الأمم المتحدة A/CONF.187/10

Distr.: General
3 February 2000
ARABIC
Original: English

مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين

فيينا، ١٠-١٧ نيسان/أبريل ٢٠٠٠

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

الجرائم المتصلة بشبكات الحواسيب

ورقة معلومات أساسية من أجل حلقة العمل بشأن الجرائم المتصلة بشبكة الحواسيب

ملخص

يستلزم منع الجريمة السيبرانية ومكافحتها مكافحة فعالة اتباع نهج دولي منسق على مختلف المستويات. فعلى المستوى المحلي، يستلزم التحقيق في مجال الجريمة السيبرانية توافر ما يفي بهذا الغرض من موظفين وخبرة فنية واجراءات. وتشجع الدول على النظر في استخدام الآليات التي تتيح الحصول على البيانات من نظم الحواسيب وشبكاتها في الوقت المناسب وبصورة دقيقة، وذلك عند الاحتياج اليها كأدلة في الاجراءات القانونية. أما التحقيق في الجريمة السيبرانية على المستوى الدولي فيستلزم اتخاذ اجراء في الوقت المناسب، وتيسيره عن طريق التنسيق بين الأجهزة الوطنية لانفاذ القانون وبين تشريع السلطة القانونية المناسبة.

وبالاضافة الى ما تم اتخاذه فعلا من مبادرات على المستوى الدولي، وما اتخذ دعما لتلك المبادرات، تبحث هذه الورقة في وسائل تبادل الخبرات التقنية والقضائية بين سلطات انفاذ القانون الوطنية، وتبحث كذلك في الحاجة الى اجراء مداولات دولية بشأن التدابير القانونية الحالية والمقبلة من أجل التعاون الدولي على اجراء التحقيق في الجرائم السيبرانية.

* A/CONF.187/1.

المحتويات

أولا - معلومات أساسية فيما يخص التشريعات

١- قررت الجمعية العامة، في قرارها ٩١/٥٢ المؤرخ ١٢ كانون الأول/ديسمبر ١٩٩٧، تكريس احدى حلقات العمل الأربع التي ستنظم في اطار مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين لبحث مسألة الجرائم المتصلة بشبكة الحواسيب. كما أقرت الجمعية العامة، في قرارها ١١٠/٥٣ المؤرخ ٩ كانون الأول/ديسمبر ١٩٩٨، برنامج أعمال المؤتمر العاشر، الذي يتضمن عقد أربع حلقات عمل تقنية تتناول احداها الجرائم المتصلة بشبكة الحواسيب. وشددت الجمعية العامة في قرارها هذا على أهمية حلقات العمل، ودعت الدول الأعضاء والمنظمات غير الحكومية وسائر الكيانات ذات الصلة الى دعم الأعمال التحضيرية لحلقات العمل دعما ماليا وتنظيميا وتقنيا، بما في ذلك اعداد مواد المعلومات الأساسية ذات الصلة وتعميمها.

٢- وفي القرار ١٢٥/٥٤ المؤرخ ١٧ كانون الأول/ديسمبر ١٩٩٩، شجعت الجمعية الدول الأعضاء وسائر الهيئات المعنية والأمين العام على العمل معا لضمان أن تركز حلقات العمل الأربع المقرر انعقادها أثناء المؤتمر العاشر، بكل وضوح على المسائل المعنية وتحقيق نتائج عملية، ودعت الحكومات المهتمة بالأمر الى متابعتها بمشاريع أو أنشطة تعاون تقني ملموسة. واستجابة لهذا القرار، نظم معهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين اجتماعين للخبراء تناولا موضوع الجرائم المتصلة بشبكة الحواسيب، وجرت في اطارهما معظم الأعمال التحضيرية الموضوعية لحلقة العمل المعنية بالجرائم المتصلة بالحواسيب. ويشيد المركز المعني بالاجرام الدولي بالجهود التي بذلها معهد آسيا والشرق الأقصى لمنع الجريمة ومعاملة المجرمين وبالجهود التي بذلها الفريق العامل من أجل تيسير تنظيم حلقة العمل.

ثانيا - هدف الوثيقة ونطاقها

٣- أتاح ظهور شبكات الحواسيب الدولية، مثل الانترنت، للمستعملين اجراء الاتصالات والتصرفات والمعاملات التجارية مع مستعملين آخرين في جميع أنحاء العالم. وحيث أن استخدام شبكات الحواسيب بصورة مشروعة واستخدامها بصورة غير مشروعة يسيران جنبا الى جنب، يندس بين صفوف الباحثين الذين يستكشفون الفرص التي تتيحها هذه الواسطة الجديدة أفراد وجماعات يتصرفون بدوافع اجرامية. وهناك ثلاثة أسباب رئيسية تؤدي الى تعقد مشكلة مكافحة الجريمة في اطار البيئة الحالية لشبكات الحواسيب الدولية، وهذه الأسباب هي:

(أ) ان السلوك الاجرامي يمكن أن يتم في بيئة الكترونية، لذا فالتحقيق في الجرائم السيبرانية، أي الجرائم التي ترتكب في اطار شبكة ما من الشبكات الالكترونية، يستلزم خبرة فنية معينة واجراءات للتحقيق وسلطات قانونية قد لا تكون متاحة لسلطات انفاذ القانون في الدولة المعنية؛

(ب) ان شبكات الحواسيب الدولية، مثل شبكة الانترنت، تعتبر بيئات مفتوحة يتسنى بسببها للمستعملين أن تتجاوز تصرفاتهم حدود البلد الذي يوجدون فيه. ومع ذلك، فان الجهود التي تبذلها سلطات انفاذ القانون بوجه عام، ينبغي أن تقتصر على اقليم الدولة التي تتبعها هذه السلطات. وهذا يعني أن مكافحة الجريمة في شبكات حواسيب مفتوحة يستلزم تكثيف التعاون الدولي؛

(ج) ان الهياكل المفتوحة لشبكات الحواسيب الدولية تتيح للمستعملين فرصة اختيار البيئة القانونية الأفضل ملاءمة لأغراضهم. فالمستعملون قد يختارون بلدا ما حيث لا تجرم فيه أشكال معينة من التصرف قابلة للتنفيذ في بيئة الكترونية. وهذا قد يجتذب نشاطا اجراميا يقوم به أشخاص من دول أخرى حيث تعتبر مثل هذه الأنشطة أفعالا اجرامية بمقتضى قانونهم المحلي ومن شأن نشوء "ملاذات البيانات" - وهي الدول التي لا تعطي أولوية للحد من اساءة استخدام شبكات الحواسيب أو منع اساءة هذا الاستخدام، أو الدول حيث لم توضع قوانين اجرائية فعالة - أن يعرقل جهود البلدان الأخرى في مكافحة الجريمة في شبكات الحواسيب.

٤- وسوف تركز المناقشة التالية على كيفية التوصل الى اجراء دولي منسق لتيسير وتعزيز وتحسين الأساليب المتبعة حاليا في مكافحة الجريمة السيبرانية. ويعتبر ذا أهمية خاصة ذلك الدور الذي يمكن للأمم

المتحدة أو غيرها من المنظمات الدولية الاضطلاع به في هذا المجال. كما ترد في ورقة البحث هذه معلومات أساسية بشأن حلقة العمل المعنية بالجرائم المتصلة بشبكة الحواسيب.

٥- وتجمل المناقشة التالية أنواع الجرائم المرتآة للشبكات الالكترونية الدولية، وتبحث الأسباب التي تدعو الى ضرورة توجيه اهتمام دولي وجهود مشتركة نحو هذه الجرائم. وسيساعد تعريف هذه الجرائم على التوصل الى تفهم دولي مشترك وعلى أن تسترشد به السياسات الجنائية الوطنية في الميدان.

ثالثا - فئات الجريمة السيبرانية

٦- يستخدم المصطلحان نظم الحواسيب أو شبكات الحواسيب في ورقة البحث هذه للاشارة بوجه عام الى البيئة الالكترونية. وبالرغم من استمرار وجود نظم حاسوبية مستقلة، فان المبدأ السائد الآن هو وجود ترابط متبادل بين نظام واحد أو اكثر من نظم الحواسيب، بما فيها الحواسيب الشخصية، وهو ترابط يؤدي الى تشكيل شبكة ما. ولا يوجد أي تمييز هنا بين الشبكات الحاسوبية العامة والخاصة ولا فيما يخص وجود صلات دائمة تربط بينها. ولأغراض هذه الوثيقة، وما لم يذكر شيء خلافا لذلك، صنفت نظم الاتصالات ضمن نفس الفئة مثل نظم وشبكات الحواسيب.

٧- ومن بين الأمثلة المعروفة في الوقت الحاضر عن الشبكات الحاسوبية العامة شبكة الانترنت، التي تفجر نموها أثناء العقد الأخير. ومعظم نجاحها يعزى الى اتباع بروتوكولات اتصال مشتركة. حيث يسهل لأي مشغل لنظام أو لشبكة يطبق تلك البروتوكولات أن يصبح حلقة اتصال في الشبكة بوصفه "مقدم خدمات"، أو بعبارة أدق يصبح مقدما لخدمات الانترنت. ولأغراض تجارية وتقنية، ينتظم مقدمو خدمات الانترنت في بعض البلدان في رابطات أو جمعيات، مع اتخاذ مواقف مشتركة بشأن بعض المسائل.[١] وتبين التقديرات أن ما يزيد على ٢٠٠ مليون شخص في العالم اليوم يستخدمون شبكة الانترنت، منهم ١١٢ مليون شخص في أمريكا الشمالية و٤٧ مليون في أوروبا و٣٣ مليون في منطقة آسيا والمحيط الهادىء.[٢] وبينت الاحصاءات في نهاية عام ١٩٩٥ أن هناك ٢٦ مليون شخص يستخدمون الشبكة يقيم معظمهم في الولايات المتحدة الأمريكية. وقدرت نسبة الزيادة الشهرية في عدد المستعملين في عام ١٩٩٩ بأكثر من ٣ في المائة.

٨- وتعتبر الوظيفة الجوهرية التي يقوم بها أي نظام حاسوبي هي معالجة البيانات. ويعرف مصطلح البيانات بأنها حقائق أو تعليمات أو مفاهيم ممثلة بأسلوب تقليدي في شكل مناسب لفهم الانسان أو للمعالجة الآلية.[٣] وتمثل البيانات الالكترونية بسلسلة من النقط المغنطيسية على وسط للتخزين المؤقت أو الدائم، ولكنها تتخذ أثناء نقلها شكل الشحنات الكهربائية. ويمكن من الناحية القانونية اعتبار البيانات شيئا ماديا ملموسا، وذلك عند وجود امكانية للتعرف على تلك البيانات والتحكم فيها بواسطة حامل معين للبيانات، كالبيانات المخزنة في (مجموعة من) الأقراص اللينة. وبصورة عامة لا يمكن لهذا الحامل تقييد البيانات أو التحكم فيها بعد أن تتم معالجتها في نظام حاسوبي. كذلك، فالنظم التشغيلية تنقل على نحو مستقل ملفات البيانات من موضع مادي على وسط للتخزين الى موضع آخر. ومعالجة البيانات الموزعة في اطار الشبكات الحاسوبية لا تسمح مطلقا للأشخاص الذين يتحكمون في البيانات انشاء الموقع المادي لملف البيانات أو لجزء منه ما لم يتخذ هؤلاء تدابير معينة. وعملية التحكم في هذه البيانات لا يمكن أن تتم الا بعملية منطقية وليست باجراءات مادية، لذا يصعب من الناحية القانونية اعتبار هذه البيانات المحضة كما لو كانت شيئا ملموسا.

