الجهود الدولية في مكافحة الجرائم المعلوماتية

الدكتور/ أسامة بن غانم العبيدي
أستاذ القانون المشارك - معهد الإدارة العامة
الرياض - المملكة العربية السعودية

ملخص:

يمكن ارتكاب الجريمة المعلوماتية في أي مكان على وجه الأرض، ويستطيع الجاني ارتكاب جريمته دون أن يترك أدلة تساعد إلى الوصول إليه، كما أن الأدلة التي يمكن تتبعها قد تزول إذا لم يتم اتخاذ إجراءات سريعة لحماية الدليل. وتصبح هذه المهمة بالغة الصعوبة والتعقيد إذا كانت أدلة الجريمة تتواجد في حاسب آلي موجود في دولة أخرى، مما يحتم ضرورة تعاون سلطات ذلك البلد أو البلدان التي عبر من خلالها الفعل الإجرامي وهو في طريقه إلى الهدف، أو حيث توجد أدلة الجريمة. وهذا يحتم وجود تعاون دولي بين الدول لمكافحة هذا النوع من الجرائم حتى يتم الوصول إلى الأدلة والمجرمين ومعاقبتهم.

ويتناول هذا البحث موضوع أهمية التعاون الدولي في مواجهة الجرائم المعلوماتية؛ نظراً لأهمية مثل هذا التعاون في مكافحة مثل هذه الجرائم. وقد أوضحنا في المبحث الأول نظرة الدول إلى الجرائم المعلوماتية والصعوبات التي تواجه التعاون الدولي في مجال المكافحة، ثم بينا في المبحث الثاني مظاهر التعاون الدولي في مكافحة الجرائم المعلوماتية، ثم بينا في المبحث الثالث جهود الأمم المتحدة والاتفاقيات والمعاهدات والجهود الدولية الأخرى في مجال مكافحة الجرائم المعلوماتية.

المقدمة:

في ظل التطورات الكبيرة لتقنية المعلومات، ونظراً للعدد الهائل من الأفراد والمؤسسات الذين يستخدمون شبكة الإنترنت، فقد أصبح من السهولة بمكان استخدامها في ارتكاب الجرائم، فشبكة الإنترنت لا تعرف حدوداً جغرافية، ومستخدم الشبكة يمكنه التنقل بين دول العالم وهو موجود في منزله، ويترتب على هذه الطبيعة الدولية لشبكة الإنترنت أن الجرائم التي ترتكب باستخدامها تكون لها صفة الدولية، أي تكون جرائم عابرة للحدود. وقد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة واحدة يقع ضحيتها عدة أشخاص يقيمون في بلدان متعددة، كما يترتب عليها أيضاً أن الأدلة الرقمية التي يمكن تتبعها تكون ضعيفة أو من الممكن زوالها بشكل سريع، ولذا تستلزم اتخاذ إجراء سريع لحفظها من الزوال والتلف، فعندما ترتكب جريمة معلوماتية تستحق التحقيق فيها للوصول إلى مرتكبها، قد تظهر الحاجة إلى مساعدة السلطات في البلد الذي نشأت منه الجريمة أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط

المجرّم وهو في طريقه إلى الهدف، أو حيث توجد أدلة الجريمة. ومما يزيد من صعوبة المشكلة اختلاف التشريعات في الدول المختلفة في تأسيس اختصاصها الجنائي، مما قد يؤدي إلى تنازع الاختصاص بين الدول بالنسبة للجرائم المعلوماتية عابرة الحدود، فقد يحدث أن ترتكب جريمة في إقليم دولة معينة، ويكون مقترف هذه الجريمة أجنبياً، فتخضع هذه الجريمة لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكون الجريمة المرتكبة على إقليم الدولة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتخضع للاختصاص الجنائي الإقليمي من جهة، وتخضع لاختصاص الدولة المجنى عليه من جهة أخرى، استناداً لمبدأ الاختصاص العيني(١).

فالتحقيق والمحاكمة في الجرائم المعلوماتية يتطلبان توحيد التشريعات المختلفة وتوحيد القواعد المتعلقة بالإثبات باستخدام الأدلة الإلكترونية بين الدولة التي وقعت فيها الجريمة من ناحية، والدولة التي يقيم فيها المتهم، ولذلك لا بد من وجود تعاون دولي يتفق مع طبيعة الجرائم المعلوماتية، ولإتمام التحقيق والمحاكمة قد تكون هناك حاجة إلى مساعدة السلطات في البلد الذي كان منشأ الجريمة، أو من سلطات البلد أو البلدان التي عبر من خلالها النشاط المجرّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة. وهناك نوعان من المساعدة هما المساعدة الرسمية والمساعدة غير الرسمية. وقد تكون المساعدة غير الرسمية أسرع إنجازاً، وهي الوسيلة المثلى حين لا تكون هناك حاجة إلى صلاحيات إلزامية مثل أذون التفتيش أو طلبات تسليم المجرمين، وهي تعتمد على وجود علاقات عمل جيدة بين الأجهزة الأمنية للدول المعنية.

ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هي عملية أكثر تعقيداً يتم اللجوء إليها استناداً إلى معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية. وهي تشترط عادة أن تكون الجريمة المعنية على درجة من الجسامة، وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب، وهو ما يطلق عليه بالتجريم المزدوج (Dual Criminality)(٢).

---

(١) فتحي محمد عزت، الحماية الجنائية والموضوعية والإجرائية – الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، ٢٠٠٧م. ص ٤٠٧ وما بعدها.

(٢) خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩، ص ٣٩٣ وما بعدها. انظر أيضاً: يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة. ٢٠١١م. ص ١٤٠، وما بعدها. انظر أيضاً:
Donald Mason R, Sentencing Policy and Procedure As Applied to Cyber crime: A call for Reconsideration And Dialogue, Missippi Law Journal, winter 2007. At 12.

وبما أن التعاون الدولي هو الطريق الوحيد لمكافحة الجرائم المعلوماتية، فإن هذا التعاون يتطلب توحيد القوانين والتشريعات العقابية للبلدان المختلفة، لأن التباين بين تلك القوانين والتشريعات يؤدي في النهاية إلى استفادة الجناة بالإفلات من العقاب بسبب هذا التباين والاختلاف.

فملاحقة مرتكبي الجرائم المعلوماتية ومحاكمتهم وإيقاع العقوبة عليهم، يتطلب القيام بأعمال إجرائية استدلالية وتحقيقية خارج حدود الدولة التي ارتكبت فيها الجريمة أو جزء منها، مثل معاينة مواقع الإنترنت في الخارج أو ضبط الأقراص الصلبة التي توجد عليها معلومات أو بيانات غير مشروعة أو صور ذات طبيعة جنسية، أو القيام بسماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم المعلومات التي يمكن أن تساهم في تحقيق هذه الجرائم، وكل ذلك لا يتم بدون مساعدة الدول الأخرى، فمكافحة الجرائم المعلوماتية لا يمكن أن تتحقق بدون وجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المعلوماتية وتعميمها(٣).

ولكي تكون هناك مواجهة دولية فعالة للجرائم المعلوماتية يجب على الدول الدخول أطرافاً في اتفاقيات ومعاهدات دولية لتنظيم التعاون القضائي وتسليم المجرمين في الجرائم المعلوماتية، وإيجاد آليات لحل التنازع بين قوانين الدول المختلفة فيما يتعلق بالتحقيق ومحاكمة مرتكبي تلك الجرائم.

وفي ضوء ما تم ذكره، فقد أصبح من الضروري وجود تعاون دولي فعال في مكافحة الجرائم المعلوماتية، وعلى الرغم من أهمية هذا التعاون وهذه الجهود إلا أن هناك عدداً من العقبات والمشاكل التي تعيق تحقيقه.

ويهدف هذا البحث إلى تناول الجهود الدولية في مكافحة الجرائم المعلوماتية وأهمية التعاون الدولي في مكافحتها، وذلك باستعراض مظاهر التعاون الدولي في

(٣) فمثلاً في جرائم الإتلاف المعلوماتي قد يكون مرتكب جريمة نشر الفيروس يحمل جنسية معينة، ويشن الهجوم الفيروسي من أجهزة حاسب آلي موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة، فمن الطبيعي أن تقف مشاكل الحدود والاختصاص القضائي عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها. انظر: يوسف حسن يوسف، المرجع السابق. ص ١٤١ وما بعدها. انظر أيضاً: فتحي محمد عزت، المرجع السابق. ص ٤٠٩ وما بعدها. انظر أيضاً: خالد ممدوح إبراهيم، المرجع السابق. ص ٣٩٤ وما بعدها.

مكافحة هذه الجرائم والصعوبات التي تواجه مثل هذا النوع من التعاون واستعراض وتحليل جهود الأمم المتحدة والاتفاقيات والمعاهدات الدولية في مكافحة هذه الجرائم.

هدف البحث وأهميته:

يهدف هذا البحث إلى دراسة موضوع الجهود الدولية في مكافحة الجرائم المعلوماتية من حيث أهمية التعاون الدولي في مواجهة هذه الجرائم، والصعوبات التي تواجه مكافحتها، ومظاهر التعاون الدولي في مكافحتها، وصولاً إلى تبيين جهود الأمم المتحدة والاتفاقيات والمعاهدات والجهود الدولية الأخرى في مجال مكافحة الجرائم المعلوماتية. وتكمن أهمية البحث في مدى خطورة الجرائم المعلوماتية وكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي بين الدول، إذ أنه يستحيل على الدولة بمفردها القضاء على الجرائم العابرة للحدود، ولذلك فإن الحاجة ملحة إلى تعاون الدول والتنسيق فيما بينها لمطاردة المجرمين ومكافحة الجرائم المعلوماتية التي تتجاوز حدود الدولة الواحدة بمقتضى قواعد مستقاة من مبادئ القانون الدولي.

خطة البحث:

يشتمل هذا البحث على ثلاثة مباحث:

المبحث الأول: نظرة الدول إلى الجرائم المعلوماتية والصعوبات التي تواجه التعاون الدولي في مجال مكافحة هذه الجرائم.

المبحث الثالث: مظاهر التعاون الدولي في مكافحة الجرائم المعلوماتية.

المبحث الثالث: جهود الأمم المتحدة والاتفاقيات والمعاهدات والجهود الدولية الأخرى في مجال مكافحة الجرائم المعلوماتية.

منهج البحث:

يعتمد هذا البحث على المنهج التحليلي لنصوص الاتفاقيات والمعاهدات والقرارات والتوصيات الدولية في مجال مكافحة الجرائم المعلوماتية، مع الاعتماد على المراجع العلمية القانونية ذات العلاقة.

المبحث الأول
نظرة الدول إلى الجرائم المعلوماتية والصعوبات التي تواجه التعاون الدولي في مجال مكافحة هذه الجرائم

نظراً لاختلاف مواقف الدول في التعامل مع الجرائم المعلوماتية فسنتطرق في هذا المبحث إلى نظرة الدول إلى الجرائم المعلوماتية في المطلب الأول، ثم سنتطرق في المطلب الثاني إلى الصعوبات التي تواجه التعاون الدولي في مجال مكافحة هذه الجرائم.

المطلب الأول
نظرة الدول إلى الجرائم المعلوماتية

حتى يتحقق التعاون الدولي في مجال مكافحة الجرائم المعلوماتية يجب على الدول كافة أن تصدر قوانين على قدر من التناسق تجرم الجرائم المعلوماتية، وأن تقوم بصياغة قوانين جديدة قادرة على التعامل مع تلك الجرائم المستحدثة.

وقد تباينت مواقف الدول المختلفة في التعامل مع الجرائم المعلوماتية، فبينما توجد في بعض الدول نصوص قانونية قابلة للتطبيق على تلك الجرائم، نجد أن دولاً أخرى لا تتعامل تشريعاتها مع مثل هذه الجرائم، ويرجع ذلك بشكل أساسي إلى اختلاف تجارب تلك الدول مع الجرائم المعلوماتية، ويمكن بشكل عام التمييز بين اتجاهين رئيسيين في هذا الشأن:

الاتجاه الأول:

ينظر هذا الاتجاه إلى الجرائم المعلوماتية على أنها جرائم تقليدية لا تتميز بخصائص تميزها عن غيرها من الجرائم بحيث تتطلب نصوصاً جديدة وقوانين جديدة لمواجهتها(٤). وتأخذ غالبية الدول العربية بهذا الاتجاه، ففي غالبية الدول العربية لا توجد قوانين خاصة بالجرائم المعلوماتية، وإنما تتعامل مع هذه الجرائم بموجب نصوص القوانين التقليدية، والتي توفر بعض الحماية ضد الأفعال المماثلة، بحيث يمكن تطبيق النصوص القانونية التقليدية وتطويعها للتعامل مع الجرائم المعلوماتية، وعليه فإن وجد نص قانوني يعاقب على جريمة شبيهة بالجريمة المعلوماتية يتم إدراجها تحته وتتقرر العقوبة المنصوص عليها في ذلك النص، وعليه

(٤) نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، بيروت، ٢٠٠٥م. ص٤٠٦ وما بعدها. انظر أيضاً: ناصر محمد البقمي، فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية، مجلة البحوث الأمنية، المجلد ١٧، العدد ٤٠، أغسطس ٢٠٠٨. ص ١٢١ وما بعدها.

فإنه في غالبية الحالات لا تكون العقوبة المنصوص عليها في هذا النص القانوني متناسبة وحجم الخسائر الناتجة عن ارتكاب مثل هذه الجريمة المعلوماتية، ولأنه لا يوجد نص صريح خاص بها ويعاقب عليها ويفرض العقوبة المناسبة للأضرار الناتجة عن تلك الجريمة، فيتم إدراج تلك الجريمة المعلوماتية تحت هذا النص القانوني غير الخاص بها، والذي تم توصيفه للعقاب على جريمة أخرى، وبالتالي لا يكون العقاب المنصوص عليه مناسباً في هذه الحالة.

