع قانون الطرف متلقي الطلب، بما في ذلك المبادئ القانونية سارية المفعول في الطرف متلقي الطلب والتي لم يتم تدوينها في تشريعاته. على سبيل المثال، أثناء التداول بالفيديو، يكون الإجراء المفضل هو السماح للطرف متلقي الطلب لسلطات الطرف مقدم الطلب باستجواب الشخص الذي تُطلب منه الشهادة أو الأقوال مباشرة. سيكون المدعي العام للطرف مقدم الطلب أو قاضي التحقيق أو المحقق الذي يكون على دراية بالتحقيق أو الدعوى الجنائية بشكل أعمق، وبالتالي يعرف بشكل أفضل الأسئلة الأكثر فائدة للتحقيق أو المقاضاة، وكذلك أفضل طريقة لصياغتها بطريقة تمتثل لقانون الطرف مقدم الطلب. في هذه الحالة، لن تتدخل سلطة الطرف متلقي الطلب للمشاركة في جلسة الاستماع إلا إذا لزم الأمر في حالة تصرف سلطة الطرف مقدم الطلب بطريقة لا تتوافق مع قانون الطرف متلقي الطلب. في هذه الحالة، يجوز للطرف متلقي الطلب عدم السماح بالأسئلة أو تولي الاستجواب أو اتخاذ أي إجراء آخر قد يكون مناسبًا بموجب قانونه وظروف التداول بالفيديو. لا يشمل مصطلح " بطريقة لا تتوافق مع قانون الطرف متلقي الطلب" الحالات التي يختلف فيها الإجراء فقط عن ذلك في الطرف متلقي الطلب، وهو ما يحدث غالبًا. بدلاً من ذلك، يُقصد به معالجة الحالات التي يكون فيها الإجراء مخالفًا أو غير عملي بموجب قانون الطرف متلقي الطلب. في مثل هذه الحالات، أو عندما لا يطلب الطرف مقدم الطلب إجراءً محددًا، يكون الإجراء الافتراضي هو الإجراء المطبق بموجب قانون الطرف متلقي الطلب. إذا تسبب تطبيق قانون الطرف متلقي الطلب في حدوث مشكلة للطرف مقدم الطلب، على سبيل المثال من حيث مقبولية الشهادة أو الاقوال في المحاكمة، يمكن للأطراف مقدم الطلب والأطراف متلقي الطلب السعي للوصول إلى اتفاق بشأن إجراء مختلف يرضي الطرف مقدم الطلب مع تجنب المشكلة بموجب قانون الطرف متلقي الطلب.

الفقرة 5

197. الغرض من الفقرة 5، المتعلقة بالعقوبة أو العقاب على التصريح الكاذب، ورفض الإجابة وغير ذلك من سوء السلوك، هو حماية سلامة عملية الإدلاء بالشهادة أو الأقوال عندما يكون الشاهد في بلد مختلف عن البلد الذي توجد فيه دعوى جنائية جارية. وبقدر ما يكون الطرف متلقي الطلب قد وضع على عاتق الشخص التزامًا بالإدلاء بشهادته أو الإدلاء بأقواله بصدق، أو منعه من القيام بسلوك معين (على سبيل المثال تعطيل الإجراءات)، سيصبح الشاهد

خاضعًا للعواقب في الولاية القضائية المتواجد بها. في مثل هذه الحالات، يجب أن يكون الطرف متلقي الطلب قادرًا على تطبيق العقوبة التي ينبغي أن تطبق إذا حدث هذا السلوك في سياق إجراءاته الوطنية. يجب تطبيقها دون المساس بأي اختصاص قضائي للطرف مقدم الطلب. يوفر هذا الشرط حافزًا إضافيًا للشاهد بشهادته والإدلاء بأقواله بصدق وعدم القيام بسلوك محظور. إذا لم تكن هناك عقوبة من شأنها أن تنطبق في الإجراءات الوطنية للطرف متلقي الطلب (على سبيل المثال لتصريح كاذب من قبل شخص متهم)، فليس مطلوبًا إثبات أي من هذا السلوك المرتكب أثناء التداول بالفيديو. سيكون هذا الحكم مفيدًا بشكل خاص لضمان محاكمة الشاهد الذي يدلي بشهادته زورًا ولكن لا يمكن تسليمه للمحاكمة في الطرف مقدم الطلب بسبب، على سبيل المثال، حظر طرف متلقي الطلب تسليم رعاياه.

الفقرة 6

198. تنص الفقرة 6 على القواعد المتعلقة بتحميل التكاليف الناشئة في سياق التداول بالفيديو. كقاعدة عامة، يتحمل الطرف متلقي الطلب جميع التكاليف الناشئة عن التداول بالفيديو، باستثناء (i) أتعاب الشاهد الخبير؛ (ii) تكاليف الترجمة الكتابية والشفهية والتدوين؛ و (iii) التكاليف الكبيرة بحيث تكون ذات طبيعة غير عادية. غالبًا ما لا تكون تكاليف السفر وتكاليف المبيت داخل الطرف متلقي الطلب كبيرة، بحيث يتحمل الطرف متلقي الطلب هذه التكاليف، إن وجدت. مع ذلك، يمكن تعديل القواعد المتعلقة بالتكاليف من خلال الاتفاق بين الأطراف مقدمة الطلب والأطراف متلقية الطلب. على سبيل المثال، إذا كان الطرف مقدم الطلب ينص على وجود مترجم فوري أو خدمات التدوين في نهاية التداول بالفيديو، فقد لا تكون هناك حاجة إلى أن يدفع للطرف متلقي الطلب تكاليف مثل هذه الخدمات. عندما ينص الطرف متلقي الطلب على تكاليف غير عادية في تقديم المساعدة، وفقًا للفقرة 6 (ب)، يجب على الطرف مقدم الطلب والطرف متلقي الطلب التشاور قبل تنفيذ الطلب لتحديد ما إذا كان الطرف مقدم الطلب يمكنه تحمل هذه التكاليف، وإذا لم يكن الأمر كذلك، كيف يمكن تجنبها.

الفقرة 7

199. بينما تسمح الفقرة 1 صراحة باستخدام تكنولوجيا التداول بالفيديو للإدلاء بالشهادة أو الأقوال، تنص الفقرة 7 (أ) على أنه يجوز تطبيق أحكام المادة 11 لأغراض التداول بالصوت متى تم الاتفاق على ذلك بشكل متبادل. بالإضافة إلى ذلك، تنص الفقرة 7 (ب) على أنه في حالة الاتفاق بين الأطراف مقدمة الطلب والأطراف متلقية الطلب، يجوز استخدام التكنولوجيا "لأغراض أخرى، أو لجلسات الاستماع، ... بما في ذلك لأغراض تحديد هوية الأشخاص أو الأشياء". بالتالي، إذا تم الاتفاق بشكل متبادل، يجوز للأطراف مقدمة الطلب والأطراف متلقية الطلب التفكير في استخدام تقنية التداول بالفيديو من أجل الاستماع

أو تنفيذ الإجراءات المتعلقة بالمشتبه به أو المتهم (تجدر الإشارة إلى أن بعض الأطراف قد تعتبر المشتبه فيه أو المتهم "شاهدًا" بحيث يكون أخذ شهادة أو تصريح ذلك الشخص مشمولاً بالفعل بالفقرة 1 من هذه المادة). في حالة عدم انطباق الفقرة 1، تنص الفقرة 7 على السلطة القانونية للسماح باستخدام التكنولوجيا في مثل هذه الحالات.

الفقرة 8

200. الفقرة 8 تتناول الحالة التي يختار فيها الطرف متلقي الطلب السماح بسماع مشتبه به أو متهم، على سبيل المثال لأغراض الإدلاء بشهادة أو أقوال أو للإشعارات أو التدابير الإجرائية الأخرى. بنفس الطريقة التي يتمتع بها الطرف متلقي الطلب بالسلطة التقديرية للسماح بالتداول بالفيديو لشاهد عادي أو خبير، فإنه يتمتع بسلطة تقديرية فيما يتعلق بالشخص المشتبه فيه أو المتهم. علاوة على ذلك، بالإضافة إلى أي شرط أو قيود أخرى قد يفرضها الطرف متلقي الطلب من أجل السماح بإجراء التداول بالفيديو، قد يتطلب القانون الوطني للطرف شروطًا معينة فيما يتعلق بجلسة الاستماع للمشتبه بهم أو المتهمين. على سبيل المثال، قد يقتضي قانون الطرف موافقة الشخص المشتبه به أو المتهم للإدلاء بشهادة أو أقوال، أو قد يحظر قانون الطرف أو يحد من استخدام التداول بالفيديو للإشعارات أو الإجراءات الإجرائية الأخرى. وبالتالي، فإن الهدف من الفقرة 8 هو التأكيد على حقيقة أن الإجراءات التي تستهدف المشتبه فيه أو المتهم قد تؤدي إلى الحاجة إلى شروط أو ضمانات تكميلية لتلك التي قد تنشأ لولا ذلك.

المادة 12 - فرق التحقيق المشتركة والتحقيقات المشتركة

201. بالنظر إلى الطبيعة عبر الوطنية للجريمة الالكترونية والأدلة الإلكترونية، فإن التحقيقات والملاحقات القضائية المتعلقة بالجرائم الإلكترونية والأدلة الإلكترونية غالباً ما تكون لها صلات بدول أخرى. يمكن أن تكون فرق التحقيق المشتركة وسيلة فعالة للتعاون العملي أو التنسيق بين دولتين أو أكثر. وتنص المادة 12 على أساس لمثل هذه الأشكال من التعاون.

202. أظهرت التجربة أنه عندما تحقق دولة في جريمة ذات بعد عابر للحدود فيما يتعلق بالجرائم الإلكترونية أو التي يلزم الحصول على أدلة إلكترونية بشأنها، يمكن أن يستفيد التحقيق من مشاركة سلطات الدول الأخرى التي تحقق أيضا في نفس السلوك أو السلوك المرتبط به أو حيث يكون التنسيق مفيدًا بطريقة أخرى.

203. كما هو مبين في المادة 5 من هذا البروتوكول والفقرات 182 إلى 186 من التقرير التفسيري، لا تنطبق أحكام المادة 12 في حالة وجود معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف مقدمة الطلب والأطراف متلقية الطلب، ما لم تقرر الأطراف المعنية بشكل متبادل تطبيق أي أو كل ما تبقى من هذه المادة بدلاً منها، إذا لم تحظر المعاهدة أو الترتيب ذلك. كما هو موضح

أدناه، تنطبق الفقرة 7 سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريعات موحدة أو متبادلة سارية المفعول بين الأطراف المعنية أم لا.

الفقرة 1

204. تنص الفقرة 1 على أنه يجوز للسلطات المختصة لطرفين أو أكثر أن توافق على إنشاء فريق تحقيق مشترك عندما تعتبره ذا فائدة خاصة. يتم تشكيل فريق التحقيق المشترك بالاتفاق المتبادل. لا ينبغي أن تُفهم مصطلحات "اتفاق متبادل" و "اتفاق" و "يوافق" - على النحو المستخدم في المادة 12 - على أنها تتطلب اتفاقًا ملزمًا بموجب القانون الدولي.

205. تستخدم هذه المادة مصطلحين مرتبطين: "السلطات المختصة" و "السلطات المشاركة". يحدد كل طرف أي السلطات تكون مختصة -أي "السلطات المختصة"- لإبرام اتفاق تشكيل فريق تحقيق مشترك. قد تأذن بعض الأطراف لمجموعة من المسؤولين، مثل المدعين العامين أو قضاة التحقيق أو غيرهم من كبار موظفي إنفاذ القانون الذين يقودون التحقيقات أو الدعاوى الجنائية، لإبرام مثل هذا الاتفاق؛ قد يطلب البعض الآخر من السلطة المركزية - المكتب المسؤول عادة عن مسائل المساعدة المتبادلة - للقيام بذلك. القرار بشأن أي السلطات تشارك فعليًا في فريق التحقيق المشترك - "السلطات المشاركة" - بالمثل سيتم تحديده من قبل الأطراف المعنية.

الفقرة 2

206. تنص الفقرة 2 على الإجراءات والشروط التي يتعين على فرق التحقيق المشتركة العمل في ظلها، مثل الأغراض المحددة لكل منها؛ وتكوينها؛ المهام؛ المدة وأي فترات تمديد؛ الموقع؛ التنظيم؛ شروط جمع ونقل واستخدام المعلومات أو الأدلة؛ شروط السرية وشروط مشاركة السلطات المشاركة لطرف ما في أنشطة التحقيق التي تجري على إقليم طرف آخر، يجب أن تكون على النحو المتفق عليه بين تلك السلطات المختصة. على وجه الخصوص، عند إعداد الاتفاق، قد ترغب الأطراف المعنية في مناقشة شروط رفض أو تقييد استخدام المعلومات أو الأدلة، بما في ذلك، على سبيل المثال، على الأسس المنصوص عليها في المادة 27، الفقرتين 4 أو 5، من الاتفاقية، و ما الإجراء الذي يجب اتباعه إذا كانت المعلومات أو الأدلة مطلوبة لأغراض أخرى غير تلك التي تم إبرام الاتفاق من أجلها (بما في ذلك استخدام المعلومات أو الأدلة من قبل الادعاء أو الدفاع في قضية أخرى أو حيث قد تكون هناك حاجة لمنع حدوث حالة طوارئ على النحو المحدد في المادة 3، الفقرة 2 (ج)، أي الحالة التي يوجد فيها خطر كبير ووشيك على حياة أو سلامة شخص طبيعي). يتم تشجيع الأطراف على أن تحدد في الاتفاق حدود صلاحيات المسؤولين المشاركين من أحد الأطراف الموجودين فعليًا على إقليم طرف آخر. كما يتم تشجيع الأطراف على السماح في الاتفاق بالنقل الإلكتروني للمعلومات أو الأدلة التي تم جمعها.

207. من المتوقع أن تحدد الأطراف بشكل متبادل هذه الإجراءات والشروط كتابةً. في أي اتفاق، ينبغي النظر في مستوى التفاصيل المطلوبة. قد يوفر النص المبسط المستوى اللازم من الدقة للظروف المتوقعة، مع القدرة على إضافة أحكام تكميلية إذا تطلبت الظروف المستقبلية مزيدًا من الدقة. يجب على الأطراف النظر في النطاق الجغرافي ومدة اتفاق فريق التحقيق المشترك وحقيقة أن الاتفاق قد يحتاج إلى تعديل أو توسيع مع وجود وقائع جديدة.

208. قد تتضمن المعلومات أو الأدلة المستخدمة كجزء من فريق التحقيق المشترك بيانات شخصية في شكل معلومات عن المشتركين أو بيانات الحركة أو بيانات المحتوى. كما في حالة التدابير التعاونية الأخرى بموجب هذا البروتوكول، تنطبق المادة 14 على نقل البيانات الشخصية وفقًا لفرق التحقيق المشتركة.

209. كما هو الحال بشكل عام فيما يتعلق بجميع المعلومات أو الأدلة التي يتلقاها أي طرف بموجب هذا البروتوكول، فإن قواعد الإثبات السارية لذلك الطرف تحكم ما إذا كانت المعلومات أو الأدلة ستكون مقبولة في الدعاوى القضائية.

الفقرة 3

210. تسمح الفقرة 3 للطرف بأن يعلن أثناء التوقيع على هذا البروتوكول، أو عند إيداع صك التصديق أو القبول أو الموافقة، أن سلطته المركزية يجب أن تكون موقعة أو توافق على اتفاق إنشاء الفريق. تم إدراج هذا الحكم لعدة أسباب. أولاً، يعتبر عدد من الأطراف أن الاتفاقات المشتركة الدولية هي شكل من أشكال المساعدة المتبادلة، وفي عدد من الأطراف الأخرى، قد تلعب السلطات المركزية للمساعدة المتبادلة دورًا في ضمان تلبية المتطلبات القانونية الوطنية سارية المفعول عندما تكون السلطات المختصة (التي قد تكون مدعين عامين أو الشرطة ذات الخبرة المحدودة نسبيًا في التعاون الدولي) تقوم بإعداد اتفاق فريق التحقيق المشترك بموجب هذه المادة. يمكن أن تساعد تجربة السلطة المركزية مع الاتفاقات الدولية التي تحكم المساعدة المتبادلة وغيرها من أشكال التعاون الدولي (بما في ذلك هذا البروتوكول) على لعب دور قيم في ضمان تلبية متطلبات البروتوكول. أخيرًا، إذا قدم أحد الأطراف الإعلان المنصوص عليه في هذه الفقرة، فإن سلطات الأطراف الأخرى التي تسعى إلى الدخول في فريق مشترك مع الطرف المعلن على علم أن السلطة المركزية للطرف المعلن يجب أن توقع على اتفاق فريق التحقيق المشترك أو توافق عليه بطريقة أخرى لكي يكون ساري المفعول بموجب البروتوكول. وهذا يحمي من إبرام اتفاق فريق التحقيق المشترك الذي لا يشترط الحصول على إذن أو لا يمتثل للمتطلبات القانونية الواجبة التطبيق للطرف المعلن.

الفقرة 4

211. بموجب الفقرة 4، عادة ما تقوم السلطات المختصة التي تحددها الأطراف بموجب الفقرة 1 والسلطات المشاركة المبينة في الفقرة 2 بالاتصال مباشرة مع بعضها البعض

لضمان الكفاءة والفعالية. ومع ذلك، عندما تتطلب الظروف الاستثنائية مزيدًا من التنسيق المركزي - مثل القضايا ذات التشعبات الخطيرة أو القضايا التي تثير مشاكل تنسيق معينة - يمكن الاتفاق على قنوات أخرى مناسبة. على سبيل المثال، قد تكون السلطات المركزية للمساعدة المتبادلة متاحة للمساعدة في تنسيق مثل هذه الأمور.

الفقرة 5

212. تنص الفقرة 5 على أنه في حالة الحاجة إلى اتخاذ تدابير التحقيق على إقليم أحد الأطراف المشاركة، يجوز للسلطات المشاركة في ذلك الطرف أن تصدر طلباً إلى سلطاتها لتنفيذ هذه التدابير. تحدد هذه السلطات ما إذا كان بإمكانها اتخاذ إجراء التحقيق على أساس قانونها الوطني. حيثما أمكنها القيام بذلك، قد لا تكون هناك حاجة إلى طلب المساعدة المتبادلة من قبل الأطراف المشاركة الأخرى. يوفر هذا أحد الجوانب الأكثر ابتكارًا في فرق التحقيق المشتركة ومع ذلك، في بعض الحالات، قد لا يكون لهذه السلطات صلاحية وطنية كافية لاتخاذ إجراء تحقيق معين نيابة عن طرف آخر دون طلب المساعدة المتبادلة.

الفقرة 6

213. تتناول الفقرة 6 استخدام المعلومات أو الأدلة التي حصلت عليها السلطات المشاركة لطرف من السلطات المشاركة لطرف آخر. قد يتم رفض الاستخدام أو تقييده وفقًا لشروط الاتفاق الموضح في الفقرتين 1 و2؛ ومع ذلك، إذا كان هذا الاتفاق لا ينص على شروط لرفض أو تقييد الاستخدام، فيمكن استخدام المعلومات أو الأدلة على النحو المنصوص عليه في الفقرات من 6 (أ) إلى (ج). لا تخل الظروف المنصوص عليها في الفقرة 6 بالمتطلبات المنصوص عليها لنقل المعلومات أو الأدلة إلى دولة أخرى في المادة 14.

214. تجدر الإشارة إلى أنه عند تطبيق الفقرات من 6 (أ) إلى (ج) يجوز للسلطات المشاركة مع ذلك أن تقرر بشكل متبادل تقييد استخدام معلومات أو أدلة معينة من أجل تجنب العواقب السلبية على أحد تحقيقاتها، سواء قبل ذلك أو على وجه الخصوص بعد تقديم المعلومات أو الأدلة. على سبيل المثال، حتى إذا كان استخدام الأدلة من أجل الغرض الذي تم إنشاء الفريق من أجله من قبل الطرف الذي استلمها، فقد يكون له تأثير سلبي على تحقيق الطرف الذي يقدم المعلومات أو الأدلة (مثل الكشف عن وجود تحقيق مع جماعة إجرامية، مما قد يتسبب في هروب المجرمين أو إتلاف الأدلة أو تخويف الشهود). في هذه الحالة، يجوز للطرف الذي قدم المعلومات أو الأدلة أن يطلب من الطرف الآخر الموافقة على عدم نشرها إلى أن يزول هذا الخطر.

215. في الفقرة 6 (ب)، قصد فريق الصياغة، في حالة عدم وجود اتفاق ينص على شروط رفض أو تقييد الاستخدام، أن موافقة السلطات التي تقدم المعلومات أو الأدلة لن تكون مطلوبة، بموجب المبادئ القانونية الأساسية للطرف التي تلقت سلطاتها المشاركة هذه المعلومات

أو الأدلة المهمة لإجراء دفاع فعال في الدعاوى المتعلقة بتلك الجرائم الأخرى يجب الكشف عنها للدفاع أو للسلطة القضائية. على الرغم من أن الموافقة في هذه الحالة غير مطلوبة، يجب تقديم الإشعار بالكشف عن المعلومات أو الأدلة لهذا الغرض دون تأخير غير مبرر. إذا أمكن، يجب تقديم هذا الإشعار قبل الكشف، لتمكين الطرف الذي قدم المعلومات أو الأدلة من التحضير للكشف والسماح للأطراف بالتشاور حسب الاقتضاء.

216. فهم فريق الصياغة أن الفقرة 6 (ج) تشير إلى الظروف الاستثنائية حيث يمكن لسلطات الطرف المتلقي أن تستخدم المعلومات أو الأدلة مباشرة لمنع حدوث حالة طوارئ على النحو المحدد في المادة 3، الفقرة 2 (ج)، من هذا البروتوكول. سلامة الشخص الطبيعي تعني ضررًا جسديًا خطيرًا. تم شرح مفهوم "الخطر الجسيم والوشيك على حياة أو سلامة أي شخص طبيعي" بمزيد من التفصيل في الفقرة 42 من التقرير التفسيري، والتي تقدم أيضًا أمثلة على مثل هذه الحالات. واعتبر فريق الصياغة أن الحالات التي يكون فيها تهديد كبير ووشيك للأصول أو الشبكات ينطوي على حياة أو سلامة شخص طبيعي سيتم إدراجه في هذا المفهوم. في الحالات التي يتم فيها استخدام المعلومات أو الأدلة بموجب الفقرة 6 (ج)، يتم إشعار السلطات المشاركة للطرف الذي قدم المعلومات أو الأدلة دون تأخير غير مبرر بهذا الاستخدام، ما لم يقرر الطرفان خلاف ذلك. على سبيل المثال، قد تقرر السلطات المشاركة أنه ينبغي إشعار السلطة المركزية.

الفقرة 7

217. أخيراً، ينبغي التذكير عموماً بأن هناك تاريخاً طويلاً لجهود التعاون الدولي المضطلع بها بين الشركاء في إنفاذ القانون على أساس مخصص، حيث تعاون فريق من المدعين العامين و / أو المحققين من بلد ما مع نظرائهم الأجانب في تحقيق معين، بالإضافة إلى فريق التحقيق المشتركة. تنص الفقرة 7 على هذه الجهود التعاونية الدولية وتوفر أساسًا تعاهديًا للدخول في تحقيق مشترك في حالة عدم وجود الاتفاق الموصوف في الفقرتين 1 و2، إذا طلب أحد الأطراف مثل هذا الأساس القانوني. تنطبق هذه الفقرة سواء كانت هناك معاهدة أو ترتيب للمساعدة المتبادلة على أساس تشريع موحد أو متبادل ساري المفعول بين الأطراف المعنية أم لا. كما هو الحال مع جميع التدابير بموجب هذا البروتوكول، تخضع التحقيقات المشتركة بموجب الفقرة 7 لشروط وضمانات الفصل الثالث.

الفصل الثالث - الشروط والضمانات

المادة 13 - الشروط والضمانات

218. استناداً إلى المادة 15 من الاتفاقية، تنص المادة 13 على أن "على كل طرف أن يضمن أن وضع وتنفيذ وتطبيق الصلاحيات والإجراءات المنصوص عليها في هذا البروتوكول تخضع

للشروط والضمانات المنصوص عليها في قانونه الوطني، والذي يجب أن ينص على الحماية الكافية لحقوق الإنسان وحرياته". نظرًا لأن هذه المادة تستند إلى المادة 15 من الاتفاقية، فإن شرح تلك المادة في الفقرات 145 إلى 148 من التقرير التفسيري للاتفاقية صالح أيضًا للمادة 13 من هذا البروتوكول، بما في ذلك مبدأ التناسب "يجب تنفيذه من خلال كل طرف وفقاً لمبادئ قانونه الوطني ذو الصلة"(انظر الفقرة 146 من التقرير التفسيري للاتفاقية).

219. تجدر الإشارة إلى أنه بالإضافة إلى هذه المادة، تحتوي مواد أخرى على ضمانات مهمة. على سبيل المثال، فإن تدابير هذا البروتوكول محدودة النطاق، أي "للتحقيقات أو الدعاوى الجنائية المحددة المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، وجمع الأدلة في شكل إلكتروني للجريمة الجنائية" (انظر المادة 2). بالإضافة إلى ذلك، تحدد المواد الفردية المعلومات التي يجب إدراجها في الطلبات والأوامر والمعلومات المصاحبة التي قد تساعد في تطبيق الضمانات الوطنية (انظر المادة 6، الفقرة 3؛ المادة 7، الفقرتان 3 و4؛ المادة 8، الفقرة 3؛ المادة 9، الفقرة 3). بالإضافة إلى ذلك، يتم تحديد أنواع البيانات التي سيتم الكشف عنها في كل مادة، على سبيل المثال، في المادة 7 التي تقتصر على معلومات المشترك. أيضًا، يجوز للأطراف إبداء تحفظات وإعلانات، على سبيل المثال للحد من نوع المعلومات التي يجب تقديمها، كما هو الحال في المادتين 7 و8. أخيرًا، عند نقل البيانات الشخصية وفقًا لهذا البروتوكول، يتم تطبيق ضمانات حماية البيانات المنصوص عليها في المادة 14.

المادة 14 - حماية البيانات الشخصية

الفقرة 1 – النطاق

220. غالباً ما تتضمن التدابير المنصوص عليها في الفصل الثاني من هذا البروتوكول نقل البيانات الشخصية. نظرًا لأن العديد من الأطراف في هذا البروتوكول قد تكون مطالبة، من أجل الوفاء بالتزاماتها الدستورية أو الدولية، بضمان حماية البيانات الشخصية، تنص المادة 14 على ضمانات حماية البيانات للسماح للأطراف بالوفاء بهذه المتطلبات، وبالتالي لتمكين معالجة البيانات الشخصية لأغراض هذا البروتوكول.

221. عملاً بالفقرة 1 (أ)، يجب على كل طرف معالجة البيانات الشخصية التي يتلقاها بموجب هذا البروتوكول وفقًا للضمانات المحددة المنصوص عليها في الفقرات من 2 إلى 15. وهذا يشمل البيانات الشخصية المنقولة كجزء من أمر أو طلب بموجب هذا البروتوكول. مع ذلك، لا تنطبق الفقرات من 2 إلى 15 إذا كانت شروط الاستثناءات الموضحة في الفقرات 1 (ب) أو 1 (ج) قابلة للتطبيق.

222. يرد الاستثناء الأول في الفقرة 1 (ب)، التي تنص على أنه " أثناء استلام البيانات الشخصية بموجب هذا البروتوكول، يكون كل من الطرف الناقل والطرف المتلقي ملزمين بشكل متبادل

باتفاق دولي ينشئ إطار شامل بين تلك الأطراف لحماية البيانات الشخصية، والذي ينطبق على نقل البيانات الشخصية لغرض منع الجرائم الجنائية والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها، والذي ينص على معالجة البيانات الشخصية بموجب ذلك الاتفاق يتوافق مع متطلبات تشريعات حماية البيانات للأطراف المعنية، تسري شروط هذا الاتفاق، بالنسبة للتدابير التي تقع ضمن نطاق هذا الاتفاق، على البيانات الشخصية الواردة بموجب البروتوكول بدلاً من الفقرات 2 إلى 15، ما لم يتفق الطرفان المعنيان على خلاف ذلك". في هذا السياق، يمكن اعتبار إطار العمل بشكل عام على أنه "شامل" حيث يغطي بشكل شامل جوانب حماية البيانات لعمليات نقل البيانات. من الأمثلة على الاتفاقات المبرمة بموجب الفقرة 1 (ب)، اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (سلسلة المعاهدات الأوروبية رقم 108) بصيغتها المعدلة بموجب بروتوكول (سلسلة معاهدات مجلس أوروبا رقم 223)، والاتفاق بين الولايات المتحدة الأمريكية والاتحاد الأوروبي بشأن حماية المعلومات الشخصية المتعلقة بمنع الجرائم الجنائية والكشف عنها والتحقيق فيها ومقاضاة مرتكبيها. تنطبق أحكام هذه الاتفاقات بدلاً من الفقرات من 2 إلى 15 بالنسبة للتدابير التي تدخل في نطاق هذه الاتفاقات. فيما يتعلق بالأطراف في اتفاقية سلسلة المعاهدات الأوروبية رقم 108 بصيغتها المعدلة ببروتوكول سلسلة معاهدات مجلس أوروبا رقم 223، فإن هذا يعني أن المادة 14، الفقرة 1، من تلك المعاهدة، كما هو موضح بمزيد من التفصيل في الفقرات 105 إلى 107 من تقريرها التفسيري، قابلة للتطبيق. فيما يتعلق بالتوقيت، سيتم إلغاء الفقرات من 2 إلى 15 من هذه المادة فقط إذا كان الطرفان ملزمين بالاتفاق أثناء استلام البيانات الشخصية بموجب هذا البروتوكول. ينطبق هذا طالما أن الاتفاق ينص على استمرار معالجة البيانات المنقولة بموجبه بموجب شروط ذلك الاتفاق.

223. يرد الاستثناء الثاني في الفقرة 1 (ج) التي تنص على أنه حتى إذا لم يكن الطرف الناقل والطرف المتلقي ملزمين بشكل متبادل بموجب اتفاق من النوع الموصوف في الفقرة 1 (ب)، فإنه يجوز لهما مع ذلك أن يقررا بشكل متبادل أن يتم نقل البيانات الشخصية بموجب هذا البروتوكول على أساس اتفاقات أو ترتيبات أخرى بينهما بدلاً من الفقرات 2 إلى 15 من هذه المادة. وهذا يضمن احتفاظ الأطراف بالمرونة في تحديد ضمانات حماية البيانات التي تنطبق على عمليات النقل فيما بينها بموجب البروتوكول. من أجل توفير اليقين القانوني والشفافية للأفراد ولمقدمي الخدمات والكيانات المعنية بعمليات نقل البيانات عملاً بالتدابير الواردة في الفصل 2، المادة 2 من هذا البروتوكول، تشجع الأطراف على إبلاغ الجمهور بوضوح بإرادتها المتبادلة على أن مثل هذا الاتفاق أو الترتيب يحكم جوانب حماية البيانات في عمليات نقل البيانات الشخصية فيما بينها.

224. اعتبر فريق الصياغة أنه من خلال ضمانات حماية البيانات المنصوص عليها في الفقرات من 2 إلى 15 من هذه المادة، يضمن هذا البروتوكول الحماية المناسبة

لعمليات نقل البيانات بموجب هذا البروتوكول. تحقيقًا لهذه الغاية، ووفقًا للفقرة 1 (د)، فإن عمليات نقل البيانات بموجب الفقرة 1 (أ) يجب أن تفي بمتطلبات الإطار القانوني لحماية البيانات لعمليات النقل الدولية للبيانات الشخصية لكل طرف، ولا يجوز إجراء أي ترخيص آخر لعمليات النقل هذه بموجب هذه الأطر القانونية.

بالإضافة إلى ذلك، بقدر ما تنص الاتفاقات الموصوفة في الفقرة 1 (ب) بموجب شروطها على أن معالجة البيانات الشخصية بموجب تلك الاتفاقات تتوافق مع متطلبات تشريعات حماية البيانات للأطراف المعنية، فإن الفقرة 1 (د) توسع نطاق هذا التأييد إلى عمليات النقل بموجب هذا بروتوكول. بالتالي توفر هذه الفقرة اليقين القانوني لعمليات النقل الدولية للبيانات الشخصية وفقًا للفقرتين 1 (أ) أو 1 (ب) استجابةً للأوامر والطلبات بموجب هذا البروتوكول من أجل ضمان التبادل الفعال والذي يمكن التنبؤ به للبيانات. نظرًا لأن الاتفاقات أو الترتيبات الموضحة في الفقرة 1(ج) قد لا تشير دائمًا إلى الامتثال للإطار القانوني لحماية البيانات الخاصة بالأطراف لعمليات النقل الدولية - على سبيل المثال في حالة معاهدات المساعدة المتبادلة الثنائية - فإنها لا تتلقى نفس التأييد بموجب هذا البروتوكول كما في الفقرات 1 (أ) أو 1 (ب) ومع ذلك، يجوز للأطراف المعنية توفير مثل هذا التأييد عن طريق الإرادة المتبادلة.

225. بالإضافة إلى ذلك، تنص الفقرة 1 (د) على أنه يجوز للطرف فقط رفض أو منع نقل البيانات الشخصية إلى طرف آخر بموجب هذا البروتوكول لأسباب تتعلق بحماية البيانات: (1) بموجب الشروط المنصوص عليها في الفقرة 15 فيما يتعلق بالتشاور والتعليق، عندما تنطبق الفقرة 1 (أ)، أو (2) بموجب شروط الاتفاقات أو الترتيبات المحددة المشار إليها في الفقرتين 1 (ب) أو 1 (ج)، عندما تنطبق إحدى هاتين الفقرتين.

226. أخيراً، فإن الهدف من المادة 14 هو وضع ضمانات مناسبة تسمح بنقل البيانات الشخصية بين الأطراف بموجب هذا البروتوكول. لا تتطلب المادة 14 مواءمة الأطر القانونية الوطنية لمعالجة البيانات الشخصية بشكل عام، ولا الإطار الخاص بمعالجة البيانات الشخصية لأغراض إنفاذ القانون الجنائي على وجه التحديد. تنص الفقرة 1 (هـ) أنه لا يُمنع الأطراف من تطبيق ضمانات أقوى لحماية البيانات من تلك المنصوص عليها في الفقرات من 2 إلى 15 لمعالجة البيانات الشخصية التي تتلقاها تلك السلطات بموجب هذا البروتوكول. على العكس من ذلك، الفقرة 1 (هـ). لا تهدف إلى السماح للأطراف بفرض متطلبات حماية بيانات إضافية لعمليات نقل البيانات بموجب هذا البروتوكول بخلاف تلك المسموح بها تحديدًا في هذه المادة.

الفقرة 2 - الغرض والاستخدام

227. تتناول الفقرة 2 الأغراض والاستخدام الذين يجوز للأطراف أن تعالج من أجلهما البيانات الشخصية بموجب هذا البروتوكول. تنص الفقرة 2 (أ) على أن "الطرف الذي

تلقى البيانات الشخصية يجب أن يعالجها للأغراض الموضحة في المادة 2"، أي لغرض "تحقيقات أو إجراءات جنائية محددة المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات" ومن أجل "جمع الأدلة في شكل إلكتروني لجريمة جنائية"، وفيما بين الأطراف في البروتوكول الأول، لغرض "تحقيقات أو دعاوى جنائية محددة تتعلق بالجرائم الجنائية المحددة بموجب البروتوكول الأول". بعبارة أخرى، أن تقوم السلطات بالتحقيق في نشاط إجرامي محدد أو مقاضاة مرتكبيه، وهو الغرض المشروع الذي يمكن من أجله البحث عن أدلة أو معلومات التي تحتوي على بيانات شخصية ومعالجتها.

228. بينما لا يجوز، في المقام الأول، الاحتجاج بهذا البروتوكول إلا من أجل الحصول على معلومات أو أدلة في تحقيقات أو دعاوى جنائية محددة وليس لأغراض أخرى، تنص الفقرة 2 (أ) أيضًا على أن الطرف "لا يجوز له مواصلة معالجة البيانات الشخصية لغرض غير متوافق، ولا يجوز له معالجة البيانات مرة أخرى عندما لا يُسمح بذلك بموجب إطاره القانوني الوطني". عند تحديد ما إذا كان الغرض من المعالجة الإضافية لا يتعارض مع الغرض الأولي، يتم تشجيع السلطة المختصة على إجراء تقييم شامل للظروف المحددة، مثل (1) العلاقة بين الغرض الأولي والغرض الإضافي (على سبيل المثال أي صلة موضوعية)؛ (2) العواقب (المحتملة) للاستخدام الإضافي المقصود للأفراد المعنيين، مع مراعاة طبيعة البيانات الشخصية (على سبيل المثال حساسيتها) ؛ (3) أي توقعات معقولة للأفراد المعنيين فيما يتعلق بالغرض من الاستخدام الإضافي والكيانات التي قد تعالج البيانات؛ و (4) الطريقة التي ستتم بها معالجة البيانات وحمايتها من الاستخدام غير السليم. الذي قد يضع الإطار القانوني لطرف ما قيودًا خاصة فيما يتعلق بالأغراض الأخرى التي يمكن استخدام البيانات من أجلها.

229. تشمل المعالجة لغرض غير متوافق عادة استخدام البيانات من أجل التعاون الدولي وفقاً للقوانين الوطنية والاتفاقات أو الترتيبات الدولية (على سبيل المثال المساعدة المتبادلة) في مجال القانون الجنائي. ويمكن أن تشمل أيضا، من بين أمور أخرى، استخدامات وظائف حكومية معينة، مثل تقديم التقارير إلى هيئات الرقابة؛ التحقيقات ذات الصلة في انتهاكات القانون الجنائي أو المدني أو الإداري (بما في ذلك التحقيقات من قبل الهيئات الحكومية الأخرى) والفصل فيها؛ عمليات الكشف التي تتطلبها أوامر المحكمة الوطنية؛ الكشف للمتقاضين من القطاع الخاص؛ الكشف عن معلومات معينة لمحامي المتهم؛ والكشف مباشرة للجمهور أو وسائل الإعلام الإخبارية (بما في ذلك في سياق الوصول إلى طلبات الوثائق والإجراءات القانونية العامة). بالمثل، يمكن اعتبار المعالجة الإضافية للبيانات الشخصية لأغراض الأرشفة للصالح العام أو البحث العلمي أو التاريخي أو الأغراض الإحصائية متوافقة.

230. تسمح الفقرة 2 (أ) كذلك للأطراف بفرض شروط وقيود إضافية على استخدام البيانات الشخصية في القضايا الفردية، بالقدر المنصوص عليه في الفصل الثاني من هذا البروتوكول.

مع ذلك، يجب ألا تتضمن هذه الشروط شروطًا عامة لحماية البيانات - أي تلك التي ليست خاصة بقضية معينة - بخلاف تلك المنصوص عليها في المادة 14. على سبيل المثال، يتم قبول أنظمة رقابة مختلفة بموجب الفقرة 14 ولا يجوز للطرف جعلها شرطا للنقل في قضية فردية ما لم يكن للطرف مقدم الطلب ما يعادل سلطة حماية البيانات المتخصصة.

231. أخيرًا، تتطلب الفقرة 2 (ب) أنه عند البحث عن البيانات الشخصية واستخدامها وفقًا لهذا البروتوكول، "يجب على الطرف المتلقي أن يضمن بموجب إطاره القانوني الوطني أن البيانات الشخصية المطلوبة والمعالجة ذات صلة وليست مفرطة فيما يتعلق بـأغراض هذه المعالجة". يمكن تنفيذ هذا المطلب، على سبيل المثال، من خلال قواعد الإثبات والقيود على نطاق الأوامر الإجبارية، ومبادئ الضرورة والتناسب، ومبادئ المعقولية، والمبادئ التوجيهية والسياسات الداخلية التي تحد من جمع البيانات أو استخدامها. كما يتم تشجيع الأطراف على النظر، بموجب أطرها القانونية الوطنية، في الحالات التي تنطوي على أفراد مستضعفين، مثل الضحايا أو القصر على سبيل المثال.

الفقرة 3 - الجودة والسلامة

232. تقتضي الفقرة 3 من الأطراف "اتخاذ خطوات معقولة لضمان الحفاظ على البيانات الشخصية بهذه الدقة والاكتمال، وأن تكون محدثة بالقدر الضروري والمناسب للمعالجة القانونية للبيانات الشخصية، مع مراعاة الأغراض التي من أجلها يتم معالجتها". السياق مهم، بحيث يمكن تطبيق هذا المبدأ بشكل مختلف حسب الظروف. على سبيل المثال، سيُطبق المبدأ على القضايا الجنائية بشكل مختلف عن تطبيقه للأغراض الأخرى.

233. فيما يتعلق بالتحقيقات والقضايا الجنائية، لا ينبغي النظر إلى الفقرة 3 على أنها تتطلب من سلطات إنفاذ القانون الجنائي تعديل المعلومات - حتى لو كانت هذه المعلومات غير دقيقة أو غير كاملة - التي قد تشكل دليلاً في قضية جنائية، لأن عدم دقة البيانات قد يكون أمرا أساسياً للجريمة (على سبيل المثال في قضايا الاحتيال)، كما أنه من شأنه أن يقوض هدف الإنصاف للمتهمين عندما تقوم السلطات بتعديل دليل تم جمعه عبر هذا البروتوكول.