٩- يقصد بالجرعة السيبرانية أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوبي أو شبكة حاسوبية، أو ضد نظام حاسوبي أو شبكة حاسوبية. والجريمة تلك تشمل، من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية. ويشير مصطلح "جريمة" في هذه الوثيقة الى الأنماط السلوكية التي تعرف عموما بأنها أنماط غير مشروعة، أو التي يحتمل تجريمها في غضون فترة قصيرة. وقد يجرم سلوك معين في دولة ما حيث لا يجرم في دول أخرى، بيد أنه، كما ورد شرحه في

الفقرة ١٣، ظهر في اطار بعض المحافل الدولية فهم مشترك بخصوص السلوك الذي يمكن تجريمه فيما يخص النظم والشبكات الحاسوبية. ويعتبر هذا نقطة الانطلاق في المناقشة التالية.

١٠- ويدور محور التركيز هنا حول التحقيق الجنائي في الجريمة السيبرانية ومحاكمتها. والمقصود بتسمية "سلطات انفاذ القانون" هنا الأشخاص المكلفون بموجب القانون بالتحقيق في الجرائم ومحاكمتها. وقد أنشأ بعض الدول الأعضاء وحدات متخصصة للتحقيق أو للمساعدة على التحقيق في الجرائم المتصلة بالحواسيب. وعلى المستوى الدولي، فان المنظمة الدولية للشرطة الجنائية (الانتربول) هي المنظمة التي تقوم بالتنسيق فيما يتصل بتسجيل معلومات الشرطة وتوزيعها، كالمعلومات التي تخص الأفراد المطلوب القبض عليهم والممتلكات المسروقة.

١١- وقد يحدث أن تلتمس السلطات المكلفة بانفاذ القانون في دولة ما، أثناء التحقيق بشأن جريمة سيبرانية، تعاون السلطات من دول أخرى في شكل مساعدة بخصوص قضايا معينة وفي تبادل المعلومات العامة بشأن المنظمات والقضايا الاجرامية. ويجوز أيضا أن تطلب تلك السلطات، أثناء اجراء تحقيق معين، استخدام المواد المتوافرة في دولة أخرى. ويتحدد نطاق التعاون بين السلطات الوطنية المكلفة بانفاذ القانون بموجب القانون الوطني لكل دولة، وكذلك بموجب الاتفاقات الدولية، بما في ذلك الاتفاقات الخاصة بتبادل المساعدة القانونية.

١٢- ومن الأمثلة الشائعة عن اساءة استعمال الشبكات الحاسوبية الدولية ابلاغ عبارات محظورة بموجب القانون، وعروض منتجات غير مشروعة وعروض مزيفة لغرض الحصول على أرباح مالية غير مشروعة. وفي هذه الحالة تستخدم الانترنت بنفس أسلوب استخدام أي وسيلة أو أداة أخرى يمكن استخدامها لارتكاب جريمة ما. وتشكل الشبكة نفسها البيئة التي تجري فيها الجريمة وهي ليست السند اللازم جزءا أصيلا لا غنى عنه في ارتكاب الجريمة. وتتميز الانترنت بصفات خاصة يمكن أن تحرض مرتكب الجريمة على استعمالها عوضا عن استعمال الوسائل التقليدية: فهي تتيح تسهيلات ممتازة لاجراء الاتصالات المحلية والدولية، مع امكانية اخفاء هوية المتصل، كما أن خطر التعرض للتحقيق الجنائي في أي من الاختصاصات القضائية المعنية يعتبر قليلا نسبيا. والى جانب الأنماط الاجرامية المذكورة، هناك بعض مستعملي الانترنت الذين يحصلون بصورة غير مشروعة على سبل نفاذ الى نظم موصولة بأجهزتهم، حيث يستطيعون التدخل في عملها أو في فحواها. ويطلق على هذا النشاط "الجريمة الحاسوبية". ويستفيد مرتكبو هذا النوع من الجرائم من معرفة تقنية معينة أو من خبرة فنية أو أجهزة تساعدهم على ارتكاب أنشطة غير مشروعة. ومن السهولة بمكان استهداف نظم الحواسيب بالجريمة لأنه لم تتخذ تدابير أمنية كافية، أو في حالة جهل مستعملي الحواسيب بالمخاطر التي تنطوي عليها. وعلاوة على ذلك، فان العوامل التي تجعل أي نظام مريحا ييسر الاستعمال تميل الى جعله نظاما غير مأمون. وأي خلل في برامج حاسوبية ناجحة تجاريا سيصبح على الأغلب معروفا لدى عامة الناس.

١٣- وفي حين تدارست البلدان المهتمة بالأمر المشاكل الناجمة من الجريمة السيبرانية عبر الوطنية، لم تنل قدرا كبيرا من الاهتمام على المستوى الدولي. فالأمم المتحدة، على سبيل المثال، لم تعتمد حتى الآن سياسة خاصة لتجريم الجرائم السيبرانية؛ وتطبيق القوانين الوطنية على الجريمة السيبرانية يمكن أن يتم بأساليب متنوعة، ذلك فيما لو طبقت عليها فعلا. ومن بين أسباب عدم الاهتمام بالجريمة السيبرانية الانخفاض النسبي لمستويات المشاركة في الاتصالات الالكترونية الدولية، وضعف مستويات الخبرة في انفاذ القانون، وضعف تقديرات الضرر المتوقع حدوثه في المجتمع نتيجة لارتكاب جرائم الكترونية. وفي مجال الشبكات الحاسوبية العالمية، تؤثر السياسة الجنائية لدولة ما تأثيرا مباشرا على المجتمع الدولي. وقد يوجه مرتكبو الجرائم السيبرانية أنشطتهم الالكترونية عن طريق دولة معينة لا يشكل هذا السلوك فيها نشاطا اجراميا، وبالتالي فهم محميون بحكم قوانين ذلك البلد . ولربما تنظر دولة ما ليست لها مصلحة وطنية معينة في تجريم سلوك معين في مسألة القيام بذلك من أجل تجنب تحولها الى ملاذ للبيانات وتجنب انعزالها دوليا. لذا فان التوفيق بين القوانين الجنائية الموضوعية فيما يخص الجرائم السيبرانية يشكل أمرا أساسيا لتحقيق التعاون

بين سلطات انفاذ القانون والسلطات القضائية في شتى البلدان.

١٤- وهناك فئتان فرعيتان للجرائم السيبرانية هما:

(أ) الجريمة السيبرانية بالمعنى الضيق ("جريمة حاسوبية"): وهي أي سلوك غير مشروع يوجه بواسطة عمليات الكترونية تستهدف أمن نظم الحواسيب والبيانات التي تعالجها تلك النظم؛

(ب) الجريمة السيبرانية، بالمعنى الأوسع، ("الجرائم المتصلة بالحواسيب"): وهي أي سلوك غير مشروع يرتكب بواسطة نظام أو شبكة حواسيب أو فيما يتعلق بنظام حاسوبي أو شبكة حاسوبية، بما في ذلك جرائم من قبيل حيازة المعلومات أو عرضها أو توزيعها بصورة غير مشروعة بواسطة نظام أو شبكة حواسيب.

١٥- وجرائم الحاسوب، كما عُرّفت الفقرة السابقة، تتعلق بكل سلوك غير مشروع موجه ضد أمن النظم أو البيانات بواسطة عمليات الكترونية. ويمكن وصف أمن النظم والبيانات بثلاثة مبادىء: ضمان سرية أو سلامة أو توافر البيانات ووظائف معالجتها. وبموجب القائمة التي أصدرتها منظمة التعاون والتنمية في الميدان الاقتصادي في عام ١٩٨٥،[٤] وتوصيات مجلس أوروبا الأدق تفصيلا الصادرة عام ١٩٨٩، فان الجرائم المتعلقة بالسرية والسلامة والتوافر تشمل ما يلي:

(أ) النفاذ من غير اذن، أي النفاذ من غير حق الى نظام حاسوبي أو شبكة حاسوبية عن طريق خرق التدابير الأمنية؛

(ب) الحاق الضرر ببيانات الحاسوب أو برامجه، أي محو البيانات أو البرامج أو افسادها أو اتلافها أو ازالتها دون وجه حق؛

(ج) تخريب الحواسيب، أي ادراج بيانات أو برامج الحاسوب، أو تغييرها أو محوها أو ازالتها، أو التدخل في نظم الحواسيب بهدف اعاقة تشغيل نظام حاسوبي أو نظام للاتصال؛

(د) الاعتراض غير المرخص، أي الاعتراض دون اذن وبوسائط تقنية، للاتصالات من نظام أو شبكة للحواسيب واليها وفي اطارها؛

(هـ) التجسس بالحواسيب، أي الحصول على سر تجاري أو افشائه أو نقله أو استعماله دون اذن أو مبرر قانوني، بهدف التسبب في خسارة اقتصادية للشخص المرخص الذي يحق له استخدام السر، أو للحصول بصورة غير مشروعة على مزايا شخصية أو لشخص ثالث.

١٦- والجريمة الأولى، وهي محاولة النفاذ غير المرخص الى الحاسوب وتعرف أحيانا باسم القرصنة فانها، جريمة متكررة الحدوث وغالبا ما تقترن بالجريمة الثانية وهي الحاق الضرر بالبيانات أو التجسس بواسطة الحواسيب. ومن الأشكال المختلفة الشائعة حديثا القرصنة في موقع شبكة ويب وادراج معلومات ضارة أو مؤذية فيها. وعادة يقتضي التحقيق الفعال في جرائم القرصنة التعاون من جانب الضحية وبعض وسائل القبض على المجرم أثناء القيام بفعلته. والمجرمون هم في الغالب من الشباب الشديدي الذكاء المولعين بالتكنولوجيا الحديثة، ممن ليس لديهم سوى فهم محدود لأخلاقيات الأفعال التي يرتكبونها أو لما يحتمل من الحاق الضرر. والى جانب جرائم القرصنة، تجرم بعض البلدان أنشطة مثل الاتجار بكلمات السر أو وسائل القرصنة.

١٧- ويتضمن افساد بيانات وبرامج الحواسيب اطلاق ما يعرف باسم "برامج ديدانية" أو "فيروسات" الحاسوب. وقد يتسبب البرنامج الديداني آخر الأمر في توقف الحاسوب عن العمل تماما، بينما يمكن أن يتسبب الفيروس في ضياع جميع البيانات المخزنة في القرص الممغنط. ومن الأساليب الحديثة المتبعة في نشر الفيروسات استخدام رسائل البريد الالكتروني التافهة وغير المطلوبة، وقد لا يدرك مستعملو الانترنت الحظر المرتبط بالشبكات الالكترونية المفتوحة واستقبال رسائل غير ملتمسة، أو أنهم لا يستخدمون، لأسباب مالية، برامج مسح الفيروسات المتوافرة تجاريا. وقد يجد المسؤولون عن التحقيقات الجنائية صعوبة في اثبات هوية المسؤول عن اطلاق الفيروس الذي تسبب في الضرر. كذلك يمكن

أن يستغل قراصنة الحواسيب أوجه الخلل الأمني (المؤقتة) التي تصيب برامج النظم التي يكثر استعمالها وقد يستطيعون النفاذ الى النظم الحاسوبية، أو في حالات استثنائية السيطرة على النظم الحاسوبية التي يستخدمها الآخرون عن طريق تخزين وظائف برنامجية معينة في تلك النظم. ولربما لا يكون لدى مستعملي الانترنت معلومات كافية أو مستوفاة عن المخاطر المحتملة والتدابير الأمنية الاضافية التي يتيحها صانعو برمجيات النظم الحاسوبية.