الاتجاه الثاني:

ينظر هذا الاتجاه إلى الجرائم المعلوماتية على أنها تتمتع بصفات تميزها عن غيرها من الجرائم. ويرى أيضاً ضرورة إصدار قوانين جديدة تتعامل مع الجرائم المعلوماتية، أو تعديل نصوص القوانين التقليدية بحيث تستطيع التعامل مع هذا النوع من الجرائم المستحدثة. وقد قامت الدول التي اتبعت هذا الاتجاه وهي غالبية الدول الصناعية والمملكة العربية السعودية والإمارات العربية المتحدة وغيرها من الدول بإصدار قوانين خاصة تعنى بجميع الأفعال التي ترتكب من خلال النظام المعلوماتي، أو التي تقع عليه، لمواجهة تلك الجرائم والحد من ارتكابها، كما قامت دول أخرى بتعديل قوانينها أو الإضافة إليها لذات الغرض(٥).

وأياً كان الاتجاه الذي تتبعه دول العالم فإنه لا بد من أن تكون القوانين المتعلقة بمكافحة الجرائم المعلوماتية على قدر من التناسق، بحيث تمكن تلك الدول من التنسيق والتعاون فيما بينها في مكافحة هذا النوع من الجرائم المستحدثة التي تتطلب قدراً كبيراً من التعاون بين الدول للتعامل معها، فلا بد أن تنص قوانين دول العالم كافة على جميع الأفعال المجرمة فيما يتعلق بالجرائم المعلوماتية بحيث لا تستثني أياً منها، وأن تقوم بتسليم الأدلة والمجرمين للدول المجنى عليها أو محاكمتهم بنفسها حتى لا يفلت المجرم من العقاب تحت ذريعة عدم النص على الفعل في النصوص القانونية، أو عدم إمكانية تسليمه للدولة الطالبة في حالة عدم محاكمته في الدولة التي يتواجد فيها(٦).

---

(٥) سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، ٢٠٠٧م. ص ٤٣١ وما بعدها. انظر أيضاً: ناصر البقمي، المرجع السابق، ص ١٢٠ وما بعدها.

(٦) انظر:
Doon Paker, Fighting Computer Crime,John Wiley Publishing, U.K, 1998, at 241.
انظر أيضاً:
Gina Angelis, Cyber Crmes, Chelsea House Publishers, New York, 2000. At 139.

المطلب الثاني
الصعوبات التي تواجه التعاون الدولي في مجال مكافحة الجرائم المعلوماتية

هناك بعض الصعوبات التي تعيق التعاون الدولي بكافة صوره في مجال مكافحة ومواجهة الجرائم المعلوماتية، ومن هذه الصعوبات ما يلي:

أولاً – عدم الاتفاق على مفهوم موحد للجرائم المعلوماتية :

ويعود ذلك إلى أن الأنظمة القانونية والتشريعات في دول العالم كافة لا تتفق على الأفعال المجرمة فيما يتعلق بالجرائم المعلوماتية، فبالنظر إلى قوانين الدول المختلفة والمتعلقة بمواجهة الجرائم المعلوماتية يتبين لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظام المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مشروعاً في أحد الأنظمة قد يكون مجرماً وغير مشروع في نظام آخر، ويمكن عزو ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والثقافات والديانات من مجتمع لآخر، إضافة إلى قصور التشريع ذاته في العديد من دول العالم وعدم مسايرته لسرعة التقدم المعلوماتي التقني ومن ثم الجرائم المعلوماتية(٧).

ثانياً – عدم وجود تعاون فيما يتعلق بالإجراءات الجنائية:

عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجرائم المعلوماتية بين الدول، وبشكل خاص ما يتعلق منها بأعمال الاستدلال والتحقيق، خاصة وأن عملية الحصول على دليل في مثل هذه الجرائم قد يتم خارج إقليم الدولة(٨).

ثالثاً – اختلاف النظم القانونية الإجرائية:

نظراً لتنوع واختلاف النظم القانونية الإجرائية، فإن طرق الاستدلال والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة

---

(٧) عبدالفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٧م. ص ١٨٨ وما بعدها. انظر أيضاً: حسين سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة) دار النهضة العربية، القاهرة، ٢٠٠٩م. ص ٦٩٠ وما بعدها.

(٨) خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق. ص ٤٠٨ وما بعدها. انظر أيضاً: عبدالفتاح حجازي، المرجع السابق. ص ١٩٨ وما بعدها.

أخرى، أو قد لا يسمح بإجرائها فيها، كما هو الوضع بالنسبة للمراقبة الإلكترونية (Electronic Monitoring)، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات المماثلة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق على أنها مشروعة في دولة ما، فقد تكون غير مشروعة في دولة أخرى.

رابعاً – مشكلة تنازع الاختصاص القضائي:

تثير جرائم المعلوماتية مسألة الاختصاص (Jurisdiction) على المستويين الوطني والدولي، ولا توجد مشكلة بالنسبة للاختصاص على المستوى الوطني حيث يتم الرجوع إلى القواعد المحددة قانوناً لذلك، ولكن المشكلة تثار فيما يتعلق بالاختصاص على المستوى الدولي حيث يوجد اختلاف بين الدول فيما يتعلق بجرائم المعلوماتية التي تتميز بكونها عابرة للحدود، فقد يحدث أن ترتكب الجريمة في إقليم دولة ما من قبل شخص أجنبي، ففي هذه الحالة تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الإقليمية، كما تخضع أيضاً لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي.

خامساً – عدم وجود قنوات للاتصال بين الدول:

يشكل عدم وجود قنوات اتصال (Communication Channels) بين الدول مشكلة تعيق التعاون الدولي في مكافحة الجريمة، ولتحقيق هذا الهدف يجب أن يكون هناك قنوات اتصال تسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات هامة(٩).

سادساً – تجريم ذات الفعل في التشريعات الوطنية:

يعد التجريم المزدوج (Dual Criminality) من أهم الشروط المتعلقة بنظام تسليم المجرمين، فهو منصوص عليه في غالبية التشريعات الوطنية والمعاهدات والاتفاقيات الدولية المتعلقة بتسليم المجرمين، وعلى الرغم من أهميته تلك، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة لجرائم المعلوماتية، لا سيما وأن بعض دول العالم لا تجرم كل هذه الجرائم، بالإضافة إلى أنه من الصعوبة أن

(٩) عبدالفتاح حجازي، المرجع السابق ص ١٨٩ وما بعدها. انظر أيضاً: حسين الغافري، المرجع السابق، ص ٦٩١ وما بعدها. انظر أيضاً: خالد إبراهيم، المرجع السابق، ص ٤١١ وما بعدها. انظر أيضاً:
John Nadelman, The Evolution of United States Involvement in the International Rendition of Fugitive Criminals, 25 N. Y. U. J. Int. L. L. 817 - 122. (1993).

نحدد فيما إذا كانت نصوص القوانين التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على جرائم المعلوماتية أم لا، وهو ما قد يعيق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المعلوماتية.

سابعاً – عدم وجود معاهدات ثنائية أو جماعية بين الدول:

عدم وجود معاهدات ثنائية أو جماعية (Bilateral Agreements) بين الدول على نحو يسمح بالتعاون الفعال في مكافحة الجرائم المعلوماتية، وحتى في حال وجودها فإن هذه المعاهدات قد لا تكون فعالة في توفير الحماية المطلوبة في ضوء التطور السريع للنظم والبرامج المعلوماتية(١٠).

(١٠) وقد حث مؤتمر الأمم المتحدة الثامن لمنع الجريمة والمجرمين – والذي تم عقده في هافانا بكوبا عام ١٩٩٠م – في قراره المتعلق بجرائم الحاسب الآلي، الدول الأعضاء على تكثيف جهودها في مكافحة إساءة استخدام الحاسب الآلي. كما حث القرار الدول الأعضاء على الدخول كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في مكافحة جرائم الحاسب الآلي، كما حث القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بشكل تام على جرائم الحاسب الآلي. ودعا القرار أيضاً إلى وضع معايير دولية لأمن المعالجة الآلية للبيانات، واتخاذ تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، كما دعا القرار الدول الأعضاء إلى الدخول في اتفاقيات دولية تنطوي على نصوص وأحكام تنظم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود، على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة مع ضرورة كفالة الحماية لحقوق الأفراد وحرياتهم واحترام سيادة الدول. كذلك فقد نص المجلس الأوروبي (Council of Europe) في توصيته رقم (٩٥/١٣) على أن إجراءات التحقيق في البيئة التقنية تقتضي التدخل السريع لمد الإجراءات إلى أنظمة حاسبات قد تكون موجودة خارج الدولة، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة يجب وضع قواعد قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك فثمة حاجة ملحة لاتفاقيات تنظم كيفية القيام بمثل هذه الإجراءات، كما يجب أن تتوافر إجراءات عاجلة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة، وهو ما يتطلب أن تسمح السلطات الأخيرة بإجراءات التفتيش والضبط. انظر: حسين سعيد الغافري، المرجع السابق. ص ٦٩٢ وما بعدها. انظر أيضاً: عبدالفتاح حجازي، المرجع السابق. ص ١٨٨ وما بعدها. انظر أيضاً:
Jack Brown, Jurisdiction to Prosecute Crimes. Committed by use of the Internet, 38 Jurimetrics J. 611, 1998.

المبحث الثاني
مظاهر التعاون الدولي في مكافحة الجرائم المعلوماتية

نظراً لأهمية تعاون الدول كافة في مكافحة الجرائم المعلوماتية والقبض على مرتكبيها، سنتطرق في هذا المبحث إلى مظاهر التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، حيث لا تستطيع أية دولة بمفردها النجاح في هذه المهمة دون تعاون الدول الأخرى.

المطلب الأول
التعاون الشرطي الدولي

لا يمكن مكافحة الجرائم المعلوماتية إلا بوجود تعاون دولي بين أجهزة الشرطة في دول العالم المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالحاسب الآلي والإنترنت وتعميمها.

فنتيجة للتطور الكبير في الاتصالات وتقنية المعلومات وظهور شبكة الإنترنت والانتشار الواسع والسريع لها وانتقال المجرمين من بلدٍ لآخر، فقد أدركت دول العالم بأنه يستحيل على دولة ما بمفردها القضاء على الجرائم عابرة الحدود، وبالتالي تظهر الحاجة لوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، ذلك أن الإجراءات العامة للشرطة في كل دولة لا تسمح لأجهزة الشرطة العاملة فيها بتعقب المجرمين ومتابعتهم متى ما تجاوزوا حدود الدولة، فمثلاً في جرائم الاختراق والإتلاف المعلوماتي قد يكون مرتكب الجريمة يحمل جنسية دولة ما، ويرتكب جريمته من حاسبات آلية موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة، فمن الطبيعي أن تقف مشاكل الحدود والاختصاص القضائي عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها. ولذلك فقد قطع التعاون الشرطي الدولي شوطاً طويلاً سواء على مستوى التعاون الثنائي أو المتعدد الأطراف إقليمياً أو دولياً، ومن أبرز الإنجازات على طريق هذا التعاون إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول) وظهور العديد من صور وأشكال ووسائل التعاون بين أجهزة الشرطة في دول العالم(١١).

(١١) يوسف حسن يوسف، المرجع السابق، ص ١٤١ وما بعدها. انظر أيضاً: سليمان أحمد فضل، المرجع السابق. ص ٤١٢ وما بعدها. انظر أيضاً:
Neal Kummar Katyal, Criminal Law in Cyber space, 149 U Pensyivania L. Review. At 1030 - 1035.

ومن أبرز هذه الصورة الوسائل ما يلي:

أولاً – تطوير وسائل الاتصال والمعلومات بين أجهزة الشرطة في الدول المختلفة:

يتم عادة استخدام القنوات الدبلوماسية (Diplomatic Channels) في إجراء الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة وبين مثيلاتها في الدول الأخرى، وبما أن الاتصالات الشرطية تحتاج إلى اتصالات خاصة سريعة، لذا فقد حاولت الدول المختلفة والمنظمة الدولية للشرطة الجنائية (الإنتربول) تطوير نظم اتصال خاصة لتبادل المعلومات فيما بينها.

ثانياً – الجهود المبذولة من المنظمة الدولية للشرطة الجنائية (الإنتربول):

تم إنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول) (Interpol) في مؤتمر دولي تم عقده في بروكسل ببلجيكا عام ١٩٤٦م لغرض تعزيز مبادئ التعاون الأمني بين دول العالم، وانتهى هذا المؤتمر بإنشاء جهاز المنظمة الدولية للشرطة الجنائية ونقل مقرها إلى مدينة ليون (Lyon) الفرنسية(١٢). ويبلغ عدد الدول الأعضاء في هذه المنظمة ١٨٩ دولة.

وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة، حيث تقوم بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها، وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، وتزويدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم العابرة للحدود ومنها جرائم الحاسب الآلي والإنترنت(١٣). فعضو الإنتربول لا يقوم بنفسه بإجراء القبض على المجرم، بل إن هذا العمل منوط بالشرطة الوطنية في الدولة التي يتواجد المجرم على إقليمها، الأمر الذي يؤكد على احترام السيادة الوطنية (National Sovereignty).

---

(١٢) جميل عبدالباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١م. ص ٧٦ وما بعدها.
انظر أيضاً: Interpol. at http:/en.wikipedia.org/ wiki/Interpol

(١٣) فالمنظمة الدولية للشرطة الجنائية (الإنتربول) ليست سلطة دولية عليا فوق الدول الأعضاء. فالتعاون الشرطي في نطاق هذه المنظمة يحكمه مبدأ احترام السيادة الوطنية للدول الأعضاء. انظر: جميل عبدالباقي الصغير، المرجع السابق. ص ٧٩. انظر أيضاً: حسين الغافري، المرجع السابق، ص ٦٣٨ وما بعدها.