234. في كثير من الحالات، عندما تكون هناك شكوك حول موثوقية البيانات الشخصية، ينبغي الإشارة إلى ذلك بوضوح. على سبيل المثال، بالقدر الذي يتم فيه استخدام المعلومات أو الأدلة التي تم تلقيها عبر هذا البروتوكول لتتبع السلوك الإجرامي السابق، يجب أن توفر الإجراءات المعمول بها وسائل لتصحيح الأخطاء في المعلومات (مثل تعديل أو استكمال المعلومات الأصلية)، ولتحديث أو تعديل أو استكمال البيانات غير الموثوقة أو القديمة، من أجل تقليل مخاطر قيام السلطات باتخاذ إجراءات غير مناسبة وربما معاكسة لإنفاذ القانون على أساس جودة البيانات الرديئة (على سبيل المثال، القبض على الشخص الخطأ أو القبض على شخص اعتمادا على فهم خاطئ لسلوكه). يتم تشجيع الأطراف على اتخاذ

خطوات معقولة لضمان أنه في حالة اكتشاف أن البيانات المقدمة إلى سلطة أخرى أو المستلمة منها غير صحيحة أو قديمة، يتم إبلاغ السلطة الأخرى في أقرب وقت ممكن عمليًا من أجل إجراء التصحيحات بالقدر اللازم والمناسب نظرًا للأغراض من المعالجة.

الفقرة 4 - البيانات الحساسة

235. تتعلق الفقرة 4 بالتدابير التي يتعين على الأطراف اتخاذها بموجب هذا البروتوكول عند التعامل مع أنواع معينة من البيانات التي قد تكون مطلوبة، على وجه الخصوص، كدليل في تحقيق جنائي أو قضية جنائية، ولكن في نفس الوقت تكون ذات طبيعة تجعل من الضروري توفير ضمانات مناسبة للحماية من خطر التأثير الضار الذي غير مبرر على الفرد المعني من جراء استخدام هذه البيانات، ولا سيما من التمييز غير المشروع.

236. تنص الفقرة 4 على أن البيانات الحساسة تشمل "البيانات الشخصية التي تكشف عن الأصل العرقي أو الاثني؛ الآراء السياسية أو المعتقدات الدينية أو غيرها أو العضوية النقابية؛ البيانات الجينية، وبيانات القياسات الحيوية (البيومترية) التي تعتبر حساسة في ضوء المخاطر التي تنطوي عليها؛ أو البيانات الشخصية المتعلقة بالصحة أو الحياة الجنسية"، والتي قد تشمل كلاً من الميول الجنسية والممارسات الجنسية. قد تتضمن البيانات الصحية البيانات المتعلقة بالصحة الجسدية أو العقلية للشخص والتي تكشف عن معلومات حول حالته الصحية السابقة أو الحالية أو المستقبلية (على سبيل المثال، معلومات حول مرض أو إعاقة أو خطر المرض أو التاريخ الطبي للشخص أو علاجه أو الحالة البدنية أو الطبية الحيوية للشخص). قد تتضمن البيانات الجينية، على سبيل المثال، البيانات التي تنتج عن تحليل الكروموسومات أو الحمض النووي أو الحمض النووي الريبي وتتعلق بالخصائص الجينية الموروثة أو المكتسبة لشخص ما والتي تحتوي على معلومات فريدة حول طبيعته البدنية أو صحته أو نسبه.

237. يشمل مفهوم بيانات القياسات الحيوية (البيومترية) مجموعة من المعرفات الفريدة الناتجة عن الخصائص البدنية أو الفيزيولوجية القابلة للقياس المستخدمة لتحديد الهوية المزعومة لفرد ما أو التحقق منها (على سبيل المثال بصمات الأصابع أو أنماط قزحية العين أو الوريد الكفي أو الأنماط الصوتية أو الصور الفوتوغرافية أو لقطات الفيديو). كما تعتبر بعض الأطراف أن المعرفات الفريدة الناتجة عن الخصائص البيولوجية أو السلوكية تشكل بيانات بيومترية. في حين يمكن اعتبار أشكال معينة من البيانات البيومترية حساسة في ضوء المخاطر التي تنطوي عليها، إلا أن النماذج الأخرى قد لا تكون كذلك. على سبيل المثال، تعتبر بعض الأطراف البيانات البيومترية المحوسبة أو المستخرجة من عينة أو صورة بيومترية (مثل القوالب البيومترية) حساسة. وعلى العكس من ذلك، فإن بعض الصور الفوتوغرافية أو لقطات الفيديو، حتى لو كشفت عن سمات جسدية أو تشريحية مثل الندوب وعلامات الجلد والوشم ، لن يتم اعتبارها بشكل عام ضمن فئة البيانات البيومترية الحساسة. ولأن مستوى حساسية البيانات البيومترية قد يختلف، فإن الفقرة 4

توفر المرونة للأطراف لتنظيم هذا المجال من خلال الإشارة إلى أن البيانات الحساسة تشمل "بيانات بيومترية التي تعتبر حساسة في ضوء المخاطر التي تنطوي عليها". هذه العبارة تقر أن البيانات البيومترية هي مجال متطور وأن البيانات التي تعتبر "حساسة" بموجب هذه الفقرة سوف تحتاج إلى تقييم بمرور الوقت بالاقتران مع التطورات التكنولوجية والاستقصائية وغيرها والمخاطر التي يتعرض لها الفرد المعني. فيما يتعلق بالأطراف في اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية (سلسة المعاهدات الأوروبية رقم 108) المعدلة بالبروتوكول (سلسة معاهدات مجلس أوروبا رقم 223) ينبغي أن يسترشد تفسير ما يشكل بيانات بيومترية "حساسة" بالفقرة 1 من المادة 6 من تلك المعاهدة، على النحو المفصل في الفقرتين 58 و59 من تقريرها التفسيري.

238. تنطوي إساءة استخدام البيانات الحساسة ومعالجتها بشكل غير صحيح على مخاطر محتملة تتمثل في إلحاق ضرر غير مبرر بالأفراد، بما في ذلك مخاطر التمييز غير المشروع. ينبغي وضع نظام العدالة الجنائية للحماية من التأثير الضار غير المبرر والتمييز غير المشروع المستند إلى، على سبيل المثال، استخدام الأدلة التي تكشف عن العرق أو الدين أو الحياة الجنسية. كمثال آخر، تقر هذه الفقرة أيضًا أهمية الحماية من خطر الضرر الناجم عن الكشف غير المبرر أو غير المشروع، على سبيل المثال، الشخص الذي يتم نبذه بناءً على معلومات تكشف عن التوجه الجنسي أو الهوية الجنسية. وفي هذا الصدد، تتطلب الفقرة 4 من الأطراف توفير "ضمانات مناسبة" للوقاية من مثل هذه المخاطر.

239. ينبغي تقييم مدى ملاءمة الضمانات بالرجوع إلى حساسية البيانات ونطاق المعالجة وسياقها وأغراضها وطبيعتها (على سبيل المثال في حالة اتخاذ القرار الآلي)، فضلاً عن احتمال وشدة المخاطر. قد تختلف هذه الضمانات بين الأنظمة القانونية الوطنية وتعتمد على هذه العوامل. قد تتضمن القائمة غير الشاملة للضمانات تقييد المعالجة (على سبيل المثال السماح بالمعالجة فقط لأغراض معينة أو على أساس كل حالة على حدة)، وتقييد النشر، وتقييد الوصول (على سبيل المثال، تقييد الوصول إلى أفراد معينين فقط من خلال إجراءات الترخيص أو التحقق من الهوية، التي تتطلب تكوينا متخصصًا لهؤلاء الأفراد)، أو إجراءات أمنية تنظيمية أو تقنية إضافية (على سبيل المثال، الإخفاء أو التسمية المستعارة أو فصل تخزين البيانات البيومترية عن معلومات السيرة الذاتية المتصلة) أو فترات احتفاظ أقصر. في حالات معينة، قد يكون من المفيد إجراء تقييم الأثر للمساعدة في تحديد وإدارة المخاطر.

الفقرة 5 - فترات الاحتفاظ

240. تنص الجملة الأولى من الفقرة 5 على أنه "يجب على الطرف الآخر الاحتفاظ بالبيانات الشخصية فقط طالما كان ذلك ضروريًا ومناسبًا في ضوء أغراض معالجة البيانات عملاً بالفقرة 2". في هذا الصدد، ينص مبدأ تقييد الغرض الوارد في الفقرة 2 على أن الطرف الذي تلقى البيانات الشخصية يجب أن يقوم بمعالجتها لأغراض محددة وفقًا للمادة 2

ولن يقوم بمعالجتها مرة أخرى لغرض غير متوافق. تماشياً مع هذا المبدأ، ترتبط فترة الاحتفاظ بالبيانات بالغرض (أو الأغراض) المحددة التي تتم معالجة البيانات من أجلها.

241. لأنه بموجب المادة 2، فإن البيانات الشخصية التي يتلقاها الطرف بموجب هذا البروتوكول هي لغرض تحقيقات أو دعاوى جنائية محددة، يمكن الاحتفاظ بالبيانات الشخصية طالما كانت هناك حاجة (1) طوال مدة التحقيق والإجراءات اللاحقة، بما في ذلك أيّ استئناف أو فترات يمكن خلالها إعادة فتح القضية بموجب القانون الوطني؛ و(2) بعد تحقيق الغرض من الجمع الأصلي، لمزيد من المعالجة لغرض "لا يتعارض" مع الغرض الأصلي. على سبيل المثال، يجوز للطرف أن يوفر الاحتفاظ بالمعلومات أو الأدلة لأغراض الأرشفة أو البحث التاريخي، أو الأغراض الأخرى المتوافقة بما يتماشى مع المادة 14، الفقرة 2، كما هو موضح بمزيد من التفصيل في الفقرات ذات الصلة من هذا التقرير التفسيري.

242. تتيح الجملة الثانية من الفقرة 5 للأطراف خيارين للوفاء بالتزام الاحتفاظ بالبيانات الشخصية فقط طالما كان ذلك ضروريًا ومناسبًا في ضوء أغراض معالجة البيانات وفقًا للفقرة 2 من هذه المادة. أولاً، يجوز للطرف أن ينص على فترات احتفاظ محددة في إطاره القانوني الوطني. وكبديل لذلك، يمكن للأطراف أن تنص في إطارها القانوني الوطني على مراجعة الحاجة إلى مزيد من الاحتفاظ على فترات زمنية مقررة. تتمتع الأطراف بسلطة تقديرية لتقرير النهج الأفضل، في سياق إطارها القانوني الوطني، الذي يناسب مجموعة البيانات المحددة. يجوز للأطراف أيضًا دمج فترة احتفاظ محددة مع نظام للمراجعة الدورية على فترات أقصر. يجب عليهم التأكد في إطارهم القانوني من قيام السلطات المختصة بوضع قواعد و / أو إجراءات داخلية لتنفيذ فترات الاحتفاظ المحددة و / أو المراجعة الدورية للحاجة إلى مزيد من الاحتفاظ. إذا انتهت فترة الاحتفاظ أو إذا قرر الطرف من خلال المراجعة الدورية أنه لا توجد حاجة أخرى للاحتفاظ بالبيانات، فيجب حذفها أو جعلها مجهولة المصدر.

الفقرة 6 - القرارات الآلية

243. تتعلق الفقرة 6 بحماية الأفراد عندما تستند القرارات التي تنتج أثرا ضارا كبيرا فيما يتعلق بمصالحهم ذات الصلة فقط إلى المعالجة الآلية لبياناتهم الشخصية. ليس من المتوقع، عندما يتلقى طرف بيانات شخصية من طرف آخر بموجب هذا البروتوكول، أنه غالبًا ما يتم اتخاذ القرار الآلي لأن الأدلة أو المعلومات سيتم جمعها من قبل المحققين أو السلطات القضائية لأغراض تحقيق أو دعوى جنائية محددة. مع ذلك، إذا تم اتخاذ القرار الآلي، الذي ينتج عنه تأثير سلبي كبير فيما يتعلق بالمصالح ذات الصلة للفرد المعني بالبيانات الشخصية، في التحقيق الذي تم البحث عن البيانات الخاصة به، فيجب على السلطات اتباع هذا الحكم. يجب على السلطات أيضًا اتباع هذا الحكم إذا حدثت استخدامات لاحقة للبيانات لمنع أو اكتشاف أو التحقيق أو الملاحقة القضائية لجرائم أخرى (على سبيل المثال الاعتقال على أساس المعالجة الآلية البحتة للملفات الجنائية، أو إصدار الأحكام، أو الإفراج

بكفالة، أو الإفراج المشروط)، أو من أجل غرض متوافق (على سبيل المثال في سياق عمليات التحقق من الخلفية)، إذا كانت البيانات تخضع لأدوات تحليلية آلية لأغراض صنع القرار.

244. لذلك، تحظر الفقرة 6 اتخاذ قرار يستند فقط إلى المعالجة الآلية للبيانات الشخصية حيث ينتج عنه تأثير سلبي كبير فيما يتعلق بمصالح الفرد ذات الصلة، بما في ذلك الآثار القانونية السلبية (من خلال التأثير على الوضع القانوني للفرد أو حقوقه)، مثل إصدار مذكرة توقيف أو رفض الإفراج بكفالة أو الإفراج المشروط، ما لم يكن اتخاذ مثل هذا القرار مصرحًا به بموجب القانون الوطني ويخضع للضمانات المناسبة.

245. تعتبر الضمانات المناسبة ضرورية للحد من التأثير المحتمل على المصالح ذات الصلة للفرد المعني بالبيانات الشخصية. يجب أن تغطي هذه الضمانات إمكانية حصول الفرد المعني على تدخل بشري لتقييم القرار. يتم تشجيع الأطراف أيضًا على اتخاذ خطوات معقولة لتوفير جودة وتمثيل البيانات المستخدمة لتطوير الخوارزميات ودقة الاستنتاجات الإحصائية المستخدمة، مع مراعاة الظروف المحددة وسياق المعالجة، بما في ذلك سياق إنفاذ القانون الجنائي.

الفقرة 7 - أمن البيانات والحوادث الأمنية

246. عملاً بالفقرة 7 (أ)، "يضمن الطرف الآخر أن لديه تدابير تكنولوجية ومادية وتنظيمية مناسبة لحماية البيانات الشخصية". على سبيل المثال، قد تتضمن الإجراءات التكنولوجية حماية البرمجيات من البرامج الضارة للكمبيوتر وتشفير البيانات وجدران الحماية. قد تشمل التدابير المادية تخزين خوادم وملفات الكمبيوتر في مواقع آمنة وقد تشمل التدابير التنظيمية القواعد والممارسات والسياسات والإجراءات، بما في ذلك تلك التي تحد من حقوق الوصول.

247. تنص الفقرة 7 (أ) كذلك على أن التدابير يجب أن تحمي، على وجه الخصوص، من الضياع (على سبيل المثال، الإجراءات الموحدة لإيداع البيانات ومعالجتها)، والوصول العرضي أو غير المصرح به (على سبيل المثال، الحماية من عمليات اختراقات الكمبيوتر، أو متطلبات الترخيص أو التحقق من الهوية للوصول إلى الملفات الورقية أو ملفات الكمبيوتر)، والكشف العرضي أو غير المصرح به (على سبيل المثال، التدابير التكنولوجية لاكتشاف ومنع عمليات الكشف العرضية أو غير المصرح بها، والتدابير التنظيمية لتحديد العواقب المترتبة على عمليات الكشف هذه)، والتعديل أو الإتلاف العرضي أو غير المصرح به للبيانات (على سبيل المثال تقييد إدخال أو تغيير البيانات الإلكترونية أو الملفات الورقية للموظفين المرخص لهم، واستخدام أنظمة تسجيل الدخول، وعرض فترات الاحتفاظ، ووضع أنظمة نسخ احتياطي للملفات الورقية أو ملفات الكمبيوتر).

248. الطريقة الدقيقة للوفاء بهذه المتطلبات، بطريقة تتناسب مع الظروف المحددة، متروكة للطرف المعني. يتم تشجيع الأطراف، على سبيل المثال، على إعداد وتنفيذ تدابير أمنية

تأخذ في الاعتبار عوامل مثل طبيعة البيانات الشخصية (بما في ذلك حساسيتها) والمخاطر المحددة وأي عواقب سلبية محتملة على الفرد المعني في حالة وقوع حادث أمني. في الوقت نفسه، قد تأخذ الأطراف في الاعتبار الأسئلة المتعلقة بالموارد المستخدمة في إعداد وتنفيذ تدابير أمن البيانات. يتم تشجيع الأطراف على إخضاع هذه التدابير لمراجعة دورية وتحديثها عند الاقتضاء في ضوء تطور التكنولوجيا والطبيعة المتطورة للمخاطر.

249. تحدد الفقرة 7 (ب) المتطلبات في حالة وقوع "حادث أمني" (على النحو المحدد في الفقرة 7 (أ) والموصوف أعلاه) فيما يتعلق بالبيانات الشخصية الواردة بموجب هذا البروتوكول والتي تخلق "خطرًا كبيرًا من الضرر المادي أو غير المادي" للأفراد أو للطرف مصدر البيانات. قد يشمل الضرر ذي الصلة بالفرد، على سبيل المثال، الأذى الجسدي أو الإضرار بالسمعة، أو المعاناة النفسية (على سبيل المثال من خلال الإذلال أو انتهاك السرية)، أو التمييز أو الضرر المالي (على سبيل المثال فقدان الوظيفة أو الفرص المهنية، أو درجة الائتمان السلبية، أو سرقة الهوية أو احتمال الابتزاز). فيما يتعلق بالطرف الآخر، قد يشمل الضرر ذي الصلة على وجه الخصوص التأثير السلبي المحتمل على تحقيق مواز (على سبيل المثال، هروب المشتبه به، إتلاف الأدلة). إذا كان هناك "خطر كبير" لمثل هذا الضرر، فإن الطرف المتلقي ملزم "بالتقييم الفوري لاحتمالية وحجم الضرر" و "اتخاذ الإجراءات المناسبة على الفور لتخفيف هذا الضرر". قد تشمل العوامل المتعلقة باحتمالية وحجم الضرر الواجب النظر فيه، في جملة أمور، نوع الحادث، مثل، إذا كان معروفًا، ما إذا كان ضارًا؛ الأشخاص الذين لديهم أو يمكنهم الحصول على المعلومات؛ طبيعة وحساسية البيانات المتأثرة؛ حجم البيانات المحتمل تعرضها للخطر وعدد الأفراد المحتمل تأثرهم؛ سهولة التعرف على هوية الفرد (الأفراد) المعنيين؛ احتمال الوصول إلى البيانات واستخدامها، على سبيل المثال ما إذا كانت البيانات مشفرة أو جعل الوصول إليها غير ممكن؛ والعواقب المحتملة التي قد تحدث نتيجة للحادث.

250. وفقا للتدابير الموصوفة في الفقرة 7 (أ) ولضمان الاستجابة المناسبة بموجب الفقرة 7 (ب)، يتعين على الأطراف أن تكون لديها عمليات داخلية قائمة حتى تتمكن من اكتشاف الحوادث الأمنية. يجب أن يكون لديهم أيضًا عملية للتقييم الفوري لاحتمالية الضرر المحتمل وحجمه، ولاتخاذ التدابير المناسبة على الفور لتخفيف الضرر (على سبيل المثال عن طريق استدعاء أو طلب حذف المعلومات التي تم نقلها عن طريق الخطأ إلى متلقي غير مصرح له). قد يستفيد التطبيق الفعال لهذه المتطلبات من إجراءات الإبلاغ الداخلية ومن الاحتفاظ بسجلات لأي حادث أمني.

251. الفقرة 7 (ب) تحدد أيضا الظروف التي يجب أن يتم فيها إشعار الطرف الآخر والفرد (أو الأفراد) المتضررين بشأن الحادث، مع مراعاة الاستثناءات والقيود.

252. في حالة وقوع حادث أمني ينطوي على خطر كبير بإحداث ضرر مادي أو غير مادي للأفراد أو للطرف الآخر، يجب تقديم إشعار إلى سلطة النقل أو، لأغراض الفصل الثاني، القسم 2، إلى السلطة أو السلطات المعينة وفقًا للفقرة 7 (ج). ومع ذلك، قد يتضمن الإشعار قيودًا مناسبة فيما يتعلق بمواصلة إرسال الإشعار أو تأخيره أو إغفاله إذا كان هذا الإشعار قد يعرض الأمن القومي للخطر أو تأخيره إذا كان هذا الإشعار قد يعرض للخطر تدابير حماية السلامة العامة (بما في ذلك الحالات التي يعرَض فيها الإشعار التحقيق في الجرائم الجنائية الناشئة عن الحادث الأمني للخطر). وعند البت فيما إذا كان ينبغي تأخير الإشعار أو إغفاله في الظروف التي قد يعرَض فيها الإشعار الأمن القومي للخطر، ينبغي للطرف أن ينظر فيما إذا كان من المعقول في هذه الظروف حذف الإخطار أو ما إذا كان من الأنسب بدلاً من ذلك الإشعار المتأخر.

253. في حالة وقوع حادث أمني ينطوي على خطر كبير بإلحاق ضرر مادي أو غير مادي للأفراد، يجب إخطار الفرد (أو الأفراد) المتأثرين بالحادث، من أجل السماح لهم بحماية مصالحهم، على الرغم من أن هذا يخضع للاستثناءات. أولاً، تنص الفقرة 7 (ب) على أنه لا يلزم تقديم الإشعار إذا اتخذ الطرف التدابير المناسبة بحيث لا يعود هناك خطر كبير للضرر. على سبيل المثال، لن تكون هناك حاجة إلى أي إشعار حيث تم إرسال بريد إلكتروني يحتوي على معلومات شخصية حساسة بطريق الخطأ إلى المستلم الخطأ وكان من الممكن أن يؤدي إلى خطر كبير بحدوث ضرر دون اتخاذ تدابير للتخفيف ولكن تم حذفه بسرعة وبشكل دائم من قبل المستلم عند الطلب قبل مشاركته. ثانيًا، قد يتم تأخير الإشعار إلى الفرد أو حذفه وفقًا للشروط المنصوص عليها في الفقرة 12 (أ) (1) - أي أن الإشعار "قد يخضع لتطبيق القيود المتناسبة المسموح بها بموجب إطاره القانوني الوطني، اللازمة ... لحماية حقوق وحريات الغير أو أهداف مهمة للمصلحة العامة والتي تولي الاعتبار الواجب للمصالح المشروعة للفرد المعني".

254. بشكل عام، تُشجع الأطراف على أن تُدرج في الإشعار بموجب الفقرة 7 (ب)، عند الاقتضاء، معلومات عن نوع الحادث الأمني ونوع وحجم المعلومات التي قد تكون تعرضت للخطر والمخاطر المحتملة والتدابير المتوخاة من أجل لتقليل الضرر المحتمل، بما في ذلك تدابير احتواء الحادث. نظرًا لوظيفتهم الإشرافية، وبغية الاستفادة من مشورة الخبراء بشأن التعامل مع الحادث، فقد يكون من المناسب أيضًا للطرف الذي يقوم بالإشعار إبلاغ سلطات الرقابة الموصوفة في الفقرة 14 بالحادث وأي تدابير مخففة.

255. من أجل السماح باستجابة منسقة ولدعم جهود التخفيف من المخاطر الخاصة به، يجوز للطرف الذي يقوم بالإشعار أن يطلب التشاور والمعلومات الإضافية المتعلقة بالحادث وعملية الاستجابة من الطرف الذي يقوم بالإشعار.

256. تنص الفقرة 7 (ج) على الإجراءات المطلوبة للأطراف لتعيين السلطة أو السلطات التي يتعين إشعارها بموجب الفقرة 7(ب) لأغراض الفصل الثاني، القسم 2.

الفقرة 8 - الاحتفاظ بالسجلات

257. تتطلب الفقرة 8 من الأطراف "الاحتفاظ بسجلات أو أن يكون لديها وسائل مناسبة أخرى لإثبات كيفية الوصول إلى البيانات الشخصية للفرد واستخدامها والكشف عنها في قضية معينة". الهدف هو أن يكون لدى كل طرف وسائل فعالة لتوضيح كيفية الوصول إلى بيانات فرد معين واستخدامها والكشف عنها في قضية معينة، وفقًا لهذه المادة. يُعد إثبات الامتثال أمرًا مهمًا بشكل خاص لأغراض الرقابة وبالتالي يساهم في المساءلة. بينما تُترك الوسائل الدقيقة لإثبات كيفية معالجة البيانات لكل طرف للتنفيذ، تُشجع الأطراف على تكييف أساليبها مع الظروف، مع مراعاة المخاطر التي يتعرض لها الأفراد المعنيون وطبيعة ونطاق وأغراض وسياق المعالجة.

258. على سبيل المثال، قد تقرر بعض الأطراف استخدام التسجيل الآلي للأنشطة (تسجيل الدخول) أو بدائل أخرى (مثل السجلات المكتوبة بخط اليد في حالة الملفات الورقية). كما هو مذكور أعلاه، الهدف هو تسهيل المساءلة مع السماح بدرجة من المرونة من حيث كيفية قيام الطرف بذلك، بما يتفق مع الالتزامات الأخرى السارية بموجب المادة 14. على سبيل المثال، يجب على الأطراف الاحتفاظ بسجلات أو وثائق أخرى بشأن الوصول أو الاستخدام أو الكشف بطريقة تسهل عمل جهات الرقابة.

الفقرة 9 - المشاركة اللاحقة داخل أحد الأطراف

259. تنص الفقرة 9 على أنه "عندما تقدم سلطة تابعة لأحد الأطراف البيانات الشخصية التي تتلقاها في البداية بموجب هذا البروتوكول إلى سلطة أخرى تابعة لذلك الطرف، يجب على السلطة الأخرى معالجتها وفقًا لهذه المادة، مع مراعاة الفقرة 9 (ب)". بعبارة أخرى، عندما يتم تقديم البيانات الشخصية التي يتم تلقيها بموجب هذا البروتوكول لاحقًا إلى سلطة أخرى تابعة للطرف نفسه - بما في ذلك إلى سلطة تابعة لدولة مكونة أو كيان إقليمي آخر مماثل - يجب معالجة هذه البيانات وفقًا لهذه المادة ما لم ينطبق الاستثناء الوارد في الفقرة 9 (ب). تنطبق الفقرة 9 أيضًا في حالة تعدد حالات المشاركة اللاحقة.

260. الفقرة 9 (ب) تنص على استثناء للفقرة 9 (أ) عندما يبدي طرف يمثل دولة اتحادية تحفظا على التزامات هذا البروتوكول بموجب المادة 17، وفقا للشروط المنصوص عليها فيه. تماشيا مع الفقرة 297 من هذا التقرير التفسيري، يستوعب هذا الاستثناء "الصعوبات التي قد تواجهها الدول الفيدرالية نتيجة لتوزيعها المميز للسلطات بين السلطات المركزية والإقليمية". انظر أيضاً الفقرة 316 من التقرير التفسيري للاتفاقية. لذلك، تنص الفقرة 9 (ب) على أنه في حالة إبداء أحد الأطراف تحفظًا بموجب المادة 17، فإنه لا يزال بإمكانه تقديم البيانات الشخصية

التي تلقاها في البداية بموجب هذا البروتوكول إلى الدول المكونة له أو الكيانات الإقليمية الأخرى المماثلة شرط أن يكون لدى الطرف تدابير من أجل أن تواصل السلطات المتلقية حماية البيانات بشكل فعال من خلال توفير مستوى من الحماية للبيانات يمكن مقارنته مع تلك التي توفرها هذه المادة. فشل أحد الأطراف في وضع "تدابير من أجل استمرار السلطات المتلقية في حماية البيانات بشكل فعال من خلال توفير مستوى من الحماية للبيانات يمكن مقارنته مع تلك التي توفرها هذه المادة"، قد يعتمد على خطورة وأسباب وظروف الإخفاق في تلبية هذا المطلب يشكل خرقًا ماديًا أو منهجيًا بموجب الفقرة 15 من المادة 14.

261. تنص الفقرة 9 (ج) أنه في حالة وجود مؤشرات على التنفيذ غير السليم لهذه الفقرة من قبل طرف آخر، يجوز للطرف الناقل أن يطلب التشاور مع ذلك الطرف الآخر والمعلومات ذات الصلة حول تلك المؤشرات بهدف توضيح الوضعية.

الفقرة 10 - النقل اللاحق إلى دولة أخرى أو منظمة دولية أخرى

262. عملاً بالفقرة 10 (أ)، يجوز للطرف نقل البيانات الشخصية الواردة بموجب البروتوكول "إلى دولة أخرى أو منظمة دولية أخرى فقط بإذن مسبق من سلطة النقل أو، لأغراض الفصل الثاني، القسم 2، السلطة أو السلطات المحددة في الفقرة 10 (ب)". هذا النوع من التدابير الوقائية هو شرط شائع لعمليات النقل لمساعدة الشركاء الأجانب في سياق إنفاذ القانون الجنائي (على سبيل المثال وفقًا لمعاهدات المساعدة المتبادلة أو التعاون بين الشرطة)، ويتم نقل هذا النهج إلى هذه الفقرة أيضًا كوسيلة لحماية البيانات الشخصية المنقولة بموجب هذا البروتوكول.

263. تنص الفقرة 10 (ب) على أنه يجب على كل طرف، أثناء التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة، إبلاغ الأمين العام لمجلس أوروبا بالسلطة أو السلطات المعينة لتقديم الإذن بموجب الفقرة 10 (أ) لأغراض عمليات النقل بموجب الفصل الثاني، القسم 2، والتي يمكن تعديلها لاحقًا.

264. قد يستلزم الحصول على إذن بنقل لاحق طلبًا فرديًا يتم إرساله من سلطات الطرف المتلقي إلى سلطات الطرف الناقل للحصول على إذن بنقل بيانات شخصية محددة على وجه التحديد إلى بلد ثالث أو منظمة دولية معينة. مع ذلك، لا تمنع الفقرة 10 (أ) الأطراف من تحديد قواعد لعمليات النقل اللاحقة مقدمًا (على سبيل المثال من خلال اتفاق مكتوب أو ترتيبات أخرى). لا تخل الفقرة 10 (أ) أيضًا بقدرة أي طرف على وضع شروط أخرى على استخدام الطرف المتلقي للبيانات (على سبيل المثال، وضع قيود على المدى الذي يمكن للطرف المتلقي أن يستخدم أو ينشر فيه البيانات الشخصية من أجل تجنب المساس بالتحقيق مع الطرف الناقل) وفقًا للأحكام المحددة في الفصل الثاني.

265. عند تحديد ما إذا كانت ستمنح الإذن بالنقل بموجب الفقرة 10، تُشجع السلطة الناقلة أو المعينة على أن تأخذ في الاعتبار على النحو الواجب جميع العوامل ذات

الصلة، بما في ذلك خطورة الجريمة الجنائية، والغرض الذي من أجله نُقلت البيانات في الأصل، وأي الشروط المطبقة المتعلقة بالنقل الأصلي وما إذا كانت الدولة الثالثة أو المنظمة الدولية تضمن مستوى مناسبًا من حماية البيانات الشخصية.

الفقرة 11 - الشفافية والإشعار

266. تفرض الفقرة 11 (أ) بعض متطلبات الشفافية والإشعار على الأطراف فيما يتعلق بالبنود المحددة في الفقرات من 11 (أ) (i) إلى (v). تساعد متطلبات الشفافية والإشعار الأفراد على فهم كيفية معالجة الأطراف لبياناتهم. كما تُعلم هذه المتطلبات الأفراد بشأن الوصول والتصحيح وسبل الانتصاف المتاحة.

267. يتمتع كل طرف بالمرونة فيما يتعلق بما إذا كان يتم تقديم هذا الإشعار والشفافية من خلال نشر الإشعارات العامة للجمهور - على سبيل المثال على موقع الكتروني حكومي - أو عبر إشعار شخصي للفرد الذي تلقى الطرف بياناته الشخصية. يجب أن يكون الإشعار متاحًا دون صعوبة ويمكن فهمه بسهولة. سواء تم تقديم إشعار عام أو شخصي، يجب إدراج المعلومات التالية: (i) الأساس القانوني للمعالجة والغرض (الأغراض) من المعالجة، بما في ذلك أغراض عمليات الكشف المتوقعة أو المعتادة؛ (ii) فترات الاحتفاظ أو المراجعة عملاً بالفقرة 5 من هذه المادة، حسب الاقتضاء؛ (iii) المتلقين أو فئات المتلقين الذين يتم الكشف عن البيانات لهم؛ (iv) النفاذ والتصحيح وسبل الانتصاف القضائية وغير القضائية المتاحة.

268. بموجب الفقرة 11 (ب)، عندما يتم تقديم إشعار شخصي إلى الفرد الذي تلقى الطرف بياناته، فإن شرط الإشعار والشفافية الوارد في الفقرة 11 (أ) قد يخضع لقيود معقولة وفقًا للشروط المنصوص عليها في الفقرة 12 (أ) (i) لهذه المادة. على سبيل المثال، في سياق مسائل العدالة الجنائية قد تكون هناك ظروف مشروعة قد يتأخر فيها تقديم الإشعار أو يتم إغفاله. هذه الظروف مُشار إليها في الفقرة 12 (أ) (i) ومبينة في الفقرة 272 من هذا التقرير التفسيري. قد تنشأ حالات أيضًا حيث قد تكون فيها كمية التفاصيل الواردة في الإشعار العام محدودة، تبعا لحساسية المعلومات.

269. تنص الفقرة 11 (ج) على أساس للأطراف لتحقيق التوازن بين الاهتمام بالشفافية والحاجة إلى السرية في مسائل العدالة الجنائية. تنص على أنه عندما يتطلب الإطار القانوني الوطني للطرف الناقل إشعارًا شخصيًا للفرد الذي تم تقديم بياناته إلى طرف آخر بموجب هذا البروتوكول، يجب على الطرف الناقل اتخاذ تدابير بحيث يتم إبلاغ الطرف المتلقي أثناء النقل فيما يتعلق بذلك الشرط ومعلومات الاتصال المناسبة. لا يجوز للطرف الناقل إرسال إشعار إلى الفرد إذا طلب الطرف المتلقي، حيثما تنطبق شروط القيود على النحو المنصوص عليه في الفقرة 12 (أ) (i)، إبقاء إتاحة البيانات سريا، بمجرد عدم تطبيق هذه الشروط الخاصة بالقيود وإمكانية تقديم الإشعار الشخصي، يجب على الطرف المتلقي

اتخاذ تدابير لإبلاغ الطرف الناقل بأنه قد يتم إرسال الإشعار. قد يشمل ذلك مراجعة دورية للحاجة إلى مثل هذه القيود. إذا لم يتم إبلاغه بعد، يحق للطرف الناقل تقديم طلبات إلى الطرف المتلقي الذي سيبلغ الطرف الناقل بما إذا كان سيبقي على القيود أم لا.

الفقرة 12 - النفاذ والتصحيح

270. تقتضي الفقرة 12 (أ) من كل طرف أن يضمن أن أي فرد تم تلقي بياناته الشخصية بموجب هذا البروتوكول له الحق في طلب الحصول على هذه البيانات (خاضعة لقيود محتملة) والنفاذ إليها، وفقًا للإجراءات المحددة في إطاره القانوني الوطني ودون تأخير غير مبرر، وفي حالة عدم دقة هذه البيانات أو معالجتها بشكل غير صحيح، القيام بتصحيحها. تمنح عبارة "وفقًا للإجراءات المحددة في إطاره القانوني الوطني" للأطراف المرونة فيما يتعلق بطريقة كيفية البحث عن سبل النفاذ والتصحيح والحصول عليه، ويقصد بها الإشارة إلى الإجراءات الموضوعة، على سبيل المثال، القوانين والأنظمة والقواعد سارية المفعول (مثل القواعد القضائية) والسياسات، وكذلك قواعد الإثبات المنطبقة. في بعض الأنظمة القانونية، سيحتاج الفرد إلى متابعة الوصول والتصحيح إداريًا قبل التماس سبل الانتصاف القضائية.

271. تنص الفقرة 12 (أ) (i) على أنه في حالة طلب النفاذ، يحق للفرد الحصول على نسخة خطية أو إلكترونية من الوثائق التي تحتوي على البيانات الشخصية للفرد والمعلومات المتاحة التي تشير إلى الأساس القانوني والغرض (أو الأغراض) من المعالجة والاحتفاظ والمتلقين أو فئات المتلقين من البيانات ("النفاذ")، بالإضافة إلى المعلومات المتعلقة بالخيارات المتاحة للانتصاف وفقًا للفقرة 13. وقد يسمح هذا أيضًا للفرد بتأكيد أن بياناته الشخصية تم استلامها بموجب هذا البروتوكول أم لا، وأنه قد تمت معالجتها أو أنها قيد المعالجة. إن توفير الوثائق التي تحتوي على المعلومات المتاحة التي تشير إلى الأساس القانوني والغرض (الأغراض) من المعالجة سيساعد الفرد في تقييم ما إذا كانت البيانات الشخصية تتم معالجتها وفقًا للقانون ساري المفعول. قد توفر العديد من الأطراف بالفعل إطارًا لهذا الوصول من خلال خصوصيتها أو حرية المعلومات أو النفاذ إلى قوانين السجلات الحكومية.

272. قد تخضع القدرة على الحصول على مثل هذا النفاذ في قضية معينة لقيود متناسبة مسموح بها بموجب الإطار القانوني الوطني للطرف، "اللازمة، أثناء الحكم، لحماية حقوق الغير وحرياتهم أو أهداف مهمة للمصلحة العامة والتي تولي الاعتبار الواجب للمصالح المشروعة للفرد المعني". قد تشمل حقوق وحريات الغير، على سبيل المثال، خصوصية الأفراد الآخرين الذين سيتم الكشف عن بياناتهم الشخصية في حالة منح النفاذ. قد تشمل الأهداف المهمة للمصلحة العامة، على سبيل المثال، حماية الأمن القومي والسلامة العامة (على سبيل المثال المعلومات المتعلقة بالتهديدات الإرهابية المحتملة أو المخاطر الجسيمة التي يتعرض لها موظفو إنفاذ القانون)؛ منع الجرائم الجنائية أو كشفها أو التحقيق فيها

أو مقاضاة مرتكبيها؛ وتجنب المساس بالتحريات الرسمية والتحقيقات والقضايا. وبطريقة مماثلة لوصف التناسب الوارد في الفقرة 146 من التقرير التفسيري للاتفاقية، من المتوقع أن ينفذ كل طرف "القيود المتناسبة" في هذا السياق وفقاً للمبادئ ذات الصلة لإطاره القانوني الوطني. بالنسبة للأطراف في اتفاقية حماية حقوق الإنسان والحريات الأساسية (سلسلة المعاهدات الأوروبية رقم 5) أو بروتوكول سلسلة معاهدات مجلس أوروبا رقم 223 المعدل لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية، سيُستمد التناسب من متطلبات تلك الاتفاقيات. ستطبق الأطراف الأخرى المبادئ ذات الصلة في إطارها القانوني الوطني والتي تحد بشكل معقول من القدرة على الوصول لحماية المصالح المشروعة الأخرى. كما ذكر أعلاه، يجب أن تحمي القيود المتناسبة حقوق وحريات الغير أو تحمي الأهداف الهامة للمصلحة العامة وتولي الاعتبار الواجب "للمصالح المشروعة للفرد المعني". اعتبر فريق الصياغة أن عبارة "المصالح المشروعة للفرد المعني" تشمل حقوق الفرد وحرياته. في حالة الاحتجاج بأسباب القيود هذه، يتم تشجيع السلطة المطلوبة على توثيق مثل هذا القرار لأغراض الفقرة 14. يجب على الأطراف أيضًا النظر فيما إذا كان يمكن منح حق النفاذ الجزئي عندما تكون أسباب أي تقييد (على سبيل المثال لحماية السرية أو المعلومات التجارية السرية) تنطبق فقط على أجزاء معينة من المعلومات.

273. عندما تسمح أحكام أخرى من هذه المادة بفرض قيود بموجب الشروط المنصوص عليها في الفقرة 12 (أ) (i)، فإن المقصود بعبارة "أثناء الحكم"، أن تشير، في حالة الفقرة 7، إلى وقت الإشعار بحادث أمني؛ في حالة الفقرة 11 (ب)، إلى وقت تقديم الإشعار الشخصي؛ وفي حالة المادة 11 (ج)، إلى الوقت الذي يطلب فيه أحد الأطراف السرية.