١٨- ويعرّف مجلس أوروبا الاحتيال المتصل بالحواسيب (انظر الفقرة ١٥ أعلاه) كالآتي:

"ادراج بيانات أو برامج حاسوبية، أو تغييرها أو محوها أو ازالتها، أو أي تدخل آخر في سير عملية معالجة المعلومات، مما يتسبب في خسارة اقتصادية أو فقدان ما يحوزه شخص آخر من ممتلكات بقصد الحصول على ربح اقتصادي غير مشروع لصالحه أو لصالح شخص آخر."

ويشير هذا الحكم الى الحالة التي يتدخل فيها مرتكب الفعل بحق أو دون وجه حق في الوظائف اللازمة لعملية الحاسوب في معالجة البيانات مع ما يترتب عليه من الآثار المبينة في تعريف الاحتيال. وهو لا يشمل خطط الاحتيال المعروفة التي تتم بواسطة أوصاف الكترونية منتحلة أو اتصالات عن طريق الانترنت، كعروض بيع الأسهم بأسعار تفضيلية؛ والاستثمارات العقارية في دولة أجنبية؛ والقروض المالية ذات الفوائد المرتفعة بشكل غير عادي، والتسديد المسبق لثمن سلع غامضة المواصفات؛ والاغراء بالدخول في مخططات وهمية للاستثمارات للمضاربات الاضافية. ويرجح أن تنطبق الأحكام الخاصة بعمليات الاحتيال التقليدية على هذه المخططات.

١٩- ويعرّف مجلس أوروبا التزوير بواسطة الحاسوب (انظر الفقرة ١٥ أعلاه) كالآتي:

"ادراج بيانات أو برامج حاسوبية، أو تغييرها أو محوها أو ازالتها، أو أي تدخل آخر في سير عملية معالجة البيانات بطريقة أو في ظروف تشكل، بموجب القانون الوطني جرم تزوير ان ارتكب بالدافع التقليدي لهذا الجرم."

والغرض من التعريف هو تجريم تزوير البيانات الحاسوبية بأسلوب مكافىء فعليا لتجريم أنشطة تزوير الوثائق التقليدية.

٢٠- وينبغي هنا ذكر نوعين آخرين من الجرائم ذات الصلة. ويتعلق أولهما بعدد من أشكال الخداع فيما يخص خدمات الاتصالات اللاسلكية. وفي هذه الحالات، يحاول مرتكب الجريمة الحصول على خدمات دون سداد ثمنها عن طريق التلاعب التقني بالأجهزة أو بعناصرها الالكترونية. ويجرّم هذا السلوك عادة عن طريق أحكام جنائية معينة، بيد أنه يمكن تصنيفها أحيانا بموجب الأحكام التقليدية الخاصة بالخداع أو التزوير. وتتعلق الفئة الثانية باساءة استعمال وسائل الدفع، حيث يحاول مرتكب الجرم تحقيق أرباح مالية غير مشروعة عن طريق التلاعب بالبطاقات المصرفية الالكترونية أو تزويرها، أو باستخدام رموز مزيفة. ويجوز تغطية هذا الجرم بأحكام جنائية معينة أو بأحكام الاحتيال والتزوير التقليدية، أو يتم تعديله بالمعنى الموضح في الفقرة ١٩.

٢١- وتتضمن الأفعال الاجرامية المرتكبة بمساعدة الحاسوب اتاحة مواد معينة أو نقلها أو نشرها، وأحيانا مجرد تملكها. وهذه الأفعال لا تستلزم شبكات الكترونية؛ ويمكن للمجرمين هنا استغلال هذه الشبكات من أجل زيادة أثر الجريمة ولمحاولة الافلات من العدالة. وفيما يخص الأفعال الاجرامية المتعلقة بالمشتملات، ينبغي التمييز بين المشتملات غير المشروعة بالنظر لطابعها أو لمعناها، والمشتملات التي ليست بالضرورة غير مشروعة بحد ذاتها، وانما تصبح مشتملات جنائية بسبب ظروف نشرها. وتشمل الفئة الثانية انتهاك حقوق المؤلف وبيع سلع أو خدمات محظورة كالأسلحة والمخدرات والمسروقات والأدوية دون وصفات طبية والنفاذ الى مرافق المقامرة. وتتعلق الفئة الأخرى من الأفعال الاجرامية الخاصة بالمشتملات برسائل القذف، والرسائل التي تحرض على أعمال التخريب وغيرها من الأنشطة غير المشروعة، أو الرسائل التي تسبب أضرارا بالنظر لطبيعتها الدينية أو العنصرية، أو بسبب طبيعتها

الاباحية. ويتباين الى حد بعيد النطاق الذي يجرّم فيه المشرعون الوطنيون هذا السلوك. وفي معظم الأحوال، كانت هذه الأفعال الاجرامية جزءا من القوانين القائمة، مما يطرح التساؤل عما اذا كانت القوانين تنطبق على البيئة الالكترونية الجديدة.

٢٢- وهناك اتفاق عالمي من حيث المواقف والقواعد التي تدين نشر صور الأطفال الاباحية. وقد أوصت هيئات دولية منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) والاتحاد الأوروبي البلدان بسن أحكام جنائية حيثما لا يعتبر توزيع هذه المواد حتى الآن فعلا غير مشروع. وتضطلع دول عديدة بسن القوانين، أو أنها سنتها فعلا فيما يخص استغلال الأطفال في أغراض اباحية. كما تمنح سلطات الشرطة المحلية والدولية أولوية كبرى للتحقيق في مجال استغلال الأطفال في أغراض اباحية.

٢٣- وفيما يتعلق بالأعمال الاجرامية التي تتضمن مواد تتعلق بالتحريض على الكره أو التمييز لشتى الأسباب، ما زال هناك افتقار لوجود توافق عالمي في الرأي بشأن تطبيق القوانين الجنائية على التعبير أو نشر هذه المواد. ولربما يتغير الوضع مع تزايد ادراك المجتمع الدولي للآثار السلبية التي تترتب على مثل هذا السلوك.

٢٤- وقد أدى نشر مواد غير مشروعة الى اثارة نقاش حول دور مقدمي خدمات الانترنت ومسؤولياتهم. فالى جانب بضع مبادرات تشريعية متخذة من أجل تعيين وتحديد واجبات مقدمي الخدمات من حيث العناية، ظهر اتجاه على المستويين الوطني والدولي لمنح مقدمي الخدمات مركزا قانونيا مماثلا للمركز القانوني لمشغلي خدمات الاتصالات اللاسلكية التقليدية. وهذا يعني أن مقدمي خدمات الانترنت غير ملزمين عموما بموجب القانون برصد أو لربما اعاقة حركة السير التي يجري نقلها بواسطة نظمهم الحاسوبية. ومع ذلك، يلزم مقدمي خدمات الانترنت عموما اتخاذ جميع الخطوات المعقولة لمنع استمرار نشر المواد غير المشروعة بمجرد أن تتناهى على علمهم طبيعة هذا النشاط.[٦] كذلك هناك جوانب أخرى من تطبيق القوانين المحلية على مقدمي خدمات الانترنت، قد لا تكون واضحة، وهي تتضمن النطاق الممكن للمسؤولية المدنية عن بث مشتملات غير مشروعة، ومدى الالتزام المطلوب من مقدم خدمات الانترنت للتعاون مع سلطات انفاذ القانون عن طريق تقديم المعلومات أو غيرها من أشكال المساعدة الى عملية معينة للتحقيق الجنائي.

رابعا - التحقيقات الجنائية في الجريمة السيبرانية

٢٥- كما ذكر من قبل، فان الجريمة السيبرانية يمكن أن تكون أي جريمة ترتكب بوسيلة الكترونية، أو أن يرتكب جزء منها أو كلها في بيئة الكترونية. وتوجه التحقيقات الجنائية التي تتم في بيئات الكترونية ضد هذه الجرائم. بيد أن هناك جرائم أخرى قد تترك أيضا آثارا أو أدلة في البيئة الالكترونية. لذا فالتحقيقات الجنائية في بيئات الكترونية لن تقتصر على الجريمة السيبرانية بالمعنى المقصود في الفصل السابق، وانما ستشمل التحقيق في أي جريمة يلزم الحصول على دليلها (الممكن) من بيئة الكترونية.

٢٦- وتتطلب التحقيقات التي تجرى في بيئة الكترونية خبرة تقنية واتباع اجراءات مناسبة علاوة على سلطة قانونية كافية. وقد شددت التوصيتان الصادرتان من مجلس أوروبا في سنتي ١٩٨٥ و ١٩٩٥ (R (1989) 9 en R (95) 13) على ضرورة نشرالسلطات الوطنية المسؤولة عن انفاذ القانون لوحدات متخصصة في الجرائم الحاسوبية. وينبغي اتاحة عدد كاف من الموظفين لهذه الوحدات وتزويدها بما يناسب من أجهزة وأدوات البرمجيات الحاسوبية. كما ينبغي تنظيم برامج تدريبية لضمان وجود موظفين مدربين من ذوي المعارف التقنية الحديثة. وقد أنشأ العديد من الدول وحدات من هذا القبيل لمكافحة الجرائم الحاسوبية. وأنتج عدد من الدول أيضا أدلة تتضمن ارشادات تقنية واجرائية عن كيفية القيام بالتحقيق للحد من فقدان الأدلة وضمان مقبوليتها في المحاكم.

٢٧- وتتولى بعض وحدات الشرطة الوطنية "دوريات مراقبة" الانترنت، كما تم وضع أدوات من برمجيات حاسوبية معينة للكشف عن بعض الجرائم كالقرصنة

أو نشر المواد الاباحية المتعلقة بالأطفال. (وقدم الاتحاد الأوروبي تمويلا جزئيا لأعمال قامت بها الشرطة السويدية في استحداث برمجيات حاسوبية لتعقب المواد الاباحية عن الأطفال (انظر <http://www.techweb.com>). واستحداث الأدوات البرمجية الحاسوبية مثل تلك المواد التي تستند الى التعرف على الأنماط الاجرامية تعتبر مسألة لا غنى عنها، وذلك بالنظر لضخامة حجم المعلومات المتوافرة في شبكات الحواسيب الدولية.