ولذلك يجب تدعيم التعاون بين أجهزة الشرطة في الدول المختلفة بناء على اتفاقيات دولية. ولهذا التعاون أهميته بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أن جريمة معلوماتية ما قد تم ارتكابها باستخدام شبكة الإنترنت من خلال موقع على شبكة الإنترنت موجود في الخارج فإنها تقوم بالإبلاغ عن هذه الجريمة إلى سلطات الشرطة بالدولة التي ارتكبت منها الجريمة، ولذا يجب أن تعين كل دولة الجهة أو الإدارة المختصة بهذا النوع من القضايا لتلقي البلاغات واتخاذ الإجراءات المناسبة حسب قوانينها(١٤).

ومن الأمثلة على دور الإنتربول فيما يتعلق بجرائم الإنترنت ما حصل في دولة الإمارات العربية المتحدة عندما تم توقيف أحد الطلبة الجامعيين من قبل النيابة العامة في دبي بتهمة إرسال صور ذات طبيعة جنسية لأحد القصر من موقعه على شبكة الإنترنت، وذلك إثر تلقي النيابة العامة في دبي برقية من الإنتربول في بريطانيا بهذا الخصوص.

ثالثاً – الجهود المبذولة من جهاز الشرطة الأوروبية (Europol):

أنشئ جهاز الشرطة الأوروبية (Europol) في عام ١٩٩٢م بناء على معاهدة ماسترخت (Maastricht Treaty) وبدأ الجهاز عمله في عام ١٩٩٩م ويبلغ عدد موظفيه ٦٢٥ موظفاً، ويقع مقره في لاهاي بهولندا، وينسق هذا الجهاز مع أجهزة الشرطة حول العالم ومع المنظمات الدولية ذات العلاقة كالشرطة الدولية (الإنتربول).

ويغطي عمل جهاز الشرطة الأوروبية الدول الـ ٢٧ الأعضاء في الاتحاد الأوروبي (European Union) لمكافحة الجرائم العابرة للحدود ومنها جرائم الحاسب الآلي والإنترنت، وأصبح هذا الجهاز وكالة أوروبية كاملة (Full Eu Agency) في عام ٢٠١٠م مما أعطى هذا الجهاز صلاحيات واسعة في تجميع المعلومات والأدلة، ويقوم جهاز الشرطة الأوروبية بإقامة العديد من الدورات التدريبية المتعلقة بمكافحة الجريمة والتي يشارك فيها ممثلون عن الدول الأوروبية وغيرها(١٥).

---

(١٤) فمثلاً تختص الإدارة العامة للمعلومات والتوثيق - قسم جرائم الحاسب الآلي - بوزارة الداخلية المصرية بجرائم الحاسب الآلي والإنترنت والتحقيق فيها في مصر. انظر: جميل عبدالباقي الصغير، المرجع السابق، ص ٧٧.

(١٥) فمثلاً عقد جهاز الشرطة الأوروبية (Europol) دورته التدريبية الثانية عشرة في ١نوفمبر٢٠١١م وكان عنوانها مكافحة الاستغلال الجنسي للأطفال عبر شبكة الإنترنت. وكانت مدة هذه الدورة ثمانية أيام، وشارك فيها ٦٤ شخصاً يمثلون ١٩ دولة من دول الاتحاد الأوروبي و ٩ دول من غير دول الاتحاد الأوروبي هي (أستراليا، كندا، كرواتيا، =

كما يوجد توجه داخل الاتحاد الأوروبي لإنشاء وحدة أوروبية لمكافحة الجرائم المعلوماتية تهدف إلى زيادة التعاون الدولي لحماية الدول الأوروبية ومواطنيها من الجرائم المعلوماتية.

ففي اجتماع لوزراء الإتحاد الأوروبي الذي عقد في لوكسمبورغ في ٢٧ ابريل ٢٠١١م تم طرح عدد من التصورات والإستراتيجيات لمكافحة جرائم الحاسب الآلي والإنترنت في الدول الأوروبية. وأكدت هذه التصورات على أهمية حماية الأنظمة المعلوماتية في دول الإتحاد الأوروبي .(European Union) واتخاذ الإجراءات العاجلة والرد السريع في حالة حصول إنقطاعات (Disrupptions) لشبكة الإنترنت أو هجوم إلكتروني. وأيد الوزراء الأوروبيون إنشاء وحدة دائمة تعمل كمنسق ونقطة اتصال (Liaison) ليتمكن عن طريقها مستخدمي شبكة الإنترنت وضحايا الجرائم المعلوماتية والقطاع الخاص عموماً من تقديم شكاواهم في حالة حدوث أية تجاوزات أو جرائم بحقهم. وتكون مهمة هذه الوحدة جمع وتحديث أفضل الطرق والمعايير في أساليب التحقيق الإلكتروني المتبعة في الشرطة والقضاء في الدول الأوروبية وتقييم أساليب التحقيق المتبعة من قبل أجهزة الشرطة والقضاء في دول الإتحاد الأوروبي.

= أيسلندا، النرويج، صربيا، سويسرا، تركيا والولايات المتحدة الأمريكية) إضافة إلى الإنتربول، وتم عقد هذه الدورة في ألمانيا، وقام بتقديم وتنفيذ الدورة مدربون من جهاز الشرطة الأوروبية (Europol) إضافة إلى مدربين من بلجيكيا، اليونان، الدنمرك، إيطاليا، لوكسمبورغ، هولندا، البرتغال، إضافة إلى نيوزلندا، ويتمتع هؤلاء المدربون بمعرفة وخبرة واسعة في التحقيق ومكافحة الجرائم المعلوماتية، كما شارك مدربون من الإنتربول والمملكة المتحدة، وتساعد مثل هذه الدورات في تبادل الآراء والخبرات بين العاملين في مجال مكافحة الجرائم المعلوماتية مع أعضاء النيابة العامة والقضاة في الدول الأوروبية خاصة ودول العالم عامة، وتهدف أيضاً إلى زيادة الخبرات لدى القائمين بالتحقيق في هذه الجرائم. وبالإضافة إلى المحاضرات التي يتم تقديمها والمتعلقة بسيكولوجية مرتكب الجريمة وأحدث طرق وأساليب التحقيق في الجرائم المعلوماتية إضافة إلى التعاون الدولي، فإن هذه الدورة تساعد في توحيد معايير التحقيق لدى القائمين عليه، وتعطي فكرة جيدة لأعضاء النيابة العامة والقضاة عن الجرائم المعلوماتية، ومنذ بدء مثل هذه الدورات عام ٢٠٠٠م تم تدريب ما يزيد على ٥٠٠ رجل عدالة جنائية وقاضٍ من دول الاتحاد الأوروبي وغيرها من الدول. انظر: About Europol, 12th Europol training course at http: //www.europo.. Europa/news.

إضافة إلى أن هذه الوحدة سيعهد لها مهمة إعداد تقرير سنوي (Annual Report) عن الجرائم المعلوماتية في دول الاتحاد الأوروبي، وسيكون مقر هذه الوحدة في مقر الشرطة الأوروبية (Europol) في لاهاي بهولندا، وستكون من مهام هذه الوحدة تبادل المعلومات مع أجهزة الشرطة الأوروبية وغيرها عن مرتكبي هذه الجرائم والأساليب التي يستخدمونها في ارتكاب جرائمهم (Modus Operandi) ودعا الوزراء الأوروبيون أيضاً إلى تبني موقف مشترك في مكافحة الجرائم المعلوماتية(١٦).

رابعاً – التعاون عن طريق القيام بعمليات شرطية مشتركة:

وتعد هذه الصورة من التعاون الأمني من أهم الصور في مجال مكافحة الجرائم المعلوماتية خاصة وأن أجهزة العدالة الجنائية ليست بنفس المستوى والإعداد في جميع الدول وإنما يوجد تفاوت فيما بينها، فبعض الدول متقدمة تقنياً وبشرياً ولها باع كبير في مواجهة الجرائم المستحدثة ومنها الجرائم المعلوماتية، والبعض الآخر تفتقد ذلك، كما أن تتبع مرتكبي الجرائم المعلوماتية والتنقيب عن الأدلة الرقمية وضبطها والقيام بالتفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثاً عما قد تحويه من أدلة على ارتكاب جريمة معلوماتية(١٧). كلها أمور تتطلب القيام ببعض العمليات الشرطية والأمنية والتقنية المشتركة، وهو من شأنه أن يؤدي إلى زيادة الخبرات والمهارات للقائمين على مكافحة تلك الجرائم.

خامساً – مركز الشكاوى الخاصة بجرائم الإنترنت في العالم:

يعد مركز الشكاوى الخاصة بجرائم الإنترنت في العالم من أهم الأجهزة المخصصة لمكافحة جرائم الحاسب الآلي والإنترنت، فالنظام المعروف باسم (IC3) هو كناية عن نظام تبليغ وإحالة لشكاوى الأفراد في الولايات المتحدة الأمريكية والدول الأخرى في مكافحة جرائم الإنترنت، ويخدم هذا المركز وعبر تقديم شكوى ترسل عن طريق الإنترنت الأفراد والمؤسسات والأجهزة المختصة بمكافحة جرائم الإنترنت سواء الموجودة في الولايات المتحدة أو في الدول الأخرى، ويعمل في هذا المركز فريق من الموظفين والمحللين من المتخصصين في مجال الحاسب الآلي

---

(١٦) انظر: Cyber Crime Unit for Europe? The New New Internet. at http: // www. the newnewinternet.com.

(١٧) علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، إيتراك للنشر والتوزيع، القاهرة، ٢٠٠٠م، ص ١٧٤ وما بعدها، انظر أيضاً: حسين الغافري، المرجع السابق. ص ٦٣٥ وما بعدها.

وشبكة الإنترنت. ويقوم هؤلاء بتلقي الشكاوى المتعلقة بجرائم الإنترنت من الأشخاص المجنى عليهم، ثم يقومون بالبحث في الشكاوى وإعداد ملفها وإحالتها إلى وكالات تطبيق القوانين الفيدرالية والمحلية الأمريكية وإلى أجهزة تطبيق القوانين الدولية كالإنتربول وغيرها من الوكالات التنظيمية وفرق العمل (Task Forces) التي تشارك فيها عدة وكالات، للقيام بالتحقيق فيها(١٨).

ويستطيع الأشخاص من كافة دول العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بجرائم الإنترنت، ويطلب الموقع اسم الشخص المجني عليه أو المبلغ وعنوانه البريدي ورقم هاتفه، إضافة إلى اسم وعنوان ورقم هاتف والعنوان الإلكتروني، إذا كان متوافراً للشخص أو الجهة المشتبه بقيامهما بنشاط إجرامي، إضافة إلى تفاصيل تتعلق بكيفية حدوث الجريمة حسب ما يورده مقدم الشكوى ووقت حدوثها وسبب اعتقاده بحدوثها، إضافة إلى أية معلومات أخرى تدعم الشكوى(١٩).

المطلب الثاني
التعاون القضائي الدولي

يقتضي التعاون الدولي لغرض مكافحة الجرائم المعلوماتية من كل دولة أن تقوم بالتوفيق بين ممارستها لاختصاصها الجنائي على إقليمها، وتوقيع العقوبة على الجاني وبين ضرورات التعاون مع الدول الأخرى التي قد تتضرر من ارتكاب الجرائم المعلوماتية.

وللتعاون القضائي الدولي صور عديدة فيما يتعلق بالجرائم المعلوماتية التي تتعدى آثارها عدة دول، وبالتالي فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقوبة عليهم يتطلب اتخاذ إجراءات خارج إقليم الدولة التي ارتكبت فيها الجريمة أو جزء منها، مثل معاينة مواقع الإنترنت خارج إقليم الدولة أو ضبط الأقراص الصلبة (Hard Drives) التي توجد عليها معلومات تمت سرقتها أو اختراقها أو صور ذات طبيعة جنسية، أو تفتيش الوحدات الطرفية في حال الاتصال عن بعد، أو سماع الشهود أو القبض على المتهمين، أو اللجوء إلى الندب القضائي، أو تقديم المعلومات والأدلة التي يمكن أن تساهم في تحقيق هذه الجرائم، وكل هذا لا يتحقق

(١٨) انظر: موقع المركز على شبكة الإنترنت http://www.ic3.gov
انظر أيضاً: عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، ٢٠٠٧م. ص ١١٥ وما بعدها.

(١٩) انظر: http://www.ic3.gov.

بدون تعاون الدول الأخرى ومساعدتها عن طريق عقد الاتفاقيات بهدف تحقيق السرعة والفاعلية في إجراءات ملاحقة وعقاب مرتكبي هذه الجرائم.

وتعرف المساعدة القضائية الدولية بأنها "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"(٢٠).

والمساعدة القضائية لاتتحقق إلا بواسطة خطوات ثلاث هي:

١ – الطلب: ويتم تقديمه من الدولة صاحبة الاختصاص الجنائي بالمحاكمة، ويخضع هذا الطلب لقانون الدولة الطالبة وضمن نطاق الاتفاقية التي تعقدها مع الدولة التي ستقدم المساعدة، ويتم تقديم الطلب بالطرق الدبلوماسية بحسب الأصل، ومع ذلك فإن بعض الاتفاقيات الدولية تسمح بالاتصال المباشر بين جهات العدل في الدولتين اختصاراً للوقت.

٢ – فحص الطلب: وتقوم به الدولة التي يطلب منها تقديم المساعدة، ويتم ذلك عن طريق التحقق من اعتبار الواقعة المطلوب التحقيق فيها تعد جريمة وفقاً لقوانين الدولة مقدمة الطلب، وفي ضوء مدى اختصاص الدولة المطلوب منها بإجابة هذا الطلب وفقاً لنصوص الاتفاقية التي تعقدها مع الدولة الطالبة.