274. وفقاً للفقرة 12 (أ) (ii)، يضمن كل طرف أن أي فرد تم تلقي بياناته بموجب هذا البروتوكول، يحق له أن طلب التصحيح والحصول عليه، وفقاً للإجراءات المحددة في إطاره القانوني الوطني ودون تأخير غير مبرر، عندما تكون البيانات الشخصية للفرد غير دقيقة أو تمت معالجتها بشكل غير صحيح. يجب أن يشمل التصحيح - حسب الاقتضاء وبشكل معقول بالنظر إلى أسباب التصحيح والسياق الخاص للمعالجة - التصحيح أو التكميل (على سبيل المثال من خلال الإبلاغ أو عن طريق توفير معلومات إضافية أو تصحيحية) أو الحذف أو إخفاء الهوية أو تقييد المعالجة أو الحجب. في هذا الصدد، اعتبر فريق الصياغة أن الحذف أو إخفاء الهوية هو الإجراء المناسب والمعقول إذا تمت معالجة البيانات بشكل ينتهك الفقرة 5. وفي حالة انتهاك الفقرة 2، قد يكون من المناسب للطرف تقييد المعالجة؛ ومع ذلك، فإن هذا سيعتمد في النهاية على السياق المحدد (على سبيل المثال، الحاجة إلى الاحتفاظ بالبيانات الشخصية لغرض الإثبات). عندما تصبح البيانات مجهولة المصدر، يجب على الأطراف النظر في مخاطر إعادة تحديد الهوية غير المصرح بها وتنفيذ التدابير المناسبة لتقليل هذا الخطر. تُشجع الأطراف، عندما يكون ذلك ممكناً، على إشعار الطرف مصدر البيانات والكيانات الأخرى التي تمت مشاركة البيانات معها بأي إجراءات تصحيحية تم اتخاذها.

275. وفقًا للفقرة 12 (ب)، إذا تم رفض النفاذ أو التصحيح أو تقييدهما بموجب الفقرة 12 (أ)، يجب على الطرف أن يقدم للفرد، في شكل مكتوب والذي يمكن تقديمه إلكترونيًا، دون تأخير غير مبرر، ردًا لإبلاغ ذلك الفرد بما يلي: الرفض أو التقييد. في حين أن السلطة يجب أن تقدم أسباب هذا الرفض أو التقييد، قد يكون الاتصال عامًا (أي، دون تأكيد أو نفي وجود أي سجل ذي صلة) عند الضرورة من أجل عدم تقويض هدف ما بموجب الفقرة 12 (أ) (i). ومع ذلك، يجب على الأطراف التأكد من أن الاتصال يتضمن معلومات حول الخيارات المتاحة للانتصاف.

276. يجوز للأطراف فرض رسوم للحصول على حق النفاذ (على سبيل المثال التكلفة الإدارية لتجميع وفحص الوثائق التي تم طلب الحصول عليها). ومع ذلك، من أجل منع أو تثبيط النفاذ، يجب أن تقتصر أي رسوم على ما هو معقول وليس مفرط بالنظر إلى الموارد المعنية. من أجل تسهيل ممارسة الحقوق المنصوص عليها في الفقرة 12 (أ)، تُشجع الأطراف على السماح للأفراد بطلب ممثل للمساعدة في طلب الحصول على التدابير الموضحة في هذه الفقرة والحصول عليها، أو تقديم طلب و / أو شكوى نيابة عنه. في هذه الظروف، يكون الإشعار عملاً بالفقرة 11 (أ) وكذلك المعلومات التي تم الحصول عليها استجابة لطلب النفاذ عملاً بالفقرة 12 (أ) (i) قد يشير إلى هذا الاحتمال. مع ذلك، يجب أن يكون هذا التمثيل متوافقًا مع المتطلبات القانونية الوطنية سارية المفعول للطرف الذي يتم فيه طلب مثل هذه التدابير، أو يتم تقديم الطلب و / أو الشكوى فيه على النحو الموضح أعلاه، بما في ذلك القواعد التي تحكم الشروط التي بموجبها يجوز للأشخاص أو الكيانات تمثيل مصالح قانونية للغير (على سبيل المثال، في بعض النظم القانونية الوطنية، القواعد التي تحكم التوكيل الرسمي).

الفقرة 13- سبل الانتصاف القضائية وغير القضائية

277. تنص الفقرة 13 على أنه "يجب أن يكون لدى الطرف الآخر سبل انتصاف قضائية وغير قضائية فعالة لتوفير الانتصاف لانتهاكات هذه المادة". يُترك لكل طرف تحديد نوع سبل الانتصاف الخاصة بانتهاكات أحكام هذه المادة، وليس من الضروري أن يكون كل نوع من سبل الانتصاف متاحًا لكل انتهاك لهذه المادة. يجب أن تكون سبل الانتصاف المنصوص عليها فعالة في التصدي لانتهاكات هذه المادة. يجوز للأطراف إدراج التعويض كسبيل انتصاف، عند الاقتضاء، عن الضرر المادي أو غير المادي الذي أثبت المدعي أنه نتج عن الانتهاك.

الفقرة 14 – الرقابة

278. تقتضي الفقرة 14 أن يكون لدى الأطراف "سلطة عامة واحدة أو أكثر، تمارس بمفردها أو بشكل مجتمع، وظائف وصلاحيات رقابة مستقلة وفعالة فيما يتعلق بالتدابير المنصوص عليها في هذه المادة". يترك الحكم للأطراف المرونة في كيفية تنفيذ هذا المطلب. قد تنشئ بعض الأطراف سلطات متخصصة لحماية البيانات، بينما قد يختار البعض الآخر

ممارسة الرقابة بشكل مجتمع من خلال أكثر من سلطة واحدة، قد تتداخل وظائفها. وهذا يعكس الاختلافات في الهياكل الدستورية والتنظيمية والإدارية للأطراف. وفي بعض الأطراف، قد تقع سلطات الرقابة هذه ضمن المكونات الحكومية التي تشرف على أنشطتها، وقد تكون ميزانياتها جزءًا من الميزانية الإجمالية للمكون. في مثل هذه الحالة، يجب أن تتمتع هذه السلطات بالاستقلالية للاضطلاع بمسؤولياتها الرقابية بفعالية.

279. اعتبر فريق الصياغة أن عددا من العناصر تساهم في وظائف وسلطات الرقابة المستقلة والفعالة. يجب على السلطات أداء مهامها وممارسة صلاحياتها بحيادية؛ ينبغي أن تتمتع بالقدرة على التصرف بمنأى عن التأثير الخارجي الذي قد يتعارض مع الممارسة المستقلة لسلطاتها ووظائفها؛ على وجه الخصوص، يجب ألا تخضع هذه السلطات للتعليمات، في حالة معينة، فيما يتعلق بممارسة صلاحياتها في التحقيق و / أو اتخاذ الإجراءات التصحيحية؛ وأخيراً، من المهم أن تمتلك السلطات المهارات والمعرفة والخبرة اللازمة لأداء واجباتها، وأن تتلقى الموارد المالية والتقنية والبشرية المناسبة لأداء وظائفها بفعالية.

280. يجب أن تشمل وظائف وصلاحيات هذه السلطات "سلطات التحقيق، وسلطة التصرف بناء على الشكاوى والقدرة على اتخاذ إجراءات تصحيحية". اعتبر فريق الصياغة أن صلاحيات التحقيق يجب أن تتضمن سلطة الحصول على المعلومات اللازمة لأداء مهامها، بما في ذلك، وفقًا للشروط المناسبة، الوصول إلى السجلات المحفوظة وفقًا للفقرة 8. قد تشمل الإجراءات التصحيحية إصدار تحذيرات بشأن عدم الامتثال أو التوجيهات حول كيفية جعل عمليات معالجة البيانات متوافقة (على سبيل المثال من خلال المطالبة بتنفيذ تدابير أمنية إضافية للحد من الوصول إلى البيانات أو تصحيح البيانات الشخصية)، أو طلب التعليق (المؤقت) لعمليات معالجة معينة أو إحالة الأمر إلى سلطات أخرى (على سبيل المثال المفتشون العامون أو المدعون العامون أو قضاة التحقيق أو الهيئات التشريعية). يمكن اتخاذ مثل هذا الإجراء التصحيحي بمبادرة خاصة من السلطات أو بناءً على شكاوى يقدمها الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية.

281. يتم تشجيع الأطراف على تعزيز التعاون بين سلطات الرقابة الخاصة بها. يجوز إجراء المشاورات بين سلطات الطرفين عند قيامهم بوظائفهم الرقابية بموجب هذه المادة حسب الاقتضاء. قد يشمل ذلك تبادل المعلومات والممارسات الفضلى.

الفقرة 15 - التشاور والتعليق

282. تنص الفقرة 15 أنه يجوز للطرف، بموجب المادة 14، تعليق نقل البيانات الشخصية بموجب هذا البروتوكول إلى طرف آخر عندما تعمل الأطراف بموجب الفقرة 1 (أ) من المادة 14. توضح الفقرة 15 أنه في ضوء الأغراض الهامة لإنفاذ هذا البروتوكول، يجب أن تحدث مثل هذه التعليقات فقط في ظل شروط صارمة ووفقًا للإجراءات المحددة الموضحة فيه. الغرض من

أحكام حماية البيانات الواردة في هذه المادة هو توفير الضمانات المناسبة لحماية البيانات الشخصية، بما في ذلك في حالة المشاركة اللاحقة داخل أحد الأطراف وعمليات النقل اللاحقة. اعتبر فريق الصياغة أن ضمانات هذه المادة وتنفيذها الفعال ضروريان، وبالتالي اعتبر أنه من المهم النص على تعليق عمليات نقل البيانات الشخصية في حالات معينة. لذلك، يجوز لأي طرف تعليق نقل البيانات الشخصية بموجب هذا البروتوكول إلى طرف آخر إذا كان لديه دليل قوي على حدوث خرق منهجي أو مادي لشروط هذه المادة، أو أن هناك انتهاكًا ماديًا وشيكًا. في حين أن شرط "الدليل الملموس" لا يلزم الطرف بإثبات وجود خرق منهجي أو مادي بما لا يدع مجالاً للشك، فإنه لا يجوز له تعليق عمليات النقل بناءً على مجرد شك أو تخمين. وبدلاً من ذلك، يجب أن يحظى قرار الطرف بدعم هام بأدلة واقعية موثوقة. "الانتهاك المادي" يعني انتهاكًا جسيمًا لالتزام مادي بموجب هذه المادة. قد يشمل ذلك عدم توفير الضمانات المطلوبة لهذه المادة في الإطار القانوني الوطني للطرف. أدرك فريق الصياغة أن التعليق متاح أيضًا على أساس الانتهاكات المنهجية - على سبيل المثال الانتهاكات المتكررة لضمانات هذه المادة. أدرك فريق الصياغة أيضًا أن الفشل في تطبيق بعض الضمانات فيما يتعلق بمعالجة البيانات الشخصية في حالة فردية، في حالة عدم وجود انتهاك مادي، لن يوفر أساسًا كافيًا للتذرع بهذا الحكم، حيث يجب أن يكون الفرد المعني قادرًا للتصدي لهذه الانتهاكات من خلال سبل الانتصاف غير القضائية والقضائية الفعالة وفقا للفقرة 13 من المادة 14.

283. تنص الفقرة 15 كذلك على أنه "لا يجوز للطرف أن يعلق عمليات النقل دون إشعار معقول، ولا حتى بعد أن تكون الأطراف المعنية قد شرعت في فترة تشاور معقولة دون التوصل إلى حل". يقر شرط التشاور هذا بأن تعليق عمليات النقل المهمة لإنفاذ القانون يجب ألا يتم إلا بعد تزويد الطرف الآخر بفرصة معقولة لتوضيح الوضع أو معالجة الشواغل المذكورة. في بداية هذه المشاورات، يجوز للطرف الذي يحتج بالفقرة 15 أن يطلب من الطرف الآخر تقديم المعلومات ذات الصلة. مع ذلك، وكما تم الإقرار به في الفقرة 15، يجب أن يكون لدى الطرف الذي يحتج بهذه الفقرة دليل قوي مسبقًا على وجود انتهاك مادي أو منهجي أو انتهاك مادي وشيك؛ لذلك، لا ينبغي استخدام آلية التشاور من أجل جمع مزيد من الأدلة عند الاشتباه في الانتهاك فقط. لا يجوز تعليق عمليات نقل البيانات بموجب هذا البروتوكول إلا بعد إشعار معقول وفترة تشاور معقولة دون التوصل إلى حل. ومع ذلك، يجوز لأي طرف تعليق عمليات النقل مؤقتًا في حالة حدوث انتهاك منهجي أو مادي يشكل خطرًا كبيرًا ووشيكًا على حياة شخص طبيعي أو سلامته، أو خطر كبير ووشيك بإلحاق ضرر كبير بسمعته أو ماله. وهذا يشمل وجود خطر كبير ووشيك بحدوث أذى جسدي أو بصحة شخص طبيعي. في هذه الحالات، يجب على الطرف أن يقوم بإشعار الطرف الآخر ويبدأ المشاورات مع الطرف الآخر فور تعليق عمليات النقل مؤقتًا. واعتبر فريق الصياغة أن التعليق المؤقت يجب أن يقتصر بشكل عام على عمليات النقل المرتبطة مباشرة بالضرورة التي تبرر التعليق المؤقت.

284. إذا استوفى الطرف الذي قام بالتعليق الشروط المنصوص عليها في الفقرة 15، فيجوز له تعليق عمليات النقل ولا يجوز للطرف الآخر الرد بالمثل. مع ذلك، إذا كان لدى الطرف الآخر دليل قوي على أن التعليق من قبل الطرف الذي قام بالتعليق كان مخالفًا لأحكام الفقرة 15، فيجوز له بشكل متبادل تعليق عمليات نقل البيانات إلى الطرف الذي قام بالتعليق. في هذا السياق، فإن مصطلح "دليل ملموس" له نفس المعنى كما هو الحال بالنسبة للتعليق الأولي من قبل الطرف الذي قام بالتعليق. سيكون التعليق من قبل الطرف الذي قام بالتعليق مخالفاً لأحكام الفقرة 15، على سبيل المثال، إذا لم يكن لدى الطرف الذي قام بالتعليق "أدلة ملموسة"، أو أن الانتهاك لم يكن "منهجياً" ولا "جوهرياً" أو فشل الطرف الذي قام بالتعليق في تلبية المتطلبات الإجرائية للتعليق، ولا سيما تلك المتعلقة بالمشاورات.

285. أخيرًا، تنص الفقرة 15 على أن "الطرف الذي قام بالتعليق يجب أن يرفع التعليق بمجرد تصحيح الانتهاك الذي يبرر التعليق" وأن "أيّ تعليق متبادل يجب أن يرفع في ذلك الوقت". تنطبق قاعدة مماثلة لتلك المطبقة في المادة 24، الفقرة 4، في سياق التعليق بموجب هذه الفقرة. وهذا يعني أن الفقرة 15 تنص على أنه "يجب الاستمرار في التعامل مع البيانات الشخصية المنقولة قبل التعليق وفقًا لهذا البروتوكول".

286. تُشجع الأطراف على الإعلان أو إشعار مقدمي الخدمات والكيانات التي قد يتم توجيه الطلبات أو الأوامر إليها بموجب الفصل الثاني، القسم 2، بأي تعليق أو تعليق مؤقت بموجب هذه الفقرة. يمكن أن يكون هذا الاتصال مهمًا من أجل التعليق الفعال لنقل البيانات الشخصية إلى طرف يكون في حالة انتهاك مادي أو منهجي للمادة 14 ولكن أيضًا لضمان أن مقدمي الخدمات والكيانات لا يقيدون نقل المعلومات أو الأدلة بموجب هذا البروتوكول بناءً على الاعتقاد الخاطئ بأن أحد الأطراف يخضع لحكم التعليق هذا.

287. على الرغم من أن الفقرة 15 تنص على إجراءات محددة تتعلق بالتشاور وتعليق عمليات نقل البيانات الشخصية لأسباب تتعلق بحماية البيانات، فإن الإجراءات الواردة في الفقرة 15 لا تهدف إلى التأثير على المشاورات بموجب المادة 23، الفقرة 1، أو حقوق التعليق التي قد تكون قابلة للتطبيق بموجب القانون الدولي فيما يتعلق بالمواد الأخرى من هذا البروتوكول.

الفصل الرابع - أحكام ختامية

288. تستند الأحكام الواردة في هذا الفصل، في معظمها، إلى "الأحكام الختامية النموذجية للاتفاقيات والبروتوكولات الإضافية والبروتوكولات المعدلة المبرمة في مجلس أوروبا"، والتي اعتمدتها لجنة الوزراء في الاجتماع رقم 1291 لنواب الوزراء في يوليو 2017، والأحكام الختامية للاتفاقية. نظرًا لأن بعض المواد الواردة في هذا الفصل إما تستخدم اللغة الموحدة للأحكام النموذجية أو تستند إلى ممارسة طويلة الأمد لإبرام المعاهدات في مجلس

أوروبا، فإنها لا تتطلب تعليقات محددة. ومع ذلك، فإن بعض التعديلات على الأحكام النموذجية الموحدة والانحراف عن الأحكام النهائية للاتفاقية تتطلب بعض الشرح.

المادة 15 - آثار هذا البروتوكول

289. تتضمن الفقرة 1 (أ) من المادة 15 الفقرة 2 من المادة 39 من الاتفاقية. على النحو المعترف به في الفقرة 312 من التقرير التفسيري للاتفاقية، تنص هذه الفقرة على أن الأطراف لها الحرية في تطبيق الاتفاقات القائمة بالفعل أو التي قد تدخل حيز التنفيذ في المستقبل. هذا البروتوكول، مثل الاتفاقية، ينص بشكل عام على الحد الأدنى من الالتزامات؛ لذلك، تعترف هذه الفقرة بأن للأطراف الحرية في تحمل التزامات أكثر تحديدًا بالإضافة إلى تلك المنصوص عليها بالفعل في هذا البروتوكول، عند إقامة علاقاتهم فيما يتعلق بالمسائل التي تم تناولها فيه. ومع ذلك، يجب على الأطراف احترام أهداف ومبادئ البروتوكول عند القيام بذلك، وبالتالي لا يمكنها قبول الالتزامات التي من شأنها أن تحبط الغرض المنشود منه.

290. تقر الفقرة 1 (ب) من هذه المادة بالتكامل المتزايد للاتحاد الأوروبي منذ فتح باب التوقيع على الاتفاقية في عام 2001، ولا سيما في مجالات إنفاذ القانون والتعاون القضائي في المسائل الجنائية وكذلك حماية البيانات. بالتالي، فإنه يسمح للدول الأعضاء في الاتحاد الأوروبي بتطبيق قانون الاتحاد الأوروبي الذي يحكم الأمور التي يتناولها هذا البروتوكول فيما بينها. قصد فريق الصياغة أن يشمل قانون الاتحاد الأوروبي التدابير والمبادئ والإجراءات المنصوص عليها في النظام القانوني للاتحاد الأوروبي، ولا سيما القوانين أو اللوائح أو الأحكام الإدارية بالإضافة إلى المتطلبات الأخرى، بما في ذلك قرارات المحاكم. تهدف الفقرة 1 (ب)، بالتالي، إلى تغطية العلاقات الداخلية بين الدول الأعضاء في الاتحاد الأوروبي وبين الدول الأعضاء في الاتحاد الأوروبي والمؤسسات والهيئات والوكالات التابعة للاتحاد الأوروبي. إذا لم يكن هناك قانون خاص بالاتحاد الأوروبي يتعلق بمسألة تقع ضمن نطاق هذا البروتوكول، فسيظل هذا البروتوكول يحكم هذه المسألة بين الأطراف التي هي دول أعضاء في الاتحاد الأوروبي.

291. توضح الفقرة 1 (ج) أن الفقرة 1 (ب) لا تؤثر على التطبيق الكامل لهذا البروتوكول بين الأطراف التي هي أعضاء في الاتحاد الأوروبي والأطراف الأخرى. لا يُقصد من الفقرة 1 (ب)، إذن، أن يكون لها أي تأثير يتجاوز العلاقات الداخلية للاتحاد الأوروبي كما هو موضح في الفقرة 290 أعلاه؛ ينطبق هذا البروتوكول بالكامل بين الدول الأعضاء في الاتحاد الأوروبي والأطراف الأخرى. اعتبر فريق الصياغة أن مثل هذا الحكم أمر هام لضمان حصول الأطراف من غير الدول الأعضاء في الاتحاد الأوروبي على جميع مزايا هذا البروتوكول في علاقاتهم مع الأطراف التي هي دول أعضاء في الاتحاد الأوروبي. على سبيل المثال، ناقش فريق الصياغة أن أي دولة عضو في الاتحاد الأوروبي تتلقى معلومات أو أدلة من طرف غير عضو في الاتحاد الأوروبي يجب أن تسعى للحصول على موافقة الطرف

غير المنتمي إلى الاتحاد الأوروبي قبل نقل المعلومات أو الأدلة إلى طرف آخر في الاتحاد الأوروبي، بما يتوافق مع المادة 14، الفقرة 10. وبالمثل، تنطبق الفقرة 1 (أ) من هذه المادة بالكامل بين الدول الأعضاء في الاتحاد الأوروبي والأطراف الأخرى غير الأعضاء.

292. تتضمن الفقرة 2 من المادة 15، الفقرة 3 من المادة 39 من الاتفاقية. على غرار الاتفاقية، كما هو موضح في الفقرة 314 من التقرير التفسيري للاتفاقية، لا يهدف هذا البروتوكول إلى معالجة جميع القضايا المعلقة المتعلقة بأشكال التعاون بين الأطراف أو بين الأطراف والكيانات الخاصة ذات الصلة بالجرائم الإلكترونية وجمع الأدلة في شكل إلكتروني للجرائم الجنائية. لذلك، تم إدراج الفقرة 2 من المادة 15 لتوضيح أن هذا البروتوكول يؤثر فقط على ما يتناوله. لم تتأثر الحقوق والقيود والالتزامات والمسؤوليات الأخرى التي قد تكون موجودة ولكن لم يتم التعامل معها من خلال هذا البروتوكول.

293. لا تتضمن المادة 15 حكماً مشابهاً للفقرة 1 من المادة 39 من الاتفاقية. وأوضح هذا الحكم في الاتفاقية أن الغرض من الاتفاقية هو استكمال المعاهدات أو الترتيبات الثنائية سارية المفعول بين الأطراف، بما في ذلك معاهدات معينة لتسليم المجرمين والمساعدة المتبادلة. لا يحتوي هذا البروتوكول على أي أحكام لتسليم المجرمين، ويحتوي على العديد من الأحكام التي لا تعتبر أحكامًا للمساعدة المتبادلة. كما هو موضح بمزيد من التفصيل في المادة 5 وفي التقرير التفسيري المصاحب لها، يتعامل كل قسم من تدابير التعاون في الفصل الثاني بطرق مختلفة مع معاهدات المساعدة المتبادلة. لذلك، خلص فريق الصياغة إلى أنه لا يحتاج إلى إدراج حكم مشابه للمادة 39، الفقرة 1.

المادة 16 - التوقيع ودخول حيز النفاذ

294. تسمح المادة 16 لجميع الأطراف في الاتفاقية بالتوقيع والانضمام إلى هذا البروتوكول. على عكس البروتوكول الأول (المادة 11)، لا ينص هذا البروتوكول على إجراء للانضمام إلى هذا البروتوكول. يجب على الدولة التي ترغب في التوقيع والانضمام إلى هذا البروتوكول أن تصبح طرفًا في الاتفاقية أولاً.

295. تنص الفقرة 3 على أن "يبدأ نفاذ هذا البروتوكول في اليوم الأول من الشهر الذي يلي انقضاء فترة ثلاثة أشهر بعد التاريخ الذي أعرب فيه خمسة أطراف في الاتفاقية عن موافقتهم على الالتزام بهذا البروتوكول". بينما نصت الاتفاقية في المادة 36، الفقرة 3، على أن ثلاثة على الأقل من الأطراف الخمسة يجب أن يكونوا دولًا أعضاء في مجلس أوروبا حتى تدخل الاتفاقية حيز التنفيذ، لم يتم إدراج هذا الشرط هنا نظرًا لأن هذا بروتوكول إضافي لاتفاقية وأن يكون لجميع الأطراف نفس الحق في تطبيق هذا البروتوكول بمجرد أن يعرب عدد لا يقل عن خمسة أطراف في الاتفاقية عن موافقتهم على الالتزام. وهذا يتبع نهج المادة 10 من البروتوكول الأول.

296. تصف الفقرة 4 عملية دخول هذا البروتوكول حيز النفاذ بالنسبة للأطراف في الاتفاقية التي تعرب عن موافقتها على الالتزام بهذا البروتوكول بعد دخوله حيز النفاذ بموجب الفقرة 3. وهذا يتبع نهج المادة 36، الفقرة 4 من الاتفاقية.

المادة 17 - البند الاتحادي

297. على غرار البند الاتحادي المنصوص عليه في المادة 41 من الاتفاقية، تحتوي المادة 17 من هذا البروتوكول على بند اتحادي يسمح للطرف الذي هو دولة اتحادية بإبداء تحفظ "بما يتفق مع مبادئه الأساسية التي تحكم العلاقة بين حكومته المركزية والدول المكونة أو الكيانات الإقليمية المماثلة الأخرى". الهدف من المادة 17 هو نفس الهدف من المادة 41 من الاتفاقية. وهذا، كما ورد في الفقرة 316 من التقرير التفسيري للاتفاقية، "لمراعاة الصعوبات التي قد تواجهها الدول الاتحادية نتيجة لتوزيعها المميز للسلطة بين السلطات المركزية والإقليمية".

298. يُسمح للدول الاتحادية بإبداء تحفظ على الالتزامات الواردة في الفصل الثاني من الاتفاقية (تحديد الجرائم الجنائية الوطنية والتدابير الإجرائية الوطنية)، إلى الحد الذي لا تقع فيه هذه التدابير ضمن سلطة الحكومة المركزية لدولة اتحادية في التنظيم. مع ذلك، يتعين على الدول الاتحادية أن تكون قادرة على توفير التعاون الدولي للأطراف الأخرى بموجب الفصل الثالث من الاتفاقية.

299. على الرغم من أن هذا البروتوكول ينص على التعاون الدولي بدلاً من التدابير الوطنية، فقد أقر المفاوضون بأنه لا تزال هناك ضرورة لبند اتحادي في هذا البروتوكول. في حين أن الاتفاقية لم تنص على أي تحفظ اتحادي بشأن المساعدة المتبادلة، فإن غالبية تدابير هذا البروتوكول لا تعمل بنفس الطريقة التي تعمل بها المساعدة المتبادلة التقليدية. ينص هذا البروتوكول على عدد من تدابير التعاون الأكثر كفاءة من المساعدة المتبادلة التقليدية والتي لا تتطلب بالضرورة مشاركة الحكومة المركزية. على وجه الخصوص، ينص هذا البروتوكول على تدبيرين، المادتين 6 و7، حيث يمكن للسلطات المختصة في أحد الأطراف أن تطلب التعاون مباشرة من الشركات الخاصة في طرف آخر. تتطلب هذه التدابير بعض الخطوات الإجرائية التي قد تواجه الدولة الاتحادية صعوبة في مطالبة السلطات المختصة من الدول المكونة لها أو الكيانات الإقليمية بالامتثال لها. على سبيل المثال، تنص المادة 7 على أنه يجوز لأي طرف، من خلال إشعار إلى الأمين العام، أن يطلب من السلطات من الأطراف الأخرى إشعار السلطة الحكومية المعينة في وقت واحد عند إرسال أمر إلى مقدم خدمة يسعى للحصول على معلومات المشترك. تحتوي المواد الأخرى على متطلبات لاتخاذ تدابير تشريعية أو غيرها من التدابير التي قد لا تتمكن دولة اتحادية من مطالبة الدول المكونة لها أو الكيانات الإقليمية المماثلة الأخرى بسنها. أخيرًا، يحتوي هذا البروتوكول على أحكام مفصلة لحماية البيانات، في حين أن الاتفاقية لا تحتوي على ذلك. على سبيل المثال، في الولايات

المتحدة، بموجب دستورها والمبادئ الأساسية للنظام الاتحادي، تسن الدول المكونة لها قوانين الإجراءات الجنائية وقوانين العقوبات الخاصة بها (منفصلة عن القوانين الاتحادية)؛ إنشاء محاكمهم والمدعين العامين والشرطة؛ والتحقيق في الجرائم الجنائية للدولة ومقاضاة مرتكبيها. السلطات المختصة في الدولة مستقلة عن السلطات الاتحادية وليست تابعة لها.

300. إذا سعت سلطات الدولة المكونة لدولة اتحادية أو كيان إقليمي مماثل إلى أشكال التعاون المنصوص عليها في هذا البروتوكول، فقد يكون الأمر هو (1) أنها تعمل بموجب قوانين إجرائية وقوانين خصوصية مختلفة عن تلك التي بموجبها السلطات الحكومية تعمل؛ (2) لا تخضع للحكومة المركزية من حيث التسلسل الهرمي التنظيمي؛ أو (3) لا تملك الحكومة المركزية السلطة القانونية لتوجيه أعمالها. في مثل هذه الحالات، يمكن أن يكون هناك ضمان فقط بأن الدولة المكونة أو الكيان الإقليمي المشابه سيفي بمتطلبات هذا البروتوكول - تلك المتعلقة بطلب الحصول على معلومات أو أدلة، وكذلك تلك المتعلقة بالتعامل اللاحق لهذه المعلومات أو الأدلة - إذا (1) طبقتها بنفسها، أو (2) إذا سعت سلطاتها إلى التعاون عبر، أو بمشاركة، سلطات الحكومة المركزية التي ستعمل على الوفاء بها (على سبيل المثال من خلال المساعدة المتبادلة أو نقطة الاتصال التي تعمل على مدار الساعة طوال أيام الأسبوع، أو بمشاركة الحكومة المركزية في فريق تحقيق مشترك.

301. في ضوء هذه الاعتبارات، تنص الفقرة 1 على إمكانية التحفظ للأطراف التي هي دول اتحادية. قد تحتفظ هذه الأطراف بالحق في تحمل الالتزامات بموجب هذا البروتوكول بما يتفق مع مبادئها الأساسية التي تحكم العلاقة بين حكومتها المركزية والدول المكونة لها أو الكيانات الإقليمية المماثلة الأخرى، وفقًا للفقرات 1 (أ) إلى (ج)، التي تحد من نطاق هذا التحفظ. بموجب الفقرة 1 (أ)، يتعين على الحكومة المركزية لدولة اتحادية تتذرع بهذا التحفظ أن تطبق جميع شروط هذا البروتوكول (مع مراعاة التحفظات والإعلانات المتاحة). فيما يتعلق بالتزامات حماية البيانات بموجب هذا البروتوكول، بالنسبة للأطراف التي تعمل بموجب المادة 14، الفقرة 1 (أ)، وهذا يشمل الالتزامات الواردة في المادة 14، الفقرة 9 (ب)، فيما يتعلق بالمشاركة اللاحقة مع الدول المكونة أو الكيانات الإقليمية المماثلة الأخرى (انظر التقرير التفسيري، الفقرة 260) حيث طلبت سلطة اتحادية معلومات بموجب هذا البروتوكول، إما لأغراضها الخاصة أو نيابة عن سلطة على المستوى الاتحادي الفرعي، وبعد ذلك تشارك هذه المعلومات مع هذه السلطة على المستوى الاتحادي الفرعي. بالإضافة إلى ذلك، تنص الفقرة 1 (ب) على أنه، على غرار الفقرة 1 من المادة 41 من الاتفاقية، لا يؤثر هذا التحفظ على التزامات تلك الدولة الطرف الاتحادية بالنص على التعاون الذي تسعى إليه الأطراف الأخرى وفقًا لأحكام الفصل الثاني. أخيرًا، بموجب الفقرة 1 (ج)، على الرغم من تحفظ الدولة الاتحادية، فإن المادة 13 من هذا البروتوكول - التي تتطلب، وفقًا للمادة 15 من الاتفاقية،

حماية حقوق الإنسان والحريات بموجب القانون الوطني - تنطبق على الدول المكونة للدولة الاتحادية أو الكيانات الإقليمية المماثلة بالإضافة إلى الحكومة المركزية بموجب الفقرة 1 (أ).

302. تنص الفقرة 2 على أنه إذا أبدت دولة اتحادية تحفظا بموجب الفقرة 1، وسعت سلطات الدولة المكونة أو الكيان الإقليمي المماثل في ذلك الطرف إلى التعاون مباشرة من سلطة أو مقدم خدمة أو كيان في طرف آخر، يجوز للطرف "منع السلطات أو مقدمي الخدمات أو الكيانات على أراضيه من التعاون ردًا على ذلك". يجوز للطرف الآخر تحديد الطريقة التي يمنع بها سلطاته أو مقدمي الخدمات أو كياناته على أراضيه من التعاون. هناك استثناءان لصلاحية طرف آخر لمنع التعاون.

303. أولاً، تنص الفقرة 2 على أنه لا يجوز لهذا الطرف الآخر أن يمنع التعاون إذا كانت الدولة المكونة أو كيان إقليمي آخر مشابه يفي بالتزامات هذا البروتوكول، فإن الدولة الاتحادية الطرف المعنية لديها "قامت [بإشعار] الأمين عام لمجلس أوروبا أن الدولة المكونة أو أي كيان إقليمي مشابه يطبق التزامات هذا البروتوكول المنطبقة على تلك الدولة الاتحادية". يعني مصطلح "التزامات هذا البروتوكول المطبقة على تلك الدولة الاتحادية" أن سلطة دولة مكونة أو كيان إقليمي مشابه قد لا تخضع لأي شرط لا تخضع له الحكومة المركزية، على سبيل المثال بسبب تحفظ ساري المفعول. إذا كانت الدولة الاتحادية قد قدمت هذا الإشعار إلى الأمين العام فيما يتعلق بدولة مكونة معينة، فيجب على طرف آخر أن ينص على تنفيذ أمر أو طلب من تلك الدولة بنفس القدر كما لو كان قد تم استلامه من سلطات الحكومة المركزية. بالطبع، لا تزال المتطلبات والإجراءات الواردة في كل تدبير من تدابير التعاون الواردة في الفصل الثاني سارية على الطلبات أو الأوامر المقدمة من هذه الدول المكونة أو الكيانات الإقليمية المماثلة، والامتثال لهذه المتطلبات ضروري. تتطلب هذه الفقرة أن يقوم الأمين العام لمجلس أوروبا بإنشاء سجل لهذه الإشعارات وتحديثه. يتم تشجيع الأطراف على تزويد الأمين العام بمعلومات محدثة.

304. ثانيًا، بموجب الفقرة 3، إذا تم تقديم طلب أو أمر من دولة مكونة أو كيان إقليمي مماثل آخر عن طريق الحكومة المركزية أو، بموجب المادة 12، عملاً باتفاق فريق تحقيق مشترك تم إبرامه بمشاركة من الحكومة المركزية، لا يجوز لطرف آخر منع السلطات أو مقدمي الخدمات أو الكيانات على إقليمه من نقل المعلومات أو الأدلة وفقًا لبنود هذا البروتوكول على أساس أن التعاون مطلوب من قبل دولة مكونة أو كيان إقليمي مماثل لدولة اتحادية التي قامت بالتحفظ المنصوص عليه في الفقرة 1. هذا لأنه عندما يتم تقديم الطلب أو الأمر عن طريق الحكومة المركزية أو يتم إبرام اتفاق فريق التحقيق المشترك بمشاركة الحكومة المركزية، فإن الحكومة المركزية هي التي مطلوب منها "النص على الوفاء بالالتزامات الواجبة التطبيق بموجب البروتوكول". نظرًا لأن الحكومة المركزية تقدم الطلب أو الأمر (أو تشارك في فريق التحقيق المشترك، فإن لديها الفرصة والالتزام للتحقق من استيفاء

متطلبات هذا البروتوكول فيما يتعلق بهذه الإجراءات. على سبيل المثال، إذا كان يجب، بموجب المادة 7، الفقرة 5 (أ)، إشعار طرف آخر بإرسال أمر يطلب فيه الحصول على معلومات المشترك، فإن الحكومة المركزية ملزمة بتقديم هذا الإشعار. فيما يتعلق بحماية البيانات (للأطراف التي تعمل بموجب المادة 14، الفقرة 1 (أ)، إذا كانت الدولة المكونة أو أي كيان إقليمي مشابه يسعى إلى التعاون من خلال الحكومة المركزية، فإن الحكومة المركزية تقدم البيانات إلى الدولة المكونة أو دولة أخرى مماثلة كيان إقليمي ويجب أن يطبق المتطلبات المنصوص عليها في المادة 14، الفقرة 9 (ب) (المشاركة اللاحقة داخل أحد الأطراف). أي أنه يجب أن يكون لدى الحكومة المركزية تدابير من أجل استمرار السلطات المستقبلة في حماية البيانات بشكل فعال من خلال توفير مستوى مماثل من الحماية مقارنة بالمستوى الذي تنص عليه المادة 14. سلطات الدولة المكونة أو الكيان الإقليمي المشابه التي تطلب وتتلقى البيانات الشخصية بهذه الطريقة ليست ملزمة بخلاف ذلك بتطبيق المادة 14. إذا كان الأطراف المعنيون يطبقون اتفاقا أو ترتيبًا آخر مبين في المادة 14، الفقرتين 1 (ب) أو 1 (ج)، تنطبق الشروط المنطبقة على ذلك الاتفاق أو الترتيب.

305. الفقرة 4 لها نفس النص تقريبا والتأثير نفسه كما في المادة 41، الفقرة 3، من الاتفاقية. وبالتالي، فيما يتعلق بأحكام الاتفاقية، التي يخضع تطبيقها للولاية القضائية للدول المكونة أو الكيانات الإقليمية المماثلة الأخرى (ما لم يتم تقديم إشعار إلى الأمين العام لمجلس أوروبا وفقًا للفقرة 2 من هذه المادة)، يتعين على الحكومة المركزية للدولة الاتحادية (1) إبلاغ سلطات الدول المكونة لها أو الكيانات الإقليمية المماثلة الأخرى بأحكام هذا البروتوكول؛ و (2) إبداء "رأيها الإيجابي، وتشجيعها على اتخاذ الإجراءات المناسبة لتنفيذها"، مما يشجع الدول المكونة أو الكيانات الإقليمية المماثلة على تطبيق هذا البروتوكول بالكامل. بالنسبة لهذا البروتوكول، يهدف هذا أيضًا إلى السماح في نهاية المطاف لهذه الدول المكونة أو الكيانات الإقليمية المماثلة الأخرى بأن يتم إشعارها بموجب الفقرة 2 من هذه المادة.

المادة 18– التطبيق الإقليمي

306. تسمح المادة 38 من الاتفاقية للأطراف بتحديد الإقليم أو الأقاليم التي ستطبق عليها الاتفاقية. تطبق المادة 18 من هذا البروتوكول تلقائيًا هذا البروتوكول على الأراضي التي يحددها أحد الأطراف بموجب المادة 38، الفقرتين 1 أو 2، من الاتفاقية طالما لم يتم فيه سحب هذا الإعلان بموجب المادة 38، الفقرة 3، من الاتفاقية. واعتبر فريق الصياغة أنه سيكون من الأفضل أن يطبق نفس النطاق الإقليمي للاتفاقية وهذا البروتوكول كقاعدة عامة افتراضية.

307. تنص الفقرة 2 من هذه المادة على أنه "يجوز للطرف [أثناء]، التوقيع على هذا البروتوكول أو عند إيداع صك التصديق أو القبول أو الموافقة، أن يعلن أن هذا

البروتوكول لا ينطبق على إقليم واحد أو أكثر محدد في إعلان الطرف بموجب المادة 38، الفقرتين 1 و / أو 2 من الاتفاقية". وفقا للفقرة 3، يجوز للأطراف سحب الإعلان بموجب الفقرة 2 من هذه المادة، وفقا للإجراءات المحددة. إن سحب الإعلان الوارد في الفقرة 2 سيكون له تأثير تطبيق هذا البروتوكول على أقاليم إضافية كانت مشمولة بالاتفاقية ولكن لم يتم تطبيق هذا البروتوكول عليها من قبل.

308. لا تسمح هذه المادة بتطبيق هذا البروتوكول على الأقاليم غير المشمولة بالاتفاقية.

المادة 19 - التحفظات والإعلانات

309. تنص هذه المادة على عدد من إمكانيات التحفظ. بالنظر إلى النطاق العالمي للاتفاقية والهدف المتمثل في تحقيق نفس المستوى من العضوية في هذا البروتوكول، فإن هذه التحفظات تمكن الأطراف في الاتفاقية من أن تصبح أطرافاً في هذا البروتوكول، مع السماح لهذه الأطراف بالحفاظ على نُهج ومفاهيم معينة تتسق مع قوانينها الوطنية، المبادئ القانونية الأساسية أو اعتبارات السياسة، حسب الاقتضاء.

310. إن إمكانيات التحفظ مقيدة من أجل ضمان التطبيق الموحد للأطراف لهذا البروتوكول إلى أقصى حد ممكن. بالتالي، لا يجوز إبداء أي تحفظات أخرى غير تلك المذكورة. بالإضافة إلى ذلك، لا يجوز إبداء تحفظات إلا من قبل طرف في الاتفاقية أثناء التوقيع على هذا البروتوكول أو عند إيداع صك تصديقه أو قبوله أو موافقته.