٢٨- وهناك وسيلتان للحصول على البيانات من نظام حاسوبي، وهما تستندان الى معايير تقنية وقانونية. وفي الوسيلة الأولى، يتم الحصول على المعلومات كجزء من البحث عن المرافق أو المكان الذي يقع فيه النظام. وتتضمن الوسيلة الثانية اعتراض أو رصد البيانات المنقولة من النظام أو اليه أو في اطاره. وليس هنا مكان لمناقشة الموضوع الخاص بالسلطة القانونية المعنية بتفتيش المرافق. والمفترض أن السلطات القانونية ستشمل سلطة تفتيش نظام حاسوبي في موقع ما. ويمكن الكشف عن المعلومات بوسائل تقنية من خارج النظام، أو بواسطة عناصر مدرجة لهذه الغاية داخل النظام.

٢٩- وبوجه عام، ينص قانون الاجراءات الجنائية التقليدية على ضبط النظم الحاسوبية برمتها وعلى تجميد تلك النظم مثلما ينص بشأن أي دليل آخر. ولكن حيثما يتعذر امكان تطبيق ذلك، قد لا تكون هناك سلطات قانونية مناسبة للتحقيق في مشتملات نظام حاسوبي ضد رغبة المالك (الحقيقي) للنظام. ولربما لا يمكن من الناحية التقنية ضبط نظام حاسوبي برمته، أو قد يكون أمرا غير مناسب بالنظر لتعدد بيئات المستعملين واهتماماتهم بمشتملات البيانات. وقد لا تكون السلطات التقليدية كافية للحصول على البيانات اللازمة لاجراء تحقيقات معينة، وذلك للأسباب التالية: (أ) المشكلات المتعلقة بسبل النفاذ الى نظام حاسوبي ما؛ و(ب) طابع البيانات غير الملموس؛ و(ج) حقيقة أن البيانات لربما تكون مخزنة في نظام موصول يقع خارج المرفق الذي يجري تفتيشه.

٣٠- وفي حالة وجود النظام الحاسوبي في المرفق الذي يتم تفتيشه، فان القانون يجيز عموما لسلطات انفاذ القانون النفاذ الى النظام وتفتيش مشتملاته. وهذا سيكون ممكنا اذا كان النظام قيد التشغيل بالفعل، فيقوم الشخص المعني بفتح النظام عن طواعية، أو تتوافر وسيلة للنفاذ الى النظام في المرفق نفسه. والسؤال الذي يطرح عند عدم توافر أي من هذه الظروف هو ان كان القانون ينص على حق يجيز لسلطات انفاذ القانون امكان ولوج النظام ضد رغبة الشخص المعني.

٣١- وقد تكون النظم الحاسوبية أو البرامج أو الملفات مأمونة من أجل منع الوصول اليها من غير اذن. وعندئذ يتم الوصول اليها باجراءات تعيين الهوية والتحقق من الشخصية، حيث يقدم المستعمل كلمة السر - يدويا، أو مضمورة في بطاقة شذرة، أو الاثنين معا - أو يسمح بالتحقق من علامات بيولوجية احصائية. ويتضمن أمان البيانات عموما رموزا سرية تسمح بالتحقق من الشخصية وبحماية السرية، وتتضمن استخدام التشفير العشري ومفتاح واحد أو أكثر. وهذا يثير مخاطرة شديدة تتمثل في عدم القدرة على الوصول الى النظام الحاسوبي أو البيانات المنشودة من غير مساعدة طوعية من المسؤول عن حفظ النظام أو الشخص المخول له ذلك. ولهذا، تفرض بعض القوانين على المسؤولين عن حفظ النظام السماح بالوصول الى النظام أو البيانات، ومعاقبة عدم الامتثال بتطبيق القواعد الخاصة بانتهاك حرمة المحكمة. وقد لا تنطبق هذه القوانين عندما يكون مشغّل النظام هو نفسه الشخص المشتبه في ارتكابه للجريمة، وذلك لأن هذا التطبيق ينتهك القواعد أو المبادىء الخاصة بالتجريم الذاتي. ويجوز أيضا اعفاء أفراد آخرين تمنعهم أسباب قانونية أخرى عن التعاون، لوجود صلة القرابة بينهم وبين المشتبه فيه، أو ممن لديهم التزامات بحفظ سر المهنة. وفي بعض الحالات عندما لا يوجد شخص يصدر له الأمر بتقديم المساعدة، يجوز اصدار الأمر لأي شخص آخر (وهو عادة خبير خارجي) لتقديم المساعدة. أما في حالة التشفير بالرموز، فقد لا يكفي مجرد الوصول الى البيانات. وفي مثل هذه الحالات، يجوز للقوانين أن تفرض تقديم المزيد من التعاون لنقل البيانات الى صيغة مقروءة.

٣٢- والبيانات في شكلها هذا غير ملموسة، ولهذا لا تنطبق عموما السلطات التقليدية للضبط. ففي أثناء التحقيقات الجنائية، يتم ضبط الأشياء الملموسة واقصاؤها، أو تتخذ التدابير التي تضمن عدم تصرف أي جهة، باستثناء سلطات التحقيق، في تلك الأشياء وفي حالة البيانات، يكفي عادة استنساخها. بيد أنه يلزم اتخاذ خطوات اضافية أخرى، وذلك عندما تكون البيانات من نوع خطر أو غير مشروعة أو قيّمة، أو عند احتمال تسببها في الحاق مزيد من الضرر بضحايا أو بالتحقيق ذاته. ولمعالجة هذه المسألة، يجوز للقوانين أن تنص على سلطات يتاح بموجبها لسلطة التحقيق محو البيانات أو منع مواصلة استخدامها. وقد تستلزم حماية البيانات استنساخها بغرض اعادة تلك البيانات الى حالتها الأصلية عندما يطلبها القاضي. وفي حالة تقديم الشخص المعني شكوى بشأن استنساخ البيانات ومواصلة استخدامها، يجوز للقانون الالزام باصدار بيان رسمي بشأن البيانات المأخوذة.

٣٣- وعملية تفتيش نظام حاسوبي ما تجري عموما كجزء من عملية تفتيش المرافق أو الأماكن. وعادة تكون هذه السلطة القانونية مقتصرة على الحدود المادية للمكان الذي يجري تفتيشه، ولكن شبكة حاسوبية ما قد لا تكون في مكان واحد بعينه، وانما تكون موصولة بأجزاء أخرى من الشبكة بواسطة خطوط اتصالية ثابتة أو متحولة. والسؤال في هذه الحالات هو ما اذا كان القانون يسمح باجراءات التفتيش في النظم الموصولة، عندما لا تكون النظم موجودة في المرافق التي يجري تفتيشها. والحظر المحتمل عند عدم اجراء تفتيش موسّع هو أن تمحى البيانات قبل الحصول على اذن اضافي بتفتيش المكان الذي تتواجد فيه البيانات ماديا. وقد يكون التثبت من الموقع المادي الصحيح للبيانات في الشبكات الكبيرة أمرا مستحيلا من الناحية العملية.

٣٤- وفيما يلي شرح مجمل للأساس القانوني لسلطة اجراء تفتيش واسع النطاق. فالشخص المقيم في المرفق المراد تفتيشه مخول بالنفاذ الى النظام الحاسوبي الموصول واستخدام وظائفه وسعته التخزينية. فهذا الشخص بوسعه أن يتحكم في البيانات دون ضرورة التوجه الى مكان آخر. وعند تعرضه للتفتيش يصبح هذا الشخص ملزما بحكم القانون بقبول تفتيش المرفق الذي يخضع ماديا لادارته. ويمكن طرح الحجة بأن القواعد ذاتها ينبغي أن تطبق على البيانات التي يتمتع الشخص المعني بالقدرة الفعلية على الوصول اليها، حتى وان وجدت تلك البيانات في مكان آخر. ويستتبع هذا أن نطاق مثل هذا التفتيش الموسع سيقتصر على الأنشطة المرخص للشخص المعني اجراؤها فيما يتعلق بالنظام الموصول والبيانات الموصولة، وأن حقوق ذلك الشخص ليست منتهكة الى أي حد يتجاوز المسموح به في اطار التفتيش الأساسي. ويمكن أن تقتصر هذه السلطات على التحقيقات في الجرائم الخطيرة، أو على الحالات التي تقتضي اتخاذ اجراء فوري من أجل تجنب ضياع الأدلة، أو تقتصر عليهما معا. ويمكن تطبيق قيود أخرى عند وجود النظام الموصول المطلوب أو البيانات الموصولة المطلوبة في نطاق اختصاص قضائي أجنبي (انظر الفقرة ٥٩ أدناه).

٣٥- ويؤدي تفتيش واختيار البيانات في نظام حاسوبي ما الى اثارة عدد من المشاكل القانونية الاضافية. المشكلة الأولى هي مدى الدقة التي ينبغي أن يكون عليها الأمر القضائي فيما يخص طبيعة البيانات المنشودة وصيغتها، وذلك لضمان أن يكون هذا الأمر قانونيا. ويحتمل أن تفرض القوانين الوطنية شروطا تقييدية مختلفة في هذه الحالة. وعلاوة على ذلك، فان تنفيذ الأمر القضائي باخلاص ودقة يمكن أن يستغرق فترة زمنية غير متناسبة، مما يتطلب من السلطات المكلفة بانفاذ القانون استنساخ أكبر قدر مما يبدو ذات صلة من بيانات لاجراء تحليل لاحق. وقد تسمح القوانين الوطنية أو لا تسمح بذلك. والسؤال الهام الآخر هو ما اذا كان ينبغي ابلاغ الشخص المعني بشأن البيانات التي يجري استنساخها واقصاؤها، وما هو حجم المعلومات المفصلة التي ينبغي له تقديمها، وفيما لو كان الشخص يتمتع قانونيا بحق الطعن في اجراء الضبط. كما تنشأ مشكلة أخرى في حالة تمتع البيانات بالحصانة أو بحماية قانونية أخرى. والسؤال هو كيف يتم الاهتداء الى مثل هذه البيانات وحمايتها في القضايا حيث تقوم السلطات باستنساخ مقادير كبيرة منها لغرض فحصها فيما بعد.

٣٦- وتجدر الاشارة علاوة على ذلك الى الصفة سريعة الزوال التي تتميز بها البيانات، اذ يمكن بسهولة نقلها أو محوها أو تغييرها دون ترك آثار واضحة. ومعالجة البيانات الموزعة ليست العامل الوحيد الذي يجعل البيانات سريعة الزوال. فمعالجة البيانات الالكترونية يشمل معالجة مقادير كبيرة من البيانات السريعة الزوال التي هي معرضة لأن تمحى بمجرد انتفاء الحاجة اليها. ومن الأمثلة على هذه البيانات سجلات الوقائع وبيانات مرور الاتصالات. وما لم تعرف مجموعة البيانات "الأصلية" - (ان كان للمصطلح أي معنى فيما يخص معالجة البيانات) - سيصعب الكشف عن عمليات التلاعب، وسيكون استرداد الملفات الممسوحة أمرا مستحيلا ما لم يتم حفظ المعلومات الأساسية المساندة. وعندما ينطوي التحقيق على اجراء تفتيش مادي، تصبح طبيعة البيانات هذه مصدرا لمشكلتين لا حل لهما، وهي:

(أ) أن البحث عن البيانات المخزنة الكترونيا أو التي يجري نقلها يقتضي في معظم الحالات اجراء سريعا وفي الوقت المناسب من أجل منع اعاقة البحث عن البيانات أو التلاعب بها؛

(ب) يلزم اتخاذ تدابير وقائية خاصة لاتاحة عرض البيانات كأدلة أمام القضاء. ويجب التثبت من سلامة البيانات من حيث التحميل النازل (نقل المعلومات من جهاز بعيد الى جهاز المستعمل) أو الاستنساخ من النظام الحاسوبي الذي تم تفتيشه للاستعمال أمام القضاء.