٣ – القيام بالمساعدة القضائية: ويتم وفقاً لقواعد الدولة المقدم إليها الطلب، فالإجراء يتم وفقاً لقوانين الدولة التي تقوم به(٢١).

وتتخذ المساعدة القضائية في المجال الجنائي صور عدة منها:

أولاً – تبادل المعلومات (Exchange of Information):

وهو يشمل تقديم المعلومات والبيانات والوثائق والأدلة التي تطلبها سلطة قضائية أجنبية بصدد جريمة معينة عن الاتهامات التي وجهت إلى أحد رعاياها في الخارج والإجراءات التي تم اتخاذها ضده، وقد يشمل التبادل السوابق القضائية للجاني، ومن خلالها تتعرف الجهات القضائي بدقة على الماضي الجنائي للمتهم المطلوب تسليمه، وهي تساعد في تقرير الأحكام الخاصة بالعود، وعدم الأهلية ووقف تنفيذ العقوبة.

---

(٢٠) خالد ممدوح إبراهيم، المرجع السابق، ص ٤٠ وما بعدها. انظر أيضاً: فتحي محمد عزت، المرجع السابق، ص ٤٠٧ وما بعدها.

(٢١) خالد ممدوح إبراهيم، المرجع السابق، ص ٤٠٥ وما بعدها. انظر أيضاً: سليمان أحمد فضل، المرجع السابق، ص ٤٢٠ وما بعدها.

وقد تم إيراد تلك الصورة من صور المساعدة القضائية الدولية في المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[٢٢]. كما تم إيرادها أيضاً في المادة الرابعة من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي[٢٣]. وذات الصورة نجدها أيضاً في المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي[٢٤]، والمادتين الأولى والثانية من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي[٢٥].

ثانياً – نقل الإجراءات (Transfer of Proceedings):

ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، وذلك في حالة توافر شروط معينة من أهمها أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات. بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة. وأيضاً يجب أن تكون الإجراءات المطلوب اتخاذها تؤدي إلى الوصول إلى الحقيقة، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب إليها، كما يجوز للدولة المطلوب إليها أن ترفض نقل الإجراءات في الحالات الآتية:

أ – إذا كان طلب نقل الإجراءات ليس له ما يبرره، كأن تكون الأسباب التي ذكرتها الدولة الطالبة لا تدعو لاتخاذ مثل هذه الإجراءات.

ب – إذا ثبت أن الدافع وراء طلب نقل الإجراءات اعتبارات سياسية أو دينية عنصرية.

---

(٢٢) صدرت هذه المعاهدة في ١٤/١٢/١٩٩٠م في الجلسة العامة (٦٨) للجمعية العامة للأمم المتحدة، وتقضي باتفاق أطرافها على أن يقدم كل طرف أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات وإجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلاً في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة.

(٢٣) صدرت هذه المعاهدة في عام ١٩٩٩م من قبل مؤتمر وزراء خارجية دول المنظمة في اجتماعهم الذي انعقد في أواغا دوغو في عام ١٩٩٩م.

(٢٤) صدرت هذه الاتفاقية في ٦/٤/١٩٩٣م بمدينة الرياض بالمملكة العربية السعودية.

(٢٥) تم اعتماد هذا النموذج من المجلس الأعلى لمجلس التعاون الخليجي في دورته الرابعة والتي انعقدت في دولة الكويت في الفترة من ٢١-٢٢/١٢/٢٠٠٣م. انظر: سليمان أحمد فضل، المرجع السابق. ص ٤٢٢ وما بعدها. انظر أيضاً: حسين سعيد الغافري، المرجع السابق. ص ٦٤٢ وما بعدها.

ج – إذا كانت الدولة المطلوب إليها قد طبقت قوانينها على الجريمة قبل استلامها من الدولة الطالبة، وكان الإجراء الذي سبق اتخاذه مطابقاً للقانون(٢٦).

د – إذا كانت الإجراءات التي تطلبها الدولة الطالبة مخالفة لواجبات تلتزم بها الدولة المطلوب إليها.

هـ – إذا كانت الإجراءات المطلوبة مخالفة لقوانين الدولة المطلوب إليها(٢٧).

ثالثاً – الإنابة القضائية الدولية:

ويقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على الجهات القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها، وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على مشكلة السيادة (Sovereignty) التي تمنع الدولة الأجنبية من ممارسة بعض الإجراءات القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو استجواب المتهمين أو إجراء التفتيش وغيرها.

وتتطلب الإنابة القضائية الدولية إرسال الملف الخاص بالدعوى الجنائية بمرفقاته من مستندات ووثائق ومحاضر التحقيق التي تم إجرائها من قبل السلطة القضائية في الدولة المطلوب فيها اتخاذ بعض إجراءات التحقيق.

وعادة ما يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية، فمثلاً طلب

---

(٢٦) خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص ٤٠٦ وما بعدها. انظر أيضاً: سليمان أحمد فضل، المرجع السابق، ص ٤٢١ وما بعدها. انظر أيضاً:
Terrence Berg, State Criminal Jurisdiction in Cyber Space, Is There A Sheriff on The Electronic Frontier? 79 Mich. B.J.670- 675 (2000).

(٢٧) ومن التطبيقات العملية للمساعدة القضائية قيام المجلس الأوروبي (Council of Europe) بإقرار اتفاقية نقل الإجراءات الجنائية التي تعطي للأطراف المنضمة خيار محاكمة الجاني طبقاً لقوانينها، بناء على طلب دولة أخرى طرف في هذه الاتفاقية، بشرط أن يكون معاقباً عليه في الدولتين. كما أقر المجلس الأوروبي في ١١ سبتمبر عام ١٩٩٥م التوصية رقم ٩٥/١٣ المتعلقة بمشاكل الإجراءات الجنائية المرتبطة بتقنية المعلومات. وقد حثت هذه التوصية الدول الأعضاء على مراجعة قوانين الإجراءات الجنائية على ضوء المبادئ التي وضعتها وهي: ١- تفتيش الأنظمة المعلوماتية وضبط البيانات. ٢- الرقابة الفنية التقنية من أجل التحقيق الجنائي ٣- الالتزام بالتعاون مع سلطات التحقيق. ٤- الإجراءات والوسائل التقنية والفنية لمعالجة الدليل الإلكتروني. انظر أيضاً: سليمان أحمد فضل، المرجع السابق، ص ٤٢٢ وما بعدها.

الحصول على دليل إثبات وهو عادة من شأن النيابة تقوم بتوثيقه المحكمة المختصة في الدولة الطالبة، ثم يرسل بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب، وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات(٢٨).

إلا أن مرور إجراءات التعاون القضائي الدولي بالطرق الدبلوماسية يجعلها تتسم بالبطء وكثرة الشكليات، وهو ما يتعارض مع طبيعة شبكة الإنترنت التي تتميز بسرعة مرور وتبادل المعلومات، ولذلك فإن مكافحة جرائم المعلوماتية تتطلب تعاملاً سريعاً تجنباً لاحتمالية التلاعب في البيانات التي قد تشكل دليلاً ضد المتهم(٢٩).

وتتضمن الاتفاقيات شروط وأساليب تنفيذ الإنابة القضائية، وعادة ما تتضمن شرطاً باستبعاد تنفيذ الأحكام في الجرائم السياسية والضريبية والعسكرية، أو إذا قدرت الدولة المطلوب منها أن التنفيذ المطلوب من شأنه المساس بسيادة الدولة، أو النظام العام أو المصالح الأساسية، الأمر الذي يسمح للدولة بإعمال سلطتها التقديرية لتنفيذ أو عدم تنفيذ ما يطلب منها، وبالمقابل فإنه في ظل عدم وجود اتفاقية فإن

(٢٨) وقد نص البند الثاني من المادة (٣٠) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام ١٩٩٩م والمادة (١٩) من اتفاقية الرياض العربية للتعاون القضائي لعام ١٩٨٣م، والمادة (٥٣) من اتفاقية شينجن لعام ١٩٩٠م والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف، والفقرة (١٣) من المادة (٤٦) من اتفاقية الأمم المتحدة لمكافحة الفساد على ضرورة وجود تعاون بين السلطات القضائية للدول في مكافحة الجريمة. انظر: خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق. ص ٤٠٧ وما بعدها. انظر أيضاً: حسين سعيد الغافري، المرجع السابق. ص ٦٤٦ وما بعدها. انظر أيضاً: عفيفي كامل عفيفي، جرائم الكمبيوتر، بدون ناشر، بدون تاريخ. ص ٤٢٢ وما بعدها.

(٢٩) ومن أمثلة الاتفاقيات التي تبرم في مجال الإنابة القضائية تلك التي أبرمتها فرنسا مع ألمانيا في أكتوبر عام ١٩٧٤م، ومع مصر في ١٥ مارس عام ١٩٨٢م، ومع الجزائر في ٢٨ أغسطس عام ١٩٦٢م، والاتفاقية الأوروبية للتعاون القضائي في المواد الجنائية عام ١٩٦٢م. وكذلك الاتفاقية المبرمة بين دول الجامعة العربية في ٩ يونيو لعام ١٩٥٣م، والاتفاقية الخاصة بالتعاون القضائي في المواد الجنائية مع المملكة المغربية في ٤ يونيو ١٩٨٩م، وكذلك اتفاقية بودابست لمكافحة الجرائم المعلوماتية والتي أكدت على ضرورة التعاون الدولي القضائي وتقديم المساعدة القضائية بين الدول الأعضاء. انظر: خالد ممدوح إبراهيم، المرجع السابق. ص ٤٠٨ وما بعدها. انظر أيضاً: سليمان أحمد فضل، المرجع السابق. ص ٤٢٣ وما بعدها.

الإنابة القضائية لا يمكن تنفيذها إلا إذا وافقت الدولة المطلوب إليها ذلك، وفقاً للإجراءات والشروط المنصوص عليها في قانونها الداخلي(٣٠).

المطلب الثالث
التعاون الدولي في مجال تسليم المجرمين

يعد تسليم المجرمين شكلاً من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين حتى لا يبقى هؤلاء المجرمون بمنأى عن العقاب على جرائمهم التي ارتكبوها، فإمكانية ارتكاب الجرائم المعلوماتية من خلال وحدة طرفية في دولة أجنبية أدت إلى ابتعاد المجرمين عن سلطات الدولة المتضررة من الجريمة وإفلاتهم من العقاب في أحيان كثيرة، ولضمان توقيع العقاب على مرتكبي هذه الجرائم، فقد قامت العديد من دول العالم بإبرام اتفاقيات فيما بينها بشأن تسليم المجرمين في الجرائم المعلوماتية، تهدف إلى قيام الدولة المطلوب إليها بتسليم أحد الأشخاص المتواجدين على إقليمها إلى الدولة الطالبة لمحاكمته أو تنفيذ عقوبة قضت بها عليه إحدى محاكمها(٣١).

ويعد هذا النوع من التعاون الدولي نتيجة طبيعية للتطورات التي تمت في مجال الاتصالات وتقنية المعلومات، حيث لم تعد الحدود الجغرافية بين الدول تشكل حاجزاً أمام مرتكبي الجرائم، كما أن نشاطهم الإجرامي لم يعد مقتصراً على دولة معينة بل امتد إلى أكثر من دولة، وحيث إن أجهزة الشرطة لا تستطيع تجاوز حدودها الإقليمية لتعقب المجرمين، فكان لا بد من إيجاد آلية للتعاون مع الدولة التي يوجد المتهم على أراضيها(٣٢). ولكي يتم ذلك ويكون هناك تعاون دولي فعال في مجال تحقيق العدالة كان ضرورياً تنظيم هذا النوع من التعاون الدولي من الناحية التشريعية والقضائية والتنفيذية، فالدولة ما دامت عضواً في المجتمع الدولي لا بد لها من الإيفاء بالالتزامات

---

(٣٠) فتحي محمد عزت، المرجع السابق. ص ٤١٠ وما بعدها. انظر أيضاً: سليمان أحمد فضل، المرجع السابق. ص ٤٢٥ وما بعدها.
انظر أيضاً:
Nick Nykodym and Robert Taylor, The Worlds Current Legislative efforts Against Cyber Crime, Computer Law and Security Report, Volume 20, Issue No. 5, September, 2004.

(٣١) سليمان أحمد فضل، المرجع السابق. ص ٤٣٨ وما بعدها. انظر أيضاً: حسين الغافري، المرجع السابق. ص ٤٣٩ وما بعدها.

(٣٢) سليمان أحمد فضل، المرجع السابق. ص ٤٣٩ وما بعدها.

الناشئة عن هذه العضوية ومن ضمنها الارتباط بعلاقات دولية وثنائية تتعلق بتسليم المجرمين، ويقوم مبدأ تسليم المجرمين على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم عابرة الحدود مثل جرائم الحاسب والإنترنت عليها أن تقوم بمحاكمته، إذا كان تشريعها يسمح بذلك، وإلا عليها أن تقوم بتسليمه لدولة أخرى تطلب محاكمته، أو لتنفيذ حكم صادر ضده بعقوبة في جريمة جنائية. ويشترط لتسليم المجرم أن يكون الفعل المطلوب التسليم من أجله مجرّماً في تشريع الدولة طالبة التسليم، ومجرّماً كذلك في تشريع الدولة المطلوب إليها التسليم، فمن غير الجائز مطالبة الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب فعل ما هو في الأساس غير مجرّم وفقاً لقانونها الوطني(٣٣).

