الأمم المتحدة A/CONF.187/L.10

مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين

Distr.: Limited
16 April 2000
ARABIC
Original: English

فيينا، ١٠-١٧ نيسان/أبريل ٢٠٠٠

البند ٥ من جدول الأعمال
منع الجريمة منعا فعالا: مواكبة التطورات الجديدة

تقرير اللجنة الثانية

حلقة العمل المعنية بالجرائم المتصلة بشبكات الحواسيب

مقدمة

١- عقدت حلقة العمل المعنية بالجرائم المتصلة بشبكات الحواسيب، التي نظمها معهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين، في ١٥ نيسان/أبريل ٢٠٠٠. وكان معروضا على حلقة العمل ورقة معلومات خلفية بشأن هذا الموضوع (A/CONF.187/10).

٢- وألقى مدير المعهد، السيد ميكيناو كايتادا، كلمة افتتاحية في حلقة العمل.

٣- وأشارت معالي السيدة آن ماك ليلان، وزيرة العدل ورئيسة النيابة العامة في كندا، في كلمة رئيسية ألقتها في حلقة العمل، الى تزايد خطورة الجرائم الحاسوبية الوطنية وعبر الوطنية وأهمية وضع قوانين واجراءات فعالة لمكافحتها دون التدخل الذي لا مسوغ له في الآثار المشروعة والخيّرة الناجمة عن التكنولوجيات الجديدة.

٤- وعقدت حلقة العمل سلسلة من المناقشات أجرتها أفرقة مناقشة. فقد استعرض الفريق الأول الجرائم الحاسوبية من منظور علم الاجرام. أما مناقشات الفريق الثاني فقد شملت مخططا افتراضيا لدراسة حالة افرادية بشأن القضايا التقنية والقانونية التي تنشأ عن التفتيش القانوني عن البيانات من الشبكات الحاسوبية وضبط تلك البيانات. وتمثلت مناقشات الفريق الثالث في مخطط افتراضي لدراسة حالة افرادية بشأن تعقب الاتصالات الحاسوبية في الشبكات المتعددة الجنسية. أما المناقشات التي دارت في الفريق الرابع والأخير، فقد تناولت العلاقة بين انفاذ القوانين وصناعتي الحاسوب والانترنت. وقد ألقى كلمة خلال المناقشات ممثلو ٩ حكومات و١٧ خبيرا.*

* ترد قائمة الخبراء في مرفق هذا التقرير.

المناقشة العامة

٥- أشير الى أن استحداث تكنولوجيات جديدة أتاح فرصا جديدة للمجرمين. وقد استحدث تعبير "الجريمة الحاسوبية" لكي يشمل كلا من الأشكال الجديدة تماما من الجرائم التي تستهدف الحواسيب والشبكات ومستخدميها وأشكال الجريمة ذات الطابع التقليدي أكثر التي ترتكب الآن باستخدام معدات حاسوبية أو بالاستعانة بها. وأجري استعراض للردود القانونية على الجرائم الجديدة. وجرى التشديد في هذا الصدد على أهمية وضع قوانين جنائية وافية بالغرض في كل بلد، نظرا للسهولة التي يمكن بها ارتكاب هذه الجرائم عبر الحدود الوطنية.

٦- وأشير الى أن البيئة الجديدة التي أوجدتها الشبكات الحاسوبية تطرح تحديا للعديد من الافتراضات التقليدية لدى النظم القانونية. ونوقشت الحاجة الى عصرنة القوانين من أجل مواكبة التكنولوجيا. ولوحظ أن مفاهيم قانونية، كالممتلكات والسرقة والحيازة، شائعة التطبيق في القوانين الجنائية للبلدان، لكنها لا تطبق بالضرورة على البيانات الحاسوبية التي هي غير ملموسة بحكم طبيعتها. وأفيد بأن السهولة التي يمكن بها تحوير البيانات تسببت أيضا في ظهور مشاكل قانونية جديدة مقترنة بجمعها وحفظها واستخدامها كأدلة في الاجراءات القانونية.