٣٧- ومما يذكر أن الفروق التقنية والقانونية بين ضبط البيانات المخزونة واعتراض تدفق البيانات عبر الشبكة قد أصبحت أيضا غير واضحة. فالبيانات تعالج بواسطة نظام حاسوبي، يوصف أحيانا بأنه الجهاز الآلي لمعالجة البيانات. وتتضمن معالجة البيانات عدة خطوات منها الادخال، والنقل الى المعدات الطرفية (شاشة الفيديو مثلا) ووسائط التخزين الوسطية، والمعالجة الفعلية، ونقل النتائج الى الأجهزة الطرفية لتخزينها، والاخراج أو الارسال مرة أخرى الى مكونات نظم أخرى. واعتراض بيانات في نظام حاسوبي ينتهي عموما الى البحث عن بيانات مخزنة، ويتم ذلك بالاستفادة من وظائف النظام أو برامج حاسوبية معينة. ويمكن البحث عن البيانات أثناء الارسال بواسطة الوسائل التي يتيحها النظام (الرصد)، ان وجدت، أو باعتراض تدفق البيانات تقنيا في موقع ما في مرافق الارسال. وحيث ان البيانات تكون في كثير من الحالات مخزونة وفي حالة متدفقة معا، أو أنها تنتقل مرارا من حالة الى أخرى، فسوف يتسنى للمحققين في أغلب الحالات الاختيار بين الضبط والاعتراض للحصول على نفس البيانات. وهذا قد يثير شواغل قانونية مقلقة، ذلك لأن المعايير أو الضمانات التي تنطبق على اعتراض الاتصالات وضبط المواد المخزونة ليست هي نفس الشيء في كثير من الدول. فاعتراض البيانات أثناء ارسالها يخضع غالبا لمعيار أكثر صرامة لأن الاعتراض عملية خفية وقد يستهدف بيانات لم تكن موجودة عندما أعطى الاذن بالتفتيش أو عندما بدأ التفتيش، وفي معظم الحالات لن تكون الأطراف المعنية على دراية بالاعتراض، وقد لا تبلغ الأطراف بذلك، اذا حدث أصلا، الا بعد أن يحدث التفتيش بفترة طويلة. وكون بيانات الشبكة يمكن ضبطها أو اعتراضها، فان هذا يمحو حقوق المشتبه بهم في بعض القضايا، حيث انه سيسمح لأجهزة انفاذ القانون أن تطبق سلطات تفتيش قانونية أقل تقييدا على بعض العمليات التي تعتبر أقرب الى طبيعة الاعتراضات.

٣٨- والبيانات الالكترونية، التي تستنسخ من ملفات البيانات أو تسجل من تدفقات البيانات، تستلزم عادة اتخاذ اجراءات وقائية وتدابير خاصة من أجل استخدامها كأدلة في القضاء، اذا قدر لها أن تستخدم بصفتها هذه على الاطلاق. وفي العديد من النظم القضائية، يقتضي مبدأ الفورية، أي وجود تقديم جميع الأدلة الى القضاء، أن تكون جميع المواد الاستدلالية ذات جودة عالية. ويجوز أن يفرض بعض البلدان شروطا رسمية تعيق أو تمنع استخدام البيانات الالكترونية كأدلة. وهناك، على سبيل المثال، بعض القوانين التي تشترط تقديم المواد تحريريا لكي يمكن قراءتها في المحكمة. والبيانات التي تمثل صوتا أو صورا لا تستوفي هذا الشرط في بعض البلدان، ومن ثم فانها تشكل أدلة مرفوضة. كذلك، فأي تشكك في موثوقية المواد الاستدلالية يجعلها عموما أدلة مرفوضة. وحيث يمكن تغيير البيانات الالكترونية بسهولة ودون ترك أي أثر، فان هذا يفرض عبئا ثقيلا على كاهل سلطات انفاذ القانون في جمع هذه الأدلة وفقا

لاجراءات شفافة ومضمونة تتيح تثبيت مطابقتها للقواعد المرعية. والتحقق من أصالة الأدلة وصحتها يستلزم تمكن القضاء من استعراض موثوقية عملية استنساخ وتسجيل الدليل من حامل البيانات الأصلي أو من قناة البيانات. ويجب أن يكون قادرا أيضا على اختبار صحة ما يلي: (أ) اجراء الحفظ وضمان الحفظ نفسه؛ (ب) أي تحليل يجرى على المواد؛ (ج) تطابق المواد المقدمة في القضاء مع المواد التي تم في الأصل ضبطها وصونها.

٣٩- وبالاضافة الى السلطات التقليدية التي يستلزمها تفتيش المرافق، تسمح نظم قانونية وطنية عديدة للمحاكم باصدار أوامر بتقديم أدلة ملموسة. ويجوز في بعض الحالات منح سلطات موازية أخرى لاصدار أمر بتقديم بيانات معينة. ويجوز أن تخضع هذه السلطات لقيود وشروط معينة لا تنطبق على الأوامر التقليدية لتقديم الأدلة، وذلك لمنع استخدامها كوسيلة للحصول على معلومات غير المعلومات المحددة. وبغير هذه الضوابط يمكن لأمر ما، على سبيل المثال، أن يلزم شخصا بجمع أو معالجة أو اختيار أي نوع من البيانات التي خزنت دون أن تخضع لرقابة ذلك الشخص. وهذا الالتزام يتجاوز نطاق أمر تقديم الأدلة ومعناه. ولعل من المفيد لسلطات انفاذ القانون، لدى التماس واستخدام أوامر لتقديم الأدلة، أن تدرج ملفات تسجيل الأداء في أي نظام حاسوبي بالاضافة الى البيانات الأخرى المطلوبة. فمثل هذه الملفات تسجل جميع المعاملات على النظام بالترتيب الزمني، مع تسجيل المعلومات عن أشياء مثل التواقيت والفترات المستغرقة والطرفيات التي تم منها الاطلاع على البيانات أو تغييرها.

٤٠- وفي العديد من البلدان، تجيز القوانين التقليدية للسلطة القضائية، أو لسلطة أخرى، اعتراض الاتصالات التي تتم عن طريق شبكات الاتصال العامة ثم تسجيلها. ولقد وسع بعض البلدان هذه السلطة بحيث أصبحت تشمل الشبكات الخاصة وأشكال جديدة معينة من الاتصالات اللاسلكية كالنظم المتنقلة أو نظم الاتصالات الساتلية، والشبكات الحاسوبية. والغاية المنطقية لهذه التدابير التشريعية هي أن اعتراض الاتصالات التي تجري عن طريق شبكة ما دون اعتراض الاتصالات التي تتم عن طريق شبكات أخرى سيجعل المجرمين يستخدمون النظام الذي ينطوي على أدنى درجة من خطر اعتراض سلطات انفاذ القانون لاتصالاتهم. ويستلزم الاعتراض المشروع لاتصالات معينة استخدام مرافق تقنية خاصة، بما فيها وجود أساس قانوني واضح لانشاء المرافق والتنفيذ العاجل للأمر القضائي بالاعتراض.

٤١- ويمثل التعاون بين مشغلي الشبكات، مثل مشغلي الاتصالات اللاسلكية ومقدمي خدمات الانترنت أمرا ضروريا لتحديد الاتصالات التي يتعين اعتراضها والأشخاص الذين يجرون تلك الاتصالات موضع الاعتراض. فالمعلومات اللازمة التي تتعلق بالمشتركين في خدمات الاتصال لا تتوافر الا لهؤلاء المشغلين. ويجوز أن يفرض القانون الوطني، عند الاقتضاء، التزاما قانونيا على مشغلي الخدمات ومقدميها بتقديم البيانات الخاصة بالمشترك فور اصدار السلطات المختصة لأمر تقديمها. كذلك فوضوح هذا النوع من الالتزامات القانونية يحمي الأفراد والشركات من المسؤولية المدنية تجاه المشتركين.

٤٢- وتتوافر عادة لمشغلي الاتصالات اللاسلكية ومقدمي خدمات الانترنت بيانات حركة الرسائل من الاتصالات السابقة، التي تصدرها معدات تسجيل تفاصيل الاتصالات، وتتضمن موعد الاتصال ومدته وتاريخه والأطراف التي تم بينها الاتصال ونوع الخدمة أو النشاط المقدم (قارن مع مثال ملف تسجيل في نظام حاسوبي الذي يرد في الفقرة ٣٧ أعلاه). وتحفظ هذه البيانات عموما لفترة زمنية محدودة، متوقفا ذلك على الاحتياجات التجارية لمشغل الخدمة أو مقدمها وعلى المقتضيات القانونية (في الاتحاد الأوروبي) أو التجارية اللازمة لحماية الحرية الشخصية. ويجيز العديد من القوانين الوطنية لسلطات انفاذ القانون أو للسلطات القضائية اصدار أمر بجمع بيانات المرور الخاصة باتصالات ستجري في المستقبل. وفي الحالات التي تعتبر فيها بيانات حركة مرور الرسائل جزءا من الاتصال، مثل معلومات الترويسة في رسائل البريد الالكتروني، فان جمع بيانات المرور هذه ربما يعتبر بمثابة اعتراض للاتصال نفسه، وبالتالي، فانه يخضع للقيود القانونية على هذا الأساس، وفي حالات أخرى، يعتبر جمع بيانات

المرور دون اعتراض محتويات الاتصال نفسها تدخلا أقل درجة في خصوصيات أولئك الأشخاص المعنيين، ومن ثم فانه يخضع لدرجة أقل في مبتدى القيود القانونية.

٤٣- وفيما يخص قضايا القرصنة أو اقتحام البيئة الالكترونية، هناك حاجة خاصة للتدخل الفوري لاعتراض الاتصال الالكتروني، بالاضافة الى ضرورة التوافر الفوري لبيانات حركة مرور الرسائل والبيانات الخاصة بالمشترك من أجل تعقب أثر مصدر الاتصال وحفظ البيانات وفي آخر المطاف القاء القبض على المجرم أثناء ارتكابه للجرم، وذلك لأسباب تتعلق باتاحة أدلة الاثبات. وفي حالة تجريم القرصنة الالكترونية، هناك بعض القوانين التي لا تعتبر هذه القرصنة جريمة ذات خطورة تكفي لتبرير استعمال تدابير الاعتراض. فأي مخطط للقرصنة يتضمن عموما أفعالا أشد خطورة من تلك الخطورة التي يمكن ثبوتها لحظة الكشف عن أنشطة مرتكب القرصنة. وقد يعتبر هذا سببا آخر للسماح باعتراض الاتصالات فيما يتعلق بحالات اقتحام البيئة الالكترونية.