وبالإضافة إلى ما سبق فإنه يوجد نوع آخر من مظاهر التعاون الدولي في مجال تسليم المجرمين يتمثل في الاعتراف المتبادل بأوامر القبض أو الحبس أو التوقيف. وبمقتضاه تصدر السلطة المختصة بإحدى الدول أمراً بالقبض أو الحبس أو التوقيف، وتعترف بصلاحيته الدول الأخرى، ويتعين عليها تنفيذه، وبالإضافة إلى ذلك فإنه يجب

(٣٣) ففي إحدى القضايا تمكن شاب فرنسي في عام ٢٠٠٦م من اختراق أحد البنوك الأمريكية. فباستخدام حاسبه الآلي الموجود في فرنسا، تمكن هذا الشاب من الاختراق غير المشروع لوحدات خدمة الحاسب الآلي لذلك البنك في الولايات المتحدة، كما قام بالاشتراك مع عدد من المتواطئين لفتح حسابات بنكية في أنحاء مختلفة من العالم، ثم قام بإصدار تعليمات إلى حاسب البنك الأمريكي بتحويل أموال إلى تلك الحسابات، وعند اكتشاف المخطط وتحديد هوية المتهم، صدر بحقه مذكرة اعتقال (Arrest Warrant) من محكمة نيويورك الفدرالية في الولايات المتحدة، ولم تكن هناك معاهدة لتسليم المجرمين بين فرنسا والولايات المتحدة. ولكن عند قيام المتهم بزيارة عمل لبريطانيا تم القبض عليه من السلطات البريطانية التي قامت بتسليمه إلى الولايات المتحدة لمواجهة التهم القائمة ضده، فوفقاً لمعاهدة تسليم المجرمين النافذة بين المملكة المتحدة والولايات المتحدة، يمكن للسلطات البريطانية تقديم المساعدة ما دامت الجريمة موضع الاتهام لها ما يقابلها في قوانين المملكة المتحدة، وطلب المتهم أن تنظر المحكمة في قانونية توقيفه للطعن في تسليمه، وأورد دفوعاً منها أن أمر تحويل الأموال قد صدر في فرنسا حيث يوجد حاسبه الآلي وليس في الولايات المتحدة الأمريكية، وقررت المحكمة أن وجود المتهم في باريس هو أقل أهمية من كونه باشر عملياته على أقراص ممغنطة موجودة في الولايات المتحدة، إضافة إلى أن التهم الموجهة للمتهم لها مقابلها الواضح في قانون إساءة استعمال الحاسبات الآلية الإنجليزي لعام ٢٠٠١م، ولو ارتكب هذا المتهم أفعاله من المملكة المتحدة بدلاً من فرنسا لانعقد الاختصاص القضائي للمحاكم الإنجليزية، وقد تم تسليم المتهم إلى الولايات المتحدة حيث تمت إدانته وحكم عليه بالسجن لمدة خمس سنوات. انظر: جريدة الرياض، ٢٢ نوفمبر ٢٠٠٨م، العدد ١٤٧٢٩. ص٤٥.

عند تسليم المتهم محل التسليم تسليم كل ما كان في حوزته أثناء القبض عليه، وكل ما يمكن أن يكون دليلاً على الجريمة(٣٤).

المطلب الرابع
التعاون الدولي في مجال التدريب على مواجهة الجرائم المعلوماتية

تبرز الحاجة إلى وجود تعاون بين الدول في مجال التدريب على مواجهة جرائم المعلوماتية، حيث إن التقدم المستمر والسريع في تقنية الحاسب الآلي والإنترنت يفرض على جهات العدالة أن تكون مواكبة لهذه التطورات السريعة التي تشهدها هذه التقنية، والإلمام بها حتى تستطيع أن تتصدى للأفعال الإجرامية التي صاحبت هذه التقنية ومواجهتها. إضافة إلى أن تطبيق القانون في مواجهة جرائم المعلوماتية يتطلب اتخاذ إجراءات قد تتجاوز ما هو منصوص عليه في قوانين العقوبات التقليدية، لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها والقدرة على محو آثارها(٣٥). وحتى تتمكن أجهزة العدالة من رجال ضبط جنائي ومحققين ومدعين وقضاة من مكافحة هذا النوع المستحدث من الجرائم لا بد من أن تتمتع هذه الأجهزة بقدر كبير من الخبرة والكفاءة والمعرفة والقدرة على كشف غموض هذه الجرائم والتعرف على مرتكبيها بسرعة ودقة كبيرتين. وهذا لن يتم إلا

---

(٣٤) سليمان أحمد فضل، المرجع السابق. ص ٤٤٠. انظر أيضاً: حسين الغافري، المرجع السابق. ص٦٥١ وما بعدها.

(٣٥) فقد ثبت في حالات متعددة أن هناك جرائم متعلقة بالحاسب الآلي وشبكة الإنترنت قد ارتكبت على مرأى ومسمع من رجال الشرطة، بل قام بعض رجال الشرطة بتقديم يد المساعدة لمرتكبي هذه الجرائم دون قصد منهم، مثلما حدث حينما طلبت إحدى دوائر الشرطة بمدينة سياتل الأمريكية من إحدى الشركات التي تعرض نظامها المعلوماتي للاختراق أن تقوم بوقف تشغيل هذا النظام المعلوماتي لتتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة، ونتيجة لذلك أتلف ما كان قد سلم من البرامج والملفات، وقد يقع إتلاف الأدلة أيضاً عن خطأ مشترك بين الخبراء وبين الجهة المجني عليها، فمثلاً في تحقيق إحدى جرائم المعلوماتية والتي تتمثل وقائعها حول زعم أحد الأشخاص لإحدى الشركات بأنه قام بوضع قنبلة منطقية (Logical Bomb) بالنظام المعلوماتي الخاص بها، فقامت الشركة وقبل إبلاغ السلطات المختصة باستدعاء خبير للتحقق من صحة هذا الزعم وإبطال مفعول هذه القنبلة في حالة وجودها، وبالفعل نجح هذا الخبير في اكتشاف القنبلة وإزالتها من النظام المعلوماتي العائد للشركة، وعندما تولت الشرطة التحقيق تبين أنه بإزالة القنبلة المنطقية من قبل الخبير أتلفت كل الأدلة المتعلقة بها. انظر: هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م. ص ٤٣٩ وما بعدها.

بالتدريب المستمر. ومن هنا كانت أهمية التدريب ووجوب تأهيل العاملين بهذه الأجهزة. وفي المقام نفسه فإنه لا يمكن لدولة ما أن تنجح في مكافحة مثل هذا النوع من الجرائم دون تعاون وتنسيق مع غيرها من الدول فيما يسمى بالتدريب المشترك(٣٦). فتدريب الكوادر البشرية القائمة على تطبيق القانون ليس بذات المستوى في كل الدول وإنما يختلف من دولة لأخرى بحسب تقدم الدولة وإمكاناتها المادية والبشرية. ولو نظرنا إلى العديد من الاتفاقيات الدولية والإقليمية لوجدنا أنها دعت إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينها(٣٧).

والتعاون الدولي في مجال تدريب العاملين في مجال العدالة الجنائية على مواجهة الجرائم المتعلقة بالجرائم المعلوماتية قد يكون بين الدول وأجهزة العدالة الجنائية لديها. فعلى سبيل المثال يوجد تنسيق بين المعاهد القضائية العربية لتوفير التدريب والتأهيل للقضاة العرب والعاملين في المحاكم في الدول العربية(٣٨). كما نجد أن العديد من الدول تقوم بعقد العديد من المؤتمرات والندوات وحلقات النقاش، إضافة إلى قيام العديد من الدول بإرسال أعضاء النيابة العامة التابعين لها في برامج تدريبية خارجية بالتعاون مع أجهزة النيابة العامة في الدول الأخرى والهيئات والمنظمات الدولية بهدف الاطلاع على أحدث الدورات والحلقات التدريبية، وقد يتم ذلك من خلال عقد ندوات ومؤتمرات أو ورش عمل جماعي متخصصة في مواجهة تلك الجرائم تعقد على المستوى الدولي أو الإقليمي(٣٩). حيث يتم في مثل هذه الفعاليات العلمية والتدريبية ومن خلال الأبحاث والدراسات والموضوعات المطروحة فيها الاطلاع على أحدث المستجدات المتعلقة بجرائم الحاسب الآلي والإنترنت من خلال مناقشة وتحليل

---

(٣٦) ومثال ذلك التوصية الصادرة من اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية بدول مجلس التعاون بالمملكة العربية السعودية في الفترة من ٤-٥/٤/٢٠٠٤م. والبند (د) من القرار الصادر بشأن الجرائم ذات الصلة بالحاسب الآلي من مؤتمر الأمم المتحدة لمنع الجريمة ومعامل السجناء المنعقد في هافانا عام ١٩٩١م.

(٣٧) انظر مثلاً: المادة (٢٩) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠م. والمادة (٩) من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

(٣٨) وقد نتج عن تلك الاجتماعات الاتفاق على إعداد مشروع اتفاقية للتعاون بين المعاهد القضائية العربية تسمى اتفاقية عمّان للتعاون العلمي بين المعاهد القضائية العربية والتي تم التوقيع عليها في ٩ ابريل لعام ١٩٩٧م. انظر: خالد ممدوح إبراهيم، المرجع السابق. ص ٤١٠ وما بعدها. انظر أيضاً: حسين الغافري، المرجع السابق. ص ٦٧٥ وما بعدها.

(٣٩) ومن أمثلة ذلك المؤتمر الدولي لقانون الإنترنت والذي تم عقده في مدينة الغردقة بجمهورية مصر العربية في الفترة من ٢١- ٢٠٠٥/٨/٢٥م والذي تم تنظيمه من قبل المنظمة العربية للتنمية الإدارية.

أبعادها؛ مما يمكن العاملين في مجال مكافحتها من التعرف على أحدث الوسائل والأساليب المستخدمة في مكافحة تلك الجرائم، كما يتم في مثل تلك الفعاليات من مؤتمرات وندوات وورش عمل تبادل الآراء والخبرات بين العاملين في مجال مكافحة الجرائم المعلوماتية(٤٠).

(٤٠) فعلى سبيل المثال تحرص الولايات المتحدة الأمريكية على توفير المساعدة التقنية والتدريب لرفع قدرات أجهزة العدالة الجنائية لدى الدول الأخرى، ومساعدة أجهزة الشرطة، والإدعاء العام، والقضاة في تلك الدول ليصبحوا أكثر فاعلية في مكافحة الجرائم المعلوماتية. ومثل هذه المساعدة لا تؤدي إلى بناء إطار للتعاون في مجال تطبيق القانون فحسب، بل تؤدي أيضاً إلى تعزيز قدرة تلك الدول على مكافحة الجرائم المعلوماتية، فمكتب المساعدة والتدريب على تطوير أجهزة الإدعاء العام في الدول الأخرى، التابع لوزارة العدل الأمريكية (Ministry of Justice) مكلف تحديداً بتوفير المساعدة اللازمة لتعزيز وتدعيم أجهزة العدالة الجنائية (Criminal Justice) في الدول الأخرى وتعزيز إدارة القضاء في الخارج. سليمان فضل المرجع السابق. ص ٤٤٢. انظر أيضاً:
Scot charney, computer Crime, 45 Emory L. J. 941-950 (1996).
انظر أيضاً: حسين الغافري، المرجع السابق. ص ٦٨٥ وما بعدها.

المبحث الثالث
جهود هيئة الأمم المتحدة والاتفاقيات والمعاهدات والجهود الدولية الأخرى في مجال مكافحة جرائم المعلوماتية

سنبين في هذا المبحث جهود هيئة الأمم المتحدة والاتفاقيات والمعاهدات الدولية والجهود الدولية الأخرى في مجال مكافحة الجرائم المعلوماتية.

المطلب الأول
جهود هيئة الأمم المتحدة (United Nations) في مجال مكافحة الجرائم المعلوماتية

أكدت جميع المؤتمرات التي عقدتها الأمم المتحدة والمتعلقة بمنع الجريمة والعدالة الجنائية على أهمية التعاون الدولي في مكافحة الجريمة، إذ صدر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين والمنعقد في فيينا في عام ٢٠٠٠م التركيز على مواجهة الجريمة.

حيث ورد في الإعلان الصادر عن هذا المؤتمر "نحن الدول الأعضاء في الأمم المتحدة، إذ يساورنا القلق إزاء الأثر الذي يتركه ارتكاب جرائم خطيرة ذات طبيعة عالمية على مجتمعاتنا، واقتناعاً منا بضرورة التعاون الثنائي والإقليمي والدولي في مجال منع الجريمة والعدالة الجنائية، وإذ يساورنا القلق بشكل خاص إزاء الجريمة المنظمة عبر الوطنية والارتباطات بين مختلف أشكالها، واقتناعاً منا بأن وجود برامج مناسبة للوقاية وإعادة التأهيل يشكل ضرورة أساسية لأي إستراتيجية فعالة لمكافحة الجريمة، وبأنه ينبغي لتلك البرامج أن تأخذ بالاعتبار العوامل الاجتماعية والاقتصادية التي تجعل الأشخاص أكثر عرضة للانخراط في السلوك الإجرامي (Criminal Conduct)[٤١].

كما برز اهتمام هيئة الأمم المتحدة بالجرائم المعلوماتية من خلال ما دعت إليه الجمعية العامة للأمم المتحدة (General Assembly) بخصوص التطورات في مجال المعلومات والاتصالات، حيث دعت الدول الأعضاء بضرورة إبلاغ الأمين العام للأمم المتحدة بأدائها وتقييماتها بشأن ما يلي:

(٤١) انظر: قرار الجمعية العامة للأمم المتحدة رقم ٥٦/ ١٩ بتاريخ ٢٩ نوفمبر ٢٠٠١م. انظر أيضاً: ناصر محمد البقمي، المرجع السابق، ص ١٠٩ وما بعدها.

١ – التقييم العام لمسائل أمن المعلومات.

٢ – تحديد المفاهيم الأساسية المتعلقة بأمن المعلومات .(Information Security)

٣ – مضمون المفاهيم الدولية (International Concepts) ذات العلاقة الهادفة إلى تعزيز وتدعيم أمن النظم العالمية للمعلومات والاتصالات. كما دعت الجمعية العامة إلى دراسة الأخطار القائمة والمحتملة لأمن المعلومات والتدابير التعاونية التي يمكن للدول اتخاذها للتصدي لهذه الأخطار(٤٢).