311. كما هو وارد في الاتفاقية، فإن التحفظات الواردة في هذا البروتوكول تستبعد أو تعدل الأثر القانوني للالتزامات المنصوص عليها في هذا البروتوكول (انظر الفقرة 315 من التقرير التفسيري للاتفاقية). في هذا البروتوكول، يسمح بالتحفظات لاستبعاد أشكال كاملة من التعاون. على وجه التحديد، تسمح المادة 7، الفقرة 9 (أ)، للطرف بالاحتفاظ بالحق في عدم تطبيق المادة 7 بأكملها. يُسمح أيضًا للتحفظات باستبعاد التعاون لمواد كاملة فيما يتعلق بأنواع معينة من البيانات. على وجه التحديد، تسمح المادة 7، الفقرة 9 (ب)، للطرف بالاحتفاظ بالحق في عدم تطبيق المادة 7 على أنواع معينة من أرقام الوصول إذا كان الكشف عن أرقام الوصول هذه يتعارض مع المبادئ الأساسية لنظامه القانوني الوطني. بالمثل، تسمح المادة 8، الفقرة 13، للطرف بالاحتفاظ بالحق في عدم تطبيق المادة 8 على بيانات الحركة.

312. تشير المادة 19 أيضاً إلى الإعلانات. على غرار الاتفاقية، من خلال الإعلانات الواردة في هذا البروتوكول، يُسمح للأطراف بإدراج بعض الإجراءات الإضافية المحددة التي تعدل نطاق الأحكام. تهدف هذه الإجراءات الإضافية إلى استيعاب بعض الاختلافات المفاهيمية أو القانونية أو العملية، والتي تكون مبررة بالنظر إلى النطاق العالمي للاتفاقية والتطلع إلى الوصول المتكافئ لهذا البروتوكول. تنقسم الإعلانات المعدودة إلى فئتين عامتين.

313. تسمح العديد من الإعلانات للطرف بأن يعلن أن سلطات أو تدابير معينة يجب أن تقوم بها سلطات معينة أو أن يتم نقل التعاون عبر قنوات معينة. هذا هو الحال بالنسبة للمادة 10، الفقرة 9 (السماح بالإعلان عن إمكانية إرسال الطلبات إلى السلطات بالإضافة إلى السلطة المركزية)؛ المادة 12، الفقرة 3 (يجب أن تكون السلطة المركزية موقعة على اتفاق فريق التحقيق المشترك أو توافق عليه)؛ المادة 8، الفقرة 11 (يجوز للطرف المُعلن أن يطلب إرسال طلبات الأطراف الأخرى بموجب هذه المادة عن طريق سلطاته المركزية أو سلطة أخرى يقررها الطرفان).

314. هناك فئة ثانية من الإعلانات تسمح للأطراف بطلب خطوات إجرائية منفصلة أو إضافية لبعض تدابير التعاون من أجل الامتثال للقانون الوطني أو تجنب إثقال كاهل السلطات. على سبيل المثال، المادة 7، الفقرة 8، والمادة 9، الفقرة 1 (ب)، تسمح للطرف بإصدار إعلانات لمطالبة الأطراف الأخرى باتخاذ خطوات إجرائية معينة فيما يتعلق بمعلومات المشترك. تسمح المادة 7، الفقرتان 2 (ب) و5 (أ)، والمادة 8، الفقرة 4، والمادة 9، الفقرة 5 بخطوات إجرائية إضافية لتوفير ضمانات إضافية أو الامتثال للقانون الوطني. لا يُقصد من تأثيرات الإعلانات أن تكون متبادلة. على سبيل المثال، إذا أصدر أحد الأطراف إعلانًا بموجب المادة 10، الفقرة 9 - أي أنه يجوز إرسال الطلبات بموجب هذه المادة إلى السلطات بالإضافة إلى سلطاتها المركزية - يجوز للأطراف الأخرى توجيه طلبات إلى السلطات الإضافية للطرف الذي أصدر الإعلان، ولكن يجوز للطرف الذي أصدر الإعلان فقط توجيه الطلبات إلى السلطات المركزية للأطراف الأخرى ما لم يصدروا مثل هذا الإعلان أيضًا.

315. يجب أن تكون الإعلانات المدرجة في الفقرة 2 من هذه المادة أثناء توقيع الطرف أو عند إيداع صك التصديق أو القبول أو الموافقة. وعلى النقيض من ذلك، يجوز إصدار الإعلانات الواردة في الفقرة 3 في أي وقت.

316. تقتضي الفقرة 3 من الأطراف إشعار الأمين العام لمجلس أوروبا بأي إعلانات أو إشعارات أو بلاغات مشار إليها في المادة 7، الفقرتين 5 (أ) و5 (هـ)، والفقرتين 4 و10 (أ) و (ب) من المادة 8، المادة 14، الفقرتان 7 (ج) و10 (ب)، والمادة 17، الفقرة 2، من هذا البروتوكول وفقًا للشروط المحددة في تلك المواد. على سبيل المثال، بموجب المادة 7، الفقرة 5 (هـ)، "يجب على الطرف، في الوقت الذي يتم فيه تقديم إشعار إلى الأمين العام لمجلس أوروبا بموجب الفقرة 5 (أ)، أن يرسل إلى الأمين العام معلومات الاتصال الخاصة بتلك السلطة".

كما يتعين على الأطراف إبلاغ الأمين العام لمجلس أوروبا، "بالسلطات" المشار إليها في المادة 8، الفقرتين 10 (أ) و (ب). وقد تم تكليف الأمين العام بإنشاء وتحديث سجل لهذه السلطات المعينة من قبل الأطراف، ويتم توجيه الأطراف لضمان صحة التفاصيل التي يقدمونها للسجل في جميع الأوقات (انظر المادة 7، الفقرة 5 (و)، والمادة 8، الفقرة 12).

المادة 20 - حالة التحفظات وسحبها

317. على غرار المادة 43 من الاتفاقية، تقتضي هذه المادة، دون فرض حدود زمنية محددة، من الأطراف سحب التحفظات بمجرد أن تسمح الظروف بذلك. من أجل ممارسة بعض الضغوط على الأطراف ودفعهم على الأقل إلى النظر في سحب تحفظاتهم، تسمح الفقرة 2 للأمين العام لمجلس أوروبا بالاستفسار بشكل دوري عن احتمالات السحب. إن إمكانية الاستفسار هذه هي ممارسة حالية بموجب العديد من صكوك مجلس أوروبا وهي واردة في المادة 43، الفقرة 3، من الاتفاقية والمادة 13، الفقرة 2، من البروتوكول الأول. وهكذا تُمنح الأطراف فرصة للإشارة إلى ما إذا كانت لا تزال بحاجة إلى الإبقاء على تحفظاتها فيما يتعلق ببعض الأحكام وسحب تلك التي لم تعد ضرورية لاحقًا. ومن المأمول أن تتمكن الأطراف بمرور الوقت من سحب أكبر عدد ممكن من تحفظاتها من أجل تعزيز التنفيذ الموحد لهذا البروتوكول.

المادة 21 - التعديلات

318. تتبع المادة 21 نفس الإجراء المتوخى لإجراء تعديلات في المادة 44 من الاتفاقية. يسمح هذا الإجراء المبسط بإجراء تعديلات دون الحاجة إلى التفاوض على بروتوكول تعديل إذا دعت الحاجة إلى ذلك. من المفهوم أن نتائج المشاورات مع الأطراف في الاتفاقية بموجب الفقرة 3 من هذه المادة ليست ملزمة للأطراف في البروتوكول. وكما هو مبين في الفقرة 323 من التقرير التفسيري للاتفاقية، "يُعتقد في الغالب أن إجراء التعديل يتعلق بتغييرات طفيفة نسبيًا ذات طابع إجرائي وتقني".

المادة 22 - تسوية النزاعات

319. تنص المادة 22 على أن آليات تسوية النزاعات المنصوص عليها في المادة 45 من الاتفاقية تنطبق أيضاً على هذا البروتوكول (انظر الفقرة 326 من التقرير التفسيري للاتفاقية).

المادة 23 – هيئة مشاورات الأطراف وتقييم التنفيذ

320. تنص الفقرة 1 من المادة 23 على أن المادة 46 من الاتفاقية (هيئة مشاورات الأطراف) تنطبق على هذا البروتوكول. وفقًا للفقرة 327 من التقرير التفسيري للاتفاقية، أنشأت المادة 46 "إطارًا للأطراف للتشاور بشأن تنفيذ الاتفاقية، وتأثير التطورات القانونية أو السياساتية أو التكنولوجية الهامة المتعلقة بموضوع الكمبيوتر أو الجرائم المتعلقة بالكمبيوتر وجمع الأدلة في شكل إلكتروني وإمكانية استكمال الاتفاقية أو تعديلها". وقد تم وضع الإجراء ليكون مرنًا وترك للأطراف تقرير كيف ومتى ينعقد الاجتماع. بعد دخول الاتفاقية حيز التنفيذ في عام 2004، بدأت الأطراف في الاجتماع على أساس منتظم باسم "لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية". بمرور الوقت، قامت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية،

المنشأة وفقًا للمادة 46 واستنادًا إلى النظام الداخلي المعتمد من قبل الأطراف في الاتفاقية، بإجراء تقييمات لتنفيذ الاتفاقية من قبل الأطراف، واعتمدت مذكرات توجيهية لتسهيل الفهم المشترك للأطراف فيما يتعلق باستخدام الاتفاقية، وأعدت مشروع البروتوكول الحالي. تظل إجراءات مشاورات الأطراف مرنة ويمكن بالتالي تكييفها من قبل الأطراف في هذا البروتوكول حسب الاقتضاء، لمراعاة الاحتياجات التي قد تنشأ عن تنفيذ هذا البروتوكول.

321. على غرار الاتفاقية (انظر الفقرة 327 من التقرير التفسيري)، ينبغي للمشاورات بموجب المادة 23 أن "تدرس القضايا التي أثيرت أثناء استخدام الاتفاقية وتنفيذها، بما في ذلك آثار الإعلانات والتحفظات المقدمة". يمكن أن يشمل ذلك إجراء مشاورات وتقييم تنفيذ هذا البروتوكول من قبل الدول المكونة أو الكيانات الإقليمية المماثلة للدول الاتحادية التي يتم إشعار الأمين العام لمجلس أوروبا بها بموجب المادة 17، الفقرة 2، وللأطراف الأعضاء في الاتحاد الأوروبي لإبلاغ والتشاور مع الأطراف الأخرى في هذا البروتوكول بشأن قوانين الاتحاد الأوروبي سارية المفعول فيما يتعلق باستخدامها وتنفيذها لهذا البروتوكول فيما يتعلق بالمادة 15، الفقرة 1 (ب). بالإضافة إلى المشاورات من خلال لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية بموجب هذه المادة التي تمت مناقشتها في الفقرة التالية، يجوز للأطراف المشاركة في المشاورات على أساس ثنائي. بالنسبة للدول الاتحادية، ستتم هذه المشاورات والتقييمات عبر حكومتها المركزية.

322. تحدد الفقرة 2 من المادة 23 إجراءات محددة لاستعراض استخدام وتنفيذ البروتوكول ضمن الإطار الأوسع الذي أنشأته المادة 46 ولجنة الاتفاقية المتعلقة بالجريمة الإلكترونية الذي تمت مناقشته أعلاه. تنص الفقرة 2 على أنه "يتعين على الأطراف تقييم الاستخدام الفعال لأحكام هذا البروتوكول وتنفيذها بشكل دوري" وتشير إلى أن المادة 2 من القواعد الإجرائية التي وضعتها لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية، بصيغتها المنقحة في 16 أكتوبر 2020، ستحكم هذه التقييمات. هذه الإجراءات متاحة على الموقع الإلكتروني للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية. نظرًا لأن لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية قد استعرضت العديد من أحكام الاتفاقية وأصدرت تقارير وفقًا لهذه الإجراءات، فقد اعتبر فريق الصياغة أن هذه الإجراءات الراسخة يجب أن تطبق مع ما يلزم من تعديل على تقييم أحكام هذا البروتوكول. في ضوء الالتزامات الإضافية التي تعهدت بها الأطراف في هذا البروتوكول وتدابير التعاون الفريدة التي يوفرها، قرر فريق الصياغة أن الأطراف في هذا البروتوكول وحدها هي التي ستجري هذه التقييمات. في ضوء الخبرة ذات الصلة اللازمة لتقييم استخدام وتنفيذ بعض أحكام هذا البروتوكول، بما في ذلك المادة 14 بشأن حماية البيانات، قد تنظر الأطراف في إشراك الخبراء المتخصصين في التقييمات.

323. بينما كان من الضروري من ناحية، التنبؤ بقواعد مثل هذه التقييمات، فإن التجربة الفعلية قد تؤدي إلى الحاجة إلى تكييف هذه الإجراءات، دون اشتراط تعديل رسمي لهذا البروتوكول

وفقًا للمادة 21. لذلك، تنص الفقرة 2 على أن يتم الاستعراض الأولي للإجراءات بعد خمس سنوات من بدء نفاذ هذا البروتوكول، وعندئذ يجوز للأطراف تعديل هذه الإجراءات بتوافق الآراء. يجوز للأطراف تعديل الإجراءات بتوافق الآراء في أي وقت بعد ذلك الاستعراض الأولي.

324. بالنظر إلى أهمية ضمانات حماية البيانات الواردة في المادة 14، اعتبر فريق الصياغة أنه ينبغي تقييم المادة 14 بمجرد وجود سجل كاف للتعاون بموجب هذا البروتوكول لاستعراض استخدام الأطراف لهذا الحكم وتنفيذه بفعالية. ولذلك، تنص الفقرة 3 على أن تقييم المادة 14 يبدأ بمجرد أن تعرب عشرة أطراف في الاتفاقية عن موافقتها على الالتزام بهذا البروتوكول.

المادة 24 – الانسحاب

325. الفقرتان 1 و2 من المادة 24 مماثلة لتلك الواردة في المادة 47 من الاتفاقية ولا تتطلبان مزيدا من التوضيح. وتنص الفقرة 3 على أن "[انسحاب] أحد الأطراف في هذا البروتوكول من الاتفاقية يشكل انسحابا من هذا البروتوكول". نظرًا لتأكيد هذا البروتوكول على تبادل المعلومات أو الأدلة، التي قد تتضمن بيانات شخصية، اعتبر فريق الصياغة أنه من الحكمة إضافة الفقرة 4 لتوضيح أن "المعلومات أو الأدلة المنقولة قبل تاريخ نفاذ الانسحاب يجب أن يستمر التعامل معها وفقًا لهذا البروتوكول".

بخصوص المذكرات التوجيهية

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[15].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

إن اتفاقية بودابست "تستخدم لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية"[16]، وذلك بغية ضمان أن الاتفاقية تشمل الأشكال الجديدة للبرمجيات الخبيثة أو الجرائم.

15. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
16. الفقرة 36 من التقرير التفسيري.

المذكرة التوجيهية 1# بشأن مفهوم "نظام الكمبيوتر"[17]

المقدمة

ناقشت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام الأول (ستراسبورغ، 20-21 مارس/آذار 2006) نطاق تعريف "نظام الكمبيوتر" في المادة الأولى، البند "أ" من اتفاقية بودابست على ضوء الأشكال المتطورة للتكنولوجيا التي تتجاوز أنظمة الحواسيب الكبرى أو المكتبية التقليدية.

منذ تاريخ صياغة الاتفاقية، تم تطوير أجهزة جديدة من قبيل الجيل الحديث للهواتف النقالة أو الهواتف "الذكية"، وأجهزة المساعد الرقمي الشخصي (PDAs)، واللوحات وغيرها من الأجهزة التي تنتج البيانات، أو تعالجها أو تنقلها. لذلك، كانت هنالك حاجة لمناقشة إن كانت هذه الأجهزة مضمنة في مفهوم "نظام الكمبيوتر" كما هو وارد في اتفاقية بودابست.

اتفقت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية، في عام 2006، على أن تلك الأجهزة مشمولة بتعريف "نظام الكمبيوتر" الوارد في المادة الأولى، البند "أ" من الاتفاقية.

وتشير هذه المذكرة التوجيهية إلى الفهم المشترك بين الأطراف كما يعكس ذلك تقرير الاجتماع الأول (الوثيقة T-CY (2006) 11).

المادة الأولى، البند "أ" من اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية رقم 185)

نص الاتفاقية

المادة 1 – التعريفات

لأغراض هذه الاتفاقية:

أ. يُقصد بـ " منظومة الكومبيوتر " أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقا لبرنامج، بالمعالجة الآلية للبيانات.

مقتبس من التقرير التفسيري

23. بموجب الاتفاقية، يقصد بنظام الكمبيوتر أي جهاز يتألف من أجهزة وبرمجيات تم تطويرها من أجل المعالجة التلقائية للبيانات الرقمية. ويمكن أن يشمل المدخلات والمخرجات،

17. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام الثامن.

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 المُعالج (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.

24. 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.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية بشأن مفهوم "نظام الكمبيوتر" (المادة الأولى (ألف) من اتفاقية بودابست)

تعرف المادة الأولى، البند "أ" من الاتفاقية "نظام الكمبيوتر" باعتباره أي " أي جهاز يتألف من أجهزة وبرمجيات تم تطويرها من أجل المعالجة التلقائية للبيانات الرقمية ".

تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن هذا التعريف يشمل، على سبيل المثال، الهواتف النقالة الحديثة متعددة الوظائف التي تتوفر من بين وظائفها على القدرة على إنتاج البيانات، ومعالجتها ونقلها من قبيل الولوج إلى الإنترنت، إرسال البريد الإلكتروني، نقل الملفات المرفقة، تحميل المحتويات أو تنزيل الوثائق.

وبالمثل، تعترف اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن أجهزة المساعدة الرقمية الشخصية، سواء كانت تتوفر على خاصية اللاسلكي أم لا، تقوم أيضا بإنتاج البيانات ومعالجتها ونقلها.

وتشير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية إلى أن هذه الأجهزة عندما تؤدي وظائف من هذا القبيل تقوم بمعالجة "بيانات الكمبيوتر" وفقا للتعريف الوارد في المادة 1 "ب".

فضلا عن ذلك، تعتبر اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن تلك الأجهزة عندما تؤدي تلك الوظائف تنتج "بيانات الحركة" وفقا للتعريف الوارد في المادة 1، البند "د".

لذلك، فإنها عندما تعالج مثل هذه البيانات فإنها تعمل بمثابة " نظام الكمبيوتر" وفقا للتعريف الوارد في المادة 1، البند "أ".

وتتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن هذا يتفق مع تفسير "نظام الكمبيوتر" الوارد في التقرير التفسيري للاتفاقية وأن الغرض من الاتفاقية هو أن تشمل جميع هذه الأجهزة بتلك الصفة.

الخلاصة

تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن تعريف "نظام الكمبيوتر" الوارد في المادة 1.أ يشمل الأشكال المتطورة للتكنولوجيا التي تتجاوز أنظمة الحواسيب الكبرى أو المكتبية التقليدية، من قبيل الهواتف النقالة الحديثة، الهواتف الذكية، أجهزة المساعد الرقمي الشخصي (PDAs)، واللوحات أو ما شابهها.

المذكرة التوجيهية 2# بشأن أحكام اتفاقية بودابست التي تشمل شبكات البناء والتشغيل والنقل "بوتنت" (botnets)[18]

المقدمة

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[19].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة مسألة شبكات البناء والتشغيل والنقل "بوتنت".

إن اتفاقية بودابست "تستخدم لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية"[20]، وذلك بغية ضمان أن الاتفاقية تشمل الأشكال الجديدة للبرمجيات الخبيثة أو الجرائم.

وتبين هذه المذكرة التوجيهية كيف تنطبق مواد مختلفة من الاتفاقية على البوتنت.

الأحكام ذات الصلة في اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية 185)

يمكن أن يفهم مصطلح "بوتنت" على أنه يشير إلى:

> "شبكة من الحواسيب المصابة ببرمجية خبيثة (فيروس حاسوبي). ويمكن أن يتم تنشيط مثل هذه الشبكة من الحواسيب المعبوث بها (المدمرة) من أجل أداء إجراءات محددة، مثل مهاجمة نظم المعلومات (الهجمات السيبرانية). ويمكن التحكم في هذه "الحواسيب المدمرة" – في كثير من الأحيان دون معرفة مستخدمي أجهزة الكمبيوتر للخطر – بواسطة كمبيوتر آخر. ويعرف هذا الكمبيوتر "المتحكم" أيضا باسم "مركز القيادة والتحكم"[21].

18. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام التاسع (4-8 يونيو/حزيران 2013)
19. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
20. الفقرة 36 من التقرير التفسيري.
21. اقتراح من أجل مبدأ توجيهي للبرلمان الأوروبي والمجلس بشأن الهجمات على نظم المعلومات وإلغاء القرار الإطاري للمجلس رقم 2005/222/JHA (com (2010) 517 الصيغة النهائية).

يمكن أن تكون الحواسيب متصلة من أجل أغراض إجرامية أو أغراض حسنة.[22] لذلك، فإن البوتنت التي تنطوي على حواسيب متصلة فيما بينها لا تعتبر ذات صلة، لأن العوامل ذات الصلة هي أن الحواسيب المعنية بالبوتنت تُستخدم دون موافقة ولأغراض إجرامية ولإحداث ضرر هام.

تغطي الأقسام التالية من الاتفاقية البوتنت بحسب ما يقوم به كل بوتنت فعليا. ويتضمن كل مقتضى معيار النية ("عن غير حق"، "بنية الاحتيال"، إلخ.) الذي يجب أن يكون إثباته سهلا بالبرهان عندما يتعلق الأمر بالبوتنت.

المواد ذات الصلة	أمثلة
المادة 2 – النفاذ غير المشروع	يتطلب تطوير وتشغيل بوتنت نفاذ غير مشروع إلى أنظمة الكمبيوتر.[23] يمكن استخدام البوتنت من أجل النفاذ غير المشروع إلى أنظمة كمبيوتر أخرى.
المادة 3 - الاعتراض غير المشروع	يمكن للبوتنت أن تستخدم وسائل فنية من أجل الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر.
المادة 4 – التدخل في البيانات	يؤدي تطوير بوتنت دائما إلى إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها. البوتنت بذاتها تقوم بإتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.
المادة 5 – التدخل في النظام	يمكن أن تعيق البوتنت تشغيل نظام الكمبيوتر. ويشمل ذلك هجمات حجب الخدمة الموزعة.[24]
المادة 6 – إساءة استخدام الأجهزة	جميع البوتنت هي أجهزة وفقا للتعريف الوارد في المادة 6 لأنه تم تصميمها أو ملاءمتها مبدئيا، بغرض ارتكاب الجرائم المنصوص عليها في المواد من 2 إلى 5.[25] تقع البرامج المستخدمة لتطوير وتشغيل البوتنت أيضا تحت طائلة المادة 6. لذلك، تجرم المادة 6 عملية إنتاج، بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأي طرق أخرى، علاوة على حيازة أجهزة من قبيل البوتنت أو البرامج المستخدمة لتطوير أو تشغيل البوتنت.

22. يمكن تطوير شبكات من الحواسيب عمدا لأغراض إجرامية. وبالتالي، تكون الجرائم المرتكبة من قبل تلك الشبكات مشمولة بالاتفاقية لكن هذه المذكرة لم تناقش هذه المسألة.
23. راجع أيضا المذكرة التوجيهية رقم 1 بشأن مفهوم "نظام الكمبيوتر".
24. راجع المذكرة التوجيهية المنفصلة.
25. مع ذلك، يجب على الأطراف التي تحفظت على المادة 6 تجريم عملية بيع، توزيع أو إتاحة الأجهزة المشمولة بهذه المادة.

المواد ذات الصلة	أمثلة
المادة 7 – التزوير المرتبط بالكومبيوتر	وفقا لتصميم البوتنت، يمكنه إدخال، تغيير، حذف أو إتلاف بيانات كومبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية.
المادة 8 – الاحتيال المرتبط بالكومبيوتر	يمكن أن تتسبب البوتنت في إلحاق خسارة بملكية شخص أو أن تؤدي إلى حصول شخص آخر على منفعة اقتصادية من خلال إدخال، تغيير، حذف أو إتلاف بيانات الكومبيوتر؛ و/أو التدخل في وظيفة نظام الكومبيوتر.
المادة 9 – الجرائم ذات الصلة بمواد إباحية عن الأطفال	يمكن أن توزع البوتنت مواد لاستغلال الأطفال.
المادة 10 – الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة	يمكن أن توزع البوتنت بشكل غير قانوني بيانات محمية بموجب قوانين الملكية الفكرية.
المادة 11 – المحاولة، والمساعدة والتحريض	يمكن استخدام البوتنت من أجل المساعدة أو التحريض على ارتكاب العديد من الجرائم المحددة في المعاهدة.
المادة 13 – العقوبات	تخدم البوتنت العديد من الأغراض الإجرامية التي يحدث بعضها آثارا وخيمة على أفراد، مؤسسات من القطاع العام أو الخاص أو بنى تحتية هامة. غير أنه يجوز لدولة طرف أن تنص في قانونها الوطني على عقوبة متساهلة بشكل غير ملائم مع جريمة متصلة بالبوتنت، وقد لا تسمح بمراعاة ظروف تشديد العقوبة، المحاولة، المساعدة أو التحريض. وقد يعني ذلك أن الأطراف بحاجة إلى النظر في إدخال تعديلات على قوانينها الوطنية. لذلك، ينبغي للدول الأطراف أن تضمن، عملا بالمادة 13، أن الجرائم ذات الصلة بالبوتنت " مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية". وقد يشمل ذلك بالنسبة للأشخاص الاعتباريين عقوبات جنائية أو غير جنائية، بما في ذلك العقوبات المالية. يمكن للدول الأطراف أيضا أن تنظر في ظروف تشديد العقوبة، مثلا في حال أثرت البوتنت على عدد هام من الأنظمة أو تسببت هجماتها في إلحاق ضرر جسيم، بما في ذلك الوفيات أو الإصابات الجسدية، أو أضرار ببنية تحتية هامة.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تبين قائمة المواد ذات الصلة بالبوتنت أعلاه الاستخدام الإجرامي متعدد الوظائف للبوتنت من جهة، والأحكام الجنائية التي يمكن أن تنطبق عليها من جهة أخرى.

لذلك، تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) أن مختلف أشكال البوتنت مشمولة باتفاقية بودابست.

المذكرة التوجيهية 5# بشأن هجمات حجب الخدمة الموزعة (DDOS)[26]

المقدمة

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[27].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة مسألة الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS).

إن اتفاقية بودابست " تستخدم لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية "[28]، وذلك بغية ضمان أن الاتفاقية تشمل الأشكال الجديدة للبرمجيات الخبيثة أو الجرائم.

وتبين هذه المذكرة التوجيهية كيف تنطبق مواد مختلفة من الاتفاقية على الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS).

الأحكام ذات الصلة في اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية 185)

هجمات الحرمان من الخدمات (DOS) هي محاولات لجعل نظام الكمبيوتر غير متوفر للمستخدمين من خلال مجموعة متنوعة من الوسائل، يمكن أن تشمل تشبع أجهزة الكمبيوتر المستهدفة أو الشبكات عبر طلبات الاتصالات الخارجية، وبالتالي إعاقة الخدمة للمستخدمين الشرعيين. أما هجمات حجب الخدمة الموزعة (DDOS) فهي هجمات الحرمان من الخدمات تنفذها العديد من أجهزة الكمبيوتر في نفس الوقت. ويوجد حاليا عدد من الطرق الشائعة التي يمكن من خلالها تنفيذ هجمات

26. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام التاسع (4-5 يونيو/ حزيران 2013)
27. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
28. الفقرة 36 من التقرير التفسيري.

الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS)، تشمل، على سبيل المثال، إرسال استعلامات غير صحيحة إلى نظام كمبيوتر؛ وتجاوز الحد الأقصى لقدرة المستخدمين؛ وإرسال رسائل البريد الإلكتروني إلى خوادم البريد الإلكتروني أكثر مما يمكن للنظام تلقيه والتعامل معه.

وتغطي الأقسام التالية من الاتفاقية هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS)، وفقا لما يفعله كل هجوم في الواقع. ويتضمن كل مقتضى معيار النية ("عن غير حق"، "بنية الاحتيال"، إلخ.)، الذي يجب أن يكون إثباته سهلا بالبرهان عندما يتعلق الأمر بحالات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS).

تفسير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية لهجمات حجب الخدمة الموزعة (DDOS).

المواد ذات الصلة	أمثلة
المادة 2 – النفاذ غير القانوني	يمكن النفاذ إلى نظام الكمبيوتر من خلال هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS).
المادة 4 – التدخل في البيانات	يمكن أن تؤدي هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS)، إلى إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.
المادة 5 – التدخل في النظام	يتلخص الهدف من هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS) تحديدا في عرقلة اشتغال نظام الكمبيوتر بشكل خطير.
المادة 11 – المحاولة، المساعدة والتحريض	يمكن استخدام هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS) لمحاولة ارتكاب عدة جرائم محددة في المعاهدة، أو المساعدة على ارتكابها أو التحريض عليها (من قبيل التزوير المرتبط بالكمبيوتر، المادة 7؛ الاحتيال المرتبط بالكمبيوتر، المادة 8؛ الجرائم ذات الصلة بمواد إباحية عن الأطفال، المادة 9؛ والجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة، المادة 10).
المادة 13 – العقوبات	تتفاوت خطورة هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS) بطرق مختلفة، خاصة عندما تكون موجهة ضد أنظمة أساسية للحياة اليومية – مثلا إذا أصبحت أنظمة بنكية أو استشفائية غير متاحة.

المواد ذات الصلة	أمثلة
	غير أنه يجوز لدولة طرف أن تنص في قانونها الوطني على عقوبة متساهلة بشكل غير ملائم مع هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS)، وقد لا تسمح بمراعاة ظروف تشديد العقوبة، المحاولة، المساعدة أو التحريض. وقد يعني ذلك أن الأطراف بحاجة إلى النظر في إدخال تعديلات على قوانينها الوطنية. لذلك، ينبغي للدول الأطراف أن تضمن، عملا بالمادة 13، أن الجرائم الجنائية ذات الصلة بمثل هذه الهجمات " مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية". وقد يشمل ذلك، بالنسبة للأشخاص الاعتباريين، عقوبات جنائية أو غير جنائية، بما في ذلك العقوبات المالية. يمكن للدول الأطراف أيضا أن تنظر في ظروف تشديد العقوبة، مثلا في حال أثرت هجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS) على عدد هام من الأنظمة أو تسببت هجماتها في إلحاق ضرر جسيم، بما في ذلك الوفيات أو الإصابات الجسدية، أو أضرار ببنية تحتية هامة.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تبين قائمة المواد ذات الصلة بهجمات الحرمان من الخدمات (DOS) وهجمات حجب الخدمة الموزعة (DDOS) أعلاه الاستخدام الإجرامي متعدد الوظائف لمثل هذه الهجمات.

لذلك، تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) أن اتفاقية بودابست تشمل مختلف أشكال الجرائم من هذا القبيل.

المذكرة التوجيهية 4# بشأن انتحال الشخصية والتصيد المرتبطين بالاحتيال[29]

المقدمة

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[30].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة مسألة انتحال الشخصية والتصيد والأفعال المشابهة[31] ذات الصلة بالاحتيال.

إن اتفاقية بودابست " تستخدم لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية "[32]، وذلك بغية ضمان أن الاتفاقية تشمل الأشكال الجديدة للبرمجيات الخبيثة أو الجرائم.

وتبين هذه المذكرة التوجيهية كيف تنطبق مواد مختلفة من الاتفاقية على انتحال الشخصية المرتبط بالاحتيال والمنطوي على أنظمة الكمبيوتر.

سرقة الهوية والتصيد

ولئن لم يكن هنالك أي تعريف مقبول عموما ولا استخدام متسق لمصطلح سرقة الهوية (identity theft)، فإن هذا المصطلح عادة ما ينطوي على أعمال إجرامية للحصول عن طريق الاحتيال على معلومات هوية شخص آخر واستخدامها (دون علمه أو موافقته). ويستخدم مصطلح "الاحتيال المتصل بالهوية" (identity fraud) أحيانا كمرادف، على الرغم من أنه ينطوي أيضا على استخدام هوية مزيفة وليس بالضرورة هوية حقيقية.

29. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام التاسع (5-4 يونيو/ حزيران 2013)
30. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
31. تعرف الأفعال المشابهة بأسماء متنوعة من قبيل التصيد الموجه (spear phishing)، والتصيد الاحتيالي عبر الرسائل النصية القصيرة على الهواتف النقالة (SMiShing)، واسترزاع المواقع على الإنترنت (pharming) والتصيد الصوتي (vishing).
32. الفقرة 36 من التقرير التفسيري.

وإذا كان من الممكن إساءة استخدام المعلومات الشخصية لشخص حقيقي أو وهمي لمجموعة من الأعمال غير القانونية، فإن هذه المذكرة التوجيهية تركز على سرقة الهوية فيما يتعلق بالاحتيال فقط.

وقد ينطوي ذلك على اختلاس هوية شخص آخر (من قبيل الاسم، تاريخ الميلاد أو العنوان الحالي أو العناوين السابقة) دون علمه أو موافقته. ثم يتم استخدام تفاصيل الهوية للحصول على سلع وخدمات باسم ذلك الشخص.

ويمكن أن تشمل الأفعال ذات الصلة "التصيد" أو واستزراع المواقع على الإنترنت (pharming) أو "التصيد الموجه" (spear phishing) أو "محاكاة البريد الإلكتروني" (spoofing) أو أي سلوك مماثل للحصول، على سبيل المثال، على كلمة المرور أو بيانات اعتماد الوصول الأخرى، في كثير من الأحيان من خلال البريد الإلكتروني أو المواقع المزورة.

وتؤثر سرقة الهوية على الحكومات والشركات والمواطنين وتسبب ضررا كبيرا. كما يقوض الثقة والائتمان في تكنولوجيات المعلومات.

ولا توجد في كثير من الأنظمة القانونية جريمة محددة تتعلق بسرقة الهوية. وعادة ما تنسب لمرتكبي سرقة الهوية تهمة ارتكاب جرائم أكثر خطورة (مثلا، الاحتيال المالي). وعادة ما ينطوي الحصول على هوية مزورة على جريمة، مثل تزوير الوثائق أو تغيير بيانات الكمبيوتر. وتسهل الهوية المزيفة ارتكاب العديد من الجرائم، بما في ذلك الهجرة غير الشرعية والاتجار بالبشر وغسل الأموال والاتجار بالمخدرات والاحتيال المالي ضد الحكومات والقطاع الخاص، ولكن ينظر إليها عموما كفعل مقترن بالاحتيال.

من الناحية النظرية، يمكن فصل سرقة الهوية إلى ثلاث مراحل متميزة:

- المرحلة 1: الحصول على معلومات الهوية، على سبيل المثال، من خلال السرقة المادية، محركات البحث والهجمات من الداخل والهجمات من الخارج (النفاذ غير القانوني إلى أنظمة الكمبيوتر، وأحصنة طروادة، راصد لوحة المفاتيح (keyloggers)، وبرامج التجسس وغيرها من البرامج الخبيثة) أو من خلال استخدام التصيد الاحتيالي و أو غيرها من تقنيات الهندسة الاجتماعية.
- المرحلة 2: حيازة معلومات الهوية والتصرف فيها، والتي تشمل بيع هذه المعلومات إلى أطراف ثالثة.
- المرحلة 3: استخدام معلومات الهوية لارتكاب جرائم الاحتيال أو غيرها من الجرائم، على سبيل المثال، من خلال انتحال هوية أخرى لاستغلال الحسابات البنكية وبطاقات الائتمان، وفتح حسابات جديدة، والحصول على قروض وتسليف، وطلب سلع وخدمات أو نشر برامج خبيثة.

في الختام: تستخدم سرقة الهوية (بما في ذلك التصيد الاحتيالي والسلوك المماثل) بشكل عام لإعداد المزيد من الأعمال الإجرامية مثل الاحتيال المتصل بالكمبيوتر. ولئن لم يتم تجريم سرقة الهوية كفعل منفصل، ستكون وكالات إنفاذ القانون قادرة على متابعة الجرائم اللاحقة.

تفسير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية لتجريم انتحال الشخصية المرتبط بالاحتيال بموجب اتفاقية بودابست

تركز اتفاقية بودابست على السلوك الإجرامي وليس على التقنيات أو التكنولوجيات المستخدمة تحديدا. لذلك، فإنها لا تتضمن أحكاما خاصة بسرقة الهوية أو التصيد الاحتيالي. ومع ذلك، سيسمح الإعمال الكامل لأحكام القانون الأساسي للاتفاقية للدول بتجريم السلوك المتعلق بسرقة الهوية.

تطالب الاتفاقية الدول بتجريم السلوك من قبيل النفاذ غير القانوني لنظام الكمبيوتر، والاعتراض غير القانوني للبيانات، والتدخل في النظام وإساءة استخدام الأجهزة والاحتيال المتصل بالكمبيوتر:

المرحلة	مادة الاتفاقية	أمثلة
المرحلة 1 – الحصول على معلومات الهوية	المادة 2 – النفاذ غير القانوني	إذا كان مجرم يرتكب أفعال "القرصنة"، أو التحايل على حماية كلمة السر، أو رصد لوحة المفاتيح أو استغلال ثغرات البرمجيات، فإن النفاذ إلى الكمبيوتر بشكل غير قانوني يتم من خلال أفعال سرقة الهوية / التصيد الاحتيالي. ويعتبر النفاذ غير القانوني إلى أنظمة الحاسوب أحد أكثر الجرائم شيوعا المرتكبة للحصول على معلومات حساسة مثل معلومات الهوية.
	المادة 3 – الاعتراض غير القانوني	كثيرا ما تنطوي سرقة الهوية على استخدام أجهزة رصد لوحة المفاتيح أو أي نوع آخر من البرامج الخبيثة من أجل الاعتراض غير القانوني للإرسال غير العمومي لبيانات الكمبيوتر، إلى نظام كمبيوتر يحتوي على معلومات حساسة مثل معلومات الهوية، أو منه أو داخله.
	المادة 4 – التدخل في البيانات	يمكن أن تنطوي سرقة الهوية / التصيد الاحتيالي على إتلاف أو حذف أو تخريب أو تغيير أو إلغاء بيانات الكمبيوتر. غالبا ما يتم ذلك خلال عملية الحصول على النفاذ غير القانوني من خلال تثبيت راصد لوحة المفاتيح للحصول على معلومات حساسة.

المرحلة	مادة الاتفاقية	أمثلة
	المادة 5 – التدخل في النظام	قد تنطوي سرقة الهوية / التصيد الاحتيالي على عرقلة تشغيل نظام الكمبيوتر من أجل سرقة أو تسهيل سرقة معلومات الهوية.
	المادة 7 – التزوير المرتبط بالكمبيوتر	قد تنطوي سرقة الهوية / التصيد الاحتيالي على إدخال أو تغيير أو حذف أو إتلاف بيانات الكمبيوتر، مما يؤدي إلى اعتبار البيانات غير الصحيحة وكأنها صحيحة أو التصرف فيها على ذلك الأساس. يعتبر التصيد الاحتيالي التمثيل الأكثر شيوعا للتزوير المرتبط بالكمبيوتر (على سبيل المثال، صفحة إلكترونية مزورة على شبكة الإنترنت لمؤسسة مالية) ونتيجة لذلك، فهو النشاط غير المشروع الأكثر شيوعا الذي يتم من خلاله جمع المعلومات الحساسة، من قبيل معلومات الهوية.
المرحلة 2 – حيازة معلومات الهوية والتصرف فيها	المادة 6 – إساءة استخدام الأجهزة	يمكن اعتبار معلومات الهوية المسروقة – بما في ذلك كلمات السر ووثائق الاعتماد للدخول وبطاقات الائتمان وغيرها – بمثابة "جهاز، بما في ذلك برنامج كومبيوتر، تم تصميمه أو ملاءمته مبدئيا، بغرض ارتكاب أي من الجرائم المنصوص عليها في المواد من 2 إلى 5"، أو " كلمة سر خاصة بكومبيوتر، أو رمز الولوج، أو بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل أو جزئي إلى نظام كومبيوتر".
المرحلة 3 – استخدام معلومات الهوية لارتكاب جرائم الاحتيال أو غيرها من الجرائم	المادة 8 – الاحتيال المرتبط بالكمبيوتر	يؤدي استخدام هوية مزورة عن طريق إدخال، تغيير، أو حذف أو إتلاف بيانات الكمبيوتر أو التدخل في وظيفة نظام الكمبيوتر إلى استغلال حسابات مصرفية أو بطاقات ائتمان أو الحصول على قروض أو تسليف أو طلب سلع مما يتسبب في فقدان شخص ما لممتلكات ويؤدي إلى حصول شخص آخر على منفعة اقتصادية.
جميع المراحل	المادة 11 – المحاولة، المساعدة والتحريض	قد يشكل الحصول على معلومات الهوية وحيازتها والتصرف فيها محاولة ومساعدة وتحريض على عدة جرائم محددة في الاتفاقية.