٤٤- وقد يعيق تشفير الاتصالات الالكترونية عملية اعتراض تلك الاتصالات. ويستخدم التشفير لضمان صحة رسالة ما والتعرف على مرسلها، وكذلك لضمان سلامة الرسالة، وهناك مهمة ثانية للتشفير وهي ضمان سرية الرسالة بحمايتها من الغير. وقد كانت سياسات التشفير الممكنة موضوعا لنقاش شهده مؤخرا عدد من المنظمات الدولية. فالمهتمون بتيسير انفاذ القانون ومكافحة الجريمة يساورهم قلق بشأن صعوبات في الحصول بصورة قانونية على سبيل الاطلاع على البيانات المشفرة، في حين يريد المهتمون بالخصوصية والمصالح التجارية اتباع التشفير لحماية معلوماتهم الشخصية والتجارية.

٤٥- ويخرج معظم هذه الماقشات عن نطاق الوثيقة الحالية، بيد أنه يلزم هنا النظر في مسألتين معينتين، فبعض البلدان المنتجة لوسائل التشفير ارتأت التحكم في انتشار هذه المنتجات من أجل منع الجماعات الاجرامية والارهابية من الحصول عليها، مستخدمة في ذلك أشياء مثل اشتراطات الترخيص للمنتجات، "متشددة" بما يكفي لجعل الوصول الى انفاذ القانون على درجة من الصعوبة. وسعى بعض البلدان أيضا الى استعمال تدابير عملية في محاولة لضمان امكانية الوصول بطريقة مشروعة الى الاتصالات الالكترونية المحمية بالتفشير. وتشمل هذه التدابير استخدام شفرات حاسوبية خاصة ونظم ايداع مفاتيح الرسائل كوديعة عالقة (حيث تحفظ مفاتيح رموز الرسائل لدى أطراف ثالثة موثوقة يجوز وضع اليد عليها قانونيا للوصول الى تلك الرسائل)، أو تشمل تلك التدابير جهودا خاصة لحل شفرات الرسائل بواسطة رسائل تقنية. وتواجه السياسات من هذا النوع بعض الصعوبات مع استخدام التكنولوجيا، وتواجه معارضة من دعاة حماية حقوق الخصوصية والمصالح التجارية.

٤٦- ومن المفهوم أن الحصول على سبل الاطلاع على الاتصالات المشفرة أو البيانات المخزنة أثناء اجراء التحقيقات الجنائية يعتبر مسألة تثير القلق والاهتمام لدى الأجهزة المكلفة بانفاذ القانون في جميع أنحاء العالم. ولربما توجد في بعض البلدان فعلا تدابير لمعالجة جزء من هذه المشكلة. وفي حالات عديدة، يتولى نفس مشغلي الاتصالات اللاسلكية والشبكات استعمال التشفير من أجل حماية نظمهم والاتصالات التي يقوم بها المشتركون في تلك النظم. وعندما يخضع هؤلاء المشغلون لالتزام قانوني بالتعاون مع سلطات انفاذ القانون على اعتراض اتصال معين، يبدو من المنطقي الافتراض أن هذا الالتزام يتضمن (أو يمكن أن يتضمن) واجب حل أي تشفير كانوا قد استعملوه على ذلك الاتصال. ولكن هذا لا يمتد ليشمل التشفير الذي يطبقه الزبون بشكل مباشر، والذي يستحيل عموما على المشغل أن يفك رموز شفرة الاتصال. وهناك امكانية أخرى، وهي أن ينظر المشرعون الوطنيون في الزام الأشخاص المشاركين في اتصال مشفر باتاحة وسائل حل التشفير عندما تصدر السلطة القضائية المختصة أمرا بذلك. ولغرض الحماية من التجريم الذاتي، يجوز منع اتاحة اصدار هذا الأمر ضد المشبوهين أو غيرهم ممن ينطبق عليه اعفاء قانوني.

٤٧- وكما يرد في الفقرة ٣٧ أعلاه، فان معظم البلدان تميز بين اعتراض البيانات المتدفقة وبين الاستيلاء على البيانات المخزنة، ولكن البريد الالكتروني يشكل تحديا لهذا التمييز، لأنه يجمع بين نقل البيانات وتخزينها. فعند ارسال رسالة ما، فانها تنقل من جهاز

مقدم الخدمات للمرسل الى مقدم الخدمات لشخص المرسل اليه. ولدى الاستلام، يقوم مقدم الخدمات بتخزين الرسالة في صندوق بريد الشخص المرسل اليه الى أن يفتح ذلك الصندوق. وتتاح للمرسل اليه سبل الاطلاع على تلك الرسالة، وهو يقرر مدة الاحتفاظ بها في صندوق البريد. وهكذا تخضع الرسائل الموجودة في صندوق البريد لتحكم المرسل اليه ومقدم الخدمات على السواء، ويمكن لسلطات انفاذ القانون بوجه عام الحصول على سبل للاطلاع باستخدام سلطات قسرية ضد المرسل اليه أو مقدم الخدمات. وعادة، فان سلطات انفاذ القانون سوف تفضل القيام بذلك ضد مقدم خدمات الانترنت، حيث ان هذا يمكن أن يتم دون تنبيه المرسل اليه بوجود تحقيق. وفي هذه الحالات يجوز أن تصبح الاجراءات متبادلة بالفعل بين السلطات القانونية التي تتيح اعتراض الاتصال وتلك التي تتيح اجراء تفتيش مادي للمرافق وللحواسيب الموجودة فيها. وفي هذا السياق يمكن اثارة تساؤلات بشأن مدى شرعية اصدار أمر بتقديم الرسائل الموجودة وتسليمها والرسائل التي قد تصل أثناء مدة زمنية معينة، وذلك ما لم تطبق معايير قانونية (وهي عادة معايير أعلى درجة) على عملية الاعتراض. وكون البيانات تخضع لسيطرة مقدم الخدمات والزبون في آن واحد، فان هذا يثير تساؤلات بشأن حق حصانة الخصوصيات والملكية وغيرها من الحقوق أو المصالح التي يجب تناولها عند الحصول على ترخيص قانوني باجراء عملية للتفتيش أو للاعتراض.

خامسا - التعاون الدولي بين السلطات الوطنية لانفاذ القانون

ألف - أشكال التعاون والمبادرات الدولية

٤٨- ان البعد الدولي الذي اكتسبته الشبكات الالكترونية يؤدي الى تضاؤل احتمال اقتصار عناصر الجريمة السيبرانية على اقليم وطني واحد. فعند اجراء التحقيقات، تتعاون سلطات انفاذ القانون في شتى الدول بأسلوبين، التعاون بالأسلوب الرسمي، باستخدام أطر وهياكل المساعدة القانونية المتبادلة، مثل الانتربول، وبالأسلوب غير الرسمي، عن طريق تقديم معلومات يحتمل أنها ذات فائدة وتوجيهها مباشرة الى سلطات دولة أخرى. ويفترض في تعاون الشرطة على الصعيد الدولي عموما وجود موافقة من سلطات الدول المعنية. ووفقا للعلاقة بين الدول المعنية، فان طبيعة المعلومات المتبادلة، أو غيرها من العوامل، قد تقتضي هي الأخرى تحديد السلطات والاجراءات في اطار اتفاق دولي.

٤٩- وفي عام ١٩٩٧، اعتمدت مجموعة الثمانية، المؤلفة من رؤساء دول أو حكومات البلدان السبعة الصناعية الكبرى والاتحاد الروسي، عددا من المبادئ القانونية وخطة عمل مشتركة لمكافحة ما وصفته بأنه "جرائم التكنولوجيا المتقدمة".[٧] وتتضمن هذه المبادئ بعض اقتراحات من أجل التعاون العملي فيما بين سلطات انفاذ القانون، ووضع مبادئ قانونية بشأن المساعدة القانونية المتبادلة. وتضمنت عناصر التعاون العملي التي جرت مناقشتها ما يلي:

(أ) تدابير لضمان توافر عدد كاف من الموظفين المتدربين من ذوي الخبرات الفنية الكافية، عن طريق التعاون في مجال اعداد موظفي انفاذ القانون وتدريبهم؛

(ب) التعاون في وضع المعايير القضائية لاسترجاع البيانات الالكترونية والتحقق من صحتها.

٥٠- ومن أجل تيسير الاستجابات في وقتها المناسب لطلب المساعدة الذي يرد من دولة أخرى، اتفقت مجموعة الثمانية على تأسيس نظام لمراكز الاتصال، وهو نظام قائم الآن ويتيح خدماته طوال أربع وعشرين ساعة يوميا وطوال أيام الاسبوع ("٧/٢٤") وهو منفذ حاليا. وتتباين مهمات مراكز الاتصال هذه تباينا كبيرا. ويقوم مركز الاتصال عند الطلب، بتقديم معلومات بالوقائع يمكن أن تساعد على توسيع نطاق التحقيق الى دولة أخرى أو طلب مساعدتها، واتخاذ جميع التدابير اللازمة من أجل الاستجابة دون تأخير الى طلب رسمي التماسا للمساعدة القانونية أو لاتخاذ التدابير الأولية، التي يسمح بها القانون الوطني، بانتظار وصول طلب من هذا القبيل. ولا تقتصر مراكز الاتصال المنشأة بموجب نظام "٧/٢٤" على مجموعة الثمانية، وانما تم تأسيسها أيضا على أساس تطوعي في عدد من الدول الأخرى.

وفي بعض البلدان، قد لا يكون تأسيس الوحدات الاختصاصية هذه أمرا ممكنا بالنظر الى نقص الخبرات الفنية أو الموارد المالية. وفي دول أخرى قد تحظى مكافحة الجريمة السيبرانية بقدر أقل من الأولوية. وواضح أن تزايد فعالية نظام المكافحة مرهون بزيادة ما توفره الدول من تدريب واعداد الموظفين وجعل خدماتهم متاحة على أساس نظام "٧/٢٤".

٥١- وقد تم في اطار الانتربول تأسيس عدد من أفرقة الخبراء العاملة المعنية بجرائم تكنولوجيا المعلومات. وقد أعد الفريق العامل الأوروبي المعني بجرائم تكنولوجيا المعلومات دليلا عن الجرائم المتصلة بالحواسيب (متوافر على قرص مدمج مجهز بذاكرة قراءة فقط CD-ROM). ويضم الدليل ارشادات عن كيفية التحقيق في قضايا الجرائم المتصلة بالحواسيب، وشرحا لأدوات وتقنيات البحث عن المواد الالكترونية والحصول عليها، ومعلومات بشأن القوانين الموضوعية والاجرائية ذات الصلة في شتى البلدان. وتعمل الأفرقة العاملة بهمة ونشاط على استحداث أدوات لبرمجيات حاسوبية معينة من أجل الشكف عن جرائم معينة ترتكب على شبكة الانترنت. كما تم تنظيم العديد من الدورات التدريبية في مجال التحقيقات في الجرائم المرتكبة باستعمال الحواسيب.