أولاً – القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء المنعقد في هافانا عام ١٩٩٠م:

أقر مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء الذي عقد في هافانا في عام ١٩٩٠م إطاراً دولياً في مكافحة جرائم الحاسب الآلي، كما أكد على ضرورة تطوير سبل ووسائل التعاون في المسائل الجنائية، كما ربط المؤتمر بين الجريمة المنظمة وما يتصل بها من إساءة استخدام الحاسب الآلي، وأن الحاسب الآلي يستخدم من قبل الجريمة المنظمة (Organized Crime) لارتكاب جرائم مثل غسيل الأموال أو في إدارة الأصول المتحصلة بطريقة غير مشروعة. وقد جاء القرار الصادر عن هذا المؤتمر متماشياً مع قرارات وتقارير منظمة التعاون الاقتصادي والتنمية وبشكل خاص تقريرها الصادر عام ١٩٨٦م وتوصية وتقرير مجلس أوروبا بشأن الجرائم المتعلقة بالحاسب الآلي والمبادئ الإرشادية التشريعية المعتمدة من اللجنة الوزارية لمجلس أوروبا. (Ministerial Committee of the Council of Europe) بتاريخ ١٣ سبتمبر ١٩٨٩م(٤٣).

ويمكن إجمال توصيات مؤتمر هافانا في المبادئ الآتية:

١ – التأكيد على أن وضع إطار قانوني دولي ملائم يتطلب بذل جميع الدول الأعضاء جهداً جماعياً مشتركاً.

٢ – الطلب من الدول الأعضاء تكثيف جهودها في مكافحة الجرائم ذات الصلة بالحاسب

(٤٢) انظر: قرار الجمعية العامة للأمم المتحدة رقم ١٩/٥٦، مرجع سابق. انظر أيضاً: وليد الزيدي، القرصنة على الإنترنت والحاسوب، دار أسامة، عمان، ٢٠٠٣م. ص ١٤٩ وما بعدها. انظر أيضاً:

Nick Nykodyum and Robert Taylor, Supra, 260-269.

(٤٣) خالد ممدوح إبراهيم، المرجع السابق. ص ٤٠١ وما بعدها. انظر أيضاً: عبدالله عبدالكريم عبدالله، المرجع السابق، ص ١٠٧ وما بعدها.

الآلي، ومكافحة عمليات إساءة استخدام الحاسب الآلي والتي تستدعي تطبيق جزاءات جنائية على المستوى الوطني بما في ذلك النظر – إذا دعت الضرورة إلى ذلك – في اتخاذ التدابير الآتية:

أ – تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة لضمان تطبيق الجزاءات والقوانين المعمول بها بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وإدخال تعديلات ملائمة إذا دعت الضرورة إلى ذلك، إضافة إلى وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي، إضافة إلى مصادرة ورد الأصول المتحصل عليها بصورة غير مشروعة والناتجة عن ارتكاب جرائم ذات صلة بالحاسب الآلي.

ب – تحسين تدابير الأمن والوقاية المتعلقة بالحاسب الآلي مع وجوب مراعاة حماية الخصوصية واحترام حقوق الإنسان وحرياته الأساسية.

ج – اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة إنفاذ القانون (Law Enforcement) بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحاسب الآلي.

د – اعتماد تدابير مناسبة لتدريب القضاة والموظفين والأجهزة المسئولة عن منع الجرائم الاقتصادية والجرائم ذات الصلة بأجهزة الحاسب الآلي والتحقيق فيه، ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها.

هـ – ضرورة التعاون مع المنظمات المعنية بهذا المجال في وضع قواعد للآداب المتبعة في استخدام أجهزة الحاسب الآلي والدخول إلى الشبكات(٤٤).

و – اعتماد سياسات بشأن ضحايا الجرائم المتعلقة بالحاسب الآلي تتناسب مع إعلان الأمم المتحدة بشأن مبادئ العدل المتعلقة بضحايا الإجرام والتعسف في استغلال السلطة، وتتضمن إعادة الممتلكات

(٤٤) سليمان أحمد فضل، المرجع السابق. ص ٤٢٨ وما بعدها. انظر أيضاً: عبدالله عبدالكريم عبدالله، المرجع السابق. ص ١٠٨ وما بعدها.

التي يتم الحصول عليها بطرق غير مشروعة، وتدابير لتشجيع الضحايا على إبلاغ السلطات المختصة بهذه الجرائم(٤٥).

ثانياً – مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات:

تم عقد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في ريودي جانيرو في البرازيل في عام ١٩٩٤م بشأن جرائم الحاسب الآلي، وقد أوصى المؤتمر المذكور بأن تتضمن قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الحاسب الآلي.

وسوف نستعرض فيما يلي القواعد الموضوعية والإجرائية لهذه القائمة.

أولاً – القواعد الموضوعية:

وتضمنت القواعد الموضوعية النص على قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل جرائم الحاسب الآلي، وهي تلك الجرائم المتضمنة فيما يلي:

١ – جريمة الاحتيال أو الغش المرتبط بالحاسب الآلي:

ويشمل ذلك الإدخال والإتلاف والمحو لمعطيات الحاسب الآلي أو برامجه أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص وذلك بقصد جني الجاني منافع مادية له أو للغير.

٢ – جريمة التزوير التي تطال برامج الحاسب الآلي:

ويشمل ذلك إدخال أو إتلاف أو محو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الحاسب الآلي وتعد – فيما لو تم ارتكابها بغير هذه الطرق – من قبيل أفعال التزوير المنصوص عليها في القوانين الوطنية.

٣ – جريمة الإتلاف:

وتشمل المحو والإتلاف والتعطيل والتخريب لمعطيات الحاسب الآلي وبرامجه.

٤ – جريمة تخريب وإتلاف الحاسب الآلي:

وتشمل الإدخال أو المحو أو الإتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الحاسب الآلي أو نظم الاتصالات (الشبكات).

---

(٤٥) محمد الأمين البشرى ومحسن أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ١٩٩٨م. ص ١٩ وما بعدها.

٥ – جريمة الدخول غير المشروع:

وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الحماية.

٦ – جريمة الاعتراض غير المشروع:

وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام حاسب آلي أو نظم أو شبكة اتصالات.

ثانياً – القواعد الإجرائية:

وضع هذا القرار بعض الأسس الواجب اتباعها في مكافحة الجرائم المتعلقة بالحاسب الآلي.

أ – وجوب تحديد السلطات القائمة بإجراء التفتيش والضبط في بيئة تقنية المعلومات، وخاصة ضبط الأشياء غير المحسوسة وتفتيش شبكات الحاسب الآلي.

ب – وجوب وجود قدر كبير من التعاون الفعال من قبل المجني عليهم والشهود، وغيرهم من مستخدمي تقنية المعلومات، لكي تكون المعلومات متاحة في صورة يمكن استخدامها للأغراض القضائية بالنسبة لهذه الجرائم.

ج – السماح للسلطات العامة باعتراض الاتصالات داخل نظام الحاسب الآلي ذاته، أو بينه وبين نظم الحاسبات الآلية الأخرى، مع استخدام الأدلة التي يتم الحصول عليها في الإجراءات أمام المحاكم.

د – يجب أن يوضع في الاعتبار كل المسائل المرتبطة ببيئة تقنية المعلومات، مثل ضياع الفرص الاستثمارية، التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسائر الاقتصادية، كلفة إعادة بناء قواعد البيانات كما كانت من قبل وإرجاعها إلى الوضع السابق قبل إجراء أي تفتيش أو تحقيق.

هـ – القواعد القائمة في مجال الإثبات الإلكتروني ومصداقية الأدلة، والمشاكل التي يمكن أن تثيرها عند تطبيقها[٤٦].

(٤٦) انظر: مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات والذي تم عقده في الفترة من ٤-٩ تشرين الأول ١٩٩٤م في ريودي جانيرو في البرازيل بشأن جرائم الحاسب الآلي. انظر أيضاً: عبدالله عبدالكريم عبدالله، المرجع السابق. ص ١١٢ وما بعدها..

المطلب الثاني
الاتفاقيات والمعاهدات والجهود الدولية الأخرى في مجال مكافحة الجرائم المعلوماتية

تعد المعاهدات والاتفاقيات الدولية من أهم صور التعاون الدولي بشكل عام، وفي مكافحة جرائم الحاسب الآلي والإنترنت بشكل خاص.

إذ أن إبرام المعاهدات والاتفاقيات الدولية في مجال مكافحة الجرائم المعلوماتية سيترتب عليه التقريب بين القوانين الجنائية الوطنية من أجل مكافحة هذه الجرائم. وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في القيام بإجراءات التحقيق وجمع الأدلة وتسليم المجرمين والاعتراف بالأحكام القضائية الأجنبية، وبدون هذا التعاون بين الدول وعدم وجود معاهدات واتفاقيات فيما بينها لمكافحة الجرائم المعلوماتية سيؤدي إلى زيادة كبيرة في ارتكاب مثل هذه الجرائم(٤٧). ومن هذه المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم المعلوماتية توصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتقنية المعلومات (Information Technology)، واتفاقية بودابست لمكافحة جرائم الإنترنت لعام ٢٠٠١م، إضافة إلى مؤتمر الفضاء الإلكتروني لعام ٢٠١١م، وسيتم تناولها في هذا المبحث في ثلاثة مطالب على النحو التالي:

أولاً – توصيات المجلس الأوروبي:

نتيجة للتطور الكبير في مجال تقنية الحاسب الآلي والإنترنت قررت الدول الأوربية إعادة النظر في الإجراءات الجنائية في هذا المجال، فأصدر المجلس الأوروبي عدداً من التوصيات في شأن المشاكل التي تعترض الإجراءات الجنائية المتعلقة بتقنية المعلومات لحث الدول الأعضاء في المجلس الأوروبي على مراجعة وتعديل قوانين الإجراءات الجنائية الوطنية حتى تلائم التطور في هذا المجال. ومن أهم هذه التوصيات ما يلي:

---

(٤٧) انظر:
Laura Quarntile, Cyber Crime: How To Protect Yourself From Computer Crime, Limelight Books, Tier Publications, 1997. at 73.

انظر أيضاً:
John Kntile, The Danger of Computer Hacking, Rosen Publishing Group, New York, 2000. at 132.

١ – وجوب توضيح القوانين في دول المجلس إجراءات تفتيش أجهزة الحاسب الآلي وضبط المعلومات أثناء انتقالها.

٢ – ضرورة أن تسمح الإجراءات الجنائية في دول المجلس لجهات التحقيق بتفتيش وضبط برامج الحاسب الآلي والمعلومات والبيانات المخزنة في أجهزة الحاسب الآلي وفقاً لذات الشروط الخاصة بإجراءات التفتيش العادية، كما يتعين إبلاغ الشخص القائم على الأجهزة بأن النظام كان محلاً للتفتيش مع بيان المعلومات والبيانات التي تم ضبطها.

٣ – أن يتم السماح أثناء إجراء التفتيش للجهات القائمة على التنفيذ باحترام الضمانات المقررة بمد التفتيش إلى أنظمة الحاسب الآلي في دائرة اختصاصهم، والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات وبيانات.

٤ – يجب أن تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تقنية المعلومات، ويتعين توفير السرية والاحترام للمعلومات والبيانات التي يعطيها القانون حماية خاصة.

٥ – يجب أن يوضح قانون الإجراءات أن الإجراءات الخاصة بالوثائق التقليدية تنطبق بشأن المعلومات والبيانات الموجودة بأجهزة الحاسب الآلي(٤٨).

٦ – ضرورة إلزام العاملين بالمؤسسات العامة والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل.

٧ – يجب منح سلطات التحقيق سلطة إصدار أوامر لمن لديه معلومات خاصة للدخول على نظام معلوماتي أو الدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لجهة التحقيق بالاطلاع عليها، وأن تخول سلطة التحقيق بإصدار أوامر مماثلة لأي شخص آخر لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

٨ – يجب تعديل القوانين الإجرائية بإصدار أوامر لمن لديه معلومات أو برامج أو بيانات تتعلق بأجهزة حاسب آلي بتسليمها للكشف عن الحقيقة.

٩ – يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية، حتى يتم الاعتراف بها في الدول المختلفة، ويتعين أيضاً تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.

---

(٤٨) انظر: التوصية الخاصة بالمجلس الأوروبي (Council of Europe) رقم١٣/٩٥ في ١١ سبتمبر لعام ١٩٩٥م. انظر أيضاً: سليمان أحمد فضل، المرجع السابق. ص ٤٢٨ وما بعدها.

١٠- يجب تشكيل وحدات خاصة لمكافحة جرائم الحاسب الآلي، وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تقنية المعلومات.

١١- قد تتطلب إجراءات التحقيق مد الإجراءات إلى أنظمة معلوماتية أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل مثل هذا الأمر اعتداء على سيادة الدولة يجب وضع قواعد قانونية واضحة تسمح بمثل هذا الإجراء(٤٩).

ثانياً - اتفاقية بودابست (Budapest) لمكافحة الجرائم المعلوماتية لعام ٢٠٠١م:

صادقت دول مجلس أوروبا (The Council of Europe) على اتفاقية بودابست لمكافحة الجرائم المعلوماتية في عام ٢٠٠١م. والتي تعد أول اتفاقية دولية شاملة تتعلق بجرائم الحاسب الآلي، والجرائم المرتكبة عبر شبكة الإنترنت وأجهزة تقنية المعلومات الأخرى(٥٠). وتسعى هذه الاتفاقية إلى التعاون والتضامن الدولي في محاربة الجرائم المعلوماتية ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات، كما تسعى هذه الاتفاقية إلى تحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية، ويعد التوقيع على هذه الاتفاقية الخطوة الأولى في طريق تكوين تضامن دولي مناهض لجرائم الحاسب الآلي والإنترنت. وقد وقعت على هذه الاتفاقية ٢٦ دولة أوروبية إضافة إلى كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية.