٧- وأشير الى أن الصلاحيات والأساليب اللازمة لاجراء تحقيقات فعالة في الشبكات الحاسوبية تثير أيضا شواغل كبيرة بشأن حقوق الانسان والحرمة الشخصية، لسببين هما طبيعتها الاقتحامية والكميات الكبيرة من المعلومات الشخصية وغيرها المخزونة والمرسلة على تلك الشبكات. واتفق على أن احدى القضايا الأساسية التي تواجه الحكومات في الحاضر والمستقبل هي الحاجة الى العثور على التوازن الصحيح بين الحق الفردي للمواطن في أن تصان حرمته الشخصية والمصالح التي يمليها انفاذ القانون. ولوحظ أن المسائل المتعلقة بالحرمة الشخصية قد تظهر في عدد من الحالات. ولوحظ أيضا أن قوانين بعض البلدان تقيم تمييزا واضحا بين التفتيش عن البيانات المرسلة واعتراض سبيلها والتفتيش عن البيانات المخزونة، بينما قد يكون هذا التمييز غير واضح في نظم قانونية أخرى. وأشير الى أنه قد تكون هناك حاجة، عندما تعتبر البيانات رسائل يجري ارسالها، وبالتالي يمكن اعتراضها لا ضبطها، الى اشتراطات أكثر صرامة للحصول على التراخيص اللازمة والى ضمانات تحكم اجراء هذا التفتيش. وفي هذا الصدد، ارتئي أن الأدلة التي تلتمسها أجهزة انفاذ القوانين قد تمتزج بمواد أخرى كسجلات الأعمال التجارية أو السجلات الطبية للطرف المستهدف أو لطرف ثالث.

٨- ولوحظ أن قضايا عديدة تثار عندما تسعى سلطات انفاذ القانون الى الحصول على معلومات من موفري خدمات الانترنت. وهي تشمل المسألة العملية المتعلقة بالعثور على شخص بواسطة موفر الخدمات الذي يمكن الاتصال به عند الاقتضاء، والمسألة القانونية المتعلقة بما اذا كان يجوز لموفر الخدمات أن يفشي المعلومات طواعية أم لا. وأشير الى أن قوانين بعض البلدان فيما يتعلق بالحرمة الشخصية أو بحماية البيانات تحظر على موفري الخدمات افشاء بعض أو كل المعلومات المتعلقة بالاتصالات التي يقوم بها زبائنهم دون صدور أمر قضائي في هذا الشأن، وأن القوانين قد لا تكون واضحة بشأن ما اذا كان ينبغي لموفر الخدمات أن يحتفظ بسجلات للمحتوى أو المعاملة التجارية بحيث يتسنى استرجاعها بعد ذلك اذا كانت هناك حاجة اليها في التحقيق.

٩- ولاحظ عدد من المشاركين أنه، عندما تكون الأدلة التي تلتمس أجهزة انفاذ القانون الحصول عليها موجودة في النظم الحاسوبية لمؤسسة تجارية مشروعة، فقد يضر التفتيش عنها بالمؤسسة التجارية اذا انطوى التفتيش على تدخل في العمليات الحاسوبية. واتفق على أن التحدي في هذه الحالات يتمثل في تنفيذ التفتيش بفعالية ولكن دون تعطيل السير العادي للعمليات التجارية.

١٠- ورئي أن البعد عبر الوطني لكثير من الجرائم الحاسوبية يمكن أن يتسبب في تعقيدات أكبر بكثير، وليس أقلها التعقيدات فيما يتعلق بالاختصاص القضائي. فالمسائل ذات الصلة بتحديد البلد الذي تنطبق قوانينه، وبصلاحية التحقيق للحصول على الأدلة واقتفاء أثر المجرمين أو الكشف عن هويتهم، وصلاحية تسليم المجرمين ثم محاكمتهم، تتوقف كلها بقدر ما على المكان الذي ارتكبت فيه الجريمة. وأفيد بأن تحديد المكان غير واضح اذا ارتكبت الجريمة في أكثر من موقع بواسطة تكنولوجيات الشبكات الحاسوبية. وذكر مثال لموقع شبكي في أحد البلدان يتضمن مضاربة احتيالية بشأن شركة يتاجر بأسهمها في سوق للأوراق المالية في بلد آخر. وبالتالي، يمكن أن تكون الجريمة ارتكبت في أحد البلدين أو في البلد الآخر أو في كليهما أو لم ترتكب في أي منهما، وهذا يتوقف على قوانين البلدان المعنية.