المرحلة	مادة الاتفاقية	أمثلة
	المادة 13 – العقوبات	تخدم سرقة الهوية أغراضا إجرامية متعددة، يسبب بعضها أضرارا جسيمة للأفراد ومؤسسات القطاع العام أو الخاص. مع ذلك، يجوز لدولة طرف أن تنص في قانونها الوطني على عقوبة متساهلة بشكل غير ملائم مع سرقة الهوية، وقد لا تسمح بمراعاة ظروف تشديد العقوبة، المحاولة، المساعدة أو التحريض. وقد يعني ذلك أن الأطراف بحاجة إلى النظر في إدخال تعديلات على قوانينها الوطنية. لذلك، ينبغي للأطراف أن تضمن، عملا بالمادة 13، أن الجرائم الجنائية المتصلة بسرقة الهوية "مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية". وقد يشمل ذلك بالنسبة للأشخاص الاعتباريين عقوبات جنائية أو غير جنائية، بما في ذلك العقوبات المالية. كما يجوز للأطراف النظر في ظروف تشديد العقوبة، على سبيل المثال عندما تؤثر سرقة الهوية على عدد كبير من الأشخاص أو تسبب محنة عسيرة أو تعرض شخصا للخطر.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية على أن ما ورد أعلاه يوضح النطاق والعناصر المختلفة لسرقة الهوية والتصيد الاحتيالي والأحكام الجنائية التي يمكن أن تطبق عليها.

لذلك، تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن
اتفاقية بودابست تغطي مختلف أوجه الجرائم من هذا القبيل.

المذكرة التوجيهية #6 بشأن الهجمات على البنية التحتية للمعلومات الحيوية[33]

المقدمة

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[34].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة مسألة الهجمات على البنية التحتية للمعلومات الحيوية.

إن اتفاقية بودابست " تستخدم لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية "[35]، وذلك بغية ضمان أن الاتفاقية تشمل الأشكال الجديدة للبرمجيات الخبيثة أو الجرائم.

وتبين هذه المذكرة التوجيهية كيف تنطبق مواد مختلفة من الاتفاقية على الهجمات على البنية التحتية للمعلومات الحيوية.

الأحكام ذات الصلة في اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية 185)

يمكن تعريف البنى التحتية الحرجة بأنها نظم وأصول، فعلية كانت أو افتراضية، ذات أهمية حيوية بالنسبة إلى بلد يحدث فيه أداؤها غير السليم أو عجزها أو إتلافها أثرا مدمرا على الأمن القومي والدفاع الوطني والأمن الاقتصادي والصحة العامة أو السلامة أو أي مزيج من تلك المسائل. وتعرِّف البلدان البنى التحتية الحيوية بشكل مختلف. ومع ذلك، فإن العديد من البلدان تعتبر أن البنى التحتية الحيوية تشمل قطاعات الطاقة، والأغذية، والمياه، والوقود، والنقل، والاتصالات، والمالية والصناعة، والدفاع، والخدمات الحكومية والخدمات العامة.

33. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام التاسع (5-4 يونيو/حزيران 2013)
34. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
35. الفقرة 36 من التقرير التفسيري.

وغالبا ما يتم تشغيل البنى التحتية الحرجة عن طريق أنظمة الكمبيوتر، بما في ذلك تلك المعروفة باسم أنظمة التحكم الصناعي (ICS) أو نظم المراقبة الإشرافية واحتياز البيانات (SCADA). وعموما، تعرف هذه الأنظمة بالبنى الأساسية للمعلومات الحيوية.

ووفقا لمصادر خاصة وحكومية، فإن عددا كبيرا وإن لم يكن محددا من الهجمات على البنى التحتية الحيوية للمعلومات في جميع أنحاء العالم يحدث في كل عام. وتستخدم هذه الهجمات نفس التقنيات التي تستعمل في الجرائم الإلكترونية الأخرى. ويتلخص الفرق في تأثير هجمات من هذا القبيل على المجتمع: يمكن أن تستنزف الأموال الخزينات الحكومية، أو أن تغلق شبكات المياه، أو تربك مراقبة الحركة الجوية، وهكذا دواليك.

وتغطي الأقسام التالية من الاتفاقية الأشكال الحالية والمستقبلية لهجمات البنية التحتية الحيوية للمعلومات، بحسب طبيعة الهجوم. ويتضمن كل مقتضى معيار النية ("عن غير حق"، "بنية الاحتيال"، إلخ.) الذي ينبغي أن يؤخذ في الاعتبار عندما يقرر المسؤولون طريقة توجيه تهمة ارتكاب الجريمة.

تفسير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية لتجريم الهجمات على البنية التحتية للمعلومات الحيوية

المواد ذات الصلة	أمثلة
المادة 2 – النفاذ غير المشروع	يمكن النفاذ إلى نظام الكمبيوتر من خلال الهجمات على البنية التحتية للمعلومات الحيوية.
المادة 3 – الاعتراض غير القانوني	يمكن للهجمات على البنية التحتية للمعلومات الحيوية أن تستخدم وسائل فنية من أجل الاعتراض باستخدام وسائل فنية، للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر.
المادة 4 – التدخل في البيانات	يمكن أن تؤدي الهجمات على البنية التحتية للمعلومات الحيوية إلى إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.
المادة 5 – التدخل في النظام	يمكن أن تعرقل الهجمات على البنية التحتية للمعلومات الحيوية اشتغال نظام الكمبيوتر؛ وفي الواقع، قد يكون ذلك هو هدفها الأساسي.
المادة 7 – التزوير المرتبط بالكمبيوتر	قد تنطوي الهجمات على البنية التحتية للمعلومات الحيوية على إدخال أو تغيير أو حذف أو إتلاف بيانات الكمبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية.

المواد ذات الصلة	أمثلة
المادة 8 – الاحتيال المرتبط بالكمبيوتر	قد تتسبب الهجمات على البنية التحتية للمعلومات الحيوية في فقدان شخص ما لممتلكات وتؤدي إلى حصول شخص آخر على منفعة اقتصادية عن طريق إدخال، تغيير، أو حذف أو إتلاف بيانات الكمبيوتر أو التدخل في وظيفة نظام الكمبيوتر.
المادة 11 – المحاولة، المساعدة والتحريض	يمكن استخدام الهجمات على البنية التحتية للمعلومات الحيوية من أجل محاولة ارتكاب جرائم محددة في الاتفاقية أو المساعدة على ارتكابها أو التحريض على ارتكابها.
المادة 13 – العقوبات	يمكن أن تختلف آثار الهجمات على البنية التحتية للمعلومات الحيوية (قد تختلف من بلد إلى آخر لأسباب فنية، ثقافية أو غيرها من الأسباب)، إلا أن الحكومات عادة ما تهتم بها عندما تتسبب في ضرر خطير أو واسع النطاق. غير أنه يجوز لدولة طرف أن تنص في قانونها الوطني على عقوبة متساهلة بشكل غير ملائم مع الهجمات على البنية التحتية للمعلومات الحيوية، وقد لا تسمح بمراعاة ظروف تشديد العقوبة، المحاولة، المساعدة أو التحريض. وقد يعني ذلك أن الأطراف بحاجة إلى النظر في إدخال تعديلات على قوانينها الوطنية. لذلك، ينبغي للدول الأطراف أن تضمن، عملا بالمادة 13، أن الجرائم الجنائية ذات الصلة بمثل هذه الهجمات " مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية". وقد يشمل ذلك، بالنسبة للأشخاص الاعتباريين، عقوبات جنائية أو غير جنائية، بما في ذلك العقوبات المالية. يمكن للدول الأطراف أيضا أن تنظر في ظروف تشديد العقوبة، مثلا في حال أثرت الهجمات على البنية التحتية للمعلومات الحيوية على عدد هام من الأنظمة أو تسببت هجماتها في إلحاق ضرر جسيم، بما في ذلك الوفيات أو الإصابات الجسدية، أو أضرار ببنية تحتية هامة.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تبين قائمة المواد ذات الصلة بالهجمات على البنية التحتية للمعلومات الحيوية أعلاه الاستخدام الإجرامي متعدد الوظائف لمثل هذه الهجمات.

لذلك، تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) أن اتفاقية بودابست تشمل مختلف أشكال الجرائم من هذا القبيل.

المذكرة التوجيهية 7# بشأن الأشكال الجديدة للبرمجيات الخبيثة[36]

المقدمة

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[37].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة مسألة الأشكال الجديدة للبرمجيات الخبيثة.

إن اتفاقية بودابست "تستخدم لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية"[38]، وذلك بغية ضمان أن الاتفاقية تشمل الأشكال الجديدة للبرمجيات الخبيثة أو الجرائم.

وتبين هذه المذكرة التوجيهية كيف تنطبق مواد مختلفة من الاتفاقية على الأشكال الجديدة للبرمجيات الخبيثة.

الأحكام ذات الصلة في اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية 185)

هناك العديد من الأشكال الحالية للبرمجيات الخبيثة، والتي عرفتها منظمة التعاون والتنمية الاقتصادية بأنها "مصطلح عام لقطعة من برمجية مدرجة في نظام معلوماتي بغية إلحاق ضرر بذلك النظام أو بأنظمة أخرى، أو لتغييرها من أجل استخدامها لأغراض غير تلك التي يقصدها أصحابها ".[39] وتشمل الأشكال المعروفة الطفيليات والفيروسات وأحصنة طروادة. ويمكن للأشكال الحالية من البرمجيات الخبيثة أن تسرق البيانات عن طريق نسخها وإرسالها إلى عنوان آخر؛ كما يمكنها التلاعب بالبيانات وعرقلة تشغيل أنظمة الكمبيوتر، بما في ذلك الأنظمة التي تتحكم في البنى

36. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام التاسع (5-4 يونيو/حزيران 2013)
37. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
38. الفقرة 36 من التقرير التفسيري.
39. http://www.oecd.org/internet/ieconomy/40724457.pdf

التحتية الحيوية؛ ويمكن لبرنامج الفدية (ransomware) حذف، إتلاف أو منع النفاذ إلى البيانات؛ علاوة على أن البرمجيات الخبيثة المصممة خصيصا يمكن أن تستهدف أنظمة كمبيوتر محددة.

ووفقا لمصادر خاصة وحكومية، يتم تطوير واكتشاف أعداد كبيرة من الأشكال الجديدة من البرامج الخبيثة في كل عام. وتختلف هذه الأشكال الجديدة من حيث أهدافها. وعلى غرار الأشكال القديمة، يمكن للأشكال الجديدة للبرمجيات الخبيثة أن تسرق الأموال، أو تغلق شبكات المياه، أو تهدد المستخدمين، وما إلى ذلك.

وتعتبر أعداد أشكال البرمجيات الخبيثة وتشكيلتها واسعة بشكل يجعل وصف حتى الأشكال المعروفة حاليا بصورة قانونية جنائية غير ممكن. وبالتالي، تتجنب اتفاقية الجريمة الإلكترونية عمدا مصطلحات من قبيل الطفيليات، والفيروسات وأحصنة طروادة. ونظرا لأن أشكال البرمجيات الخبيثة تتغير، فإن استخدام مصطلحات من هذا القبيل في اتفاقية من شأنه أن يجعلها متقادمة بسرعة وأن تؤدي إلى نتائج عكسية.

وبطبيعة الحال، فإنه من غير الممكن أيضا وصف الأشكال المستقبلية في أي قانون.

لهذه الأسباب، فإنه من الأهمية بمكان التركيز على أهداف وآثار البرمجيات الخبيثة، لأنها معروفة بالفعل ويمكن وصفها في القانون.

وهكذا، تغطي الأقسام التالية من الاتفاقية كلا من البرمجيات الخبيثة الحالية والمستقبلية، وفقا لما تقوم به البرمجيات الخبيثة في الواقع. ويتضمن كل مقتضى معيار النية ("عن غير حق"، "بنية الاحتيال"، إلخ.) الذي ينبغي أن يؤخذ في الاعتبار عندما يقرر المسؤولون طريقة توجيه تهمة ارتكاب الجريمة.

تفسير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية لتجريم الأشكال الجديدة للبرمجيات الخبيثة

المواد ذات الصلة	أمثلة
المادة 2 – النفاذ غير القانوني	يمكن استخدام البرمجيات الخبيثة للنفاذ إلى أنظمة الكمبيوتر.
المادة 3 – الاعتراض غير القانوني	يمكن استخدام البرمجيات الخبيثة من أجل الاعتراض للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر.
المادة 4 – التدخل في البيانات	تؤدي البرمجيات الخبيثة إلى إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.

المواد ذات الصلة	أمثلة
المادة 5 – التدخل في النظام	يمكن أن تعرقل البرمجيات الخبيثة اشتغال نظام الكمبيوتر.
المادة 6 – إساءة استخدام الأجهزة.	البرمجيات الخبيثة هي جهاز بحسب تعريف المادة 6 (ومع ذلك، يجب على الأطراف التي أبدت تحفظات على المادة 6 تجريم عملية بيع، توزيع أو إتاحة الأجهزة المشمولة)، وذلك لأنه تم تصميمها أو ملاءمتها مبدئيا، بغرض ارتكاب الجرائم المنصوص عليها في المواد من 2 إلى 5. علاوة على ذلك، تجرم المادة عملية بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة بأي طرق أخرى، كلمات السر الحاسوبية، رموز النفاذ أو أي بيانات مشابهة يمكن من خلالها النفاذ إلى أنظمة الكمبيوتر. وهذه العناصر غالبا ما تتوفر في المتابعات الجنائية بشأن البرمجيات الخبيثة.
المادة 7 – التزوير المرتبط بالكمبيوتر	يمكن أن تؤدي البرمجيات الخبيثة إلى إدخال أو تغيير أو حذف أو إتلاف بيانات الكمبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية.
المادة 8 – الاحتيال المرتبط بالكمبيوتر.	قد تتسبب البرمجيات الخبيثة في فقدان شخص ما لممتلكات وتؤدي إلى حصول شخص آخر على منفعة اقتصادية عن طريق إدخال، تغيير، أو حذف أو إتلاف بيانات الكمبيوتر أو التدخل في وظيفة نظام الكمبيوتر.
المادة 11 – المحاولة، المساعدة والتحريض.	يمكن استخدام البرمجيات الخبيثة من أجل محاولة ارتكاب جرائم محددة في الاتفاقية أو المساعدة على ارتكابها أو التحريض على ارتكابها.
المادة 13 - العقوبات	تختلف آثار الأشكال الجديدة للبرمجيات الخبيثة بشكل كبير، حيث تكون بعض البرمجيات الخبيثة تافهة نسبيا بينما تعتبر برمجيات خبيثة أخرى خطيرة بالنسبة للأشخاص، البنى التحتية الحساسة أو خطيرة بطرق أخرى. وقد تختلف تلط الآثار من بلد إلى آخر لأسباب فنية، ثقافية أو غيرها من الأسباب. ويجوز لدولة طرف أن تنص في قانونها الوطني على عقوبة متساهلة بشكل غير ملائم مع هجمات البرمجيات الخبيثة، وقد لا تسمح بمراعاة ظروف تشديد العقوبة، المحاولة، المساعدة أو التحريض. وقد يعني ذلك أن الأطراف بحاجة إلى النظر في إدخال تعديلات على قوانينها الوطنية. لذلك، ينبغي للدول الأطراف أن تضمن، عملا بالمادة 13، أن الجرائم الجنائية ذات الصلة بمثل هذه الهجمات " مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية". وقد يشمل ذلك، بالنسبة للأشخاص الاعتباريين، عقوبات جنائية أو غير جنائية، بما في ذلك العقوبات المالية.

المواد ذات الصلة	أمثلة
	ويمكن للدول الأطراف أيضا أن تنظر في ظروف تشديد العقوبة، مثلا في حال أثرت البرمجيات الخبيثة على عدد هام من الأنظمة أو تسببت هجماتها في إلحاق ضرر جسيم، بما في ذلك الوفيات أو الإصابات الجسدية، أو أضرار ببنية تحتية هامة.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تبين قائمة المواد ذات الصلة بالبرمجيات الخبيثة أعلاه الاستخدام الإجرامي متعدد الوظائف لمثل هذه الهجمات.

لذلك، تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) أن اتفاقية بودابست تشمل مختلف أوجه جميع أشكال البرمجيات الخبيثة.

المذكرة التوجيهية 3# بشأن النفاذ العابر للحدود إلى البيانات (المادة 32)[40]

المقدمة

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[41].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة مسألة النفاذ العابر للحدود إلى البيانات بموجب المادة 32 من اتفاقية بودابست.[42]

تعتبر المادة 32 (باء) استثناء لمبدإ الإقليمية وتسمح بالنفاذ العابر للحدود بشكل أحادي الطرف دون الحاجة إلى المساعدة المتبادلة في ظل ظروف محدودة. والأطراف مدعوة إلى تعزيز الاستعمال الفعال لأحكام التعاون الدولي الواردة في اتفاقية بودابست، بما في ذلك المساعدة المتبادلة.

عموما، تتنوع الممارسات والإجراءات والظروف والضمانات بشكل كبير بين مختلف الأطراف. ولا تزال الهواجس المتعلقة بالحقوق الإجرائية للمشتبه فيهم والخصوصية وحماية البيانات الشخصية والأساس القانوني للنفاذ إلى البيانات المخزنة في الولايات القضائية الأجنبية أو "في الحواسيب السحابية" علاوة على السيادة الوطنية، قائمة وتحتاج إلى المعالجة.

وترمي هذه المذكرة التوجيهية إلى تيسير تنفيذ اتفاقية بودابست من قبل الأطراف، وإلى تصحيح سوء الفهم فيما يتعلق بالنفاذ العابر للحدود بموجب هذه المعاهدة وإلى طمأنة الأطراف الثالثة.

---

40. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام الثاني عشر (2-3 ديسمبر/كانون الأول 2014)
41. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابست).
42. يمثل إعداد هذه المذكرة التوجيهية تتبعا لنتائج التقرير بشأن "النفاذ العابر للحدود والولاية القضائية" (T-CY (2012) 3) المعتمدة خلال الاجتماع العام للجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية المنعقد في ديسمبر/كانون الأول 2012.
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

ومن ثم، ستساعد المذكرة التوجيهية الأطراف على الاستفادة الكاملة من الإمكانات التي تتيحها المعاهدة فيما يتعلق بالنفاذ العابر للحدود إلى البيانات.

المادة 32 من اتفاقية بودابست

نص أحكام المادة:

المادة 32 – النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم

يجوز لدولة طرف، دون ترخيص من دولة طرف أخرى:

أ. النفاذ إلى بيانات كومبيوتر مُخزنة متاحة للعموم (مصدر مفتوح) بغض النظر عن مكان تواجد البيانات جغرافياً؛ أو

ب. النفاذ إلى بيانات كومبيوتر مُخزنة موجودة لدى دولة طرف أخرى أو تلقيها، من خلال نظام كومبيوتر داخل أقاليمها، في حال حصول تلك الدولة الطرف على الموافقة القانونية والطوعية للشخص الذي يتوفر على السلطة القانونية للكشف عن البيانات لتلك الدولة الطرف عبر نظام الكومبيوتر المذكور.

مقتبس من التقرير التفسيري:

293. ناقش القائمون على صياغة الاتفاقية بشكل مستفيض مسألة متى يُسمح 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 32 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 3 من المادة 39 على أن الحالات الأخرى ليست لا مرخصة ولا مستبعدة.

294. تتناول المادة 32 (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.

تفسير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية للمادة 32 من اتفاقية بودابست

فيما يتعلق بالمادة 32 (ألف) (النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة ومتاحة للعموم (مفتوحة المصدر)، لم تتم إثارة أي مسائل محددة وبالتالي، لا حاجة إلى مزيد من التوجيه من قبل المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية في هذه المرحلة.

ومن المفهوم عموما أن الموظفين المكلفين بإنفاذ القانون يمكنهم الولوج إلى أي بيانات يمكن للجمهور النفاذ إليها، ولهذا الغرض يمكنهم الاشتراك في الخدمات المتاحة للجمهور أو التسجيل فيها.[43]

وإذا كان جزء من موقع إلكتروني عام أو خدمة عامة أو ما شابه ذلك مغلقا للجمهور، فإنه لا يعتبر متاحا للجمهور بالمعنى المقصود في المادة 32 (ألف).

وبخصوص المادة 32 (باء)، يمكن أن تشمل الحالات النموذجية ما يلي:

- يمكن أن يكون البريد الإلكتروني لشخص ما مخزنا في بلد آخر من قبل مزود الخدمة، أو أن يقوم شخص عمدا بتخزين بيانات في بلد آخر. ويجوز لهؤلاء الأشخاص استرجاع البيانات، ويجوز لهم، شريطة توفرهم على السلطة القانونية، أن يكشفوا طوعا عن البيانات إلى الموظفين المكلفين بإنفاذ القانون أو أن يسمحوا لهؤلاء الموظفين بالنفاذ إلى البيانات، على النحو المنصوص عليه في المادة.[44]
- عند إلقاء القبض على تاجر مخدرات بشكل قانوني ويكون علبة بريده الإلكتروني – تحتوي ربما على دليل على جريمة - مفتوحة على لوحته، أو هاتفه الذكي أو جهاز آخر. وإذا وافق المشتبه به طوعا على نفاذ الشرطة إلى الحساب وإذا كانت الشرطة على يقين من أن بيانات علبة البريد الإلكتروني موجودة في طرف آخر، يجوز للشرطة النفاذ إلى البيانات بموجب المادة 32.ب.

43. ومع ذلك، يمكن للقانون الوطني أن يحد من نفاذ سلطات إنفاذ القانون إلى البيانات المتاحة للعموم أو من استخدامهم لها.
44. الفقرة 294 من التقرير التفسيري.

ولا تعتبر الحالات الأخرى مرخصة ولا محظورة.[45]

وبخصوص المادة 32 (باء) (النفاذ العابر للحدود مع الموافقة)، تتقاسم اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) الفهم المشترك التالي:

الاعتبارات العامة والضمانات

المادة 32 (باء) تدبير يجب تطبيقه في التحقيقات والإجراءات الجنائية الخاصة في نطاق المادة 14.[46]

وكما هو مبين أعلاه، يفترض أن الأطراف في الاتفاقية تشكل مجتمعا من الثقة وأن مبادئ سيادة القانون وحقوق الإنسان تحترم وفقا للمادة 15 من اتفاقية بودابست.[47]

يجب مراعاة حقوق الأفراد ومصالح الأطراف الثالثة عند تطبيق هذا التدبير.

لذلك، يجوز للطرف الباحث النظر في تبليغ السلطات ذات الصلة في الطرف الذي يجري فيه البحث.

بخصوص مفهوم "العابر للحدود" و"الموقع"

يقصد بالنفاذ العابر للحدود "النفاذ من جانب واحد إلى بيانات الكمبيوتر المخزنة في طرف آخر دون التماس المساعدة المتبادلة".[48]

يمكن تطبيق التدبير بين الأطراف.

تشير المادة 32 (باء) إلى "بيانات الكومبيوتر المُخزنة المتواجدة في طرف آخر". وهذا يعني أنه يجوز استخدام المادة 32 (باء) إذا كان موقع تخزين البيانات معروفا.

ولا تغطي المادة 32 (باء) الحالات التي لا يتم فيها تخزين البيانات في طرف آخر أو عندما يكون موقع البيانات غير مؤكد. ولا يجوز لأي طرف استخدام المادة 32 (باء) للحصول على الكشف عن بيانات مخزنة محليا.

المادة 32 (باء) "لا ترخص، ولا تمنع" حالات أخرى. وهكذا، في الحالات التي لا يعرف أو لا يكون من المؤكد فيها ما إذا كانت البيانات مخزنة في طرف آخر، قد تحتاج الأطراف إلى أن تقيم بنفسها شرعية البحث أو أي نوع آخر من النفاذ في ضوء القانون المحلي، أو مبادئ القانون الدولي ذات الصلة أو اعتبارات العلاقات الدولية.

بخصوص مفهوم "النفاذ دون ترخيص الطرف الآخر"

45. الفقرة 294 من التقرير التفسيري. راجع أيضا المادة 39.3 من اتفاقية بودابست.
46. المادة 14 – نطاق الأحكام الإجرائية.
47. المادة 15 – السؤوط والضمانات.
48. الفقرة 293 من التقرير التفسيري لاتفاقية بودابست.

لا تتطلب المادة 32 (باء) المساعدة المتبادلة، كما أن اتفاقية بودابست لا تتطلب إشعار الطرف الآخر. وفي الوقت ذاته، لا تستبعد اتفاقية بودابست الإشعار. وبالتالي، يجوز للأطراف إشعار الطرف الآخر إذا رأت ذلك مناسبا.

بخصوص مفهوم "الموافقة"

تنص المادة 32 (باء) على أن الموافقة يجب أن تكون قانونية وطوعية بمعنى أن الشخص الذي يوفر النفاذ إلى البيانات أو يقبل بالكشف عنها لا يجوز أن يكون مجبرا أو مخدوعا.[49]

رهنا بالتشريعات المحلية، قد لا يكون الشخص القاصر أو الأشخاص الذين يعانون من اضطرابات الصحة العقلية أو غيرها قادرين على إعطاء الموافقة.

وفي معظم الأطراف، يتطلب التعاون في إجراء تحقيق جنائي الموافقة الصريحة. على سبيل المثال، قد لا تشكل الموافقة العامة لشخص على شروط وأحكام خدمة مستعملة على الإنترنت، موافقة صريحة حتى لو كانت تلك الشروط والأحكام تشير إلى إمكانية تقاسم البيانات مع سلطات العدالة الجنائية في حالات الشطط في الاستعمال.

بخصوص القانون واجب التطبيق

في جميع الحالات، يجب على سلطات إنفاذ القانون تطبيق نفس المعايير القانونية بموجب المادة 32 (باء) بالطريقة ذاتها التي يطبقونها محليا. وإذا كان النفاذ إلى البيانات أو الكشف عنها غير مرخص محليا، فإنه لن يكون مسموحا به أيضا بموجب المادة 32 (باء).

يفترض أن الأطراف في الاتفاقية تشكل مجتمعا من الثقة وأن مبادئ سيادة القانون وحقوق الإنسان تحترم وفقا للمادة 15 من اتفاقية بودابست.

بخصوص الشخص الذي يمكنه توفير النفاذ إلى البيانات أو الكشف عنها

بخصوص "من هو" الشخص "المرخص له قانونيا" بالكشف عن البيانات، قد يختلف الوضع حسب الظروف والقوانين واللوائح المعمول بها.

على سبيل المثال، قد يتعلق الأمر بشخص طبيعي، يوفر إمكانية النفاذ إلى حساب البريد الإلكتروني الخاص به أو غيره من البيانات التي خزنها في الخارج.[50]

وقد يتعلق الأمر أيضا بشخص اعتباري.

---

49. في بعض البلدان، يشكل قبول تفادي التهم الجنائية أو العقوبة الحبسية أو تخفيفهما موافقة قانونية وطوعية.
50. راجع المثال الوارد في الفقرة 294 من التقرير التفسيري.

ومن غير المرجح أن يكون مقدمو الخدمات قادرين على توفير الموافقة، بصورة صحيحة وطوعية، على الكشف عن بيانات مستخدميهم بموجب المادة 32. وعادة ما يكون مقدمو الخدمات وصيين على هذه البيانات فقط؛ فهم لا يتحكمون في البيانات ولا يملكونها، وبالتالي لن يكونوا في وضع يسمح لهم بإعطاء الموافقة. وبطبيعة الحال، قد تكون وكالات إنفاذ القانون قادرة على الحصول على البيانات عبر الحدود الوطنية بطرق أخرى، من قبيل المساعدة القانونية المتبادلة أو إجراءات حالات الطوارئ.

الطلبات القانونية المحلية مقابل المادة 32 (باء)

المادة 32 (باء) ليست ذات صلة بالأوامر المحلية بإبراز البيانات أو الطلبات القانونية المماثلة الداخلية للطرف.

بخصوص موقع الشخص الذي يوافق على توفير النفاذ إلى البيانات أو الكشف عنها

الفرضية المعيارية هي أن الشخص الذي يوفر إمكانية النفاذ إلى البيانات موجود فعليا في إقليم الطرف مقدم الطلب.

ومع ذلك، ثمة حالات متعددة ممكنة. يمكن التصور أن الشخص الطبيعي أو الاعتباري موجود في إقليم سلطة إنفاذ القانون مقدمة الطلب عندما يوافق على الكشف عن بيانات أو يوفر النفاذ الفعلي إليها، أو فقط عندما يوافق على الكشف ولكن ليس عند توفير النفاذ إليها، أو يكون الشخص موجودا في البلد حيث يتم تخزين البيانات عند الموافقة على الكشف عن البيانات و/أو توفير النفاذ إليها. ويمكن أن يكون الشخص أيضا موجودا فعليا في بلد ثالث عندما يوافق على التعاون أو عندما يوفر فعلا إمكانية النفاذ إلى البيانات. وإذا كان الشخص شخصا اعتباريا (كمؤسسة من القطاع الخاص)، يجوز تمثيل هذا الشخص في إقليم سلطة إنفاذ القانون مقدمة الطلب أو الإقليم الذي يستضيف البيانات أو حتى في بلد ثالث في نفس الوقت.

وينبغي أن يؤخذ في الاعتبار أن العديد من الأطراف قد تعترض – بل يعتبر بعضها جريمة جنائية – إذا اقتربت سلطات أجنبية لإنفاذ القانون مباشرة من شخص موجود فعليا في إقليمها للحصول على تعاونه معها.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن ما ورد أعلاه يمثل الفهم المشترك للأطراف فيما يتعلق بنطاق المادة 32 والعناصر المكونة لها.

المذكرة التوجيهية 8# بشأن البريد الإلكتروني غير المرغوب فيه (Spam)[51]

المقدمة

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[52].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة مسألة البريد الإلكتروني غير المرغوب فيه (spam).

إن اتفاقية بودابست " تستخدم لغة محايدة من الناحية الفنية بحيث يمكن تطبيق جرائم القانون الموضوعي الجنائي على التكنولوجيات الحالية والمستقبلية المعنية "[53]، وذلك بغية ضمان أن الاتفاقية تشمل الأشكال الجديدة للبرمجيات الخبيثة أو الجرائم.

وتبين هذه المذكرة التوجيهية كيف تنطبق مواد مختلفة من الاتفاقية على البريد الإلكتروني غير المرغوب فيه (spam).

الأحكام ذات الصلة في اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية 185)

غالبا ما يتم تعريف البريد الإلكتروني غير المرغوب فيه على أنه بريد إلكتروني بالجملة مزعج، حيث يتم إرسال رسالة إلى عدد كبير من عناوين البريد الإلكتروني، لا تكون فيها الهوية الشخصية للمتلقي ذات صلة لأن الرسالة تستهدف بالتساوي العديد من المتلقين الآخرين دون تمييز.

وثمة مسائل منفصلة تتعلق بما يلي:

– محتوى البريد الإلكتروني غير المرغوب فيه،

51. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام الثاني عشر (3-2 ديسمبر/كانون الأول 2014)
52. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
53. الفقرة 36 من التقرير التفسيري.

- فعل إرسال البريد الإلكتروني غير المرغوب فيه، و
- الآلية المستخدمة لنقل البريد الإلكتروني غير المرغوب فيه.

قد يكون أو لا يكون محتوى البريد الإلكتروني غير المرغوب فيه غير قانوني، وحيثما يكون المحتوى غير قانوني (من قبيل عرض أدوية مزيفة أو عروض مالية مزورة)، قد تقع الجريمة تحت طائلة التشريعات الوطنية ذات الصلة بالنسبة لتلك الجرائم. وقد يكون فعل نقل البريد الإلكتروني غير المرغوب فيه (بما في ذلك إرسال محتوى غير مقبول بالجملة) جريمة مدنية أو جنائية بحسب الولايات القضائية.

ولا تغطي الاتفاقية البريد الإلكتروني غير المرغوب فيه الذي تكون محتوياتها غير قانونية ولا يسبب تدخلا في النظام، وإن كان مصدر إزعاج للمستعملين النهائيين.

قد تكون الأدوات المستخدمة في نقل البريد الإلكتروني غير المرغوب فيه غير قانونية بموجب اتفاقية بودابست، كما يمكن أن يرتبط البريد الإلكتروني غير المرغوب فيه بجرائم أخرى غير مدرجة في المصفوفة أدناه (انظر، على سبيل المثال، المادة 7).

وكما هو الحال بالنسبة للمذكرات التوجيهية الأخرى، يتضمن كل مقتضى معيار النية ("عن غير حق"، "بنية الاحتيال"، إلخ.). وفي بعض حالات البريد غير المرغوب فيه، قد يكون من الصعب إثبات هذه النية.

تفسير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية للأحكام التي تتناول البريد الإلكتروني غير المرغوب فيه.

المواد ذات الصلة	أمثلة
المادة 2 – النفاذ غير القانوني	قد يتضمن البريد الإلكتروني غير المرغوب فيه برمجية خبيثة يمكنها النفاذ إلى نظام الكمبيوتر أو المساعدة في النفاذ إليه.
المادة 3 – الاعتراض غير القانوني	قد يتضمن البريد الإلكتروني غير المرغوب فيه برمجية خبيثة من شأنها الاعتراض غير القانوني لإرسال بيانات الكمبيوتر أو المساعدة على ذلك.
المادة 4 – التدخل في البيانات	قد يتضمن البريد الإلكتروني غير المرغوب فيه برمجية خبيثة من شأنها أن تؤدي إلى إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.
المادة 5 – التدخل في النظام	قد يؤدي إرسال بريد إلكتروني غير مرغوب فيه إلى عرقلة اشتغال أنظمة الكمبيوتر بشكل خطير. وقد يتضمن البريد الإلكتروني غير المرغوب فيه برمجية خبيثة يعوق بشكل هام اشتغال أنظمة الكمبيوتر.

المواد ذات الصلة	أمثلة
المادة 6 – إساءة استخدام الأجهزة	يمكن استخدام الأجهزة بالمعنى الوارد في المادة 6 من أجل إرسال بريد إلكتروني غير مرغوب فيه. وقد يتضمن البريد الإلكتروني غير المرغوب فيه أجهزة بالمعنى الوارد في المادة 6.
المادة 8 – الاحتيال المرتبط بالكمبيوتر	يمكن استخدام البريد الإلكتروني غير المرغوب فيه كجهاز من أجل إدخال، تغيير، أو حذف أو إتلاف بيانات الكمبيوتر أو التدخل في وظيفة نظام الكمبيوتر بغية تحقيق منفعة اقتصادية غير قانونية.
المادة 10 – الجرائم المتعلقة بانتهاكات حقوق النشر	يمكن استخدام البريد الإلكتروني غير المرغوب فيه من أجل الدعاية لبيع سلع مزيفة، بما في ذلك البرمجيات وغيرها من المواد المحمية بحقوق النشر.
المادة 11 – المحاولة، المساعدة والتحريض	يمكن استخدام البريد الإلكتروني غير المرغوب فيه أو إرساله من أجل محاولة ارتكاب جرائم محددة في الاتفاقية أو المساعدة على ارتكابها أو التحريض على ارتكابها (كما هو وارد في المادة 7 بشأن التزوير المرتبط بالكمبيوتر أو المادة 8 بشأن الاحتيال المرتبط بالكمبيوتر).
المادة 13 – العقوبات	قد يخدم البريد الإلكتروني غير المرغوب فيه أغراضا إجرامية متعددة، يسبب بعضها أضرارا جسيمة للأفراد أو مؤسسات القطاع العام أو الخاص. حتى إن لم يجرم طرف البريد الإلكتروني غير المرغوب فيه في حد ذاته، يتعين عليه تجريم البريد الإلكتروني غير المرغوب فيه المرتبط بسلوك من قبيل الجرائم المشار إليها أعلاه كما يجوز له النظر في ظروف تشديد العقوبة. ينبغي للدول الأطراف أن تضمن، عملا بالمادة 13، أن الجرائم ذات الصلة بالبريد الإلكتروني غير المرغوب فيه " مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية". وقد يشمل ذلك بالنسبة للأشخاص الاعتباريين عقوبات جنائية أو غير جنائية، بما في ذلك العقوبات المالية.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تبين قائمة المواد أعلاه الاستخدام الإجرامي متعدد الوظائف للبريد الإلكتروني غير المرغوب فيه والجرائم ذات الصلة به.

لذلك، تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) أن اتفاقية بودابست تشمل هذه الجوانب المرتبطة بالبريد الإلكتروني غير المرغوب فيه.

المذكرة التوجيهية 10# بشأن أوامر إبراز البيانات للحصول على معلومات عن المشترك (المادة 18 من اتفاقية بودابست)[54]

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[55].

ولئن كانت المذكرات التوجيهية غير إلزامية، فإنها تمثل الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة[56] مسألة أوامر إبراز البيانات للحصول على معلومات عن المشترك بموجب المادة 18، أي الحالات التي يكون فيها:

- الشخص الذي صدر في حقه أمر تقديم بيانات كمبيوتر محددة متواجدا في إقليم الطرف (المادة 1.18.ألف)[57]؛
- مزود الخدمة الذي صدر في حقه أمر تقديم معلومات حول المشترك يعرض خدماته داخل أراضي الدولة الطرف دون أن يكون متواجدا بالضرورة في أقاليمها (المادة 1.18.باء).

تعتبر مذكرة توجيهية بشأن هذه الجوانب من المادة 18 ذات صلة نظرا لأن:

- المعلومات حول المشترك غالبا ما يتم البحث عنها في التحقيقات الجنائية؛
- المادة 18 تعتبر سلطة داخلية؛
- تنامي الحوسبة السحابية وتخزين البيانات عن بعد طرح العديد من التحديات على السلطات المختصة التي تسعى إلى النفاذ إلى بيانات حاسوبية محددة – و، بالتحديد، إلى معلومات عن المشترك – من أجل المضي قدما في التحقيقات والمتابعات الجنائية؛

54. المعتمدة من قبل اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية خلال اجتماعها العام السادس عشر بإجراء كتابي (28 فبراير/ شباط 2014)
55. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).
56. تستند هذه المذكرة التوجيهية إلى عمل المجموعة المختصة بالأدلة على الحوسبة السحابية التابعة للجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية.
57. من الأهمية بمكان التذكير أن المادة 1.18.أ من اتفاقية بودابست لا تقتصر على المعلومات حول المشترك بل تخص أي نوع من بيانات الكمبيوتر المحددة. ومع ذلك، تعالج هذه المذكرة التوجيهية تقديم المعلومات بشأن المشترك فقط.

- الممارسات والإجراءات، علاوة على الشروط والضمانات للنفاذ إلى معلومات عن المشترك تختلف حاليا بشكل هام بين الأطراف في الاتفاقية؛
- الهواجس المرتبطة بالخصوصية وحماية البيانات الشخصية والأساس القانوني للولاية القضائية ذات الصلة بالخدمات المقدمة في أراضي الطرف دون استقرار مقدم الخدمة في تلك الأراضي، علاوة على النفاذ إلى البيانات المخزنة في الولايات القضائية الأجنبية أو في مواقع غير معروفة أو متعددة "على الحواسيب السحابية" تحتاج إلى المعالجة.

وتثير خدمة وقابلية إعمال أوامر إبراز البيانات المحلية ضد مقدمي الخدمات المسجلين خارج إقليم دولة طرف مسائل أخرى لا يمكن معالجتها بشكل كامل في مذكرة توجيهية. وقد تطالب بعض الأطراف أن يتم طلب معلومات عن المشترك من خلال المساعدة القانونية المتبادلة.

وتعتبر المادة 18 تدبيرا يجب تطبيقه في التحقيقات والإجراءات الجنائية المحددة في نطاق المادة 14 من اتفاقية بودابست. وهكذا، تصدر الأوامر في حالات خاصة فيما يتعلق بمشتركين محددين.

المادة 18 من اتفاقية بودابيست

نص أحكام المادة

المادة 18 – الأمر بإبراز البيانات

1. تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من إصدار أمر إلى:

أ. أي شخص داخل أراضيها بتقديم بيانات كمبيوتر محددة بحوزة ذلك الشخص أو تحت سيطرته، ومخزنة على نظام الكومبيوتر أو على أي دعامة أخرى لتخزين بيانات الكمبيوتر.

ب. أي مزود خدمة يعرض خدماته داخل أراضي الدولة الطرف بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته.

مقتبس من التقرير التفسيري:

173. ينبغي على الدولة الطرف، بموجب الفقرة 1(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 1(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 1(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.[58]

ماذا يقصد بعبارة " معلومات عن المشترك"؟

ورد تعريف مصطلح "معلومات عن المشترك" في المادة 3.18 من اتفاقية بودابست:

3 لغرض هذه المادة، يقصد بعبارة "معلومات عن المشترك" أي معلومات مدرجة في شكل بيانات الكومبيوتر أو في أي شكل آخر يحفظها مزود الخدمة والتي تتعلق بالمشتركين في الخدمات التي يزودها بخلاف بيانات الحركة أو المضمون والتي بموجبها يمكن تحديد:

أ. نوع خدمة الاتصال المستخدمة والشروط الفنية المرتبطة بها ومدة الخدمة؛

ب. هوية المشترك، وعنوانه البريدي أو الجغرافي، ورقم هاتفه وغيره من أرقام الولوج، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق أو ترتيبات الخدمة؛

ج. أي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصال والمتاحة بموجب اتفاق أو ترتيبات الخدمة.

علاوة على ذلك، تشير الفقرة من التقرير التفسيري إلى:

177. يرد تعريف "المعلومات عن المنخرط" في الفقرة 3. 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.

58. الفقرة 173 من التقرير التفسيري.

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.

يمكن أن يمثل الحصول على معلومات عن المشترك تدخلا أقلا في حقوق الأفراد من الحصول على بيانات الحركة أو بيانات المحتوى.