ولأن الاتفاقية جاءت حصيلة جهود دولية وإقليمية فقد أكدت المقدمة على أهمية ما أنجز من جهود في حقل جرائم الحاسب الآلي من قبل الأمم المتحدة ومنظمة

---

(٤٩) انظر: التوصية الخاصة بالمجلس الأوروبي (Council of Europe) في ١١ سبتمبر لعام ١٩٩٥م. انظر أيضاً: سليمان أحمد فضل، المرجع السابق. ص ٤٢٨ وما بعدها.

(٥٠) تم تأسيس مجلس أوروبا (The Council of Europe) في عام ١٩٤٩م ويتألف من ٤٦ دولة، ويقوم هذا المجلس بدور هام في مكافحة جرائم الحاسب الآلي والإنترنت من خلال إقراره للعديد من التوصيات المتعلقة بحماية البيانات من سوء الاستخدام وكذلك حماية تدفق البيانات والمعلومات، وقد أصدر هذا المجلس العديد من القواعد التوجيهية في جرائم الحاسب الآلي. انظر: هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة. ٢٠٠٧م. ص ٢٩٨ وما بعدها.

التعاون الاقتصادي والتنمية والاتحاد الأوروبي ومجموعة الدول الصناعية (مجموعة الثمانية) (G8).

وتتضمن هذه الاتفاقية ٤٨ مادة موزعة على أربعة فصول على النحو التالي:

الفصل الأول: تعريفات خاصة ببعض المصطلحات الفنية.

الفصل الثاني: ترتيبات لا بد من اتخاذها على المستوى الوطني:

القسم الأول: الجوانب الجنائية الموضوعية:

أ – بشأن الجرائم ضد الخصوصية وسلامة وتواجد معلومات الحاسب ونظم الحاسب، ويشمل وصفاً لأنواع متعددة من الجرائم.

ب – الجرائم المتصلة بالحاسب الآلي، شاملة استخدام الحاسب الآلي في التزوير وفي ارتكاب الأفعال الاحتيالية.

ج – الجرائم المتعلقة بالمحتوى.

د – الجرائم المتصلة بالتعدي على الملكية الفكرية والحقوق المجاورة.

القسم الثاني: الجوانب الإجرائية لجرائم المعلوماتية شاملة التحفظ العاجل على البيانات المعلوماتية المخزنة والأمر بإنتاج بيانات معلوماتية وتفتيش وضبط البيانات المعلوماتية المخزنة وتجميع البيانات المعلوماتية واعتراض بيانات المحتوى.

الفصل الثالث: مسائل التعاون الدولي وتسليم المجرمين والمساعدة القضائية المتبادلة والمساعدة المتبادلة في مجال سلطات التحقيق.

الفصل الرابع: فيما يتعلق بالانضمام والانسحاب من الاتفاقية وفض المنازعات بين الأعضاء في الاتفاقية(٥١).

وعلى الرغم من أن هذه الاتفاقية هي في الأصل أوروبية، إلا أنها دولية النزعة، وهي مفتوحة للدول الأخرى لطلب الانضمام إليها لتعم فائدتها الدول كافة.

وقد أكدت هذه الاتفاقية على أهمية التعاون الدولي في مجال مكافحة جرائم الحاسب الآلي والإنترنت، وبدون هذا التعاون لن يكون هناك أي أثر لأي مجهود تقوم به أية دولة بمفردها، حيث أن تلك الجرائم تكون غالباً جرائم عابرة للحدود (Transborder Crimes).

(٥١) هلالي عبداللاه أحمد، جرائم المعلوماتية عابرة الحدود، دار النهضة العربية، القاهرة، الطبعة الأولى، ٢٠٠٧م. ص ٦٣ وما بعدها.

فقد نصت هذه الاتفاقية في المادة (٢٣) منها على مدى أهمية الالتزام بالتعاون، فقررت أن التعاون يجب أن يمتد نطاقه ليشمل كل الجرائم الجنائية المعلوماتية، وأن هذا التعاون يجب أن ينفذ وفقاً للأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية،، والاتفاقيات المعتمدة في التشريعات المماثلة أو القانون الوطني.

كما أكدت هذه الاتفاقية على ضرورة الالتزام بمعاهدات تسليم المجرمين في الجرائم المعلوماتية، شريطة أن تكون معاقباً عليها في قانون الطرفين بعقوبة سالبة للحرية لا تقل عن سنة، أو بعقوبة أشد(٥٢). وتناولت هذه الاتفاقية أيضاً مسألة المساعدة القضائية المتبادلة وأوجبت على الأطراف أن توفر لبعضها البعض مساعدة قضائية متبادلة إلى أقصى مدى ممكن لأغراض التحقيقات أو الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الإلكترونية للجريمة الجنائية، كما أنه يمكن لكل طرف في حالة الاستعجال، أن يقدم طلباً للمساعدة المتبادلة أو الاتصالات عن طريق وسائل سريعة للاتصال كالفاكس أو البريد الإلكتروني، وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق (بما في ذلك التشفير لو كان ضرورياً)، مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوباً بواسطة الدولة الموجه إليها الطلب، ويجب على الدولة المقدم إليها الطلب أن توافق وأن ترد على الطلب المقدم إليها عن طريق أية وسيلة من الوسائل العاجلة للاتصال(٥٣).

ويجب أن تخضع المساعدة المتبادلة للشروط المحددة عن طريق القانون الداخلي للطرف الموجه إليه الطلب أو عن طريق الاتفاقات المطبقة للمساعدة المتبادلة، بما في ذلك الأسباب التي بناء عليها يمكن للطرف الموجه إليه الطلب أن يرفض التعاون.

كما أكدت هذه الاتفاقية أيضاً على أهمية المساعدة القضائية المتبادلة، وأنه يجب على كل طرف أن يعين هيئة مركزية أو هيئات تكون مسئولة عن إرسال أو الرد على طلبات المساعدة المتبادلة أو تنفيذه هذه الطلبات أو إرسالها إلى السلطات المختصة(٥٤).

كما أكدت هذه الاتفاقية على أنه يمكن لأي طرف أن يطلب من طرف آخر أن

---

(٥٢) المادة (٢٤) اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١م. انظر أيضاً: هلالي عبداللاه أحمد، جرائم المعلوماتية عابرة الحدود، المرجع السابق. ص ٧٣ وما بعدها.

(٥٣) المادة (٢٥)، اتفاقية بودابست لمكافحة الجرائم المعلوماتية.

(٥٤) المادة (٢٧)، اتفاقية بودابست لمكافحة الجرائم المعلوماتية.

يأمر أو يفرض بطريقة أخرى التحفظ العاجل على البيانات المخزنة بواسطة نظام معلوماتي يوجد داخل أراضي ذلك الطرف، والتي بخصوصها ينوي الطرف الملتمس أن يرسل طلباً للمساعدة المتبادلة من أجل تفتيش هذه البيانات أو الوصول إليها، أو ضبطها أو الحصول عليها، أو إفشاء سريتها(٥٥).

كما أكدت الاتفاقية على أهمية التعاون الكامل وتطبيق التشريعات الدولية فيما يتعلق بمجالات التحقيق في الجرائم المعلوماتية كسرقة البيانات والمعلومات واعتراضها وإتلافها وتعطيل أنظمة الحاسب الآلي، وكافة جرائم الحاسب الآلي والإنترنت المعروفة والمنصوص عليها في قوانين كل دولة، كما أكدت هذه الاتفاقية على أهمية تبادل المعلومات بين الدول الأطراف.

كما أوجبت هذه الاتفاقية على كل طرف أن يعين نقطة اتصال على مدار الساعة وطوال أيام الأسبوع لاستلام طلبات التحقيق في الجرائم المعلوماتية.

وأكدت الاتفاقية أيضاً على ضرورة التزام الدول الأطراف بأحكامها وتنفيذها وضرورة أن تكون قوانينها الداخلية متماشية معها(٥٦).

ثالثاً – مؤتمر الفضاء الإلكتروني (Cyber Space) بلندن لعام ٢٠١١م:

تم عقد المؤتمر الدولي للفضاء الإلكتروني في لندن بمشاركة حكومات ومنظمات دولية غير حكومية (Non-Governmental Organizations) وشركات عالمية. وشاركت أكثر من ٦٠ دولة في هذا المؤتمر منها الولايات المتحدة الأمريكية ودول الاتحاد الأوروبي والصين وروسيا ودول أخرى، وذلك بهدف تطوير فهم مشترك أفضل لكيفية حماية الإمكانات والفرص الكبيرة التي يقدمها الفضاء الإلكتروني (Cyber Space) للجميع(٥٧).

---

(٥٥) المادة (٢٩)، اتفاقية بودابست لمكافحة الجرائم المعلوماتية.

(٥٦) انظر المواد (٣١) - (٣٥) من اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١م. انظر أيضاً هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، المرجع السابق. ص ٢٩٨ وما بعدها.

(٥٧) وأكد وزير الخارجية البريطاني وليام هيغ (William Hage) في الكلمة الافتتاحية للمؤتمر على أهمية الإنترنت، قائلاً "إن شبكة الإنترنت ليست بمعزل عن المجتمع، فهي تمثل جزءاً من المجتمع وتعكس ما فيه". فهذه التقنية توفر فوائد جمة على حد سواء كما تتيح أيضاً مسألة إساءة استغلالها، وهذا ينطبق بشكل خاص على الجرائم المرتكبة عبر الإنترنت، التي هي في نمو متسارع جداً، فهناك أشخاص وجماعات في أنحاء العالم يسعون لتحويل بياناتنا الشخصية (Personal Data) إلى دخل مادي أو للتسبب بأضرار فادحة. كما أضاف الوزير =

وفي خطاب ألقاه نائب الرئيس الأمريكي جو بايدن (Joe Biden) في هذا المؤتمر قال: "تستثمر الولايات المتحدة في أمن الفضاء الإلكتروني من أجل معالجة تحدياته، وقد شمل ذلك تعيين المنسق القومي للفضاء الإلكتروني في البيت الأبيض، كما نعمل سوياً مع دول أخرى لمحاربة الجريمة التي تجتاز حدود الدول، بما في ذلك مساعدة الدول الأخرى على بناء قدراتها في فرض تطبيق القانون (Law Enforcement) لتتعاون مع بعضها البعض لأجل القضاء على التهديدات المنتشرة في الفضاء الإلكتروني (Cyber Space). وأضاف نائب الرئيس الأمريكي "لقد صادقنا على اتفاقية بودابست لمكافحة الجرائم المعلوماتية التي نشجعها بقوة والتي وضعت الخطوات التي يتوجب على الدول اتخاذها من أجل خفض الجرائم المعلوماتية". كما أشار في كلمته إلى أن "الفضاء الإلكتروني يمثل تحديات تختلف عن أي تحديات واجهناها من قبل، كما يثير أسئلة جديدة، وهو يجبرنا على ابتكار أساليب جديدة، حيث لم تعد الأساليب القديمة كافية، فتحديد الإجراءات الفعالة وبناء الثقة في مجال الفضاء الإلكتروني يشكلان تحدياً، وعلينا أن نجد طريقة لحل ذلك"(٥٨).

وقد أجمعت الدول المشاركة في هذا المؤتمر على أن الإنترنت أداة رئيسة وحيوية في النمو الاقتصادي وخاصة في الدول النامية، وعلى الفوائد الإيجابية الجمة للإنترنت في تحسين حياة المواطنين، وقدرتها على كشف انتهاكات حقوق الإنسان عند حدوثها، واتفق المشاركون على ضرورة ألا تكون جهود تحسين أمن الإنترنت

= البريطاني "من الواضح بشكل متزايد أن الدول التي لديها دفاعات وقدرات إلكترونية ضعيفة تجد نفسها عرضة للخطر على المدى البعيد، وتفتقر لميزات إستراتيجية كبيرة بالنظر إلى الزيادة الواضحة في الهجمات". وقد وجه وزير الخارجية البريطانية ويليام هيغ خلال مؤتمر الفضاء الإلكتروني ٤ رسائل لحكومات الدول، تضمنت ما يلي:

١ – أن الزيادة الكبيرة في جرائم الإنترنت تمثل تهديداً متنامياً لمواطنيها.

٢ – يجب عدم التعامل مع الفضاء الإلكتروني على أنه تابع للحكومة، فلا بد من الاستفادة من إبداع وأفكار الأفراد من خارج الحكومات.

٣ – أن الاعتداءات التي تكون برعاية الدولة (State Sponsored) ليست في صالح أي دولة على المدى البعيد، وعلى الحكومات التي تشن هذه الاعتداءات السيطرة عليها وضبطها، ولابد أن تتعاون مع بعضها البعض لأجل القضاء على التهديدات المنتشرة في الفضاء الخارجي (Cyber Space). انظر: جريدة الشرق الأوسط، العد ١٢٩٤٥، الأحد ٢٠١١/١١/٢٠م. ص٢١.

(٥٨) انظر: جريدة الشرق الأوسط، العدد ١٢٠٤٥. ص ٢١. انظر أيضاً: هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، المرجع السابق، ص ١٥٩ وما بعدها.

على حساب حقوق الإنسان، حيث أبدى المشاركون تأييداً قوياً لمبدأ وجوب أن يبدي مستخدمو الإنترنت تسامحاً واحتراماً لتنوع اللغات والأفكار والثقافات، مع التشديد على ضرورة ألا تكون حماية هذا المبدأ ذريعة لمحاولات الإخلال بحق حرية التعبير عن الرأي، وأشار مؤتمر الفضاء الإلكتروني إلى أن جرائم المعلوماتية تمثل تهديداً كبيراً للرفاه الاقتصادي والاجتماعي (Economioc and Social Prosperity).