٥٢- ويهدف الدليل الذي أصدرته الأمم المتحدة بشأن منع ومكافحة الجرائم المتصلة بالحاسوب الى تحقيق مواءمة القانون الموضوعي والقانون الاجرائي، وكذلك التعاون الدولي على مكافحة الجرائم المتصلة بالحواسيب. ويتضمن الدليل فصلا عن أمن المعلومات ومنع الجريمة السيبرانية.[٨]

٥٣- ويتسم كل من النهوج المنسقة والنهوج التي تستند الى المبادرات التي تتخذها الدول على انفراد بوجود ميزة فيها، ومن الأهمية تحقيق أقصى قدر ممكن من الاستفادة من كليهما. وفي هذا السياق، من الأهمية عقد اجتماعات دولية بصفة منتظمة لتلتقى فيها الوحدات المعنية بالجريمة السيبرانية وتتبادل المعلومات والخبرات العملية. كما ستساهم مرافق دائمة أخرى مثل مصارف البيانات ومواقع الشبكة العالمية "ويب" وأفرقة المناقشة في تحسين تبادل المعلومات.[٩]

٥٤- وتضم خطة العمل لمجموعة الثمانية عنصرا ثالثا وهو تنسيق التعاون بين الصناعة والدولة. وهذا يشمل:

(أ) تشجيع الهيئات المسؤولة عن تحديد المعايير على وضع معايير للاتصالات اللاسلكية الموثوقة والمأمونة وكذلك لمعايير تكنولوجيات معالجة المعلومات؛

(ب) استحداث نظم للمعلومات والاتصالات اللاسلكية قادرة على اكتشاف اساءة استعمال الشبكات وتعقب المجرمين وجمع الأدلة ذات الصلة.

وتعود ضرورة وأهمية التعاون والتنسيق مع القطاع الصناعي الى العبء الذي يمكن أن تفرضه التحقيقات الجنائية في البيئات الحاسوبية على هذا القطاع. ويتضمن ذلك مسائل متعددة منها أمن المعلومات وتطوير المنتجات والتعاون الفعلي في تنفيذ الأوامر القضائية. وقد تتخذ المفاوضات بين المنظمات الصناعية الحكومية شكل الترتيبات القطاعية أو غيرها من الاتفاقات غير الملزمة أو الواجبة النفاذ.

باء- المساعدات القانونية المتبادلة وغيرها من المعاهدات الدولية

٥٥- يقتضي التعاون الدولي الذي يتخذ شكل المساعدات القانونية المتبادلة وجود اتفاق دولي أو غيره من الترتيبات المماثلة كالتشريعات المتبادلة. وهذا النوع من الأحكام، سواء أكانت متعددة أم ثنائية الأطراف، يلزم سلطات الطرف المتعاقد بالاستجابة لطلب المساعدة القانونية المتبادلة في حالات متفق عليها. وتنفيذ مثل هذا الطلب لا يمكن أن يتم الا بشرط توافقه مع القانون المحلي للدولة المطلوب منها المساعدة، أو في حالة غياب القواعد المعينة، بقدر عدم انتهاكه لذلك القانون.

٥٦- وتتعاون الدول في مجال المسائل الجنائية بشكل أكثر فعالية اذا شعرت بوجود مصلحة مشتركة على النحو المبين في النظم الأساسية القانونية أو المدونات الجنائية وبالطريقة التي ينفذ بها القانون الجنائي في الدول المعنية. وفي العديد من الاتفاقيات الدولية المتعلقة بالمسائل الجنائية، تتجسد المصلحة المشتركة في قاعدة خاصة هي قاعدة الجريمة المزدوجة. ولا تستطيع دولة

ما أن تتعاون مع دولة أخرى بشأن التحقيق في أفعال معينة ومحاكمتها ما لم تعتبر تلك الأفعال أفعالا اجرامية في الدولة المطلوب منها المساعدة. لذا فان افتقار بعض الاتفاقيات القديمة لقاعدة الجريمة المزدوجة يمثل أساسا سليما لرفض المساعدة. ومعظم الاتفاقيات الحديثة لا تثير هذا الشرط الرسمي، ولكنها تتضمن معيار المعقولية. فقد لا يكون أمرا معقولا الامتثال لطلب المساعدة القانونية عندما تتضمن الجريمة، على سبيل المثال، فعلا اجراميا غير خطير أو تعنى بسلوك معين لا تعتبره الدولة التي طلبت منها المساعدة فعلا اجراميا.

٥٧- لذلك فالتوفيق بين بعض الأحكام الموضوعية في القوانين الجنائية هو أحد سبل تحسين التعاون الدولي فيما يخص المسائل الجنائية. وقد تتباين السياسات الجنائية بين الدول بسبب الاختلافات الثقافية والاجتماعية والاقتصادية في تلك الدول. لذلك، فان المداولات الدولية الموجهة نحو التوفيق بين الجرائم المتعلقة بسرية البيانات وسلامتها واتاحتها (انظر الفقرة ١٥)، كالأحكام الموجهة نحو التكنولوجيات، يمكن أن تكون أقل تعقدا من التوفيق المقصود بين الجرائم المتعلقة بمحتويات البيانات، وذلك بسبب أثرها على حقوق الانسان (مثل حرية التعبير). والاستثناء الذي يبرهن على هذه القاعدة يبدو في توافق الآراء الواسع النطاق بشأن الجرائم المتعلقة باستغلال الأطفال لأغراض اباحية.

٥٨- والمقصود بالمساعدات القانونية المتبادلة هنا أي شكل من أشكال المساعدة القانونية. وهي تتعلق عموما بسلطات قسرية معينة بخصوص التحقيق في الجريمة السيبرانية. والى جانب طلبات العون التقليدية، كاستجواب الشهود مثلا، فان المقصود بهذه المساعدات هو الحصول على بيانات معينة مخزنة في نظام حاسوبي يقع في اقليم دولة أخرى، أو بيانات يجري نقلها الكترونيا عن طريق شبكة ما يمكن رصدها أو اعتراضها في اقليم تلك الدولة.

٥٩- وتحدد الدول في اطار قوانينها المحلية أيا من سلطاتها يقبل التطبيق من أجل مساعدة دول موقعة أخرى. وهي ليست ملزمة بالطبع بتقديم جميع سلطاتها المحلية لأجل التحقيق في القضايا الجنائية الذي تقوم به دول موقعة أخرى. ويجوز في بعض القضايا تقديم المساعدة في حالة معينة، وهي مساعدة لا تقدم عادة على أساس منتظم أو اعتيادي، وانما تقدم في ضوء المصالح المتبادلة للدول المعنية. كما ان المساعدات القانونية المتبادلة، باعتبارها جزءا من القانون الدولي، تخضع في آخر الأمر لمبدأ المعاملة بالمثل. ولهذا السبب وغيره من الأسباب، فان الدول التي تتفاوض مع دول أخرى بشأن نطاق المساعدات القانونية المتبادلة قد تتردد في الذهاب الى أقصى مدى قد يتيحه القانون المحلي. كذلك يمكن رفض المساعدات القانونية المتبادلة على أساس التذرع، بشكل مباشر أو غير مباشر، بمبدأ الجريمة المزدوجة - وهو الاشتراط بأن يشكل الجرم الذي تلتمس من أجله المساعدة، جريمة في كلا الدولتين المعنيتين. وعلاوة على ذلك، فان الاتفاقات الدولية لتقديم المساعدات المتبادلة قد تتضمن استثناءات لعدم تقديمها. ومن بين الاستثناءات الشائعة أنواع معينة من الجرائم ، كالجرائم المالية والسياسية والعسكرية، والجرائم التي لا تعتبر جرائم خطيرة بدرجة تستحق بذل جهد المساعدات المتبادلة (تقيم درجة الخطورة بالعقوبات المحتملة لتلك الجرائم).

٦٠- وقد تظهر بعض المشكلات الاضافية فيما يتعلق بالمساعدات القانونية في التحقيق في الجرائم السيبرانية الدولية. فالدول الأطراف التي لا تنص قوانينها المحلية على سلطات معينة للتفتيش عن الأدلة في بيئات الكترونية، قد لا تتمكن من الاستجابة (أو تكون استجابتها غير كافية) لطلب المساعدة. ولهذا السبب، فان التوفيق بين السلطات القسرية يعتبر شرطا هاما من شروط التعاون الدولي.

٦١- ويرجح أن يكون طلب المساعدات القانونية المتبادلة ملحا في حالات الجريمة السيبرانية أكثر مما هو في التحقيقات في الجرائم التقليدية، ويعود سبب ذلك الى احتمال ضياع الأدلة الالكترونية ما لم يتم تأمين الحصول عليها بسرعة. بيد أن اتخاذ اجراء فوري قد لا يكون أمرا ممكنا على الدوام لأسباب رسمية وعملية، فقد تقتضي الضرورة مثلا اصدار أمر قضائي

في الدولة المطلوب منها المساعدة. ولتجنب ضياع الأدلة في هذه الحالات، يمكن استحداث نظام لاتخاذ اجراء أولي عاجل يقتضي أقل قدر ممكن من الخطوات الرسمية، يعقبه تطبيق الاجراءات التقليدية بمجرد الحصول على الأدلة لتحديد ما اذا كان يلزم تسليمها الى الدولة التي طلبت المساعدة. وفي اطار هذا النظام، يسمح القانون المحلي بالحصول على البيانات استجابة الى طلب غير رسمي، والمحافظة عليها بانتظار وصول طلب رسمي بالافصاح عنها بموجب ترتيبات المساعدة القانونية المتبادلة. ويتم محو البيانات المحصلة في حالة عدم ورود طلب رسمي لها في الموعد المناسب، أو في حالة رفض الطلب لعدم ملاءمته. ويمكن وضع نظام مماثل لحفظ بيانات حركة المرور التي يحتفظ بها مشغلو الاتصالات ومقدمو خدمات الانترنت.

٦٢- وتتيح الشبكات الحاسوبية الدولية القيام في اقليم معين بأنشطة قد تكون لها آثار (متعمدة أو غير مقصودة) خارج ذلك الاقليم. فعلى سبيل المثال، قد تحصل سلطات انفاذ القانون في دولة ما على بيانات من شبكة حاسوبية في اطار عملية تفتيش قانونية تجريها في تلك الدولة، ثم تكتشف أن بعض البيانات المحصلة مخزن في قسم من الشبكة يقع في دولة أخرى وبأنها بيانات محمية بموجب قوانين تلك الدولة. وبالمثل، قد تعترض دولة ما بصورة قانونية اتصالات الكترونية تمر عبر اقليمها، حى لو كانت تلك الاتصالات تدور بين أشخاص موجودين في نطاق اختصاصات قضائية أخرى يتمتعون فيها بالحماية القانونية لتلك الدولة من التدخل التعسفي في الاتصالات الخاصة. ويمكن لموظفي انفاذ القانون الذين يشغلون عملياتهم على شبكة ما أن يتصرفوا كعملاء سريين امتثالا للقوانين المعمول بها في اختصاصهم القضائي في ظروف لا تسمح القوانين في اختصاصات قضائية أخرى يعملون في اطارها، بممارسة افعالهم ولا بالأساليب التي استخدموها. وتعتبر جميع هذه التصورات جديدة لم يسبق لها مثيل، ولا ينص القانون الدولي حاليا على أحكام من شأنها أن تساعد على حل المسائل المعنية.