١١- ولوحظ أن تدابير التفتيش والضبط تصبح معقدة أيضا عندما يوجد المفتشون في ولاية قضائية وتوجد الأدلة في ولاية قضائية أخرى. فالتفتيش الذي يستهدف شبكة يمكن أن يقود الى أدلة مخزونة في بلد مختلف، مما يثير أسئلة بشأن ما اذا كانت هناك حاجة الى اذن من سلطات البلد الثاني للحصول على الأدلة، أو ما اذا كان ينبغي اخطار سلطات البلد الثاني بأن التفتيش جار. ولوحظ أنه، عندما يقتضي الأمر طلب المساعدة من خلال القنوات القانونية الرسمية للبلدين، قد يكون الوقت المستغرق للحصول على هذه المساعدة كبيرا. وأشير الى أن المسألة المتعلقة بالكيفية التي يمكن بها تعجيل هذه العملية قد تكون مسألة حاسمة في معالجة الحالات التي تنطوي على جرم حاسوبي يجري ارتكابه، أو عندما يحتمل أن يقع اتلاف الأدلة أثناء الوقت اللازم للحصول على المساعدة القانونية من خلال القنوات القائمة.

١٢- ولوحظ أن هناك مسألة أخرى تثيرها الطبيعة عبر الوطنية للجريمة الحاسوبية والسهولة التي يمكن بها تحريف الأدلة، وهي مشكلة تحديد صحة الأدلة التي يحصل عليها في عملية تفتيش عبر الحدود. وقيل ان تحديد ذلك قد يقتضي ارساء اجراءات أو بروتوكولات بغية استخدامها في عمليات التفتيش الحاسوبية من أجل ضمان صحة البيانات المسترجعة وكذلك شفافية وسلامة الاجراءات التي من شأنها أن تمكن من اثبات صحة البيانات. ولوحظ أنه قد توجد في بعض البلدان متطلبات رسمية تعوق استعمال البيانات الالكترونية كأدلة.

١٣- وكان هناك اتفاق عام على ضرورة أن تسعى الدول، حيثما كان ذلك ملائما، الى تحقيق الاتساق بين أحكامها ذات الصلة بالتجريم والأدلة والاجراءات.

الخلاصة

١٤- توصلت حلقة العمل الى الاستنتاجات التالية:

(أ) ينبغي تجريم الجرائم الحاسوبية؛

(ب) ثمة حاجة الى قوانين اجرائية ملائمة للتحقيق في المجرمين السيبرانيين وملاحقتهم قضائيا؛

(ج) ينبغي للحكومات والصناعة العمل معا في سبيل بلوغ الهدف المشترك المتمثل في منع الجرائم الحاسوبية ومكافحتها بحيث تصبح الانترنت مجالا آمنا؛

(د) ثمة حاجة الى تحسين التعاون الدولي من أجل اقتفاء أثر المجرمين على الانترنت؛

(هـ) ينبغي للأمم المتحدة أن تتخذ مزيدا من الاجراءات فيما يتعلق بتوفير التعاون والمساعدة التقنيين بشأن الجرائم ذات الصلة بالشبكات الحاسوبية.

المرفق

الخبراء المشاركون في مناقشات الأفرقة

السيد شري ل. س. أمارناتان، المقر الرئيسي لشرطة سيكيم، الهند

السيد كورماك كالانان، الرابطة الأوروبية لموفري خدمات الانترنت، ايرلندا

السيد بيتر ن. غرابوسكي، معهد علم الاجرام، استراليا

السيد ماساهيتو اينويي، جامعة طوكيو، اليابان

السيد نايجل جونز، رابطة رؤساء ضباط الشرطة، المملكة المتحدة لبريطانيا العظمى وايرلندا الشمالية

السيد ايكيهارت كابلر، المكتب الاتحادي المعني بالجريمة، ألمانيا

السيد هنريك و. ك. كاسبرسن، أستاذ، جامعة فريي، أمستردام، هولندا

السيدة مارغو ل. لانغفورد، محامية مرافعة، كندا

السيد فكتور لو، شرطة هونغ كونغ، الصين

السيد كايث ميتشال، المؤسسة المعنية بتيسير حركة السير على الانترنت في لندن، المملكة المتحدة لبريطانيا العظمى وايرلندا الشمالية

السيد هانس ج. نيلسون، مجلس الاتحاد الأوروبي

السيدة رونالد ك. بيراغوف، وزارة العدل، كندا

السيدة ماري رايلي، دائرة الخدمات السرية، الولايات المتحدة الأمريكية

السيد غريغوري ب. شافر، خبير استشاري في الأمن الحاسوبي، الولايات المتحدة الأمريكية

السيد أولريش سيبر، جامعة ميونيخ، ألمانيا

السيد فيتوريو ستانكا، الوحدة الوطنية المعنية بالجرائم الحاسوبية، ايطاليا

السيد مايكل سوسمان، وزارة العدل، الولايات المتحدة الأمريكية