كما أنها تتطلب بذل جهود دولية عاجلة ومتكاتفة لمواجهة هذه التهديدات، وضمان عدم وجود ملاذ آمن لمجرمي الإنترنت(٥٩). وطالب المشاركون في المؤتمر بضرورة أن تكون القوانين المتعلقة بالجرائم المعلوماتية متوافقة دولياً، والتعاون بين الدول متى كان ذلك ضرورياً، وحث المشاركون الدول على النظر في إمكانية الانضمام لاتفاقية بودابست لمكافحة الجرائم المعلوماتية، حيث ينظرون إلى هذه الاتفاقية على أنها أفضل شكل من أشكال الاتفاق الدولي في هذا المجال، وكذلك حث القطاع الخاص (Private Sector) على قيادة تطوير منتجات وأنظمة وخدمات تقنية متطورة لأمن شبكة الإنترنت. كما تم الاتفاق على ضرورة أن تكون الحكومات نموذجاً يحتذى، بأن تعتبر أمن الإنترنت أحد المعايير الأساسية عند توفير خدماتها عبر الإنترنت(٦٠).

الخاتمة:

أدى الانتشار الكبير في استخدام الحاسب الآلي وشبكة الإنترنت إلى زيادة كبيرة في الجرائم المعلوماتية، فشبكة الإنترنت لا تعرف الحدود وبالتالي يمكن الدخول إليها من خلال أي جهاز يتم توصيله بها، فمستخدم تلك الشبكة يمكنه ارتكاب جريمته وهو جالس في منزله أمام جهاز الحاسب الآلي، ويترتب على هذه الطبيعة العالمية لشبكة الإنترنت أن الجرائم التي ترتكب عليها أو بواسطتها تكون لها صفة العالمية، أي أنها تكون جرائم عابرة للحدود.

وإذا كانت الدول تستطيع تطبيق قوانينها الوطنية في إطار حدودها الإقليمية، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية المرتكبة عبر شبكة الإنترنت حيث لا حدود جغرافية بين الدول.

ويقتضي هذا الطابع الدولي للجرائم المعلوماتية وضع إستراتيجيات جديدة

---

(٥٩) انظر: جريدة الشرق الأوسط، العدد ١٢٠٤٥. ص ٢١. انظر أيضاً: هلالي عبداللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، المرجع السابق. ص ١٦٠ وما بعدها.

(٦٠) جريدة الشرق الأوسط، العدد ١٢٠٤٥. ص ٢١. انظر أيضاً: هلالي عبداللاه أحمد، المرجع السابق، ص ١٦٠ وما بعدها.

للتعاون الدولي في مكافحة هذا النوع من الجرائم المستحدثة، ذلك أن جرائم الإنترنت وهي من الجرائم العابرة للحدود في تزايد مستمر، ويكتسب التعاون الدولي أهمية كبيرة في محاربة هذه الظاهرة المستحدثة، إذ لن تستطيع دولة بمفردها أن تكافح هذا النوع من الجرائم دون حصولها على تعاون الدول الأخرى، وبناء على ما ذكر تم التوصل في نهاية هذا البحث إلى النتائج والتوصيات التالية:

أولاً – النتائج:

١ – الطبيعة العابرة للجرائم المعلوماتية يترتب عليها إمكانية ارتكاب الفعل الإجرامي غير المشروع عن طريق وحدة طرفية في دولة ما بينما تتحقق النتيجة الإجرامية للفعل في دولة أخرى، الأمر الذي يثير مشكلة تحديد القانون الواجب التطبيق بين قوانين الدول المختلفة، ويثير أيضاً مشكلة تحديد القانون الواجب التطبيق بين قوانين الدول المختلفة، إضافة إلى مشكلة تحديد المحكمة الجنائية المختصة بنظر الواقعة، وذلك في ضوء غياب أي تنظيم قانوني لهذه المسألة يحسم هذا النزاع.

٢ – تمثل الجرائم المعلوماتية تهديداً كبيراً للأمن والاستقرار والسلام في دول العالم، ولم تعد نتائجها مقتصرة على الأشخاص أو المؤسسات، بل أصبحت آثارها تهدد الدول نفسها، مما يؤكد على الحاجة إلى التعاون بين الدول لمواجهة هذه الجرائم.

٣ – يوجد اختلاف بين تشريعات الدول المختلفة على الأفعال المجرمة فيما يتعلق بالجرائم المعلوماتية، فما يكون مشروعاً في أحد الأنظمة قد يكون غير مشروع في نظام آخر. مما يساهم في عدم تعاون الدول فيما بينها في مكافحة هذا النوع من الجرائم.

٤ – اختلاف التشريعات في الدول المختلفة يجعل مسألة القبض على مرتكبي مثل هذه الجرائم ومحاكمتهم مسألة قد تكون صعبة في أحيان كثيرة، خاصة عند عدم وجود تعاون دولي يتفق مع طبيعة جرائم الإنترنت، والتي تتميز بطابع خاص يقتضي أن تكون هناك ردود فعل سريعة.

٥ – يوجد قصور وضعف كبيران في التعاون بين الدول المختلفة في مجال القبض والتحقيق والمحاكمة لمرتكبي هذه الجرائم، إذ أن كثير من الدول وتشريعاتها قد لا تهتم كثيراً بالجرائم المرتكبة خارج إقليمها أو التي نتجت آثارها الإجرامية خارج إقليمها، ويكون اهتمامها مركزاً على الجرائم التي تترتب آثارها الضارة في داخل إقليمها.

٦ – توجد صعوبات كبير في مسألة الحصول على أدلة في مثل هذا النوع من الجرائم

خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين، إضافة إلى الصعوبات الفنية في الحصول على الدليل ذاته.

٧ – عدم وجود قنوات اتصال سريعة وفعالة بين دول العالم فيما يتعلق بالجرائم المعلوماتية، وعدم وجود تبادل معلومات أو تسليم مجرمين في هذه الجرائم وعدم وجود مواد في القوانين الوطنية تحث الدول على التنسيق والتعاون الدولي في مكافحة مثل هذا النوع من الجرائم.

٨ – قلة خبرة رجال الشرطة والمحققين والقضاة في العديد من الدول في مجال مكافحة الجرائم المعلوماتية قد يساعد في عدم قدرتهم على تقديم التعاون المطلوب منهم من أقرانهم في الدول الأخرى في حال طلب المساعدة من تلك الدول.

ثانياً – التوصيات:

١ – ضرورة قيام الدول باستحداث قواعد مناسبة في مجال الإجراءات الجنائية والإثبات بشأن التحقيق في الجرائم المعلوماتية.

٢ – ضرورة قيام الدول بتوحيد قوانينها الخاصة بالجرائم المعلوماتية.

٣ – ضرورة التنسيق والتعاون الدولي قضائياً وإجرائياً في مجال مكافحة الجرائم المعلوماتية.

٤ – ضرورة قيام الدول بالتنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجرائم المعلوماتية، خاصة ما تعلق منها بأعمال الاستدلال والتحقيق.

٥ – ضرورة إيجاد صيغة ملائمة للتعاون الدولي لمكافحة الجرائم المعلوماتية، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وتحديد أدلتها وسبل مكافحتها.

٦ – ضرورة قيام الدول بالدخول في معاهدات ثنائية أو جماعية على نحو يسمح بالتعاون المثمر في مكافحة هذا النوع من الجرائم، فالصعوبات الإجرائية التي تثيرها الجرائم المعلوماتية لا يمكن حلها إلا من خلال الاتفاقيات الدولية، مع ضرورة إيجاد آليات كفيلة لحل التنازع بين قوانين الدول المختلفة فيما يتعلق بمحاكمة مرتكبي تلك الجرائم، إذ أن حل مشاكل الاختصاص القضائي، التي تثيرها الجرائم المعلوماتية عابرة الحدود، تساعد في تعزيز التعاون الدولي في مكافحة مثل هذا النوع من الجرائم.

٧ – ضرورة قيام الدول المختلفة بإنشاء إدارة شرطية متخصصة لمكافحة جرائم

المعلوماتية مع الاهتمام بعقد دورات تدريبية متخصصة للعاملين في تلك الإدارات بغرض تدريبهم على التحقيق في الجرائم المعلوماتية.

٨ – ضرورة تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية، وبشكل خاص الإنتربول.

٩ – ضرورة قيام أجهزة الشرطة في الدول العربية بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر شبكة الإنترنت وعقد اجتماعات تنسيقية دورية لهذا الغرض.

المراجع

أولاً – الكتب والبحوث العربية:

١ – أحمد، هلالي عبداللاه، اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٧م.

٢ – أحمد، هلالي عبداللاه، جرائم المعلوماتية عابرة الحدود، دار النهضة العربية، القاهرة، ط١، ٢٠٠٧م.

٣ – إبراهيم، خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م.

٤ – البشرى، محمد الأمين، ومحسن أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ١٩٩٨م.

٥ – البقمي، ناصر محمد، فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية، مجلة البحوث الأمنية، المجلد ١٧، العدد ٤٠، أغسطس ٢٠٠٨م.

٦ – حجازي، عبدالفتاح بيومي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٧م.

٧ – رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م.

٨ – الزيدي، وليد، القرصنة على الإنترنت والحاسوب، دار أسامة، عمان، ٢٠٠٣م.

٩ – شحاته، علاء الدين، التعاون الدولي لمكافحة الجريمة، إيتراك للنشر والتوزيع، القاهرة، ٢٠٠٠م.

١٠– الصغير، جميل عبدالباقي، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١م.

١١– عزت، فتحي محمد، الحماية الجنائية الموضوعية والإجرائية، الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والإنترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، ٢٠٠٧م.

١٢– عفيفي، كامل عفيفي، جرائم الكمبيوتر، بدون ناشر، بدون تاريخ.

١٣– الغافري، حسين سعيد، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية، القاهرة، ٢٠٠٩م.

١٤- قورة، نائلة عادل، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، بيروت، ٢٠٠٥م.

١٥- يوسف، حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١م.

ثانياً - المراجع الأجنبية:

1 - Berg, Terrence, State Criminal Jurisdiction in Cyber Space, Is There a Sheriff on the Electronic Frontier? 79 Mich. B.J.670- 675 (2000).

2 - Brown, Jack, Jurisdiction to Prosecute Crimes. Committed by Use of The Internet, 38 Jurimetrics J. 611, 1998.

3 - Charney, Scot, Computer Crime, 45 Emory L. J. 931- 953 (1996).

4 - Kntile, John, The Danger of Computer Hacking, Rosen Publishing Group, New York, 2000.

5 - Mason, Donald R, Sentencing Policy and Procedure As Applied to Cyber Crime: A Call for Reconsideration And Dialogue, Mississppi Law Journal, Winter 2007. At 12.

6 - Nadelman, the Evolution of United States Involvement in the International Rendition of Fugitive Criminals, 25 N. Y. U. Int. L. L. 813 - 14. (1993).

7 - Nykodym and Robert Taylor, The Worlds Current Legislative Efforts Against Cyber Crime, Computer Law and Security Report, Volume 20, Issue No. 5, September, 2004.

8 - Quarntile, Cyber Crime: How To Protect Yourself From Computer Crime, Limelight Books, Tier Publications, 1997.

ثالثاً - المعاهدات والاتفاقيات والقرارات الدولية:

١ - معاهدة ماسترخت (Maastricht Treaty) لعام ١٩٩٢م.

٢ - معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية لعام ١٩٩٠م.

٣ – اتفاقية الرياض العربية للتعاون القضائي لعام ١٩٩٣م.
٤ – النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي لعام ٢٠٠٣م الصادر عن مجلس التعاون الخليجي.
٥ – معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام ١٩٩٩.
٦ – توصية المجلس الأوروبي (Council of Europe) رقم ٩٥/١٣ لعام ١٩٩٥م المتعلقة بمشاكل الإجراءات الجنائية المرتبطة بتقنية المعلومات.
٧ – اتفاقية شينجن لعام ١٩٩٠م.
٨ – اتفاقية الأمم المتحدة لمكافحة الفساد.
٩ – التوصية الصادرة من اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية بدول مجلس التعاون الخليجي، الاجتماع الأول المنعقد بالأمانة العامة للمجلس بالرياض بالمملكة العربية السعودية في الفترة من ٤–٥/٤/٢٠٠٤م.
١٠– القرار الصادر بشأن الجرائم ذات الصلة بالحاسب الآلي من مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة السجناء المنعقد في هافانا في عام ١٩٩١م.
١١– اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٠م.
١٢– قرار الجمعية العامة للأمم المتحدة (General Assembly) رقم ١٩/٥٦ بتاريخ ٢٩ نوفمبر ٢٠٠١م.
١٣– مقررات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات والذي عقد في الفترة من ٤–٩ تشرين الأول ١٩٩٤م في ريودي جانيرو في البرازيل بشأن جرائم الحاسب الآلي.
١٤– اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١م.
١٥– قرارات مؤتمر الأمم المتحدة الثامن لمنع الجريمة والمجرمين، والذي تم عقده في هافانا بكوبا عام ١٩٩٠م المتعلقة بجرائم الحاسب الآلي.

رابعاً – الصحف:

١ – جريدة الرياض، العدد ١٤٧٢٩، ٢٢ نوفمبر ٢٠٠٨م. ص ٤٥.
٢ – جريدة الشرق الأوسط، ١٢٠٤٥، الأحد ٢٠/١١/٢٠١١م.

خامساً – الإنترنت:

1 - Interpol.at http:/en.wikipedia.org/wiki/Interpol.

2 - About Europol, 12 the Europol Training Course at http:// www.europa/news <http://www.europa/news>.

3 - Cyber Crime Unit For Europe? The New New Internet.at http:/ www. The new newinternet. com.

4 - Europol, at http:/ en.wikipedia.org./wiki/Europol.

5 - Internet Complaint Center, at http: // www.ic3.gov.