٦٣- كذلك، ليس هناك الآن توافق آراء واسع النطاق بشأن الحلول الممكنة للآثار المترتبة خارج حدود بلد ما على تدابير التحقيق المحلية المطبقة بصورة قانونية. والمعترف به عموما أن أية دولة لها السلطة القانونية لتطبيق تدابير التحقيق أو السلطات القسرية على أي مواطن من مواطنيها وفي حدود اقليمها الذي يخضع لاختصاصها القضائي المطلق. وقد يؤدي تطبيق هذه السلطات الى حالات يتم فيها البحث عن البيانات الموجودة في مكان آخر، أو استنساخها أو يحتمل محوها. وقد يشكل هذا في نظر الدولة موضع التفتيش عملا اجراميا بموجب قانونها الجنائي المحلي وانتهاكا لسيادتها الوطنية. ولكن القانون الدولي، من وجهة نظر أخرى، لا يحظر مثل هذا التدخل لأن هذه البيانات متاحة ويمكن الحصول عليها من الناحية التقنية في الدولة القائمة بالتفتيش دون مساعدة أو تدخل الدولة موضع التفتيش. ويمكن اعتبار البيانات الموجودة في أي مكان على الشبكة بيانات موجودة في كل مكان، وبالتالي فالحصول عليها من أي دولة توجد فيها تلك البيانات مسألة قانونية محلية بحتة لا تخضع للقانون الدولي. ومن وجهة النظر هذه، لا يلزم اشراك الدولة موضع التفتيش في أي مرحلة. وبقدر ما تكون هذه البيانات أو لا تكون موجودة في كل مكان يجب على المفتشين تحميلها فعلا من نطاق اختصاص قضائي الى اختصاص قضائي آخر، على سبيل المثال، فان هذه مسألة ما زالت تثير تساؤلات فيما يخص القانون الدولي.

٦٤- وفيما يخص الرأي القائل بأن أي تدخل في شبكة حاسوبية تقع في اقليم دولة ما يمثل انتهاكا لسيادتها الاقليمية، من المفيد النظر في رأيين مختلفين بشأن حالة القانون الدولي. ويستند الرأي الأول الى مبدأ عدم السماح للدول على أساس منفرد بتفتيش أو باستنساخ أو خلافا لذلك بالتدخل في البيانات أو النظم الحاسوبية الموجودة في دولة أخرى، وذلك استنادا الى نفس المبدأ الذي يحظر أداء نفس الأشياء بوجود مادي منفرد. وينبغي هنا اتباع اجراءات المساعدات القانونية المتبادلة القائمة للحصول على بيانات استدلالية من دولة أخرى. ويتبع هذا الرأي المبادئ التقليدية، ولكنه قد لا يدرك المشكلات العملية التي تواجه التحقيق في الجرائم المتصلة بالحواسيب.

٦٥- ويبدي البعض رأيا عملي النظرة بدرجة أكبر، وهو ان القانون الدولي لا يقدم في الوقت الحاضر

اجابات واضحة لمسائل انتهاك القوانين المحلية أو خرق مبادئ السيادة. ويقول أولئك الذين يتخذون هذا الموقف ان القانون الدولي يمكن أن يتشكل بظهور توافق في الآراء على الصعيد الدولي بشأن السماح بتنفيذ هذه الأنشطة، ويمكن أن يتشكل بتحديد واضح للظروف التي يسمح فيها بتنفيذ تلك الأنشطة. ومن العناصر المهمة المقترحة لمثل هذا الحل اشعار الدولة موضع التفتيش.

٦٦- ويمكن للمجتمع الدولي أن يعرض على بساط البحث مفاهيم جديدة لوضع قاعدة قانونية بشأن كيفية تحديد حقوق الدول فيما يخص الاستعمال المشترك للشبكات الحاسوبية الأرضية أو المتنقلة أو الساتلية. والى أن يتم ذلك، يمكن الاتفاق على نهج عملي في شكل معاهدة أو أي صك دولي آخر يتعلق باجراءات معينة يمكن بها الموازنة بشكل متناسب بين مصالح الدولة المفتشة ومصالح الدولة موضع التفتيش والمقيمين بها.

سادسا - استنتاجات

٦٧- ان تزايد حدوث الجرائم المتصلة بالحواسيب، وتيسر ذلك نتيجة لتأسيس شبكات الكترونية عالمية ودولية وعامة، جعل التنسيق والتعاون على الصعيد الدولي في هذا المجال من الأمور الأساسية. ويمكن أن تستند العناصر الرئيسية لهذا الاجراء الدولي الى المبادئ التالية:

(أ) **اذكاء الوعي لدى عامة الجمهور:** قد يؤدي تثقيف عامة الجمهور وتوعيتهم الى خفض عدد الجرائم في البيئات الالكترونية. ويمكن للقطاع الصناعي - جهات صنع المعدات والبرمجيات الحاسوبية، ومقدمو الخدمات وغيرهم - ولمنظمات حماية المستهلكين وللحكومات، أداء مهمة مشتركة في اعلام الجمهور بشأن المسائل المتعلقة بالأمن والمخاطر الأخرى الكامنة في البيئات الالكترونية المفتوحة، وتزويدهم باقتراحات عن كيفية حماية مصالحهم؛

(ب) **التوصية بانتهاج سياسة مشتركة ازاء الجريمة السيبرانية:** ان ما تتسم به جريمة الشبكات الالكترونية من طابع عبر وطني يوحي بضرورة أن يصبح وضع سياسات مشتركة بشأن المسائل الرئيسية جزءا من أية استراتيجية للمكافحة. وتعد السياسات المشتركة من هذا القبيل على درجة من الأهمية لمنع حدوث "ملاذات البيانات" في الاختصاصات القضائية حيث لم يتم، على سبيل المثال، تجريم أنشطة معينة فيها. ويمكن أن يشكل وضع السياسات المشتركة جانبا من جوانب برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، وذلك دعما للأعمال التي اضطلعت بها حتى الآن منظمات دولية أخرى؛

(ج) **تحسين التدابير الخاصة بالتحقيق:** يمكن مواصلة التدابير الفعالة من أجل تحسين القدرات الخاصة بالتحقيق في بيئات الشبكات، وخصوصا في القضايا التي تتداخل فيها اختصاصات قضائية متعددة. وهذا يشمل الاستجابة الى الحاجة الى عمليات يمكن اجراؤها بسرعة تكفي لمنع فقدان الأدلة أو عدم توفر سبل الحصول عليها. كما يستلزم تفتيش النظم الحاسوبية ومراقبة شبكات الحوسيب سلطات اضافية لا تتوافر في الوقت الحاضر في القانون الاجرائي الجنائي التقليدي. كما ان مقادير البيانات الموجودة في النظم الحاسوبية والسهولة التي يمكن بها للباحثين الوصول الى هذه البيانات تثير أيضا مسائل هامة تتعلق بالخصوصية وما يتصل بها من مسائل. اذ يجب، لدى صوغ سلطات قانونية جديدة وفي تنفيذ تلك السلطات، أن تراعي وأن توازن بدقة حقوق الانسان الخاصة بالأفراد المعنيين؛

(د) ويستلزم التحقيق في الجريمة السيبرانية توافر موظفين من ذوي خبرات قضائية وتقنية خاصة، كما يستلزم أيضا اتباع اجراءات معينة. ويتضمن ذلك صوغ برامج تدريبية واستحداث أدوات برمجية حاسوبية للتحقيق. وينبغي اعداد برامج تدريبية دولية وتقاسم الخبرات الفنية بين الدول. ويمكن للأمم المتحدة، في اطار برنامج منع الجريمة والعدالة الجنائية، أن تدرس مدى الرغبة في استعراض دليلها بشأن الجرائم المتصلة بالحواسيب وأن تواصل دعمها للأعمال التي اضطلعت بها حتى الآن منظمات دولية أخرى؛

(هـ) **تحسين اجراءات التنسيق والمساعدة عبر الحدود:** ان الجرائم السيبرانية سوف ترتكب في البيئات الالكترونية العالمية ولن تنحصر بالضرورة في اقليم دولة بعينها. وبغية اجراء تحقيق على نحو فعال، قد تعتمد الدول بالتالي على مساعدات تقدم من دول أخرى. وهذا يشمل التعاون غير الرسمي من جانب موظفي انفاذ القانون كما يشمل المساعدة القانونية المتبادلة الرسمية التي تتم عن طريق السلطات المركزية. وكون البيانات في شبكات الحواسيب تتصف بسرعة الزوال، فان هذا يجعل القدرة على اسداء مثل هذه المساعدة بسرعة وبفعالية أكثر أهمية بالنسبة لكثير من الجرائم الأخرى. ويمكن لأية مساعدات فعالة في القضايا التي تدخل فيها جريمة سيبرانية أن تدعمها الاجراءات التالية:

'١' انشاء مراكز اتصال مماثلة للمراكز التي أنشأتها مجموعة الثمانية من أجل اسداء المشورة الى الدول الطالبة بشأن المساعدات التي يمكن تقديمها، وللشروع في مباشرة التدابير اللازمة لتلبية الطلبات على النحو الذي يسمح به القانون المحلي؛

'٢' استعراض نظم المساعدات القانونية في سياق الجريمة السيبرانية. وهناك حاجة الى بحث الاحتياجات من المساعدات القانونية التقليدية والممارسات اللازمة لتحديد ما اذا كانت تلبي احتياجات التحقيق في الجرائم السيبرانية الحديثة، ولاستبانة ما يمكن أداؤه من تحسينات. ومن المجالات التي يمكن بحثها مدى ملاءمة السلطات اللازمة بوجه عام لتنفيذ التحقيقات الجنائية في اطار شبكات الحواسيب وامكانية اتخاذ اجراءات عاجلة بغية الحصول على البيانات من أجل التحقيقات الجنائية التي تجريها دول أخرى.

الحواشي

(١) تتضمن الأمثلة عن الرابطات أو الجمعيات: رابطة مقدمي خدمات الانترنت في الولايات المتحدة الأمريكية، والرابطة الكندية لمقدمي خدمات الانترنت ورابطة عموم أوروبا لرابطات مقدمي خدمات الانترنت في بلدان الاتحاد الأوروبي. كما توجد رابطات وطنية في بعض الدول الأوروبية بما فيها اسبانيا، ألمانيا، ايطاليا، بلجيكا، فرنسا، المملكة المتحدة لبريطانيا العظمى وايرلندا الشمالية، هولندا.

(٢) ١٨ تشرين الأول/أكتوبر ١٩٩٩، http://www.nua.ie/surveys/how-many-online.

(٣) انظر التعريفات التقنية للبيانات للمنظمة الدولية لتوحيد المقاييس.

(٤) Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986.

(٥) توصية مجلس أوروبا (١٩٨٩)، (Recommendation No. R (89) 9).

(٦) "Global Information Networks: Realising the Potential", Ministerial Conference, Bonn, July 1997.

(٧) انظر البلاغ الصادر من اجتماع وزراء العدل والداخلية لدول الثمانية، واشنطن ٩-١٠ كانون الأول/ديسمبر ١٩٩٧، http://www.usdoj.gov/criminal/cybercrime/communique.htm. وقد أقر رؤساء الدول أو الحكومات خطة العمل في ١٩٩٨. وتمت بشأنها توصية منظمات دولية أخرى كمنظمة الدول الأمريكية والاتحاد الأوروبي.

(٨) International Review of Criminal Policy, Nos.43 and 44, 1994 (United Nations publication, Sales No. E.94.IV.5).

(٩) مثال ذلك الشبكة العلمية لمعلومات العدالة (World Justice Information Network) <http://www.justinfo.net> أو دليل الانترنت بشأن ضابط الشرطة (The Police Officer Internet Directory) <http://www.officer.com/c_crimes.htm>.