من هو "مقدم الخدمة"؟

تطبق اتفاقية بودابست بشأن الجريمة الإلكترونية مفهوما واسعا لمصطلح "مقدم الخدمة" الذي تعرفه المادة الأولى (جيم) من اتفاقية بودابست.

لأغراض هذه الاتفاقية:

ج. يُقصد بـــــ "مُقدم الخدمة"

1. أي كيان عام أو خاص يقدم لمستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوتر، و
2. أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة.

يجب تطبيق المادة 1.18(باء) فيما يتعلق بمقدم الخدمة الذي يعرض خدماته في أراضي الدولة الطرف.[59]

تفسير اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية للمادة 18 من اتفاقية بودابست بخصوص المعلومات عن المشترك

نطاق المادة 1.18 (ألف)

- النطاق واسع: "شخص" (الذي قد يتضمن "مقدم الخدمة") موجود في إقليم الطرف.
- فيما يتعلق ببيانات الكمبيوتر، يعتبر النطاق واسعا ولكن ليس عشوائيا: أي بيانات كمبيوتر[60] "محددة" (ومن هنا لا تقتصر المادة 18.1 (ألف) على "معلومات المشترك" وتغطي جميع أنواع بيانات الكمبيوتر).

59. تمنح صكوك الاتحاد الأوروبي بني مقدمي خدمات الاتصالات الإلكترونية ومقدمي خدمات مجتمع الإنترنت. ويشمل مفهوم "مقدم الخدمة" الوارد في المادة 1 (ج) من اتفاقية بودابست كليهما.
60. "الشخص" مفهوم أوسع من "مقدم الخدمة"، وإن كان من الممكن أن يكون "مقدم الخدمة" "شخصا".

- بيانات الكمبيوتر المحددة موجودة في حيازة ذلك الشخص، أو إذا لم يتوفر الشخص على حيازة فعلية، فإن هذا الشخص يتحكم بحرية في بيانات الكمبيوتر التي يجب تقديمها بموجب المادة 1.18 (ألف) من داخل إقليم الطرف.
- بيانات الكمبيوتر المحددة مخزنة على نظام كمبيوتر أو على دعامة لتخزين بيانات الكمبيوتر.
- أمر إبراز البيانات يصدر وينفذ من قبل السلطات المختصة في الطرف الذي يطلب فيه الأمر ويمنحه.

نطاق المادة 1.18 (باء)

نطاق المادة 1.18 (باء) أضيق من نطاق المادة 18.1 (ألف):

- يقتصر القسم الفرعي (باء) على "مقدم الخدمة".[61]
- مقدم الخدمة الذي صدر في حقه الأمر لا يوجد بالضرورة في إقليم الطرف، لكنه يقدم خدماته في ذلك الإقليم.
- يقتصر القسم على "معلومات عن المشترك".
- تتعلق المعلومات عن المشترك بهذه الخدمات وهي في حيازة مقدم الخدمة أو تحت سيطرته.

وعلى النقيض من المادة 1.18 (ألف) الذي يقيد نطاق تطبيقه على "الأشخاص الموجودين على أراضي الطرف"، فإن الفقرة الفرعية 1.18 (باء) لا تلتزم بمسألة موقع مقدم الخدمة. ويجوز للأطراف أن تطبق المقتضى في الظروف التي لا يكون فيها مقدم الخدمة الذي يقدم خدماته في إقليم الطرف موجودا قانونيا أو ماديا داخل الإقليم.

الولاية القضائية

تقتصر المادة 1.18 (باء) على الظروف التي يكون فيها لسلطة العدالة الجنائية التي تصدر أمر إبراز البيانات اختصاص على الجريمة.

وقد يشمل ذلك الحالات التي يكون فيها المشترك مقيما أو موجودا، حاليا أو سابقا، في ذلك الإقليم عند ارتكاب الجريمة.

ولا يخل التفسير الحالي للمادة 18 بسلطات أوسع أو إضافية بموجب القانون المحلي للأطراف.

61. الفقرة 172 من التقرير التفسيري.

ولا ينطوي الاتفاق على هذه المذكرة التوجيهية على الموافقة على خدمة أو تنفيذ أمر محلي بإبراز البيانات صادر عن دولة أخرى خارج نطاق الولاية الإقليمية ولا يخلق التزامات أو علاقات جديدة بين الأطراف.

ما هي خصائص "أمر إبراز البيانات؟"

يعتبر "أمر إبراز البيانات" بموجب المادة 18 تدبيرا محليا، ويجب أن ينص عليه القانون الجنائي المحلي. ويتقيد "أمر إبراز البيانات" بالولاية القضائية والتنفيذية للطرف الذي يمنح فيه الأمر.

وتشير أوامر إبراز البيانات بموجب المادة 18 إلى ما يلي:

بيانات الكمبيوتر أو معلومات عن المشترك التي توجد في حوزة شخص أو مقدم خدمة أو تحت سيطرته. 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.[62]

ويشير التقرير التفسيري لاتفاقية بودابست[63] إلى أوامر التقديم كتدبر مرن أقل تطفلا من عمليات البحث أو المصادرة أو أي سلطات قسرية أخرى، كما ينص على ما يلي:

ولعل تنفيذ هذه الآلية الإجرائية من شأنه أن يكون مفيدا أيضا للأطراف الثالثة الوديعة للبيانات، مثل مقدمي خدمات الإنترنت (ISPs)، 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.

كيف يؤثر موقع البيانات؟

لا يمنع تخزين المعلومات عن المشترك في ولاية قضائية أخرى من تطبيق المادة 18 من اتفاقية بودابست ما دامت تلك البيانات في حيازة مقدم الخدمة أو تحت سيطرته. وينص التقرير التفسيري فيما يتعلق بما يلي:

- المادة 1.18 (ألف)، يشير 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.[64]

62. الفقرة 172 من التقرير التفسيري.
63. الفقرة 171 من التقرير التفسيري.
64. الفقرة 173 من التقرير التفسيري. يمكن أن يكون "الشخص" بموجب المادة 1.18 (ألف) من اتفاقية بودابست، شخصا طبيعيا أو معنويا، بما في ذلك مقدم الخدمة.

- المادة 1.18 (باء)، 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) .[65]

وفيما يتعلق بالمادة 1.18 (باء)، قد ينطوي الوضع على مقدم خدمة يقع مقره الرئيسي في ولاية قضائية معينة، لكنه يخزن البيانات في ولاية قضائية أخرى. وقد تنعكس البيانات أيضا في العديد من الولايات القضائية أو تنتقل بين الولايات القضائية وفقا لحرية تصرف مقدم الخدمة ودون معرفة المشترك أو مراقبته. وباتت الأنظمة القانونية تعترف بشكل متزايد أن موقع البيانات، في مجال العدالة الجنائية وفي مجال خصوصية وحماية البيانات على حد سواء، ليس هو العامل المحدد لإنشاء الولاية القضائية.

ما معنى "تقديم خدماته في إقليم طرف؟"

أثار تنامي الحوسبة السحابية تساؤلات بشأن متى يُعتبر مقدم الخدمة يقدم خدماته في إقليم الطرف وبالتالي يمكن إصدار أمر تقديم محلي في حقه بشأن معلومات عن المنخرط. وقد أدى ذلك إلى مجموعة من التفسيرات في مختلف الولايات القضائية من قبل المحاكم في قضايا مدنية وجنائية على حد سواء.

وفيما يتعلق بالمادة 1.18 (باء)، يمكن للأطراف أن تعتبر أن مقدم الخدمات "يقدم خدماته في إقليم الطرف"، عندما:

- يساعد مقدم الخدمة أشخاصا في إقليم الطرف على الاشتراك في خدماته[66] (ولا يمنع، على سبيل المثال، النفاذ إلى تلك الخدمات)؛

و

- قام مقدم الخدمة بإنشاء اتصال حقيقي وهام لطرف ما. وتشمل العوامل ذات الصلة مدى توجيه مقدم الخدمة لأنشطته نحو هؤلاء المشتركين (على سبيل المثال، من خلال تقديم إعلانات محلية أو إعلانات بلغة إقليم الطرف)، واستخدامه لمعلومات المشترك (أو بيانات الحركة المرتبطة بها) في سياق أنشطته، ومدى تفاعله مع المشتركين في الدولة الطرف، ويمكن خلاف ذلك أن يُعتبر أنه مستقر في إقليم الطرف.

65. الفقرة 173 من التقرير التفسيري.
66. الفقرة 183 من التقرير التفسيري: " 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".

ولا يؤدي مجرد استخدام مقدم الخدمة لاسم ميدان أو عنوان بريد إلكتروني متصل ببلد معين إلى افتراض بأن مقر عمله يوجد في ذلك البلد. لذلك، يمكن اعتبار أنه تم استيفاء الشرط الذي مفاده أن تكون المعلومات عن المشترك الواجب تقديمها متعلقة بالخدمات التي يوفرها مقدم الخدمة في إقليم الطرف، حتى إذا كانت تلك الخدمات تقدم عن طريق اسم ميدان المستوى الأعلى للرمز القطري يشير إلى ولاية قضائية أخرى.

الاعتبارات العامة والضمانات

يفترض أن الأطراف في الاتفاقية تشكل مجتمعا من الثقة وأن مبادئ سيادة القانون وحقوق الإنسان تحترم وفقا للمادة 15 من اتفاقية بودابست.

المادة 15 – الشروط والضمانات

1. تسعى كل دولة طرف إلى ضمان خضوع وضع وتنفيذ وتطبيق السلطات والإجراءات المنصوص عليها في هذا القسم، للضمانات والشروط المنصوص عليها في قانونها الوطني، الذي ينبغي أن يوفر الحماية الملائمة لحقوق الإنسان والحريات، بما في ذلك الحقوق الناشئة عن الالتزامات التي تعهدت بها بموجب اتفاقية مجلس أوروبا لعام 1950 الخاصة بحماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966 الخاص بالحقوق المدنية والسياسية، وغيرها من الصكوك الدولية ذات الصلة بحقوق الإنسان، وأن يدمج مبدأ التناسب.
2. تشمل هذه الشروط والضمانات، حسب الاقتضاء بالنظر لطبيعة الإجراءات أو السلطات المعنية، الإشراف القضائي أو بواسطة أي هيئة مستقلة أخرى، والأسس المبررة للتطبيق، وحدود نطاق تلك الإجراءات أو السلطات ومدتها، من بين أمور أخرى.
3. بقدر ما يتفق مع المصلحة العامة، خاصة الإدارة السليمة للعدالة، يقوم كل طرف بتدارس تأثير السلطات والإجراءات الواردة في هذا القسم على حقوق الأغيار ومسؤولياتهم ومصالحهم المشروعة.

تطبيق المادة 18 بخصوص المعلومات عن المشترك

يمكن، بالتالي، إصدار أمر بتقديم معلومات عن المشترك بموجب المادة 18 من اتفاقية بودابست عند استيفاء المعايير التالية في تحقيق جنائي وبخصوص مشتركين محددين:

إذا كان لسلطة العدالة الجنائية اختصاص على الجريمة؛		
وإذا كانت المعلومات عن المشترك في حيازة مقدم الخدمة أو تحت سيطرته؛		
وإذا		
المادة 1.18 (ألف) كان الشخص (مقدم الخدمة) متواجدا في إقليم الطرف.	أو	المادة 1.18 (باء) اعتبر طرف أن مقدم الخدمة "يعرض خدماته في إقليم الطرف" عندما، على سبيل المثال: – يساعد مقدم الخدمة أشخاصا في إقليم الطرف على الاشتراك في خدماته (ولا يمنع، على سبيل المثال، النفاذ إلى تلك الخدمات)؛ و – قام مقدم الخدمة بإنشاء اتصال حقيقي وهام لطرف ما. وتشمل العوامل ذات الصلة مدى توجيه مقدم الخدمة لأنشطته نحو هؤلاء المشتركين (على سبيل المثال، من خلال تقديم إعلانات محلية أو إعلانات بلغة إقليم الطرف)، واستخدامه لمعلومات المشترك (أو بيانات الحركة المرتبطة بها) في سياق أنشطته، ومدى تفاعله مع المشتركين في الدولة الطرف، ويمكن خلاف ذلك أن يُعتبر أنه مستقر في إقليم الطرف.
وإذا		
		– كانت المعلومات التي يجب تقديمها متعلقة بخدمات يعرضها مقدم خدمة في إقليم الطرف.

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن ما ورد أعلاه يمثل الفهم المشترك للأطراف بشأن نطاق المادة 18 والعناصر المكونة لها فيما يتعلق بتقديم معلومات عن المشترك.

المذكرة التوجيهية 11# بشأن الإرهاب

قررت اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (T-CY) خلال اجتماعها العام الثامن (ديسمبر/كانون الأول 2012) إصدار مذكرات توجيهية بغرض تيسير الاستعمال والتنفيذ الفعلي لاتفاقية بودابست بشأن الجريمة الإلكترونية على ضوء التطورات القانونية، والسياسية والتكنولوجية[67].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة بشأن استخدام الاتفاقية.

وتتناول هذه المذكرة كيف تنطبق مواد مختلفة من الاتفاقية على الإرهاب.

تعتبر الكثير من البلدان أطرافا في العديد من المعاهدات، وتخضع لقرارات مجلس الأمن للأمم المتحدة التي تتطلب تجريم مختلف أشكال الإرهاب، وتيسير الإرهاب، ودعم الإرهاب، والأعمال التحضيرية. وفي حالات الإرهاب، كثيرا ما تعتمد البلدان على جرائم مستمدة من تلك المعاهدات الموضوعاتية الخاصة، علاوة على جرائم إضافية في التشريعات الوطنية.

وليست اتفاقية بودابست معاهدة تركز تحديدا على الإرهاب. ومع ذلك، فإن الجرائم الموضوعية في الاتفاقية يمكن أن تنفذ بوصفها أعمالا إرهابية، وأعمالا لتيسير ودعم الإرهاب، بما في ذلك ماليا، أو أعمالا تحضيرية.

بالإضافة إلى ذلك، تعتبر أدوات المساعدة القانونية المتبادلة الإجرائية والدولية الواردة في الاتفاقية متاحة بالنسبة لقضايا الإرهاب والتحقيقات والملاحقات القضائية المتصلة بالإرهاب.

وتعرف المادتان 2.14 و1.25 من اتفاقية بودابست النطاق والحدود:

المادة 2.14

2. باستثناء ما هو منصوص عليه تحديدا خلاف ذلك في المادة 21، تطبق كل دولة طرف السلطات والإجراءات المشار إليها في الفقرة 1 من هذه المادة على:

أ. الجرائم الجنائية المقررة في المواد من 2 إلى 11 من هذه الاتفاقية؛

ب. الجرائم الجنائية الأخرى التي يتم ارتكابها بواسطة نظام الكومبيوتر؛ و

ج. جمع الأدلة الخاصة بجريمة جنائية بشكل إلكتروني.

67. راجع اختصاص اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابيست).

المادة 1.25

"توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن لأغراض التحقيقات أو المتابعات المتعلقة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر أو بجمع أدلة جريمة جنائية في شكل إلكتروني."

راجع أيضا المادتين 23 و1.27 من اتفاقية بودابست علاوة على المذكرات التوجيهية الأخرى، من قبيل المذكرات التوجيهية بشأن الهجمات على البنى التحتية الحيوية أو هجمات حجب الخدمة الموزعة.

الأحكام ذات الصلة في اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية 185)

الأحكام الإجرائية

يمكن استخدام الصلاحيات الإجرائية للاتفاقية (المواد 14-21) في تحقيق أو إجراء جنائي محدد في أي نوع من الحالات، كما تنص على ذلك المادة 14.

وفي الواقع، يمكن أن تكون التدابير الإجرائية المحددة مفيدة جدا، على سبيل المثال في حالات الإرهاب، إذا ما استخدم نظام كمبيوتر لارتكاب الجريمة أو تيسيرها، أو إذا كانت الأدلة على تلك الجريمة مخزنة في شكل إلكتروني أو إذا أمكن تحديد هوية المشتبه فيه من خلال المعلومات عن المشترك، بما في ذلك عنوان بروتوكول الإنترنت. وهكذا، يجوز للأطراف، في حالات الإرهاب، أن تلجأ إلى التعجيل بحفظ بيانات الكمبيوتر المخزنة، وأوامر التقديم، والبحث عن بيانات الكمبيوتر المخزنة ومصادرتها، وغيرها من الأدوات من أجل جمع الأدلة الإلكترونية في قضايا الإرهاب وفي التحقيقات والملاحقات المتصلة بالإرهاب ضمن النطاق المبين أعلاه.

أحكام المساعدة القانونية المتبادلة الدولية

يعتبر نطاق صلاحيات التعاون الدولي للاتفاقية (المواد 23-35) مماثلا.

ومن ثم، وجب على الأطراف أن تتيح التعجيل بحفظ بيانات الكمبيوتر المخزنة، وأوامر التقديم، والبحث عن بيانات الكمبيوتر المخزنة ومصادرتها، وغيرها من الأدوات، فضلا عن أحكام التعاون الدولي الأخرى، من أجل التعاون مع أطراف أخرى في تحقيقات وملاحقات قضائية ذات الصلة بالإرهاب، ضمن النطاق المبين أعلاه.

أحكام القانون الجنائي الموضوعي

وفي الأخير، وكما تمت الإشارة إلى ذلك أعلاه، يمكن للإرهابيين والجماعات الإرهابية الاضطلاع بأعمال تجرمها الاتفاقية في إطار تحقيق أهدافهم.

المواد ذات الصلة	أمثلة
المادة 2 – النفاذ غير المشروع	يمكن النفاذ إلى نظام كمبيوتر بشكل غير قانوني من أجل الحصول على معلومات يمكن التعرف على هوية أصحابها شخصياً (مثلا، معلومات عن موظفين حكوميين من أجل استهدافهم بالهجمة).
المادة 3 – الاعتراض غير المشروع	يمكن الاعتراض بشك غير قانوني للإرسال غير العمومي لبيانات الكومبيوتر إلى أو من أو داخل نظام كومبيوتر من أجل الحصول على معلومات عن موقع شخص (مثلا بغية استهداف ذلك الشخص).
المادة 4 – التدخل في البيانات	يمكن إتلاف أو حذف أو تخريب أو تغيير أو إلغاء بيانات الكمبيوتر (مثلا، يمكن تغيير السجلات الطبية لمستشفى حتى تصبح غير صحيحة بشكل خطير، أو يمكن للتدخل في نظام مراقبة الحركة الجوية أن يؤثر على سلامة الرحلات).
المادة 5 – التدخل في النظام	يمكن عرقلة تشغيل نظام الكمبيوتر لأغراض إرهابية (مثلا عرقلة نظام يخزن سجلات البورصة يمكن أن تجعلها غير دقيقة، أو عرقة تشغيل بنية تحتية حيوية).
المادة 6 – إساءة استخدام الأجهزة	عملية بيع، شراء بغرض الاستخدام، استيراد، توزيع أو إتاحة كلمات المرور للكمبيوتر، رموز الدخول أو أي بيانات مشابهة يمكن من خلالها النفاذ إلى بيانات الكمبيوتر، يمكنها أن تيسر هجمة إرهابية (مثلا، يمكن أن تؤدي إلى إلحاق ضرر بشبكة الطاقة الكهربائية لبلد ما).
المادة 7 – التزوير المرتبط بالكمبيوتر	يمكن إدخال أو تغيير أو حذف أو إتلاف بيانات الكمبيوتر (مثلا، البيانات المستخدمة في جوازات السفر الإلكترونية)، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية.
المادة 8 – الاحتيال المرتبط بالكمبيوتر	يمكن إدخال أو تغيير أو حذف أو إتلاف بيانات الكمبيوتر و/أو يمكن التدخل في اشتغال نظام كمبيوتر بشكل يتسبب في فقدان أشخاص آخرين لممتلكاتهم (مثلا، هجمة على نظام بنكي في بلد ما يمكن أن تؤدي إلى فقدان عدد كبير من الضحايا لممتلكاتهم).
المادة 11 – المحاولة، المساعدة والتحريض	يمكن أن تتعرض الجرائم المحددة في الاتفاقية للمحاولة، والمساعدة أو التحريض من أجل دعم الإرهاب.
المادة 12 – مسؤولية الشركات	يمكن أن ترتكب الجرائم التي تشملها المواد من 2 إلى 11 من الاتفاقية لدعم الإرهاب من قبل أشخاص اعتباريين مسؤولين بموجب المادة 12.

المواد ذات الصلة	أمثلة
المادة 13 – العقوبات	يمكن أن ينشأ عن الجرائم المشمولة بالاتفاقية تهديد بالنسبة للأفراد والمجتمع، خاصة عندما تكون هاته الجرائم موجهة ضد أنظمة تعتبر أساسية لحياتهم اليومية، من قبيل النقل العام، الأنظمة البنكية أو البنية التحتية الاستشفائية. وقد يختلف تأثيرها من بلد إلى آخر بحسب درجة ترابط أنظمتها واعتمادها عليها. ويجوز لدولة طرف أن تنص في قانونها الوطني على عقوبة متساهلة بشكل غير ملائم مع الأعمال المتصلة بالإرهاب ذات الصلة بالمواد من 2 إلى 11، وقد لا تسمح بمراعاة ظروف تشديد العقوبة، المحاولة، المساعدة أو التحريض. وقد يعني ذلك أن الأطراف بحاجة إلى النظر في إدخال تعديلات على قوانينها الوطنية. لذلك، ينبغي للدول الأطراف أن تضمن، عملا بالمادة 13، أن الجرائم الجنائية ذات الصلة بمثل هذه الأعمال " مُعاقب عليها بعقوبات فعالة، متناسبة ورادعة، بما في ذلك العقوبات السالبة للحرية". ويمكن للدول الأطراف أيضا أن تنظر في ظروف تشديد العقوبة، مثلا في حال أثرت أعمال من هذا القبيل على عدد هام من الأنظمة أو تسببت في إلحاق ضرر جسيم، بما في ذلك الوفيات أو الإصابات الجسدية، أو أضرار ببنية تحتية هامة.

فضلا عن ذلك، يمكن أن تنفذ جرائم أخرى تشملها الاتفاقية لكنها لم تُذكر على وجه التحديد أعلاه، بما في ذلك إنتاج مواد تستغل الأطفال أو الاتجار بالملكية الفكرية المسروقة، والتي تكون متصلة بالإرهاب.

وبالنسبة للأطراف في اتفاقية بودابست التي هي أيضا أطراف في البروتوكول الإضافي المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة بواسطة النظم الحاسوبية (سلسلة المعاهدات الأوروبية رقم 189)[68]، ثمة مادتان من البروتوكول ذات الصلة لأنهما تتعلقان بالتشدد والتطرف العنيف الذين قد يؤديان إلى الإرهاب. ويتعلق الأمر بالمادة 4 من البروتوكول التي تشمل التهديد بدوافع العنصرية وكراهية الأجانب، والمادة 6 التي تشمل إنكار الإبادة الجماعية أو الجرائم المرتكبة ضد الإنسانية أو التقليل منها إلى أدنى حد أو إقرارها أو تبريرها.

68. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية أن الجرائم الموضوعية الواردة في الاتفاقية يمكن أن تعتبر أعمالا إرهابية وفقا للتعريف الوارد في القانون واجب التطبيق.

ويمكن أن تنفذ الجرائم الموضوعية الواردة في الاتفاقية من أجل تسهيل الإرهاب ودعمه، بما في ذلك ماليا، أو كأعمال تحضيرية.

يمكن استخدام أدوات المساعدة الإجرائية والقانونية المتبادلة المنصوص عليها في الاتفاقية من أجل التحقيق في أعمال الإرهاب، تيسيرها، دعمها أو الأعمال التحضيرية.

بعض جوانب التدخل في الانتخابات بواسطة أنظمة الكمبيوتر المشمولة باتفاقية بودابست

المقدمة

قررت لجنة اتفاقية الجريمة الإلكترونية (T-CY)، في جلستها العامة الثامنة (ديسمبر/كانون الأول 2012)، إصدار مذكرات توجيهية بهدف تيسير الاستخدام والتنفيذ الفعّالين لاتفاقية بودابست بشأن الجريمة الإلكترونية، في ظل التطورات القانونية والسياسية والتكنولوجية[69].

وتمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة فيما يتعلق باستخدام الاتفاقية.

إن التدخل في الانتخابات، من خلال أنشطة إلكترونية خبيثة ضد أجهزة الكمبيوتر والبيانات المستخدمة في الانتخابات والحملات الانتخابية، يقوض الانتخابات الحرة والنزيهة والنظيفة وكذلك الثقة في الديمقراطية. وقد تلجأ عمليات التضليل الإعلامي، كما حدث بشكل خاص في عام 2016، إلى استخدام أنشطة خبيثة على الإنترنت وقد يكون لها نفس التأثير على الانتخابات. ولعل إجراءات الانتخابات الوطنية تحتاج إلى التأقلم مع مختلف أشكال الواقع في مجتمع المعلومات، كما أن أنظمة الكمبيوتر المستخدمة في الانتخابات والحملات ذات الصلة قد تحتاج إلى أن تكون آمنة بشكل أكبر.

وفي هذا السياق، يلزم بذل المزيد من الجهود من أجل المتابعة القضائية لتدخل من هذا القبيل حيثما يشكل جريمة جنائية: يمكن لاستجابة العدالة الجنائية الفعالة أن تردع التدخل في الانتخابات وأن تطمئن الناخبين فيما يتعلق باستخدام تكنولوجيا المعلومات والاتصال في الانتخابات.

وتتناول هذه المذكرة طريقة تطبيق مواد الاتفاقية على الجوانب المرتبطة بالتدخل في الانتخابات بواسطة أنظمة الكمبيوتر.

يمكن ارتكاب الجرائم الجنائية الموضوعية في الاتفاقية كأفعال ترتبط بالتدخل في الانتخابات أو كأفعال تحضيرية تيسر هذا التدخل.

بالإضافة إلى ذلك، تعتبر الأدوات الإجرائية الوطنية وآليات المساعدة القانونية الدولية المتبادلة للاتفاقية متاحة من أجل تحقيقات ومتابعات قضائية ذات الصلة بالتدخل في الانتخابات. وتحدد المادتان 2.14 و1.25 من اتفاقية بودابست نطاق وحدود السلطات والأدوات الإجرائية للتعاون الدولي:

69. راجع ولاية لجنة اتفاقية الجريمة الإلكترونية (المادة 46، اتفاقية بودابست).

المادة 2.14:

باستثناء ما هو منصوص عليه تحديدا خلاف ذلك في المادة 21، تطبق كل دولة طرف السلطات والإجراءات المشار إليها في الفقرة 1 من هذه الاتفاقية على:

أ. الجرائم الجنائية المقررة في المواد من 2 إلى 11 من هذه الاتفاقية؛

ب. الجرائم الجنائية الأخرى التي يتم ارتكابها بواسطة نظام الكمبيوتر،

ت. جمع الأدلة الخاصة بجريمة جنائية بشكل إلكتروني.

المادة 1.25

توفر الدول الأطراف المساعدة المتبادلة لبعضها البعض على أوسع نطاق ممكن لأغراض التحقيقات أو المتابعات المتعلقة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكمبيوتر أو بجمع أدلة جريمة جنائية في شكل إلكتروني.

فضلا عن ذلك، تخضع السلطات الإجرائية في الاتفاقية لشروط وضمانات المادة 15.

الأحكام ذات الصلة في اتفاقية بودابست بشأن الجريمة الإلكترونية (سلسلة المعاهدات الأوروبية رقم 185)

الأحكام الإجرائية

يجوز استخدام السلطات الإجرائية المنصوص عليها في الاتفاقية (المواد 14-21) في تحقيق أو متابعة جنائية محددة بالنسبة لأي نوع من أنواع التدخل في الانتخابات، كما تنص على ذلك المادة 14.

يمكن أن تكون التدابير الإجرائية المحددة مفيدة للغاية بالنسبة للتحقيقات الجنائية بخصوص تدخل في الانتخابات. على سبيل المثال، في حالات التدخل في الانتخابات، يمكن استخدام نظام الكمبيوتر لارتكاب جريمة أو تسهيل ارتكابها، ويمكن أن يكون الدليل على هذه الجريمة مخزنا في شكل إلكتروني، أو يمكن التعرف على المشتبه به من خلال المعلومات عن المشترك، بما في ذلك عنوان بروتوكول الإنترنت. وبالمثل، يمكن تتبع التمويل السياسي غير القانوني عبر البريد الإلكتروني المحفوظ، والتقاط اتصالات صوتية بين متآمرين بموجب ترخيص بالاعتراض، وتوضيح إساءة استخدام البيانات بواسطة مسارات إلكترونية.

وبالتالي، يجوز للأطراف، في التحقيقات الجنائية بشأن تدخل في انتخابات، أن تلجأ إلى التعجيل بحفظ بيانات الكمبيوتر المخزنة، وأوامر إبراز البيانات، والبحث في بيانات الكمبيوتر المخزنة ومصادرتها، وغيرها من الأدوات لجمع الأدلة الإلكترونية اللازمة للتحقيق في هذه الجرائم المتعلقة بالتدخل في الانتخابات ومتابعتها قضائيا.

أحكام المساعدة القانونية المتبادلة الدولية

تعتبر سلطات التعاون الدولي في الاتفاقية (المواد 23-35) واسعة أيضا وقد تساعد الأطراف في التحقيقات المتعلقة بالتدخل في الانتخابات.

وهكذا، ينبغي للأطراف إتاحة التعجيل بحفظ بيانات الكمبيوتر المخزنة، وأوامر إبراز البيانات، والبحث في بيانات الكمبيوتر المخزنة ومصادرتها، بالإضافة إلى أحكام التعاون الدولي الأخرى.

أحكام القانون الجنائي الموضوعي

وفي الأخير، وكما ورد ذكر ذلك أعلاه، يمكن أن ينطوي التدخل في الانتخابات على أنواع السلوك التالية، عندما يتم ذلك بغير حق، على النحو الذي تجرمه اتفاقية الجريمة الإلكترونية. وتؤكد لجنة اتفاقية الجريمة الإلكترونية على أن الأمثلة الواردة أدناه هي مجرد أمثلة – حيث أن التدخل في الانتخابات ظاهرة ناشئة، وبالتالي يمكن أن يتجلى هذا التصرف في أشكال عديدة غير مدرجة أدناه. ومع ذلك، تتوقع اللجنة أن اتفاقية الجريمة الإلكترونية مرنة بما فيه الكفاية لمعالجة كل هذه الأشكال.

المواد ذات الصلة	أمثلة
المادة 2 – النفاذ غير المشروع	يمكن النفاذ إلى نظام كمبيوتر بطريقة غير مشروعة للحصول على معلومات حساسة وسرية ذات الصلة بمرشحين، حملات، أحزاب سياسية أو ناخبين.
المادة 3 – الاعتراض غير المشروع	يمكن الاعتراض بطريقة غير مشروعة لإرسالات غير عمومية لبيانات الكمبيوتر إلى كمبيوتر آخر أو منه أو داخله، من أجل الحصول على معلومات حساسة وسرية ذات الصلة بمرشحين، حملات، أحزاب سياسية أو ناخبين.
المادة 4 – التدخل في البيانات	يمكن أن تتعرض بيانات الكمبيوتر للإتلاف، الحذف، الإفساد، التعديل أو التدمير بغية تغيير مواقع إلكترونية، أو تغيير قواعد بيانات الناخبين أو التلاعب بنتائج التصويت من قبيل العبث بآلات التصويت.
المادة 5 – التدخل في النظام	يمكن إعاقة اشتغال أنظمة الكمبيوتر المستخدمة في انتخابات أو حملات بغية التدخل في رسائل الحملة، أو عرقلة تسجيل الناخبين، أو الإدلاء بالأصوات أو منع احتساب الأصوات من خلال هجمات حجب الخدمة، أو برمجية خبيثة أو بوسائل أخرى.
المادة 6 – إساءة استخدام الأجهزة	يمكن لعملية بيع، شراء بغرض الاستخدام، توزيع أو إتاحة بأي طرق أخرى لكلمات سر خاصة بالكمبيوتر، أو رموز النفاذ أو بيانات مماثلة يمكن بواسطتها النفاذ إلى أنظمة الكمبيوتر، أن تسهل التدخل في الانتخابات عبر سرقة بيانات حساسة من مرشحين سياسيين، أحزاب سياسية أو حملات سياسة.

المواد ذات الصلة	أمثلة
المادة 7 – التزوير المرتبط بالكمبيوتر	يمكن إدخال، تغيير، حذف، إتلاف أو تدمير بيانات كمبيوتر (على سبيل المثال البيانات المستخدمة في قواعد بيانات الناخبين) بطريقة ينتج عنها اعتبار أو استخدام بيانات غير أصلية لأغراض قانونية وكأنها بيانات أصلية. على سبيل المثال، تشترط بعض الدول أن تقوم الأحزاب السياسية في الحملات الانتخابية بالكشف عن المعلومات المالية للجمهور. ولعل التزوير المرتبط بالكمبيوتر من شأنه أن ينشئ انطباعا بأن المعلومات المقدمة غير صحيحة أو أنها تخفي مصادر مشبوهة لتمويل الحملات.
المادة 11 – المحاولة، المساعدة والتحريض	يمكن محاولة ارتكاب الجرائم المنصوص عليها في الاتفاقية، أو المساعدة أو التحريض على ارتكابها سعيا للتدخل في الانتخابات.
المادة 12 – مسؤولية الشركات	يمكن للجرائم المنصوص عليها في المواد من 2 إلى 11 في الاتفاقية أن ترتكب سعيا للتدخل في الانتخابات من قبل أشخاص اعتباريين مساءلين بموجب المادة 12.
المادة 13 - العقوبات	يمكن أن تشكل الجرائم المشمولة بالاتفاقية تهديدًا على الأفراد والمجتمع ككل، خاصةً عندما تكون الجرائم موجهة ضد أساسيات الحياة السياسية من قبيل الانتخابات. وقد تختلف العمليات الإجرامية وتأثيراتها على اختلاف البلدان، لكن يمكن للتدخل في الانتخابات أن يقوض الثقة في العمليات الديمقراطية، أو أن يغير نتيجة الانتخابات، أو يقتضي عقد انتخابات ثانية مع كل التكاليف والاضطرابات التي قد تترتب عنها، أو أن يتسبب في عنف جسدي بين الأحزاب المشاركة في الانتخابات والمجتمعات المحلية. يجوز لأي طرف في الاتفاقية أن ينص في قانونه الوطني على عقوبة مخففة بشكل غير مناسب للأفعال ذات الصلة بالانتخابات فيما يتعلق بالمواد من 2 إلى 11، وقد لا يسمح بمراعاة الظروف المشددة المتمثلة في المحاولة، المساعدة أو التحريض. وقد يعني ذلك أنه يتعين على الأطراف النظر في إدخال تعديلات على قانونها الوطني. وينبغي للأطراف أن تضمن، بموجب المادة 13، أن الجرائم الجنائية المتعلقة بهذه الأفعال «يعاقب عليها بعقوبات فعالة ومتناسبة ورادعة، تشمل العقوبات السالبة للحرية». يجوز للأطراف أيضًا مراعاة الظروف المشددة، مثلا، إذا كانت هذه الأفعال تؤثر على الانتخابات بشكل هام أو تتسبب في وفيات أو إصابات جسدية أو أضرار مادية جسيمة.

إعلان لجنة اتفاقية الجريمة الإلكترونية

تتفق لجنة اتفاقية الجريمة الإلكترونية (T-CY) على أن الجرائم الموضوعية المنصوص عليها في الاتفاقية قد تشكل أيضًا أفعال تدخل في الانتخابات كما هو محدد في القانون المعمول به، بمعنى جرائم ضد انتخابات حرة ونزيهة ونظيفة.

ويمكن ارتكاب الجرائم الموضوعية المنصوص عليها في الاتفاقية لتسهيل التدخل في أفعال التدخل في الانتخابات، أو المشاركة فيه أو تحضيره.

ويمكن استخدام أدوات المساعدة القانونية والإجرائية المنصوص عليها في الاتفاقية للتحقيق في أفعال التدخل في الانتخابات، تسهيله، المشاركة فيه، أو تحضيره.

المذكرة التوجيهية رقم 12 للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية

جوانب برامج الفدية التي تغطيها اتفاقية بودابست

مقدمة

قررت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية في جلستها العامة الثامنة (ديسمبر 2012) إصدار مذكرات توجيهية تهدف إلى تسهيل الاستخدام والتنفيذ الفعالين للاتفاقية المتعلقة بالجريمة الإلكترونية، وكذلك في ضوء التطورات القانونية والسياساتية والتكنولوجية[70].

تمثل المذكرات التوجيهية الفهم المشترك لأطراف هذه المعاهدة فيما يتعلق باستخدام الاتفاقية.

على مدى عقود، ارتكب الجناة أشكالًا مختلفة من الجرائم الإلكترونية من أجل الابتزاز وطلب الفديات من المنظمات والأفراد. على سبيل المثال، لا تزال السرقة والتهديد اللاحق بالكشف العلني عن البيانات الشخصية أو غيرها من المعلومات الحساسة للإكراه على دفع الفدية سائدة. مع ذلك، ظهرت خلال العقد الماضي أشكال أكثر تعقيدًا من برامج الفدية والجرائم ذات الصلة. يستلزم ذلك تشفير بيانات أو أنظمة الكمبيوتر، وبالتالي حظر المستخدمين، متبوعًا بطلبات الفدية مقابل (الوعد) باستعادة الوصول. قد يهدد الجناة أيضًا بالإفراج عن معلومات حساسة أو شخصية، في محاولة على نحو أكثر فعالية الحصول على مدفوعات من الضحايا.

قد تكون جرائم برامج الفدية هذه ممكنة بسبب سماح التكنولوجيا بما يلي:

- التشفير المحكم لبيانات أو أنظمة الكمبيوتر الخاصة بالضحايا؛
- استخدام أنظمة الاتصال التي يصعب تتبعها لإرسال طلبات دفع الفدية وكذلك أدوات فك التشفير؛
- دفع الفدية بطريقة يصعب تتبعها مثل العملات الافتراضية التي يسهل تعتيمها أكثر من العملات الورقية التقليدية.

أثرت هجمات «WannaCry» و «NotPetya» لعام 2017/2016 على أجهزة الكمبيوتر وجذبت اهتمامًا كبيرًا في جميع أنحاء العالم. أدت جائحة كوفيد 19- اعتبارًا من عام 2020 إلى زيادة اعتماد المجتمعات على تكنولوجيا المعلومات والاتصالات، مما زاد من فرص الاستغلال للأغراض الإجرامية. وقد ساهم ذلك في زيادة جرائم برامج الفدية. وبحسب ما ورد أدت

70. انظر صلاحيات لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية (المادة 46 من اتفاقية بودابست).

الهجمات على أنظمة الكمبيوتر في المستشفيات إلى وفاة المرضى. علاوة على ذلك، تسببت جرائم برامج الفدية الضارة ضد الهياكل الأساسية الحيوية في إعلان حالة طوارئ وطنية في كوستاريكا في أبريل 2022. يعتبر استخدام برامج الفدية الآن شكلاً خطيرًا من الجرائم الالكترونية التي تؤثر على المصالح الأساسية للأفراد والشركات والمجتمعات والحكومات.

لذلك، قررت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية، في جلستها العامة السادسة والعشرين (10-11 مايو 2022)، إعداد مذكرات توجيهية لإظهار كيف يتم تجريم جوانب جرائم برامج الفدية بموجب أحكام القانون الجنائي الموضوعي للاتفاقية المتعلقة بالجريمة الإلكترونية وكيفية يمكن استخدام الصلاحيات الإجرائية وأحكام التعاون الدولي لهذه المعاهدة في التحقيق والملاحقة والتعاون ضد جرائم برامج الفدية.

تشير هذه المذكرات التوجيهية أيضًا إلى البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة معاهدات مجلس أوروبا رقم 224) الذي سيتيح أدوات إضافية «لتعزيز التعاون والكشف عن الأدلة الإلكترونية» للأطراف في هذا البروتوكول بمجرد دخوله حيز التنفيذ.

تظل المذكرات التوجيهية السابقة للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية حول البرامج الضارة وشبكات البوتات وسرقة الهوية والهجمات ضد الهياكل الأساسية الحيوية ذات صلة فيما يتعلق بجرائم برامج الفدية أيضًا.

جرائم برامج الفدية الضارة

برنامج الفدية هو نوع من البرامج الضارة المصممة لمنع وصول المستخدم إلى بيانات الكمبيوتر أو نظام الكمبيوتر الخاص به عن طريق تشفير هذه البيانات أو الأنظمة. ثم يُطلب من المستخدم المستهدف دفع فدية (للوعد) بالولوج إلى البيانات أو النظام المراد استعادته.

تتضمن جرائم برامج الفدية عادةً ما يلي:

1. الأفعال التحضيرية، بما في ذلك:

- إصدار أو بيع أو شراء أو بأي طريقة أخرى إتاحة برامج الفدية، أي «جهاز» بالمعنى المقصود في المادة 6 من الاتفاقية المتعلقة بالجريمة الإلكترونية؛
- إصدار أو بيع أو شراء أو بأي طريقة أخرى إتاحة أجهزة بالمعنى المقصود في المادة 6 المستخدمة في التحضير لجرائم برامج الفدية، مثل البرامج الضارة للحصول على وصول غير مصرح به إلى أنظمة الضحايا، أو شبكات البوتات لنشر برامج الفدية؛
- الحصول على قوائم البريد الالكتروني أو معلومات أخرى ذات صلة بالمستهدفين. قد تكون بعض هذه الأفعال التحضيرية بحد ذاتها جرائم أو يمكن اعتبارها مساعدة

أو تحريض على جرائم برامج الفدية، مثل اختراق قواعد البيانات باستخدام راصد لوحة المفاتيح، أو استخدام شبكات البوتات، أو سرقة الهوية[71].

2. نشر أو تثبيت برامج الفدية الضارة، بما في ذلك:

– - من خلال رسائل البريد الإلكتروني التي تحتوي على مرفقات تحتوي على برامج ضارة أو تستهدف مستخدمي تطبيقات المراسلة مع الروابط المدرجة في الرسائل. قد يتم تسهيل إغراء المستخدمين للوصول إلى هذه المرفقات أو الروابط - وبالتالي تثبيت البرامج الضارة - من خلال الهندسة الاجتماعية أو تقنيات أخرى لسرقة الهوية؛

– - من خلال الوصول عن بعد إلى نظام الكمبيوتر.

3. تشفير نظام الكمبيوتر، أو أجزاء منه، أو البيانات من خلال برنامج الفدية وبالتالي منع المستخدم من الولوج إلى البيانات أو النظام أو الاستفادة منها بأي طريقة أخرى.

4. طلب الحصول على الفدية واستلامها وتحويلها، بما في ذلك:

– - طلب الفدية مقابل (الوعد) باستعادة الوصول إلى البيانات و / أو النظام الذي يرقى إلى حد الابتزاز أو الاكراه وربما أيضًا جرائم أخرى؛

– - الاتصال بين الجاني والمستهدف من خلال وسائل الاتصال التي يصعب تتبعها، بما في ذلك استخدام متصفح تور (TOR) يمكن أيضًا إرسال أدوات فك التشفير بهذه الطريقة؛

– - الحصول على الفدية بطريقة تجعل من الصعب تتبعها، عادة في شكل عملة مشفرة، وغالبًا ما يتبعها تبييض العائدات لإخفاء هوية الجاني والعائدات.

منذ عام 2021، أصبح سوق برامج الفدية منظمًا واحترافيًا بشكل متزايد، حيث يقدم نموذج أعمال يُشار إليه غالبًا باسم برامج الفدية كخدمة أو (RaaS) لارتكاب جرائم برامج الفدية. أدى نموذج الأعمال هذا بمجرمي الإنترنت الذين شاركوا في خدمات مستقلة للتفاوض بشأن المدفوعات، ومساعدة الضحايا في إجراء المدفوعات، وبعض الخدمات التي تقدم مركزًا للمساعدة على مدار الساعة طوال أيام الأسبوع لتسريع دفع الفدية والمساعدة في استعادة الأنظمة أو البيانات المشفرة.

71. انظر: المذكرات التوجيهية ذات الصلة (coe.int)

الأحكام ذات الصلة في اتفاقية الجرائم الإلكترونية (سلسلة المعاهدات الأوروبية رقم 185)

تجريم الجرائم المتعلقة ببرامج الفدية

بموجب الاتفاقية المتعلقة بالجريمة الإلكترونية، يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم بعض الأفعال الإجرامية بمقتضى قانونه الوطني، عندما ترتكب عمدا ودون حق. وستكون المواد التالية والجرائم المقابلة لها بموجب القوانين الوطنية للأطراف المنفذة للاتفاقية ذات صلة بالتحقيقات والدعاوى الجنائية المتعلقة بجرائم برامج الفدية.

المواد ذات الصلة	أمثلة
المادة 2 - النفاذ غير القانوني	تنطوي جرائم برامج الفدية على النفاذ غير القانوني إلى نظام كمبيوتر للضحية وبالتالي تعتبر جريمة جنائية وفقا للمادة 2.
المادة -3 الاعتراض غير القانوني	قد تشمل متغيرات برامج الفدية القدرة على اعتراض الإرسال غير العام لبيانات الكمبيوتر إلى أو من أو داخل نظام الكمبيوتر. وقد ينطوي أيضا الحصول على معلومات عن المستهدفين أو بيانات الدخول على جريمة الاعتراض غير القانوني.
المادة -4 التدخل في البيانات	صُممت برامج الفدية خصيصًا لغرض التدخل في بيانات الكمبيوتر وبالتالي فإن استخدامها يعد جريمة جنائية وفقًا للمادة 4.
المادة 5 - التدخل في النظام	يمكن تصميم برامج الفدية لغرض التدخل في عمل نظام الكمبيوتر وبالتالي فإن استخدامها يعتبر جريمة جنائية وفقًا للمادة 5.
المادة -6 إساءة استخدام الأجهزة	برامج الفدية هي برامج ضارة وبالتالي فهي أداة «مصممة أو معدلة بشكل أساسي لغرض ارتكاب أي من الجرائم المقررة وفقًا للمواد 2 إلى 5 أعلاه». وبالتالي، فإن «تصميم برامج الفدية أو بيعها أو شرائها لاستخدامها أو استيرادها أو نشرها أو إتاحتها بأي طريقة أخرى» يعتبر جريمة جنائية وفقا للمادة 6.
المادة -7 التزوير المتعلق بالكمبيوتر	من أجل النفاذ غير القانوني إلى أنظمة الضحايا، غالبًا ما يستخدم جناة برامج الفدية تقنيات التصيد الاحتيالي وغيرها من تقنيات الهندسة الاجتماعية - والتي قد تشكل في بعض الحالات تزويرًا متعلقًا بجهاز الكمبيوتر - مما يؤدي إلى إنشاء بيانات غير أصلية بقصد النظر فيها أو التصرف بها لأغراض قانونية كما لو كانت أصلية.

المواد ذات الصلة	أمثلة
المادة -8 الاحتيال المتعلق بالكمبيوتر	تتسبب جرائم برامج الفدية في فقدان الممتلكات عن طريق التدخل في بيانات الكمبيوتر و/أو تشغيل نظام الكمبيوتر بنية احتيالية أو مخادعة أخرى للحصول، دون حق، على منفعة اقتصادية.
المادة -11 الشروع والمساعدة والتحريض	يمكن محاولة ارتكاب الجرائم المنصوص عليها في المعاهدة أو المساعدة عليها أو التحريض عليها تعزيزا للجرائم المتصلة ببرامج الفدية. وقد يشارك أشخاص مختلفون، على سبيل المثال، في إعداد برامج الفدية أو شرائها أو إتاحتها بأي طريقة أخرى، أو في شراء معلومات عن المستهدفين.
المادة -12 مسؤولية الشركات	يمكن ارتكاب جرائم برامج الفدية التي تشملها المواد من 2 إلى 11 من الاتفاقية على النحو المبين أعلاه من قبل أشخاص اعتباريين الذين يكونون عرضة للمساءلة وفقا للمادة 12.
المادة 13 - العقوبات	قد تشكل الجرائم المتعلقة ببرامج الفدية التي تعد جرائم مشمولة بالاتفاقية تهديدًا كبيرًا للأفراد والمجتمع، خاصةً عندما تكون الجرائم موجهة ضد المعلومات الحيوية للهياكل الأساسية وتسبب خطرًا كبيرًا على حياة أو سلامة أي شخص طبيعي. لذلك ينبغي للأطراف أن تضمن، عملاً بالمادة 13، أن الجرائم الجنائية المتعلقة بهذه الأفعال «يعاقب عليها بعقوبات فعالة ومتناسبة ورادعة، بما في ذلك الحرمان من الحرية». وهذا يشمل ضمان أن العقوبات المتاحة، بموجب قانونها الوطني، مناسبة بالنظر إلى التهديد الذي تشكله برامج الفدية والأخذ في الاعتبار النطاق الكامل للمسؤولية الجنائية، بما في ذلك على أساس المحاولة والمساعدة والتحريض على النشاط الاجرامي.
	قد تنظر الأطراف أيضًا في فرض عقوبات أكثر صرامة عند وجود ظروف مشددة، على سبيل المثال، إذا كانت هذه الأفعال تؤثر بشكل كبير على أداء البنية التحتية الحيوية أو تسببت في وفاة أو إصابة جسدية لشخص طبيعي أو أضرار مادية كبيرة.

لذلك، قد تشتمل جرائم برامج الفدية على سلوك يتم تجريمه وفقًا للمواد من 2 إلى 8 وكذلك بموجب المادة 11 (محاولة أو مساعدة أو تحريض)، وقد يستتبع ذلك أيضًا مسؤولية الأشخاص الاعتباريين بموجب المادة 12 من الاتفاقية المتعلقة بالجريمة الإلكترونية.

قد تشتمل أنشطة برامج الفدية على مجموعة واسعة من الجرائم الأخرى بموجب القانون الجنائي الوطني.

الأحكام الإجرائية

بموجب الاتفاقية المتعلقة بالجريمة الإلكترونية، «يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتمكين سلطاته المختصة من» اتخاذ تدابير إجرائية معينة للتحقيق في الجرائم وفقًا للمواد من 2 إلى 11 من الاتفاقية وجمع الأدلة في شكل إلكتروني (انظر المادة 14 من الاتفاقية). يمكن استخدام هذه أيضًا في التحقيقات والدعاوى الجنائية المتعلقة بجرائم برامج الفدية.

المواد ذات الصلة	أمثلة
المادة -14 نطاق الأحكام الإجرائية	يمكن استخدام الصلاحيات الإجرائية للاتفاقية (المواد 16-21) في تحقيق أو دعوى جنائية محددة ليس فقط فيما يتعلق بالجرائم المذكورة أعلاه بموجب الاتفاقية ولكن أيضا فيما يتعلق بجمع الأدلة في شكل إلكتروني عن أي جريمة أخرى تتصل ببرامج الفدية على النحو المحدد في القانون الداخلي للطرف.
المادة -15 الشروط والضمانات	تنطبق هذه الشروط والضمانات أيضا على التحقيقات والدعاوى الجنائية المتعلقة بجرائم برامج الفدية.
المادة -16 الحفظ العاجل لبيانات الكمبيوتر المخزنة	يمكن استخدام هذه الصلاحية للحفظ العاجل لبيانات الكمبيوتر المخزنة المتعلقة بجرائم برامج الفدية، بما في ذلك، على سبيل المثال، البيانات حول مصدر أو مسار نشر برامج الفدية أو الاتصالات التي تطلب فدية أو إتاحة أدوات فك التشفير إذا كان ذلك ممكنًا. يمكن أيضًا استخدام هذه الصلاحية للأمر بالاحتفاظ بالبيانات الأخرى المتعلقة بجرائم برامج الفدية، مثل الاتصالات بين المشتبه بهم أو البيانات المخزنة من قبل المشتبه بهم والتي قد تكون دليلاً على مثل هذه الجرائم.
المادة 17 - الحفظ العاجل والكشف الجزئي لبيانات الحركة	يمكن استخدام هذه الصلاحية للحصول العاجل على كمية كافية من بيانات الحركة لتحديد مقدمي الخدمة الآخرين والمسار الذي تم من خلاله إرسال الاتصالات المتعلقة بجرائم برامج الفدية.
المادة 18 - أمر التقديم	يمكن استخدام أوامر التقديم وفقًا للمادة 18 لأمر أي شخص بتقديم بيانات الكمبيوتر المخزنة المتعلقة بجرائم برامج الفدية. قد يشمل ذلك مقدمي الخدمات والمؤسسات المالية بما في ذلك مقدمو خدمات الأصول الافتراضية ومنصاتهم، وغيرهم من الأشخاص الاعتباريين أو الطبيعيين. تُعد هذه الطلبات أمرًا هاما للحصول، على سبيل المثال، على معلومات المشترك من مقدمي الخدمات المرتبطين بالحسابات والهياكل الأساسية المرتبطة ببرامج الفدية.

المواد ذات الصلة	أمثلة
المادة 19 - البحث عن بيانات الكمبيوتر المخزنة ومصادرتها	يمكن استخدام أحكام البحث والمصادرة وفقًا للمادة 19 للبحث عن بيانات الكمبيوتر المخزنة المتعلقة بجرائم برامج الفدية ومصادرتها.
المادة 20 - جمع بيانات الحركة في الوقت الفعلي	يمكن استخدام الصلاحيات وفقًا للمادة 20 لجمع بيانات الحركة في الوقت الفعلي المتعلقة بجرائم برامج الفدية
المادة -21 اعتراض بيانات المحتوى	يمكن استخدام الصلاحيات وفقًا للمادة 21 لاعتراض بعض بيانات المحتوى المتعلقة بجرائم برامج الفدية، مثل، على سبيل المثال، الاتصالات بين المشتبه بهم.

بالتالي، في التحقيقات أو الدعاوى الجنائية المتعلقة بجرائم برامج الفدية، يجوز للأطراف استخدام الحفظ العاجل لبيانات الكمبيوتر المخزنة، وأوامر التقديم، والبحث عن بيانات الكمبيوتر المخزنة ومصادرتها، وغيرها من الأدوات لجمع الأدلة الإلكترونية.

أحكام التعاون الدولي

المواد ذات الصلة	أمثلة
المبادئ والإجراءات العامة المتعلقة بالتعاون الدولي الواردة في المواد من 23 إلى 28	المبادئ والإجراءات العامة للتعاون الدولي الواردة في المواد من 23 إلى 28 من الاتفاقية - أي المتعلقة بتسليم المجرمين والمساعدة المتبادلة وغيرها - تنطبق أيضًا على الجرائم المتعلقة ببرامج الفدية. قد تكون المادة 26 مفيدة بشكل خاص من حيث أن أي طرف يمتلك معلومات قيمة عن جرائم برامج الفدية التي تم الحصول عليها من خلال تحقيقاته الخاصة يمكنه، في حدود قانونه الوطني، إرسال هذه المعلومات إلى الطرف الآخر دون طلب مسبق (انظر الفقرة 260 من التقرير التفسيري للاتفاقية المتعلقة بالجريمة الإلكترونية). وفقًا للمادة 23 والمادة 1.25، يتعين على الأطراف في الاتفاقية التعاون مع بعضها البعض، وفقًا لأحكام المواد 23-28، «إلى أقصى حد ممكن لأغراض التحقيقات أو الدعاوى المتعلقة بالجرائم الجنائية المتعلقة بأنظمة وبيانات الكمبيوتر «ومن أجل» جمع الأدلة في شكل إلكتروني لجريمة جنائية «.

المواد ذات الصلة	أمثلة
أحكام خاصة بشأن التعاون الدولي في المواد من 29 إلى 35	تنطبق الأحكام الخاصة للفصل الثالث من الاتفاقية على التعاون الدولي وجمع الأدلة المتعلقة بجرائم برامج الفدية: – المادة 29 – الحفظ العاجل لبيانات الكمبيوتر المخزنة – المادة 30 - الكشف العاجل عن بيانات الحركة المحفوظة – المادة 31 - المساعدة المتبادلة فيما يتعلق بالنفاذ إلى بيانات الكمبيوتر المخزنة – المادة 32 - الوصول عبر الحدود إلى بيانات الكمبيوتر المخزنة عن طريق الموافقة أو حيثما كانت متاحة للجمهور – المادة 33 - المساعدة المتبادلة في جمع بيانات الحركة في الوقت الفعلي – المادة 34 - المساعدة المتبادلة فيما يتعلق باعتراض بيانات المحتوى – - المادة 35 – الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع.

نظرًا لأن جرائم برامج الفدية تتضمن عادةً مرتكبي الجرائم والمستهدفين والضحايا ومقدمي الخدمات والمؤسسات المالية أو أنظمة الكمبيوتر في ولايات قضائية متعددة، فإن الاستخدام الفعال لأحكام التعاون الدولي هذه أمر مهم بشكل خاص.

البروتوكول الإضافي الثاني لاتفاقية الجرائم الإلكترونية (سلسلة معاهدات مجلس أوروبا رقم 224)

في 12 مايو 2022، تم فتح البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة معاهدات مجلس أوروبا رقم 224) للتوقيع. وبمجرد دخول هذا الصك حيز التنفيذ، سيتيح للأطراف أدوات إضافية من أجل «تعزيز التعاون والكشف عن الأدلة الإلكترونية». ستكون هذه ذات صلة، وفي بعض الحالات وثيقة الصلة للغاية، بالتحقيقات والدعاوى الجنائية المتعلقة بجرائم برامج الفدية، وتشمل:

– المادة 6 - طلب معلومات تسجيل اسم النطاق مباشرة من كيان في طرف آخر يقدم خدمات تسجيل اسم النطاق؛

- المادة 7 - الكشف عن معلومات المشترك من خلال التعاون المباشر مع مقدم خدمة في طرف آخر؛
- المادة 8 - تنفيذ أوامر من طرف آخر للتقديم العاجل لمعلومات المشترك وبيانات الحركة؛
- المادة 9 – الكشف العاجل عن بيانات الكمبيوتر المخزنة في حالات الطوارئ؛
- المادة 10 - المساعدة المتبادلة في حالات الطوارئ؛
- المادة 11 - التداول بالفيديو؛
- المادة 12 - فرق التحقيق المشتركة والتحقيقات المشتركة.

إن نطاق تطبيق هذا البروتوكول واسع مرة أخرى من حيث أنه يجب تطبيقه ليس فقط على الجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات ولكن أيضًا على جمع الأدلة في شكل إلكتروني لأي جريمة جنائية (انظر المادة 1.2 (أ))

تضمن شروط وضمانات المادة 13 أن وضع وتنفيذ وتطبيق الصلاحيات والإجراءات المنصوص عليها في البروتوكول تخضع للشروط والضمانات المنصوص عليها في القانون الوطني لكل طرف، والتي يجب أن توفر الحماية الكافية لحقوق الإنسان والحريات. بالإضافة إلى ذلك، نظرًا لأن العديد من الأطراف في البروتوكول قد تكون مطالبة، بالوفاء بالتزاماتها الدستورية أو الدولية، لضمان حماية البيانات الشخصية، تنص المادة 14 على ضمانات حماية البيانات للسماح للأطراف بالوفاء بهذه المتطلبات وتضمن أن البيانات الشخصية يمكن نقلها عند الاستفادة من هذه الأشكال العاجلة من التعاون.

بيان لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية

تقر لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية بما يلي:

- قد تشتمل الجرائم المتعلقة بهجمات برامج الفدية على سلوك يتم تجريمه وفقًا للمواد من 2 إلى 8 وكذلك بموجب المادة 11 (محاولة أو مساعدة أو تحريض) ، وقد يستتبع ذلك مسؤولية الأشخاص الاعتباريين بموجب المادة 12 من الاتفاقية المتعلقة بالجريمة الإلكترونية؛

- يمكن استخدام التدابير الإجرائية وأدوات التعاون الدولي الواردة في الاتفاقية للتحقيق في هجمات برامج الفدية والجرائم ذات الصلة ومقاضاة مرتكبيها ، فضلاً عن تسهيلها والمشاركة فيها أو الأفعال التحضيرية؛

- سيتيح البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية، بمجرد دخوله حيز التنفيذ، لأطرافه أدوات إضافية لتعزيز التعاون والكشف عن الأدلة الإلكترونية المتعلقة بهجمات برامج الفدية.

المذكرة التوجيهية رقم 13 للجنة الاتفاقية المتعلقة بالجريمة الإلكترونية

نطاق الصلاحيات الإجرائية وأحكام التعاون الدولي الواردة في اتفاقية بودابست

1 مقدمة

قررت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية في جلستها العامة الثامنة (ديسمبر 2012) إصدار مذكرات توجيهية تهدف إلى تسهيل الاستخدام والتنفيذ الفعالين لاتفاقية بودابست بشأن الجريمة الإلكترونية، وكذلك في ضوء التطورات القانونية والسياساتية والتكنولوجية[72]. تمثل المذكرات التوجيهية الفهم المشترك لأطراف هذه المعاهدة فيما يتعلق باستخدام الاتفاقية.

تتناول هذه المذكرة نطاق السلطات الإجرائية الوطنية وأحكام التعاون الدولي الواردة في الاتفاقية المتعلقة بالجريمة الالكترونية (سلسلة المعاهدات الأوروبية رقم 185) وكذلك بروتوكولها الإضافي الثاني بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية (سلسلة معاهدات مجلس أوروبا رقم 224).

في حين أن نص الاتفاقية المتعلقة بالجريمة الإلكترونية واضح إلى حد ما بأن السلطات الإجرائية وأحكام التعاون الدولي لا تنطبق فقط على الجريمة الإلكترونية (المواد من 2 إلى 11 من الاتفاقية) ولكن أيضًا «الجرائم الأخرى المرتكبة بواسطة نظام الكمبيوتر»؛ و»جمع الأدلة في شكل إلكتروني لجريمة جنائية» (انظر المادة 14 الفقرة 2 (ب) و (ج) وبالمثل المادتين 23 و 25 من سلسلة المعاهدات الأوروبية رقم 185)، وبينما تم تأكيد ذلك مرة أخرى في البروتوكول الإضافي الثاني الملحق بالاتفاقية (انظر المادة 2 من سلسلة معاهدات مجلس أوروبا رقم 224)، هذا النطاق ليس دائمًا مفهومًا تمامًا، وقوانين بعض البلدان تقصر تطبيق الصلاحيات أو الأحكام الإجرائية للتعاون الدولي على مجموعة من الجرائم الإلكترونية.

لذلك، قررت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية أن المذكرة التوجيهية، التي تؤكد على كيفية تطبيق أحكام التعاون الإجرائي والدولي الرئيسية، ليس فقط على الجرائم المرتكبة ضد أنظمة الكمبيوتر وبواسطتها، ولكن أيضًا على مجموعة من الجرائم، ستكون فائدة عملية واستراتيجية.

72. انظر صلاحيات لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية) (المادة 46 من اتفاقية بودابست).

2 الأحكام ذات الصلة في الاتفاقية المتعلقة بالجريمة الالكترونية (سلسلة المعاهدات الأوروبية رقم 185)

1.2. الأحكام الإجرائية

بموجب الاتفاقية المتعلقة بالجريمة الالكترونية، «يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاته المختصة من «القيام بالتدابير الإجرائية المنصوص عليها في المواد من 16 إلى 21 من الاتفاقية:

- المادة 16 - الحفظ العاجل لبيانات الكمبيوتر المخزنة؛
- المادة 17 - الحفظ العاجل والكشف الجزئي لبيانات الحركة؛
- المادة 18 - أمر التقديم؛
- المادة 19 - البحث عن بيانات الكمبيوتر المخزنة ومصادرتها؛
- المادة 20 - جمع بيانات الحركة في الوقت الفعلي؛
- المادة 21 - اعتراض بيانات المحتوى.

تخضع هذه الإجراءات لشروط وضمانات المادة 15.

نطاق هذه الإجراءات الإجرائية محدد في المادة 14:

المادة 14 - نطاق الأحكام الإجرائية

1. يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتحديد الصلاحيات والإجراءات المنصوص عليها في هذا القسم لأغراض التحقيقات أو الدعاوى الجنائية المحددة.
2. باستثناء ما هو منصوص عليه على وجه التحديد في المادة 21، يطبق كل طرف الصلاحيات والإجراءات المشار إليها في الفقرة 1 من هذه المادة على:
   أ) الجرائم الجنائية المقررة وفقا للمواد من 2 إلى 11 من هذه الاتفاقية؛
   ب) الجرائم الجنائية الأخرى التي ترتكب بواسطة نظام كمبيوتر؛ و
   ج) جمع الأدلة في شكل إلكتروني عن جريمة جنائية.
3. أ) يجوز لكل طرف أن يتحفظ على تطبيق التدابير المشار إليها في المادة 20 فقط على الجرائم أو فئات الجرائم المحددة في التحفظ، بشرط ألا يكون نطاق هذه الجرائم أو فئات الجرائم أكثر تقييدا من نطاق الجرائم التي تطبق عليها التدابير المشار إليها في المادة 21. ينظر كل طرف في تقييد هذا التحفظ للتمكين من تطبيق التدبير المشار إليه في المادة 20 على أوسع نطاق.

ب) إذا كان الطرف غير قادر، بسبب القيود المفروضة على تشريعاته السارية وقت اعتماد هذه الاتفاقية، على تطبيق التدابير المشار إليها في المادتين 20 و21 على الاتصالات المرسلة داخل نظام كمبيوتر تابع لمقدم الخدمة، الذي:

1) يجري تشغيله لصالح مجموعة مغلقة من المستخدمين،

2) لا يستخدم شبكات الاتصالات العامة ولا يرتبط بنظام كمبيوتر آخر، سواء كان عاما أو خاصا،

يجوز لذلك الطرف أن يتحفظ على عدم تطبيق هذه التدابير على هذه الاتصالات. وينظر كل طرف في تقييد هذا التحفظ للتمكين من تطبيق التدابير المشار إليها في المادتين 20 و21 على أوسع نطاق.

وفقا للمادة 2.14 من الاتفاقية، فإن الصلاحيات الإجرائية تنطبق على جمع الأدلة في شكل إلكتروني عن أي جريمة جنائية. وهذا «يكفل إمكانية الحصول على الأدلة في شكل إلكتروني عن أي جريمة جنائية أو جمعها عن طريق الصلاحيات والإجراءات المبينة في هذا القسم» من الاتفاقية (الفقرة 141 من التقرير التفسيري للاتفاقية).

تنص الفقرة 3 من المادة 14 على استثناءات من هذا النطاق الواسع للتطبيق وتسمح للأطراف بتقييد نطاق الصلاحيات الأكثر تدخلاً (جمع بيانات الحركة في الوقت الفعلي بموجب المادة 20 واعتراض بيانات المحتوى بموجب المادة 21)[73].

لذلك، يجوز للسلطات المختصة أن تأمر بحفظ البيانات، أو أن تأمر بتقديم البيانات، أو أن تبحث أو تصادر بيانات الكمبيوتر المخزنة، أو أن تأمر أو تقوم بجمع بيانات الحركة في الوقت الفعلي أو باعتراض بيانات المحتوى[74] في تحقيقات جنائية محددة تتعلق بأي جريمة بموجب القانون الوطني، بما في ذلك على سبيل المثال[75]:

- الفساد؛
- تزييف الأدوية أو غيرها من الأخطار التي تهدد الصحة العامة، بما في ذلك الجرائم المتصلة بكوفيد19-؛
- مختلف أشكال الاعتداء على الأطفال؛
- مختلف أشكال العنف الأسري والعنف ضد المرأة؛
- مختلف أشكال الجرائم الاقتصادية والمالية؛
- الجرائم المتعلقة بالمخدرات؛

73. انظر التحفظات والإعلانات الصادرة عن الأطراف فيما يتعلق بالمادة 14.
74. كما هو مبني في المادتي 20 و21 من الاتفاقية، قد يتم تطبيق قيود على صلاحيات جمع بيانات الحركة في الوقت الفعلي واعتراض بيانات المحتوى، مثل اقتصارها على مجموعة من الجرائم الخطيرة.
75. انظر أيضًا المراجع أدناه للمعاهدات الدولية ذات الصلة التي تغطي بعض هذه الجرائم.

- الاحتيال؛
- الاختطاف؛
- التلاعب بالمسابقات الرياضية؛
- تبييض الأموال وتمويل الإرهاب؛
- القتل العمد؛
- الجرائم ذات الصلة بالجريمة المنظمة؛
- الاغتصاب وغيره من أشكال العنف الجنسي؛
- الإرهاب؛
- الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب والجرائم الدولية الأخرى؛
- الاتجار بالبشر؛
- كره الأجانب والعنصرية والأشكال الإجرامية الأخرى لخطاب الكراهية.

2.2. أحكام التعاون الدولي

يمتد النطاق الواسع للسلطات الإجرائية الوطنية إلى المبادئ والتدابير المتعلقة بالتعاون الدولي (الفصل الثالث من الاتفاقية). توضح المادتان 23 و25 أن التعاون ليس ممكنًا فقط لأغراض التحقيقات أو الدعاوى المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، ولكن أيضًا لجمع الأدلة في شكل إلكتروني لأي جريمة جنائية:

المادة 23 - المبادئ العامة المتعلقة بالتعاون الدولي

تتعاون الأطراف مع بعضها البعض، وفقًا لأحكام هذا الفصل، ومن خلال تطبيق الصكوك الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية، والترتيبات المتفق عليها على أساس التشريع الموحد أو المتبادل، والقوانين الوطنية، إلى أقصى حد ممكن لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، أو لجمع الأدلة في شكل إلكتروني لجريمة جنائية.

المادة 25 - المبادئ العامة المتعلقة بالمساعدة المتبادلة

1. توفر الأطراف لبعضها البعض المساعدة المتبادلة إلى أقصى حد ممكن لغرض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، أو لجمع الأدلة في شكل إلكتروني لجريمة جنائية.

تؤكد الفقرة 243 من التقرير التفسيري للاتفاقية ما يلي:

"يجب أن يمتد التعاون ليشمل جميع الجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات (أي الجرائم التي تشملها المادة 14، الفقرة 2، الفقرات الفرعية (أ) و (ب)) ، وكذلك لجمع الأدلة في شكل إلكتروني لجريمة جنائية. وهذا يعني أنه إما في حالة ارتكاب جريمة عن طريق استخدام

نظام الكمبيوتر، أو في حالة عدم ارتكاب جريمة عادية باستخدام نظام كمبيوتر (على سبيل المثال، جريمة قتل) وكانت تتضمن أدلة إلكترونية، فإن شروط الفصل الثالث تنطبق".

يجوز للأطراف تقييد هذا النطاق الواسع فيما يتعلق بالمساعدة المتبادلة فيما يتعلق بجمع بيانات الحركة في الوقت الفعلي (المادة 33) والمساعدة المتبادلة فيما يتعلق باعتراض بيانات المحتوى (المادة 34). علاوة على ذلك، قد يخضع التعاون الدولي لشروط، مثل متطلبات التجريم المزدوج[76]، أو أسباب الرفض بما يتماشى مع المواد 4.25 و4.27 و5.27[77] من الاتفاقية.

تنص المواد من 23 إلى 35[78] من الاتفاقية على مبادئ وتدابير التعاون الدولي بشأن الجرائم المدرجة في الاتفاقية والجرائم الجنائية الأخرى المرتكبة بواسطة نظام الكمبيوتر، وجمع الأدلة الإلكترونية لأي جريمة جنائية أخرى:

- المادة 23 - مبادئ عامة تتعلق بالتعاون الدولي؛
- المادة 25 - المبادئ العامة المتعلقة بالمساعدة المتبادلة؛
- المادة 26 - المعلومات دون طلب مسبق؛
- المادة 27 - الإجراءات المتعلقة بطلبات المساعدة المتبادلة في حالة عدم وجود اتفاقيات دولية سارية؛
- المادة 28 - السرية والقيود على الاستخدام؛
- المادة 29 - الحفظ العاجل لبيانات الكمبيوتر المخزنة؛
- المادة 30 - الكشف العاجل لبيانات الحركة المحفوظة؛
- المادة 31 - المساعدة المتبادلة فيما يتعلق بالوصول إلى بيانات الكمبيوتر المخزنة؛
- المادة 32 - الوصول عبر الحدود إلى بيانات الكمبيوتر المخزنة
  بعد الموافقة أو حيثما تكون متاحة علنا؛
- المادة 33 - المساعدة المتبادلة في جمع بيانات الحركة في الوقت الفعلي؛
- المادة 34 - المساعدة المتبادلة فيما يتعلق باعتراض بيانات المحتوى؛
- المادة 35 – الشبكة التي تعمل على مدار الساعة طوال أيام الأسبوع.

---

76. انظر المادة 4.29 من الاتفاقية.
كما لوحظ في الفقرة 259 من التقرير التفسيري للاتفاقية، «... في المسائل التي ينطبق فيها معيار التجريم المزدوج، ينبغي تطبيقه بطريقة مرنة تسهل منح المساعدة.»
77. تشير المادة 5.27 من الاتفاقية إلى أسباب تأجيل اتخاذ إجراء بناء على طلب ما.
78. ملاحظة: الالتزام بالتسليم بموجب «المادة 24 - التسليم» ينطبق فقط على «الجرائم الجنائية المنصوص عليها في المواد من 2 إلى 11 من هذه الاتفاقية، شرط أن يعاقب عليها بموجب قوانين كلا الطرفين المعنيين بالحرمان من الحرية بسبب مدة أقصاها سنة واحدة على الأقل، أو بعقوبة أشد».

يجوز للأطراف في الاتفاقية الاستفادة من هذه التدابير والمبادئ للتعاون مع بعضها البعض إلى أقصى حد ممكن لغرض التحقيقات أو الإجراءات وجمع الأدلة في شكل إلكتروني لأي جريمة جنائية، وطلب حفظ البيانات أو الوصول إلى بيانات الكمبيوتر المخزنة أو جمع بيانات الحركة في الوقت الفعلي أو اعتراض بيانات المحتوى[79] أو الوصول إلى بيانات الكمبيوتر المخزنة عبر الحدود فيما يتعلق بأي جريمة جنائية ووفقًا للشروط المنصوص عليها في الفصل الثالث من الاتفاقية.

3 الأحكام ذات الصلة من البروتوكول الإضافي الثاني (سلسلة معاهدات مجلس أوروبا رقم 224)

في 12 مايو 2022، تم فتح البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة معاهدات مجلس أوروبا رقم 224) للتوقيع. وبمجرد دخول هذا الصك حيز التنفيذ، سيتيح للأطراف أدوات إضافية من أجل «تعزيز التعاون والكشف عن الأدلة الإلكترونية".

يعد نطاق تطبيق هذا البروتوكول واسعًا مرة أخرى ولن يتم تطبيقه فقط على الجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات ولكن أيضًا على جمع الأدلة في شكل إلكتروني لأي جريمة جنائية:

المادة 2 - نطاق التطبيق

1 باستثناء ما هو محدد في هذه الوثيقة، تطبق التدابير المبينة في هذا البروتوكول:

أ) بين الأطراف في الاتفاقية التي هي أطراف في هذا البروتوكول، لأغراض تحقيقات أو دعاوى جنائية محددة تتعلق بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، وجمع الأدلة في شكل إلكتروني لجريمة جنائية؛ و

ب) بين الأطراف في البروتوكول الأول التي هي أطراف في هذا البروتوكول، لأغراض تحقيقات أو دعاوى جنائية محددة تتعلق بالجرائم الجنائية المحددة بموجب البروتوكول الأول.

التدابير المنصوص عليها في هذا البروتوكول هي:

– المادة 6 - طلب معلومات تسجيل اسم النطاق مباشرة من كيان في طرف آخر يقدم خدمات تسجيل اسم النطاق؛

79. كما هو مبني في المادتين 20 و21 من الاتفاقية، قد يتم تطبيق قيود على صلاحيات جمع بيانات الحركة في الوقت الفعلي واعتراض بيانات المحتوى، مثل الاقتصار على مجموعة من الجرائم الخطيرة. فيما يتعلق بالمادتين 33 و34 المقابل بشأن التعاون الدولي، «يجب على كل طرف تقديم هذه المساعدة على الأقل فيما يتعلق بالجرائم الجنائية التي يكون جمع بيانات الحركة في الوقت الفعلي متاحًا لها في قضية وطنية مماثلة» (المادة 2.33)، ومن أجل اعتراض بيانات المحتوى «يجب على الأطراف تقديم المساعدة المتبادلة ... إلى الحد المسموح به بموجب المعاهدات والقوانين المحلية السارية» (المادة 34).

- المادة 7 - الكشف عن معلومات المشترك من خلال التعاون المباشر مع مقدم خدمة في طرف آخر؛
- المادة 8 - تنفيذ أوامر من طرف آخر للتقديم العاجل لمعلومات المشترك وبيانات الحركة؛
- المادة 9 - الكشف العاجل عن بيانات الكمبيوتر المخزنة في حالات الطوارئ؛
- المادة 10 - المساعدة المتبادلة في حالات الطوارئ؛
- المادة 11 - التداول بالفيديو؛
- المادة 12 - فرق التحقيق المشتركة والتحقيقات المشتركة.

تخضع هذه التدابير لشروط وضمانات المادتين 13 و14 من سلسلة معاهدات مجلس أوروبا رقم 224.

لذلك، يجوز للسلطات المختصة للأطراف في هذا البروتوكول - مع مراعاة التحفظات والإعلانات المسموح بها وفقًا للمادة 19 من سلسلة معاهدات مجلس أوروبا رقم -224 طلب معلومات تسجيل اسم النطاق، والأمر بالكشف عن معلومات المشترك، وتنفيذ أوامر التقديم الخاصة بمعلومات المشترك وبيانات الحركة، والتعاون في حالات الطوارئ، استخدام التداول بالفيديو أو إنشاء فرق تحقيق مشتركة أو المشاركة في تحقيقات مشتركة تتعلق بالتحقيقات أو الدعاوى الجنائية المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات، وجمع الأدلة في شكل إلكتروني عن أي جريمة.

4 أوجه التضافر بين الاتفاقية المتعلقة بالجريمة الإلكترونية والمعاهدات الأخرى

يمكن أيضًا استخدام الصلاحيات الإجرائية الوطنية ومبادئ وتدابير التعاون الدولي لجمع الأدلة الإلكترونية المتعلقة بالجرائم المنصوص عليها في الاتفاقيات الدولية الأخرى التي تكون الدول أطرافًا فيها، مع مراعاة أي شروط ذات صلة على النحو المشار إليه أعلاه[80]. قد تشمل هذه الاتفاقات تلك المتعلقة بالفساد[81]؛ تقليد الأدوية أو تهديدات أخرى للصحة العامة[82]؛ الاعتداء على الأطفال[83]؛ العنف المنزلي والعنف ضد المرأة[84]؛

80. مثل متطلبات التجريم المزدوج، أو أسباب الرفض بما يتماشى مع المادتين 4.25 و4.27 من الاتفاقية
81. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية القانون الجنائي بشأن الفساد (سلسلة المعاهدات الأوروبية رقم 173) أو اتفاقية الأمم المتحدة لمكافحة الفساد.
82. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية مجلس أوروبا بشأن تقليد المنتجات الطبية والجرائم المماثلة التي تنطوي على تهديدات للصحة العامة (سلسلة معاهدات مجلس أوروبا رقم 211)
83. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي (سلسلة معاهدات مجلس أوروبا رقم 201)
84. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية مجلس أوروبا بشأن منع ومكافحة العنف ضد المرأة والعنف

الجرائم المتعلقة بالمخدرات[85]؛ التلاعب بالمسابقات الرياضية[86]؛ تبييض الأموال وتمويل الإرهاب[87]؛ الجرائم ذات الصلة بالجريمة المنظمة[88]؛ الإرهاب[89]؛ الاتجار بالبشر[90]؛ أو الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب والجرائم الدولية الأخرى[91].

بالنسبة للأطراف في البروتوكول الإضافي الأول للاتفاقية المتعلقة بالجريمة الإلكترونية بشأن كره الأجانب والعنصرية عبر أنظمة الكمبيوتر (سلسلة المعاهدات الأوروبية رقم 189)[92]، تنص المادة 2.8 على أن «توسع الأطراف نطاق تطبيق التدابير المحددة في المواد من 14 إلى 21 والمواد 23 إلى 35 من الاتفاقية، للمواد من 2 إلى 7 من هذا البروتوكول ".

في عام 2018، أوصت لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية بتشجيع الأطراف في اتفاقية لانزاروت المتعلقة بالاستغلال الجنسي والاعتداء الجنسي على الأطفال (سلسلة معاهدات مجلس أوروبا رقم 201) واتفاقية اسطنبول المتعلقة بالعنف ضد المرأة والعنف المنزلي (سلسلة معاهدات مجلس أوروبا رقم 210) على «إدراج الصلاحيات الإجرائية للمواد من 16 إلى 21 من اتفاقية بودابست في القانون الوطني والنظر في أن تصبح أطرافًا في اتفاقية بودابست لتسهيل التعاون الدولي بشأن الأدلة الإلكترونية (المواد من 23 إلى 35 من اتفاقية بودابست) فيما يتعلق بالعنف الجنسي عبر الإنترنت ضد الأطفال والعنف ضد المرأة العنف الأسري»[93].

المنزلي (سلسلة معاهدات مجلس أوروبا رقم 210)

85. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقيات الأمم المتحدة لمكافحة المخدرات
86. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية مجلس أوروبا بشأن التلاعب بالمسابقات الرياضية (سلسلة معاهدات مجلس أوروبا رقم 215)
87. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية مجلس أوروبا بشأن تبييض عائدات الجريمة والبحث عنها وضبطها ومصادرتها وبتمويل الإرهاب (سلسلة معاهدات مجلس أوروبا رقم 198)
88. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وبروتوكولاتها الملحقة
89. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية مجلس أوروبا لمنع الإرهاب (سلسلة معاهدات مجلس أوروبا رقم 196) وبروتوكولاتها الملحقة
90. على سبيل المثال، السلوك الإجرامي المشار إليه في اتفاقية مجلس أوروبا بشأن إجراءات مكافحة الاتجار بالبشر (سلسلة معاهدات مجلس أوروبا رقم 197)
91. على سبيل المثال، السلوك المشار إليه في اتفاقية منع جريمة الإبادة الجماعية والمعاقبة عليها لعام 1948، أو اتفاقيات جنيف الأربع للقانون الإنساني الدولي وبروتوكولاتها الإضافية لعام 1949، أو نظام روما الأساسي للمحكمة الجنائية الدولية
92. البروتوكول الإضافي لاتفاقية الجرائم الإلكترونية بشأن تجريم الأفعال ذات الطابع العنصري وكراهية الأجانب المرتكبة من خلال أنظمة الكمبيوتر (سلسلة المعاهدات الأوروبية رقم 189)
93. انظر الدراسة المسحية التي قامت بها لجنة الاتفاقية المتعلقة بالجريمة الالكترونية على الموقع: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

5 بيان لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية

تقر لجنة الاتفاقية المتعلقة بالجريمة الإلكترونية على أن أحكام القانون الإجرائي ومبادئ وتدابير التعاون الدولي الواردة في الاتفاقية المتعلقة بالجريمة الإلكترونية لا تنطبق على الجرائم ذات الصلة بأنظمة وبيانات الكمبيوتر فحسب، بل تنطبق أيضا على جمع الأدلة الإلكترونية على أي جريمة جنائية. وينطبق هذا النطاق الواسع أيضا على تدابير البروتوكول الإضافي الثاني للاتفاقية.

ويتيح هذا النطاق أيضا أوجه التضافر بين اتفاقية بودابست وغيرها من الاتفاقات الدولية.

مذكرة توجيهية رقم 14 صادرة عن اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية

المعلومات التلقائية
(المادة 26 من الاتفاقية المتعلقة بالجريمة الإلكترونية)[94]

1 مقدمة

قررت اللجنة المعنية باتفاقية الجريمة الالكترونية (اللجنة T-CY)، في دورتها العامة الثامنة (كانون الأول/ديسمبر 2012)، إصدار مذكرات توجيهية تهدف إلى تيسير الاستخدام الفعّال لأحكام اتفاقية الجريمة الالكترونية وتنفيذها، وذلك أيضاً في ضوء التطورات القانونية والسياساتية والتكنولوجية[95].

تمثل المذكرات التوجيهية الفهم المشترك للأطراف في هذه المعاهدة فيما يتعلق باستخدام الاتفاقية.

قد تكون لدى سلطات العدالة الجنائية في إحدى الولايات معلومات تعتقد أنها قد تُفيد طرفاً آخر في تحقيق جنائي أو دعوى قضائية، غير أنه في بعض الحالات، قد لا يكون الطرف القائم بالتحقيق على علم بوجود تلك المعلومات. توفّر المادة 26 من الاتفاقية أساساً قانونياً لإحالة هذه المعلومات إلى الطرف الآخر دون الحاجة إلى طلب مسبق.

لقد ازدادت أهمية المادة 26 بمرور الوقت، لا سيّما في سياق التحقيقات المتعلقة بالشبكة المظلمة أو جمع كميات كبيرة من البيانات المستخلصة من الاتصالات. مع ذلك، لا يستفيد جميع الأطراف من الإمكانيات التي تتيحها هذه المادة بشكل متّسق.

قررت اللجنة، بالتالي، أن إصدار توجيهات بشأن المادة 26، تستند إلى الممارسات الحالية للأطراف في تطبيق هذه المادة، ستكون ذا فائدة، ويسمح للأطراف بالاستفادة الكاملة من الإمكانات التي تتيحها الاتفاقية فيما يتعلق بالمعلومات المقدّمة تلقائياً.

تتناول هذه المذكرة الجوانب الرئيسية لما يلي: (أ) نقل المعلومات المقدّمة تلقائياً؛ و (ب) استخدام تلك المعلومات من قبل الطرف المتلقّي عند الحصول عليها استناداً إلى المادة 26، بما في ذلك مسألة ما إذا كان يمكن استخدام المعلومات المستلمة بموجب هذه المادة كأدلة أم لا.

---

94. تمت مراجعتها في الدورة الثانية والثلاثين للجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية بتاريخ (2-3 حزيران/يونيو 2025)، وتم اعتمادها وفقاً للإجراء الصامت في 25 حزيران/يونيو 2025.
95. انظر ولاية اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية (المادة 46 من الاتفاقية المتعلقة بالجريمة الالكترونية).

تستند هذه المذكرة أيضاً إلى نتائج الردود الواردة من الأطراف على الاستبيان[96] بحلول كانون الثاني/ يناير 2025، وإلى مخرجات فعالية مشتركة بشأن "المعلومات التلقائية" نُظِّمت بالتعاون مع "وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية" في لاهاي، وإلى تقرير تمهيدي[97]، فضلًا عن المناقشات التي أُجريت خلال مؤتمر الأخطبوط (Octopus) المنعقد في بوخارست عام 2023.[98]

2 المادة 26 من الاتفاقية المتعلقة بالجرائم الإلكترونية

نص المادة:

المادة 26 - المعلومات التلقائية

1 يجوز لأي طرف، في حدود تشريعه الوطني ودون طلب مسبق، أن يُحيل إلى طرف آخر معلومات تم الحصول عليها في إطار تحقيقاته الخاصة، متى رأى أن الكشف عن تلك المعلومات قد يُسهم في تمكين الطرف المتلقّي من الشروع في تحقيقات أو إجراءات أو المضي فيها، فيما يتعلق بجرائم أُنشئت وفقاً لأحكام هذه الاتفاقية، أو قد يؤدي إلى تقديم ذلك الطرف طلباً للتعاون بموجب هذا الفصل.

2 يجوز للطرف الموفِّر للمعلومات، قبل إحالتها، أن يطلب الحفاظ على سريّتها أو ألا تُستخدم إلا وفقاً لشروط يحدّدها. وإذا تعذّر على الطرف المتلقّي الالتزام بهذا الطلب، يتعيّن عليه إشعار الطرف الموفِّر، الذي يقرّر بدوره ما إذا كان ينبغي، رغم ذلك، إحالة المعلومات. وإذا قبل الطرف المتلقّي المعلومات رهناً بتلك الشروط، فإنه يلتزم بها.

مقتطف من التقرير التفسيري:

260. تستند هذه المادة إلى أحكام واردة في صكوك سابقة صادرة عن مجلس أوروبا، مثل المادة 10 من الاتفاقية المتعلقة بغسل العائدات المتأتية من الجرائم، والتحري عنها، وحجزها ومصادرتها (سلسلة المعاهدات الأوروبية رقم 141)، والمادة 28 من الاتفاقية الجنائية بشأن الفساد (سلسلة المعاهدات الأوروبية رقم 173).

في ظلّ تزايد الحالات التي يكون فيها لدى أحد الأطراف معلومات قيّمة يعتقد أنها قد تُسهم في تحقيق جنائي أو إجراء جنائي يباشره طرف آخر، دون أن يكون هذا الطرف على علم بوجود تلك المعلومات، فإن طلباً بالتعاون المتبادل لن يُقدَّم في مثل هذه الظروف.

96. تم إرسال استبيان حول ممارسات الأطراف في الاتفاقية إلى ممثلي اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية في يوليو 2024.

97. أمانة اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية ومكتب برنامج الجرائم الإلكترونية التابع لمجلس أوروبا "المعلومات التلقائية" – الممارسات الحالية لاستخدام المادة 26، التي عُرضت في الجلسة العامة الحادية والثلاثين للجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية (11-12 ديسمبر 2024) وتم تحديثها في مايو 2025 (الوثيقة T-CY (2024)11rev).

98. مؤتمر Octopus 2023 (13 ديسمبر 2023) تضمن ورشة عمل حول تبادل المعلومات التلقائي.

تنص الفقرة الأولى على منح الدولة التي بحوزتها المعلومات صلاحية إحالتها إلى دولة أخرى دون طلب مسبق. وقد اعتُبر هذا البند مفيداً، نظراً لأن بعض القوانين الوطنية تتطلب منحاً صريحاً للسلطة القانونية لتقديم المساعدة في غياب طلب رسمي.

لا تُلزَم الدولة الطرف بإحالة المعلومات تلقائياً إلى طرف آخر، بل يمكنها ممارسة سلطتها التقديرية بالنظر إلى ملابسات القضية.

علاوة على ذلك، فإن الكشف التلقائي عن المعلومات لا يحول دون أن تباشر الدولة المُفصِحة، إذا كانت ذات ولاية قضائية، تحقيقاً أو إجراءات جنائية تتعلق بالوقائع التي تم الكشف عنها.

261. تتناول الفقرة الثانية الحالات التي لا يُقدِم فيها الطرف على إحالة المعلومات تلقائياً، إلا إذا توافرت ضمانات للحفاظ على سريّة المعلومات الحسّاسة أو إذا كان بالإمكان فرض شروط على استخدامها. وتُعدّ السرية، على وجه الخصوص، عاملاً حاسماً في الحالات التي قد تتعرّض فيها مصالح جوهرية للطرف الموفِّر للخطر في حال الكشف عن المعلومات، كالحاجة إلى حماية وسيلة جمع المعلومات أو عدم إفشاء كون جماعة إجرامية تخضع للتحقيق.

وإذا كشف الاستعلام المسبق أن الطرف المتلقّي لا يستطيع الالتزام بالشروط التي يطلبها الطرف الموفِّر، على سبيل المثال، إذا تعذّر الحفاظ على السرية لأن المعلومات مطلوبة كدليل في محاكمة علنية، وجب على الطرف المتلقّي إشعار الطرف الموفِّر، الذي يعود له حينئذ أن يقرّر ما إذا كان سيمضي في إحالة المعلومات.

أما إذا قبل الطرف المتلقّي الشروط، فيجب عليه احترامها والالتزام بها. ومن المتوقَّع أن تكون الشروط المفروضة بموجب هذه المادة منسجمة مع الشروط التي قد يفرضها الطرف الموفِّر في حال تلقيه طلباً للتعاون القضائي من الطرف المتلقّي.

3 تفسير اللجنة المعنية باتفاقية الجريمة الإلكترونية للمادة 26 من الاتفاقية المتعلقة بالجريمة الإلكترونية

3.1 نطاق المادة 26، الاعتبارات العامة والضمانات

3.1.1 الطابع التقديري للمادة 26

تنص المادة 26 على أساس قانوني يجيز للطرف أن يُحيل إلى طرف آخر معلومات تم الحصول عليها في سياق تحقيقاته الخاصة.

وتُرك أمر الإحالة التلقائية لتقدير الطرف ذاته، إذ تنص المادة بصيغة (”يجوز للطرف (...)“)، ما يعني أن الطرف غير مُلزَم بإحالة المعلومات تلقائيًا إلى طرف آخر؛ بل له أن يُمارس سلطته التقديرية في ضوء ظروف القضية المعروضة عليه.

3.1.2 حول مفهومي "التلقائية" و"دون طلب مسبق"

ينطوي مفهوم مصطلح "التلقائية" على أن الطرف يقوم بنقل معلومات تم الحصول عليها في إطار تحقيقاته الوطنية من تلقاء نفسه أو بمبادرة منه، دون أن يكون هناك طلب مسبق للمساعدة المتبادلة من طرف آخر.

لا تُستبعد مع ذلك إمكانية إجراء مشاورات غير رسمية بين الأطراف قبل تبادل المعلومات التلقائية. وقد تتعلق هذه المشاورات، على سبيل المثال، بشروط محددة قد يرغب الطرف الموفِّر في فرضها، أو بمسائل مثل توضيح الأسباب التي تجعل، في قضية معينة، نقل البيانات بموجب المادة 26 أكثر ملاءمة من اتباع إجراءات المساعدة القانونية المتبادلة.

في الوقت ذاته، قد ترى الأطراف فائدة في إجراء مشاورات لاحقة بعد أن يتلقى أحد الأطراف المعلومات المنقولة من خلال التبادل التلقائي. وقد أظهرت نتائج الاستبيان أن الأطراف غالبًا ما تنخرط في مشاورات لاحقة بعد الكشف الأولي، لمناقشة التفاصيل والحاجة إلى عمليات كشف إضافية عن معلومات تلقائية. وإذا اتفقت الأطراف، يمكنها مواصلة تبادل المعلومات المستقبلية ذات الصلة بالقضية التي أدّت إلى النقل الأولي، وذلك أيضًا استنادًا إلى المادة 26. وإذا رأت الأطراف أن ثمة بديلًا أنسب، يجوز لها أن تقرر تبادل المعلومات المستقبلية من خلال إجراءات المساعدة القانونية المتبادلة.

3.1.3 حول مفهوم "المعلومات"

يجوز للطرف الموفِّر أن يُحيل أي معلومات ذات صلة تم الحصول عليها في سياق تحقيقاته الخاصة. ويُفهم مصطلح "المعلومات" في هذا السياق على نحو واسع، وقد تتخذ شكل بيانات حاسوبية أو أي شكل آخر من أشكال المعلومات.

يمكن للأطراف أن تنقل أنواعًا مختلفة من المعلومات بموجب الإجراء المنصوص عليه في المادة 26. وقد أوردت الأطراف، في ردودها على الاستبيان، الأمثلة التالية:

- معلومات تم جمعها في سياق تحقيق داخلي؛
- معلومات استخبارية شرطية؛
- تقارير عن الجرائم؛
- هوية الجناة أو الضحايا أو معلومات أخرى متعلقة بارتكاب فعل إجرامي؛
- محاضر استماع إلى الشهود؛
- تقارير عن الحوادث؛
- ثغرات وعمليات استغلال أمنية سيبرانية؛

- عناوين بروتوكول الإنترنت (IP)، والبريد الإلكتروني، وحسابات وسائل التواصل الاجتماعي أو خدمات الرسائل الفورية المرتبطة بهجوم إلكتروني؛
- معلومات متعلقة بالحسابات المصرفية مثل رقم الحساب الدولي (IBAN) أو كشوفات حسابات الضحايا البنكية (أو أجزاء منها)؛
- بيانات تسجيل وبيانات أخرى غير متعلقة بالمحتوى والمرتبطة بالحسابات المستخدمة في ارتكاب الجرائم موضوع التحقيق؛
- محتويات الاتصالات.

يجوز أن تكون المعلومات المُحالة في شكل بيانات حاسوبية أو في أي شكل آخر بحسب ما يحدده الطرف المُحيل للمعلومات.

3.1.4 بشأن مفهومي "بدء أو إجراء تحقيقات أو إجراءات تتعلق بجرائم جنائية محددة وفقاً لهذه الاتفاقية" و "قد تؤدي إلى طلب تعاون من ذلك الطرف بموجب هذا الفصل"

يجوز لأي طرف أن ينظر في إحالة المعلومات التي حصل عليها في إطار تحقيقاته الخاصة إلى طرف آخر بشكل تلقائي، وفقاً للشروط التالية:

- قد تساعد هذه المعلومات الطرف المتلقي في بدء أو إجراء تحقيقات أو إجراءات تتعلق بجرائم جنائية محددة وفقاً لهذه الاتفاقية؛ أو
- قد تؤدي هذه المعلومات إلى طلب تعاون من ذلك الطرف بموجب هذا الفصل.

تنص المادة 23[99]، التي تحدد المبادئ العامة للتعاون الدولي، بوضوح على أن التعاون ليس ممكناً فقط لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المتصلة بأنظمة الحاسوب والبيانات، بل أيضاً لجمع الأدلة في شكل إلكتروني عن أي جريمة جنائية:

> المادة 23 – المبادئ العامة المتعلقة بالتعاون الدولي
>
> يتعاون الأطراف فيما بينهم، وفقًا لأحكام هذا الفصل، ومن خلال تطبيق الصكوك الدولية ذات الصلة بالتعاون الدولي في المسائل الجنائية، والترتيبات المتفق عليها استنادًا إلى تشريعات موحدة أو متبادلة، والتشريعات الوطنية، إلى أوسع حد ممكن، وذلك لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية المرتبطة بأنظمة الحواسيب والبيانات، أو بغرض جمع الأدلة الإلكترونية المتعلقة بجريمة جنائية.

99. كل من المادة 23 والمادة 26 تندرجان تحت الفصل 3 نفسه من الاتفاقية، مما يجعل المادة 23 قابلة للتطبيق بالكامل على المادة 26.

ينطبق هذا النطاق الواسع أيضًا على المادة 26. ففي الممارسة العملية، تقوم الأطراف بتقديم المعلومات تلقائيًا بموجب المادة 26 فيما يتعلق بأي جريمة جنائية، دون حصر ذلك في الجرائم المتعلقة بأنظمة الحواسيب أو البيانات.

بالإضافة إلى ذلك، تقدم الأطراف المعلومات تلقائيًا لأغراض متنوعة، بما في ذلك المعلومات التي قد تساعد الدولة المتلقية في الشروع في التحقيقات أو الإجراءات الجنائية أو في مباشرتها، أو المعلومات التي قد تُسهم في منع ارتكاب جريمة، أو تلك التي قد تؤدي إلى طلب تعاون قانوني متبادل من الدولة المتلقية.

بشكل عام، تقدم الأطراف أية معلومات تراها ذات صلة. ويعود للدولة المتلقية أن تقرر كيفية التعامل مع المعلومات المستلمة، مع مراعاة أي شروط قد تفرضها الدولة التي قدمت المعلومات.

3.1.5 حول مفهوم "في حدود قانونه الداخلي"

عند البتّ فيما إذا كان سيتمّ إحالة المعلومات إلى طرف آخر، ينبغي أن يُسترشد الطرف بـ "حدود قوانينه الداخلية". ويجوز للأطراف، وفقًا لقوانينها الوطنية، أن تحدد تلك الحدود بموجب سلطتها التقديرية. وتشمل هذه الحدود الشروط والضمانات المنصوص عليها في المادة 15 من الاتفاقية[100].

يُفترض أيضًا أن الطرفين، المرسل والمستلم، يحترمان سيادة القانون ومبادئ حقوق الإنسان، وذلك بما يتماشى مع المادة 15 من الاتفاقية.

> المادة 15 – الشروط والضمانات
>
> 1– يجب على كل طرف أن يضمن أن وضع وتنفيذ وتطبيق الصلاحيات والإجراءات المنصوص عليها في هذا القسم يخضع للشروط والضمانات المنصوص عليها في قانونه الداخلي، والتي يجب أن تكفل الحماية الكافية لحقوق الإنسان والحريات، بما في ذلك الحقوق المكفولة بموجب الالتزامات التي تعهّد بها بموجب اتفاقية مجلس أوروبا لعام 1950 لحماية حقوق الإنسان والحريات الأساسية، والعهد الدولي الخاص بالحقوق المدنية والسياسية الصادر عن الأمم المتحدة لعام 1966، وغيرها من صكوك حقوق الإنسان الدولية ذات الصلة، كما يجب أن تتضمن هذه الشروط والضمانات مبدأ التناسب.
>
> 2– ويجب أن تشمل هذه الشروط والضمانات، بحسب ما يكون مناسبًا بالنظر إلى طبيعة الإجراء أو الصلاحية المعنية، على سبيل المثال لا الحصر: الرقابة القضائية أو المستقلة الأخرى، والأسباب المبرّرة للتطبيق، وتحديد نطاق ومدّة هذه الصلاحية أو الإجراء.

100. بما في ذلك المعلومات السرية/المقيدة بسبب الامتيازات القانونية والحصانات وحماية الشهود، وما إلى ذلك، استناداً إلى الفقرة 147 من التقرير التفسيري للاتفاقية.

3- بالقدر الذي يتوافق مع المصلحة العامة، ولا سيما الإدارة السليمة للعدالة، يجب على كل طرف أن يأخذ بعين الاعتبار أثر الصلاحيات والإجراءات المنصوص عليها في هذا القسم على حقوق ومسؤوليات ومصالح الأطراف الثالثة المشروعة.

3.2 السلطات التي تعتبر مختصة وفقا للمادة 26

بعض أحكام الفصل الثالث من الاتفاقية (على سبيل المثال، المادة 24 المتعلقة بالتسليم، أو المادة 27 المتعلقة بالإجراءات الخاصة بطلبات المساعدة المتبادلة في غياب اتفاقيات دولية سارية) تُلزم الأطراف بتعيين سلطات مختصة بهذه الأنواع المحددة من التعاون.

أما المادة 26، فلا تتضمن مثل هذا الالتزام، بل تشير ببساطة إلى "الطرف". وتترك هذه المادة الحرية للطرف المعني في أن يحدد، وفقًا لتقديره، السلطات التي يعتبرها مختصة بنقل المعلومات إلى طرف آخر.

تُظهر الممارسة العملية للأطراف في الاتفاقية وجود مجموعة واسعة من السلطات التي تقوم بنقل المعلومات، بما في ذلك السلطات الشرطية، ووكلاء النيابة، والقضاة. وفي بعض الحالات، يبدأ تبادل المعلومات التلقائي كتعاون **شرطي-شرطي**[101]، ثم يتحول إلى **تعاون قضائي** عندما تُستخدم المعلومات المتبادلة ضمن الإجراءات القانونية الرسمية أو تُعتمد كدليل أمام المحكمة.

استنادًا إلى نتائج الاستبيانات، تستخدم بعض الأطراف أيضًا الاتصال المباشر بين السلطات المعنية. وقد يبدأ الأمر بتواصل أولي بين السلطات المركزية، ثم يتطور لاحقًا إلى تبادلات مباشرة بين الجهات المختصة. مع ذلك، تُفضل بعض الأطراف التواصل أو التنسيق من خلال السلطات المركزية، نظرًا لقدرتها على توفير التوجيه اللازم للسلطات الوطنية بشأن القوانين والشروط المطبقة داخليًا.

كما كشفت نتائج الاستبيانات أن الأطراف تستخدم قنوات وطنية متنوعة (مثل شبكة نقاط الاتصال[102] المتوفرة على مدار الساعة 7/24 أو السلطات المركزية) لنقل المعلومات بموجب المادة 26، كما تلجأ أيضًا إلى قنوات دولية (مثل المنظمة الدولية للشرطة الجنائية (الإنتربول)، ووحدة التعاون القضائي في الاتحاد الأوروبي (اليوروجاست)، ووكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اليوروبول) لنقل مثل هذه المعلومات.

101. مع ذلك، قد تفرض بعض الأطراف شروطاً إضافية محددة لاستخدام المعلومات التي تم الحصول عليها من خلال التعاون الشرطي كأدلة في الإجراءات الجنائية في الطرف المتلقي.
102. انظر المادة 35 من اتفاقية بودابست بشأن الجرائم الإلكترونية.

3.3 السرية وشروط أخرى

3.3.1 السرية

وفقًا للمادة 2.26 من الاتفاقية، يجوز للطرف أن يُخضع تقديم المعلومات من تلقاء نفسه لشرط يقضي بالحفاظ على سرية المعلومات الحساسة، أو أن يفرض شروطًا أخرى تتعلق باستخدام تلك المعلومات، بما في ذلك، على سبيل المثال، المهل الزمنية، أي عدم استخدام المعلومات كما هي قبل أن تصل القضية الجنائية إلى المحكمة في الدولة المقدِّمة.

تُعد السرية من أكثر الشروط التي تفرضها الأطراف شيوعًا لضمان سرية التحقيقات أو الإجراءات الجارية لدى الطرف المقدِّم.

تُعتبر السرية "عنصرًا بالغ الأهمية في الحالات التي قد تُهدَّد فيها مصالح جوهرية للطرف المقدِّم في حال إتاحة المعلومات للعامة، على سبيل المثال، في الحالات التي تستدعي حماية هوية وسيلة جمع المعلومات أو سرية التحقيق الجاري مع جماعة إجرامية" (الفقرة 261 من التقرير التفسيري للاتفاقية).

3.3.2 شروط أخرى

يجوز للأطراف أن تُخضع الكشف التلقائي عن المعلومات لشروط إضافية، يتم تحديدها على أساس كل حالة على حدة.

رغم أن الأطراف يجوز لها فرض مجموعة واسعة من الشروط بموجب هذه المادة، إلا أنه من المتوقع أن تكون الشروط المفروضة متسقة مع تلك التي يمكن أن يفرضها الطرف المقدِّم استجابةً لطلب المساعدة المتبادلة المقدم من الطرف المتلقِّي (الفقرة 261 من التقرير التفسيري للاتفاقية).

وقد كشفت ردود الأطراف على الاستبيان وملاحظاتها أثناء عملية إعداد هذه المذكرة الإرشادية، أن الشروط قد تشمل، على سبيل المثال، ما لم يتعارض مع الاتفاقات أو الترتيبات القائمة بين الأطراف المعنية:

- عدم استخدام المعلومات المقدمة لأي غرض غير الذي قُدمت من أجله (إذا تم تحديد الغرض)؛
- عدم نقل المعلومات إلى دولة أخرى دون الحصول على موافقة مسبقة؛
- استخدام المعلومات فقط للشروع في إجراء قانوني أو لتقديم طلب مستقبلي للمساعدة القانونية المتبادلة؛
- الامتثال لشروط حماية البيانات؛

- مبدأ المعاملة بالمثل: ضمان أنه في حال وقوع حالة مماثلة مستقبلاً، وإذا كان الطرف قد حصل على معلومات ذات صلة من خلال تحقيقاته الخاصة، فسيبذل كل الجهود المعقولة لتطبيق الإجراءات المنصوص عليها في المادة 26 وإحالة المعلومات ذات الصلة إلى الطرف الذي فرض شرط المعاملة بالمثل مسبقًا؛
- عدم استخدام المعلومات كدليل في الإجراءات الجنائية؛
- ضمان الاستخدام المناسب والمشروع للمعلومات؛
- تقديم إشعار بشأن أي استخدام لاحق أو متابعة لكيفية استخدام المعلومات؛
- استخدام المعلومات فقط لغرض التحقيق في ارتكاب جريمة وفي الإجراءات الجنائية؛
- إشعار الطرف المقدِّم أو الحصول على إذنه قبل أي استخدام قد يؤدي إلى نشر المعلومات أو جعلها علنية؛
- عدم استخدام المعلومات لأغراض إجراءات تنتهك الحقوق والضمانات الأساسية؛
- استخدام المعلومات وفقًا للشروط المنصوص عليها في المعاهدات متعددة أو ثنائية الأطراف؛
- استخدام المعلومات وفقًا لشروط أخرى تحددها السلطات المختصة/أو تبعًا لكل حالة؛
- بند السرية (التحفظ على الهوية): باستثناء الظروف الاستثنائية التي تُحدد وفقًا للقانون الوطني للطرف المقدِّم، لن يقدِّم هذا الطرف معلومات تتعلق بهوية المحققين، ولن يستجيب لأي طلبات لأخذ إفادة من المحققين سواء في جلسة محكمة أو في أي مكان آخر.

مع ذلك، ينبغي الإشارة إلى أن المادة 26 لا تُلزم بفرض شروط، إذ إن للطرف المقدِّم الحرية في أن يقرِّر عدم فرض أي شروط على استخدام المعلومات من قبل الطرف المتلقِّي إذا لم يرَ ضرورة لذلك في قضية معينة. ويُترك للطرف المقدِّم تقدير مسألة الكشف عن المعلومات، وكذلك الشروط التي قد تُفرض على استخدامها، إن وُجدت.

3.3.3 استخدام المعلومات كدليل في الإجراءات الجنائية لدى الطرف المتلقّي

يجوز للطرف المقدِّم أن يُقيّد الكشف عن المعلومات بشرط عدم استخدامها كدليل في الإجراءات الجنائية لدى الطرف المتلقِّي. وبدلًا من ذلك، يجوز للطرف المقدِّم أن يرفق بالكشف شروطًا مناسبة أخرى، والتي إذا تم الوفاء بها، تُجيز استخدام المعلومات كدليل في الطرف المتلقِّي، وذلك في حدود ما يتوافق مع قوانينه الوطنية. ومثال على ذلك، اشتراط الطرف المقدِّم على الطرف المتلقِّي أن يسعى للحصول على المعلومات التي تم تبادلها بموجب المادة 26 أيضًا من خلال إجراء للمساعدة القانونية المتبادلة، قبل أن يُسمح باستخدامها كدليل في الإجراءات الجنائية لدى الطرف المتلقِّي.

مع ذلك، إذا لم تُفرض مثل هذه الشروط، يجوز للطرف المتلقِّي استخدام المعلومات كدليل في الإجراءات الجنائية، في حدود ما يتوافق مع قانونه الوطني. ويتماشى هذا النهج مع أحكام الاتفاقية.

في بعض الدول الأطراف، يجيز القانون الوطني استخدام المعلومات المُقدمة تلقائيًا كدليل في الإجراءات الجنائية، إذا كان ذلك يتوافق مع القانون الوطني للطرف المقدِّم، أو إذا منح هذا الطرف تفويضًا أو موافقة على ذلك. وفي حال وجود أي غموض، غالبًا ما تلجأ الأطراف إلى التشاور.

لا تحتوي المادة 26 على أية قواعد تتعلق بقَبول الأدلة (قابليتها للإثبات)، وتعتبر اللجنة المعنية بالاتفاقية المتعلقة بالجرائم الإلكترونية أن هذه المسألة تخضع للقانون الوطني لكل طرف. ومن شأن التشاور بين الأطراف أن يقلل من خطر عدم قبول المعلومات المُحوَّلة كدليل لدى الطرف المتلقِّي.

كما ينبغي الإشارة إلى أن الطرف المقدِّم لا يمكنه إلزام الطرف المتلقِّي باستخدام المعلومات كدليل في إجراءات جنائية تخصه. فقد توجد شروط وقيود متعددة في القانون الوطني للطرف المتلقِّي تتعلق بنوع المعلومات التي يمكن استخدامها كدليل إلكتروني في إجراءاته الجنائية. بل إن القوانين الوطنية لبعض الأطراف قد تستبعد استخدام المعلومات المُقدمة تلقائيًا كدليل في الإجراءات الجنائية، على سبيل المثال، في الحالات التالية:

- إذا تم الحصول على المعلومات من خلال قناة أو جهة لا يعتبرها القانون الوطني مختصة بتبادل الأدلة (على سبيل المثال، المعلومات التي تم الحصول عليها عبر تعاون شرطي-شرطي)؛
- إذا تم الحصول على المعلومات بطريقة لا تتوافق مع القانون الوطني الذي ينظّم إجراءات الحصول على مثل هذه المعلومات لدى الطرف المتلقِّي؛
- لا يجوز استخدام المعلومات إلا لغرض محدد، مثل منع تهديد وشيك وخطير للأمن العام؛
- المعلومات قائمة في أغلبها على أقوال غير مباشرة (نقل عن الغير)، ولا يمكن تحديد مصدر أصلي يمكنه تأكيد صحتها أو موثوقيتها؛
- المعلومات ذات حساسية عالية (على سبيل المثال، تتطلّب أنواع معينة من البيانات الحساسة، مثل بيانات المحتوى أو البيانات المتعلقة بالسرية المصرفية، إجراءات خاصة مختلفة).

لذلك، قد يكون من المفيد للطرفين التشاور بشأن كيفية تبادل المعلومات بشكل تلقائي، وذلك من أجل زيادة فرص استخدامها دون الحاجة إلى تقديم طلبات أو اتخاذ إجراءات إضافية. مع ذلك، إذا كان القانون الوطني للطرف المتلقِّي يقتضي الحصول على المعلومات بوسائل أخرى حتى يمكن استخدامها كدليل في الإجراءات الجنائية، مثل الحصول عليها من خلال إجراء للمساعدة القانونية المتبادلة عبر السلطة المركزية المعيّنة رسميًا، فعلى الطرف الذي قدم المعلومات تلقائيًا أن يحترم هذه المتطلبات. ولا ينبغي لذلك الطرف أن يرفض تنفيذ طلب لاحق للمساعدة

القانونية المتبادلة بحجة أنه سبق له أن قدم تلك المعلومات من خلال الإفصاح التلقائي. علاوة على ذلك، وخاصة في الحالات التي يُتوقَّع فيها تقديم طلب لاحق للمساعدة القانونية المتبادلة، قد يكون من المفيد توثيق المعلومات التي تم تبادلها سابقًا بموجب المادة 26 بشكل واضح (على سبيل المثال، من خلال استخدام ملفات مضغوطة وقيم التجزئة "hash values")، حتى يتسنى للطرف المقدِّم إعادة تقديم البيانات بسهولة ردًا على طلب المساعدة القانونية الرسمي.

3.4 التشاور والمتابعة

إذا لم يتمكن الطرف المتلقِّي من الامتثال لشرط طلبه الطرف المقدِّم (على سبيل المثال، إذا تعذّر عليه الامتثال لشرط السرية لأن المعلومات مطلوبة كدليل في محاكمة علنية لدى الطرف المتلقِّي)، وجب على الطرف المتلقِّي إبلاغ الطرف المقدِّم بذلك، والذي يملك حينها خيار عدم تقديم المعلومات. مع ذلك، إذا وافق الطرف المتلقِّي على الشرط، فلا بد له من الالتزام به (الفقرة 261 من التقرير التفسيري للاتفاقية).

بالتالي، تنص المادة 26 على إمكانية التشاور بين الأطراف في حال إبلاغ الطرف المقدِّم بعدم القدرة على الامتثال لشرط معين.

مع ذلك، قد يكون هذا التشاور مفيدًا أيضًا في الحالات التي لم يُفرض فيها أي شرط محدد. فعلى سبيل المثال، يمكن أن يساعد في تحديد ما إذا كان يجوز استخدام المعلومات المقدمة تلقائيًا كدليل في الإجراءات الجنائية لدى الطرف المتلقِّي، إذا كان هذا الأمر غير واضح عند تقديم المعلومات.

بالإضافة إلى ذلك، وكممارسة جيدة، تستخدم العديد من الأطراف مثل هذه المشاورات للمتابعة مع الطرف الذي تم الحصول على المعلومات منه، بغرض إطلاع ذلك الطرف على كيفية التعامل مع المعلومات.

يُعد هذا الأمر مفيدًا للحفاظ على تعاون وثيق مع الطرف الآخر. وقد يتم تقديم هذه المتابعة عند طلبها صراحة من الطرف الذي قدم المعلومات تلقائيًا، ولكنها لا تقتصر فقط على هذه الحالات.

لقد أظهرت الممارسة أن المتابعة مع الطرف الذي قدّم المعلومات يمكن أن تكون مفيدة في الحالات التالية:

- خلال تحقيق تم البدء فيه أو تنفيذه استنادًا إلى المعلومات المقدمة تلقائيًا، تم الحصول على معلومات جديدة قد تكون ذات صلة بالطرف المقدِّم أو بطرف آخر؛
- ما إذا تم الشروع في تحقيق جنائي (أو ملاحقة قضائية) أو تم رفضه بناءً على المعلومات المحصل عليها؛
- ما إذا كانت المعلومات قد أدت إلى تحقيق إضافي أو كانت مفيدة له، وما هو مدى تقدم هذا التحقيق؛

- في حالة الحاجة إلى مزيد من التعاون بسبب نقص بعض عناصر المعلومات؛
- عند صدور القرار النهائي (الحكم النهائي) من قبل المحكمة.

ما لم يُطلب ذلك كشرط محدد من الطرف المقدِّم، فإن الأمر متروك للطرف المتلقِّي للمعلومات المقدمة تلقائيًا لتحديد ما إذا كان سيتم تقديم متابعة ولأي حالات تحدد ذلك.

كما أظهرت الممارسة أن الأطراف تستخدم أيضًا قنوات غير رسمية لأغراض المتابعة، بما في ذلك التواصل الشفهي أو الإلكتروني.

3.5 أمثلة على استخدام المعلومات التلقائية

- تقوم سُلطات الطرف 1، التي تُجري تحقيقًا في منتدى على الإنترنت يُستخدم لتبادل مواد استغلال وإساءة معاملة الأطفال، باكتشاف أن أحد أعضاء هذا المنتدى يتواصل باستخدام عنوان بروتوكول إنترنت (IP) يعود للطرف 2. يجوز لسلطات الطرف 1 استخدام المادة 26 لمشاركة هذه المعلومات مع سلطات الطرف 2، التي يمكنها بعد ذلك بدء تحقيق خاص بها بشأن ذلك العضو. ورغم أن هذه المعلومات يتم مشاركتها من قِبل سلطات الطرف 1 دون طلب مساعدة قانونية متبادلة، إلا أن الطرف 2 المتلقّي للمعلومات قد يقرر المتابعة بطلب مساعدة قانونية متبادلة إذا كان ذلك مطلوبًا بموجب قانونه الداخلي لاستخدام المعلومات كدليل في الإجراءات الجنائية اللاحقة.
- من خلال تحقيقاتها، حصلت سلطات أحد الأطراف على كمية كبيرة جدًا من البيانات المتعلقة بالاتصالات بين مرتكبي جرائم من عدة ولايات قضائية، بما في ذلك مرتكبي جرائم في أطراف أخرى. يمكن لتلك السلطات استخدام المادة 26 لمشاركة هذه المعلومات مع سلطات تلك الأطراف الأخرى – دون الحاجة إلى تقديم طلبات مساعدة قانونية متبادلة – والتي يمكنها بعد ذلك الشروع في تحقيقاتها الخاصة.
- تتلقى سلطات أحد الأطراف إشعارًا من شخص اعتباري موجود على إقليمها بشأن حصول دخول غير مشروع وتدخل في البيانات، بعد أن تم تحديد فقدان كبير في البيانات قد يُشير إلى التحضير لهجوم بفدية إلكترونية. وبعد التحقيق، تبيّن أن المشتبه به ينتمي إلى ولاية قضائية أخرى انطلقت منها الهجمات. يُعد تبادل المعلومات عبر المادة 26 تدبيرًا مهمًا يتيح لسلطات الطرف الثاني بدء تحقيقها الخاص ووقف النشاط الإجرامي.
- تُجري سلطات أحد الأطراف تحقيقًا في قضية احتيال عبر الحاسوب تشمل جناة وضحايا، بما في ذلك في ولايات قضائية متعددة لأطراف أخرى، حيث تم اختراق بياناتهم المالية. إن مشاركة المعلومات بشكل تلقائي مع سلطات تلك الأطراف الأخرى قد تتيح لها بدء تحقيقاتها الخاصة وتحديد الضحايا الموجودين في إقليمها. في الوقت ذاته، يجوز للطرف الذي يُقدّم المعلومات بشكل تلقائي أن يطلب من الطرف

المتلقّي تقديم متابعة لاحقة، في حال كانت لديه أي معلومات قد تكون مفيدة في التحقيقات أو الإجراءات الجنائية في الدولة التي قدّمت المعلومات بشكل تلقائي.

- قد تُعدّ المادة 26 أداة مفيدة وفعّالة بشكل خاص لتبادل المعلومات التلقائية التي تشير إلى خطر كبير ووشيك يهدد حياة أو سلامة أي شخص طبيعي[103] في دولة طرف أخرى. وقد تشمل مثل هذه الحالات الطارئة أعمالًا إرهابية أو اختطافًا أو الاستغلال والانتهاك الجنسي الجاري للأطفال. ويمكن أن تُسهم مشاركة المعلومات بشكل تلقائي في تحديد هوية وإنقاذ ضحايا الجرائم الخطيرة. وقد يفرض الطرف الذي يشارك المعلومات، على سبيل المثال، شرطًا يقضي بأن تُستخدم المعلومات فقط لمعالجة حالة الطوارئ.

4 بيان اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الالكترونية

تتفق اللجنة المعنية بالاتفاقية المتعلقة بالجريمة الإلكترونية على أن ما سبق يُمثّل الفهم المشترك بين الأطراف بشأن نطاق وعناصر المادة 26 من الاتفاقية التي تنظم تبادل المعلومات التلقائية.

تشكّل المادة 26 أساسًا قانونيًا إيجابيًا يُمكّن الطرف من مشاركة المعلومات التي حصل عليها خلال تحقيقاته مع طرف آخر دون الحاجة إلى طلب مسبق للمساعدة القانونية المتبادلة، وذلك عندما يرى أن الكشف عن تلك المعلومات قد يُسهم في مساعدة الطرف المتلقي على بدء أو تنفيذ تحقيقات أو إجراءات قانونية، أو قد يؤدي إلى طلب تعاون من ذلك الطرف.

يجوز للطرف المتلقي استخدام هذه المعلومات كدليل في الإجراءات الجنائية، ما لم تكن هناك شروط تمنع ذلك فرضها الطرف المزوِّد، أو كان هذا الاستخدام مخالفًا للقانون الداخلي للطرف المتلقي.

نظرًا للفوائد الكبيرة التي يمكن أن توفّرها المادة 26، تشجّع اللجنة الأطراف على النظر في كيفية استخدام آلية "المعلومات التلقائية" بموجب هذه المادة بشكل فعّال من قِبل سلطاتها المختصة.

103. تعرّف بأنها "حالة طارئة" في المادة 2.3.ج من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإلكترونية (سلسلة المعاهدات الأوروبية رقم 224).

PREMS 126425

ARA

مجلس أوروبا هوالمنظمة الرائدة لحقوق الإنسان في القارة الأوروبية. ويضم 46 دولة عضو، بما في ذلك جميع أعضاء الاتحاد الأوروبي. وقد وقعت جميع الدول الأعضاء في مجلس أوروبا على الإتفاقية الأوروبية حقوق الإنسان ، وهي معاهدة مصممة لحماية حقوق الإنسان، والديمقراطية، وسيادة القانون. وتشرف المحكمة الأوروبية لحقوق الإنسان على تنفيذ الاتفاقية في الدول الأعضاء.

www.coe.int

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE