

التعاون الدولي في مواجهة جرائم الإنترنت

International Cooperation in the Face of Internet Crimes

الباحث وسام الدين محمد العكلة

ملخص البحث

في بداية الستينيات ظهرت شبكة الإنترنت لاستعمالها في أغراض غير تجارية ، ثم تطورت بشكل مذهل خلال السنوات الأخيرة، فبعد أن كانت مجرد شبكة صغيرة أصبحت الآن تضم ملايين المستخدمين حول العالم ، وتحولت من مجرد شبكة بحث أكاديمي إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات .

وفي بداية تأسيس الشبكة لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببنائها وتوسيع نشاطها إلا أنه بعد إتاحة الشبكة للعموم بدأ يظهر على الوجود ما يسمى بالجرائم المعلوماتية على الشبكة أو بواسطتها، وهي جرائم تتميز بحدائثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها، إضافة إلى اتصافها بالعالمية وعبورها للحدود . وقد صاحب تطور شبكة الإنترنت وانتشارها الواسع والسريع ظهور العديد من المشاكل القانونية ، فظهر على الساحة القانونية مصطلح جديد عرف باسم " الفراغ القانوني لشبكة الإنترنت "، وإزاء ذلك كان لا بد من تكاتف جهود الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه إلى مجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات وتعزيز التعاون بين هذه الدول واتخاذ تدابير فعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها .

ولمواجهة الصعوبات التي تواجه التعاون الدولي في مكافحة جرائم الإنترنت كان لا بد من اتخاذ إجراءات سريعة تتمثل في تحديث التشريعات الوطنية المتعلقة بالجرائم المعلوماتية وجرائم الإنترنت وإبرام اتفاقيات (دولية، إقليمية، ثنائية) لمواجهة القصور في التشريعات والقوانين الحالية ، ومعالجة حالات تنازع القوانين والاختصاص القضائي وتحديث الإجراءات التحقيقية الجنائية بما يتناسب مع التطور الكبير الذي تشهده تكنولوجيا المعلومات والاتصالات ، وتأهيل القائمين على أجهزة تنفيذ القانون لتطوير معلوماتهم حول هذا النوع المستحدث من الجرائم .



مجلة العلوم

الاقتصادية والإدارية

المجلد ١٨

العدد ٦٨

الصفحات ٢٢٢ - ٢٢٤



التعاون الدولي في مواجهة جرائم الإنترنت

الفرع الأول / ماهية جرائم الإنترنت وخصائصها

أولاً : نشأة جرائم الإنترنت^١ .

تتكون شبكة الإنترنت من عدة شبكات للمعلومات ، وهذه الشبكة عبارة عن توصيل عدد كبير من أجهزة الكمبيوتر بحيث تشكل شبكة ضخمة يمكن لأي عنصر فيها الاتصال بعنصر آخر بهدف تبادل المعلومات ويتم الاتصال بين عناصر الشبكة عن طريق جهاز مُضَمَّن MODEM (جهاز لنقل الإشارات الرقمية على خطوط الاتصالات بين الحواسيب بتحويل الإشارات الرقمية إلى إشارات يمكن نقلها على قنوات اتصالات والعكس) وأيضاً خط هاتف^٢ .

ظهرت شبكة الإنترنت في بداية الأمر لاستعمالها في أغراض غير تجارية من قبل وزارة الدفاع الأمريكية عام ١٩٦٠ ، حيث عملت الوزارة على إقامة مشروع لربط الحاسبات الرئيسية التابعة لوزارة الدفاع من خلال الاتصال مع بعضها البعض لتشكيل شبكة ذات عدة مراكز ، وكان الهدف الرئيسي من المشروع هو حماية شبكة الاتصالات العسكرية في الولايات المتحدة بحيث تكون المراكز العسكرية قادرة على إتمام عملية الاتصال في حال تعرض أي من المراكز لضربة عسكرية دون أن تتأثر بما حدث للمركز أو المراكز المدمرة أي أنها تكون شبكة تصلح نفسها بنفسها ، وقد عُرفت الشبكة التي صممت آنذاك بـ **Advanced**

Research Project Agency (ARPANET) ، وفي فترة الثمانينيات أخذت مؤسسة العلوم الوطنية الأمريكية **National Science Foundation (NSF)** بإعداد برنامج موسع لربط الحاسبات المركزية العملاقة مع شبكة **(ARPANET)** وبدأت الجامعات ومراكز الأبحاث في العالم بالانضمام إلى هذه الشبكة ، وعُرفت بـ **National Science Foundation Net (NSFNET)** ثم تحولت فيما بعد إلى شبكة عالمية **Internet**^٣ .

ومع بداية عام ١٩٩٣ سُمح للشركات التجارية باستخدام الشبكة العالمية ، وبدأ ظهور المتصفحات^٤ المسماة بـ **Browser** ولعبت هذه المتصفحات دوراً أساسياً في نشر الدعاية للشبكة^٥ ، وبذلك أصبحت الشبكة ذات طابع دولي تتيح لجميع الأفراد والشركات في العالم إبرام الصفقات المختلفة وتبادل المعلومات والمراسلات الخاصة من خلالها^٦ .

إلا أنه في المراحل الأولى لبناء الشبكة كان الاهتمام الأساسي منصباً على الربط والدخول دون مراعاة تحديات أمن المعلومات ، حيث لم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة^٧ ، ولم يكن هناك قلق من إمكانية ارتكاب جرائم بواسطتها وذلك نظراً لمحدودية مستخدميها ، إلا أنه مع توسع استخدامها ودخول جميع فئات المجتمع إلى قائمة مستخدميها بدأت تظهر على الوجود ما يسمى بالجرائم المعلوماتية وهي جرائم تتميز بجدائة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها ، وتعدد صورها وأشكالها واتصافها بالعالمية وعبور الحدود .

^١ - أول استخدام لمصطلح جرائم الإنترنت كان في مؤتمر جرائم الإنترنت المنعقد في أستراليا خلال الفترة ١٦-١٧/٢/١٩٩٨ أنظر عبد الله المنشاوي، جرائم الإنترنت من منظور شرعي وقانوني، بحث منشور على شبكة الإنترنت من خلال موقع الدراسات والبحوث www.minhawi.com ، مكة المكرمة بتاريخ ١/١١/٢٠٠٢ هـ ، ص ٤ .

^٢ - أحمد صلاح الدين إبراهيم، ومضات في جرائم الإنترنت (الأنماط - المسؤولية الجنائية - استراتيجية المواجهة) بحث منشور على شبكة الإنترنت من خلال الموقع www.eastlaws.com ، ص ١ .

^٣ - أحمد صلاح الدين إبراهيم، ومضات في جرائم الإنترنت (الأنماط - المسؤولية الجنائية - استراتيجية المواجهة) ، مرجع سبق ذكره، ص ١-٢ .

^٤ - أبرز هذه المتصفحات هي **Microsoft Internet Explorer , Opera ,Firefox , Google** .

^٥ - أحمد صلاح الدين إبراهيم، ومضات في جرائم الإنترنت (الأنماط - المسؤولية الجنائية - استراتيجية المواجهة) مرجع سبق ذكره ، ص ٢ .

^٦ - جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، دار النهضة العربية ، ٢٠٠٢ ، ص ٦ .

^٧ - جرائم الإنترنت، وجه من وجوه الشر المتعددة، شبكة النبا المعلوماتية، دراسة منشورة على شبكة الإنترنت بتاريخ ٢٢ أيار/٢٠٠٨ ، متوفرة على الرابط التالي : <http://www.annabaa.org/nbanews/70/260.htm>



التعاون الدولي في مواجهة جرائم الإنترنت

وخلال السنوات العشرة الأخيرة تطورت شبكة الإنترنت بشكل مذهل ، فبعد أن كانت مجرد شبكة أكاديمية صغيرة أصبحت الآن تضم ملايين المستخدمين حول العالم وتحولت من مجرد شبكة بحث أكاديمي إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات^١ ، وقد صاحب هذا التطور ظهور العديد من المشاكل القانونية فظهر على الساحة القانونية مصطلح جديد عرف باسم " الفراغ القانوني لشبكة الإنترنت "، وإزاء ذلك كان لابد من تكاتف جهود الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة أو توجه إلى مجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات وتعزيز التعاون بين هذه الدول واتخاذ تدابير فعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها^٢ .

وأمام هذه الأشكال الجديدة من الجرائم التي أفرزتها المعلوماتية وتقنية المعلومات يبدو أن قانون العقوبات غير كافٍ وغير فعال وهو عاجز عن مواجهة هذه الجرائم ، خصوصاً لناحية الإثبات في مجال تطبيق النصوص التقليدية لقانون العقوبات على جرائم المعلومات التي لا تترك أثراً مادياً فلا تكتشف إلا بمحض الصدفة ، علاوة على ذلك فإن الفعل الجرمي يقع في بلد ما والنتيجة الجرمية قد تكون في بلداً آخر فضلاً عن أن الضحايا لا يفصحون في الأغلب عما وقع عليهم من جرائم حرصاً على ثقة المتعاملين معهم إضافة إلى صعوبة تطبيق المبدأ القائل (لا جريمة ولا عقوبة إلا بنص قانوني) فالقاضي لا يستطيع أن يعتبر فعلاً معيناً جريمة إلا إذا وجد نصاً قانونياً يجرم هذا الفعل ، وإذا لم يجد فلا سبيل إلى اعتبار الفعل جريمة ولو اقتنع بأنه مناقض للعدالة أو الأخلاق أو الدين أو ضار بالمجتمع أبلغ الضرر ومن هنا تبرز أهمية استحداث قوانين خاصة تنال من الأفعال الجرمية التي تقع عن طريق المعلوماتية والإنترنت .

ثانياً: تعريف جرائم الإنترنت وخصائصها

إن الجرائم التي ترتكب باستخدام شبكة الإنترنت كثيرة ومتنوعة ويصعب حصرها ، لكنها بصفة عامة تشمل سرقة المعلومات والجرائم الجنسية كإنشاء المواقع الجنسية وجرائم الدعارة أو الدعاية للشواذ أو تجارة الأطفال جنسياً وجرائم تزويج المخدرات أو زراعتها ، وتعليم الإجرام وصنع المتفجرات وتنفيذ العمليات الإرهابية إضافة إلى جرائم الفيروسات واقتحام المواقع والإغراق بالرسائل المزعجة والاختراق والتجسس والقرصنة وسرقة كلمات السر وانتحال الشخصية وتزوير البيانات وغسيل الأموال^٣ ، ومن هذه الجرائم ما يقع على الأموال أو على الأشخاص أو على الملكيات الفكرية والعلمية (حقوق المؤلفات والمخترعات) بل تتعدى أحياناً كثيرة ذلك إلى المساس بالمعاهدات وبأمن الدولة الداخلي أو الخارجي وصولاً إلى الجرائم ذات الطبيعة الدولية كالجرائم الإرهابية والجرائم الأخلاقية ، وغالباً ما تترتب على هذه الجرائم خسائر جسيمة تقدر بمبالغ طائلة تفوق بنسب كبيرة الخسائر الناجمة عن جرائم المال التقليدية مجتمعة . وفي هذه الجرائم من الصعوبة بمكان إثبات المسؤولية بحق مرتكبيها لما تمتاز به من سرعة التنفيذ والانتشار وصعوبة اكتشاف مرتكبيها خاصة في جرائم القرصنة^٤ وإرسال البرامج التخريبية إلى الأرصد المصرفية وجرائم سحب الأموال من البطاقات الإلكترونية ، وجرائم السب والقذف والتجسس والتحرير ضد أمن الدولة ونشر الأفكار الإرهابية والهدامة داخل المجتمعات .

وتعرف جرائم الإنترنت بأنها (الجرائم التي لا تعرف الحدود الجغرافية ويتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت وبواسطة شخص على دراية فائقة بهما)^٥ .

ويمكن تعريف الجريمة الرقمية (المعلوماتية) بأنها الجريمة التي تستخدم التقنية الحديثة (بغض النظر عن نوع هذه التقنية) في أي مرحلة من مراحل الإعداد والتحضير لارتكاب الجريمة وانتهاءً

^١ - محسن العبودي، المواجهة الأمنية لجرائم الإنترنت، دراسة منشورة على شبكة الإنترنت من خلال الموقع www.eastlaws.com ، ص ٤ .

^٢ - حسين بن سعيد الغافري ، جهود السلطنة في مواجهة جرائم الإنترنت، بحث منشور على شبكة الإنترنت من خلال الموقع www.eastlaws.com ، ص ١٦ .

^٣ - حسين بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، دراسة منشورة على شبكة الإنترنت من خلال الموقع [http:// www.eastlaws.com](http://www.eastlaws.com) .

^٤ - محمد محمد صالح الألفي، أنماط جرائم الإنترنت، دراسة منشورة على شبكة الإنترنت من خلال الموقع www.eastlaws.com .

^٥ - تقدر نسبة القرصنة في منطقة الشرق الأوسط لبرامج الكمبيوتر التجارية بـ ٥٧% في عام ٢٠٠٠ و ٥١% عام ٢٠٠١ ، أنظر تقرير اتحاد برامج الكمبيوتر التجارية، منشور على شبكة الإنترنت بتاريخ ٢٠٠٢/٦/١١ من خلال الموقع www.albawaba.com .

^٦ - محسن العبودي ، المواجهة الأمنية لجرائم الإنترنت ، مرجع سبق ذكره ، ص ٤ .



التعاون الدولي في مواجهة جرائم الإنترنت

بمحاولة التوصل من النشاط الإجرامي الإلكتروني المحدد ، وتبعاً لذلك نجد أنّ جرائم شبكة المعلومات الدولية " الإنترنت " تعد نوعاً فريداً من الجرائم المعلوماتية^{١٤} .

ويعرف خبراء منظمة التعاون الاقتصادي والتنمية جريمة الكمبيوتر بأنها (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها) وقد وضع هذا التعريف من قبل مجموعة الخبراء للنقاش في اجتماع باريس الذي عقد عام ١٩٨٣ ضمن حلقة (الإجرام المرتبط بتقنية المعلومات) ، ويعتمد هذا التعريف على معيارين : أولهما (وصف السلوك) وثانيهما (اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها) ، وقد تبني هذا التعريف الفقيه الألماني Ulrich Sieher^{١٥} .

كما يقصد بجرائم الإنترنت المسماة أيضاً الجرائم السيبرانية أو السبرانية أي نشاط غير مشروع ناشئ في مكوّن أو أكثر من مكونات الإنترنت مثل مواقع الإنترنت وغرف المحادثة أو البريد الإلكتروني ، ويمكن أن تشمل جرائم الإنترنت أيضاً أي أمر غير مشروع بدءاً من عدم تسليم البضائع أو الخدمات مروراً باقتحام الكمبيوتر (التسلل إلى ملفات الكمبيوتر) وصولاً إلى انتهاك حقوق الملكية الفكرية والتجسس الاقتصادي (سرقة الأسرار التجارية)، والابتزاز على الإنترنت، وتبييض الأموال الدولي ، وسرقة الهوية ، وقائمة متنامية من الجرائم الأخرى التي يسهلها الإنترنت كالدخول غير المشروع إلى موقع على الإنترنت أو نظام معلوماتي ما وإعاقة الوصول إلى الخدمة واعتراض المعلومات، والاحتيال والاستعمال غير المشروع للبطاقات المصرفية وانتهاك حرمة الحياة الخاصة، إضافة إلى الأعمال الدعائية على شبكة الإنترنت لارتكاب الجرائم^{١٦} .

وتتميز جرائم الإنترنت عن الجرائم التقليدية في القانون من حيث تميزها بوجود ركن مفترض هو استخدام الحاسوب^{١٧} والاتصال بشبكة الإنترنت، وغالباً ما تتم بدون علم المجنى عليه كدخول البرامج التخريبية ولكن الصعوبة في هذه الجرائم بالوصول إلى الجاني لأنه غالباً ما يستخدم الإنترنت تحت اسم مستعار أو عن طريق محلات الإنترنت العامة، إضافة إلى صعوبة إلحاق العقوبة بالجاني المقيم خارج حدود الدولة وتحديد المسؤول جنائياً عن الفعل الإجرامي خصوصاً مع القصور الواضح في أغلبية القوانين الجنائية وعدم مواكبة التشريع الجنائي للتطور الحديث للجريمة المرتبط بتطور الوسائل الحديثة .

^{١٤} - أحمد صلاح الدين إبراهيم ، ومضات في جرائم الإنترنت (الأنماط - المسؤولية الجنائية - استراتيجية المواجهة) ، مرجع سبق ذكره ، ص ٦ .

^{١٥} - جرائم الإنترنت، وجه من وجوه الشر المتعددة ، مرجع سبق ذكره .

^{١٦} - دانيال لاركين، محاربة جرائم الإنترنت، مقالة منشورة بتاريخ ١٧ أيار/مايو ٢٠٠٨، متوفرة على الرابط التالي : <http://www.america.gov/st/democraciarabic/2008/May/20081117124454snmassabla0.2601086.html>

^{١٧} - عَرَفَ نظام التعاملات الإلكترونية السعودي " الحاسب الآلي " في المادة الأولى بأنه " أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي ، يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو استقبالها أو تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له " (المادة الأولى- ٧ من نظام التعاملات الإلكترونية والمادة الأولى - ٦ من نظام مكافحة جرائم المعلوماتية الصادر في ٢٦ / ٣ / ٢٠٠٧)، أنظر شيماء عبد الغني محمد عطا الله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقاً لنظام مكافحة جرائم المعلوماتية الصادر في ٧ / ٣ / ١٤٢٨ هـ الموافق ٢٦ / ٣ / ٢٠٠٧، متوفر على الرابط التالي

: <http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifer.aspx>



التعاون الدولي في مواجهة جرائم الإنترنت

وقد أظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسب الآلي والإنترنت بأن (٢٤ - ٤٢٪) من منظمات القطاع الخاص والعام على حد سواء كانت ضحية لجرائم متعلقة بالحاسب الآلي والإنترنت وقدرت الولايات المتحدة الأمريكية خسائرها من جرائم الحاسب الآلي ما بين ثلاثة وخمسة بلايين دولار سنوياً وتعتبر هذه الخسائر بسيطة نسبياً مع الخسائر التي تسببها جرائم نشر الفيروسات التي تضر بالأفراد والشركات الكبرى على حد سواء، حيث ينتج عنها توقف أعمال بعض تلك الشركات نتيجة إتلاف قواعد بياناتها ، وقد تصل الأضرار في بعض المنشآت التجارية والصناعية إلى تكبد خسائر مادية كبيرة جداً . كما كشفت دراسة بريطانية أنّ المملكة المتحدة وحدها تشهد جريمة إلكترونية جديدة كل عشر ثوان، حيث شهدت البلاد ارتكاب أكثر من ثلاثة ملايين جريمة إلكترونية سنوياً تتراوح بين الحصول على معلومات شخصية حول مستخدمي الإنترنت، والتحرش الجنسي بهم، وممارسة الاحتيال عبر شبكة المعلومات الدولية

وفي الوقت الذي يعكف فيه ممثلو الأجهزة الأمنية والجهات المختصة بتنفيذ القانون على وضع آليات فعالة للرقابة على الإنترنت من دون أن يشكل ذلك خرقاً للقانون نجد أنّ عصابات الإنترنت ماضية في إنشاء مجالات افتراضية خاصة بها وشبكات إنترنت موازية، إضافة إلى ما بات يعرف بـ « مشروع الإنترنت الخفي » الذي يتيح للخارجين عن القانون إمكانية تبادل المعلومات دون الخوف من أعين الرقابة أو إمكانية العثور عليهم إلا في حال تضافر جهود المجتمع الدولي بكامله، وهذا بدوره يتطلب إبرام اتفاقيات ووضع شروط موحدة تحكم استخدام الشبكة ، واعتماد قانون موحد يسري على الجميع .

وتسارع الدول إلى وضع ضوابط حماية وإنشاء أمن خاص للشبكات للحد من خطر استخدام شبكة الإنترنت حيث شكلت وزارة الداخلية المصرية "دوريات أمنية " من خلال الشبكة، مهامها منع الجريمة قبل وقوعها كما شكلت الحكومة البريطانية وحدة من قوات الشرطة كلفت بمتابعة المجرمين الذين يستخدمون أجهزة الكمبيوتر، وبعد الاقتناع التام بالخطر القادم قامت ثلاثون دولة أوروبية بتوقيع معاهدة لتوحيد الجهود في محاربة جرائم الإنترنت^{١٨}.

ولا تزال الإنترنت كوسيلة إعلام دولية بمنأى عن القانون الدولي فلم تصدر حتى الآن اتفاقات ذات شأن عبر الأمم المتحدة أو اليونسكو لتنظيمها بشكل يضمن استخدامها لصالح البشرية، وتعتبر السويد أول دولة سنت تشريعات خاصة بجرائم الحاسب الآلي والإنترنت، حيث صدر قانون البيانات السويدي عام ١٩٧٣ وتبعتها الولايات المتحدة الأمريكية التي شرعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي (١٩٧٦ و ١٩٨٥) وتأتي بريطانيا كالثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي، حيث أقرت قانون مكافحة التزوير والتزييف عام ١٩٨١ وهناك قوانين لجرائم الإنترنت في كندا وفرنسا والدانمارك وهولندا واليابان والمجر.

^{١٨} - اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١ .



التعاون الدولي في مواجهة جرائم الإنترنت

وعلى مستوى الدول العربية فقد قامت مصر والسعودية^{١٩} والبحرين والإمارات والأردن بوضع قوانين خاصة بجرائم الحاسب الآلي والإنترنت، وتركزت سياسات الدول العربية لمواجهة جرائم الإنترنت في مجال الإرهاب الإلكتروني وغسيل الأموال والتجارة الإلكترونية والاعتداء على أنظمة الشبكة والحاسوب^{٢٠} وفي سورية أصدر الرئيس السوري بشار الأسد بتاريخ ١٤ شباط/فبراير ٢٠١١ المرسوم التشريعي رقم (٢٦) الخاص بقانون الإعلام الإلكتروني في سورية والمسمى "تواصل العموم على الشبكة"، وهو أول قانون ينظم عمل الإعلام الإلكتروني في سورية^{٢١}، وقد تضمن القانون عقوبات صارمة تصل في بعض الحالات إلى الحبس ثلاث سنوات والغرامة إلى مليون ليرة ومضاعفة العقوبة في حال التكرار^{٢٢}.

أما التجارب الحكومية القليلة التي اهتمت بجرائم الإنترنت وركزت بصفة خاصة على الأمن والإرهاب والجرائم الاقتصادية، ونجد مبادرة وزارة الداخلية المصرية في نهاية عام ٢٠٠٢ من خلال إنشاء "الإدارة العامة للتوثيق والمعلومات" التي تخصصت في مكافحة الجرائم المعلوماتية، ونفس الشيء قامت به الحكومة المغربية عبر إنشاء "مكتب لمكافحة جرائم الإنترنت" في الإدارة العامة للأمن الوطني، وسبق أن نظمت دول مجلس التعاون الخليجي مؤتمراً إقليمياً خلال شهر حزيران/يونيو ٢٠٠٧ حول مكافحة الجرائم الإلكترونية في دول مجلس التعاون الخليجي غير أنه ركز فقط على المعاملات التجارية، وهذه المبادرات القليلة من طرف بعض الدول العربية تضاف إليها تجارب بعض هيئات ومنظمات المجتمع المدني كالجمعية المصرية لمكافحة جرائم الإنترنت التي نظمت نحو ١٥ ندوة ومؤتمراً لمواجهة جرائم الإنترنت خلال عام ٢٠٠٧^{٢٣}.

وفي سياق الجريمة وظروف ارتكابها من خلال شبكة الإنترنت حدد بعض الخبراء أن لأفعالها خصائص متفرقة لا تتوافر في أي من أفعال الجرائم التقليدية في أسلوبها وطريقة ارتكابها، وأهم هذه الخصائص^{٢٤}:

أولاً: الحاسب الآلي هو أداة ارتكاب جرائم الإنترنت، فلا يمكن تسمية جريمة ما أو وصفها بجريمة الإنترنت دون استخدام الحاسب الآلي لأنه هو وسيلة الدخول إلى شبكة الإنترنت وبالتالي تنفيذ الجريمة.

ثانياً: الجرائم ترتكب عبر شبكة الإنترنت، فهذه الشبكة هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف التي غالباً ما تكون الضحية لتلك الجرائم وهو ما دعا معظم تلك الأهداف إلى اللجوء إلى نظم الأمن والحماية الإلكترونية في محاولة منها لحماية نفسها أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم.

ثالثاً: مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي وشبكات الاتصال "الإنترنت" وذو دراية كبيرة في مجال استخدامهما التي تمكنه من تنفيذ جريمته والعمل على عدم اكتشافها.

رابعاً: جريمة الإنترنت لا حدود جغرافية لها ويمكن أن تتخطى آثارها حدود الدولة التي ارتكبت فيها لتتعدى آثارها كافة البلدان على مستوى العالم

^{١٩} - فرضت السعودية عقوبات بالحبس لمدة عام واحد وغرامات تصل إلى ما يعادل ١٣٣ ألف دولار لجرائم القرصنة المرتبطة بالإنترنت.

^{٢٠} - جرائم الإنترنت، وجه من وجوه الشر المتعددة، مرجع سبق ذكره.

^{٢١} - وكالات الأنباء، بتاريخ ٢٠/٢/٢٠١١.

^{٢٢} - انظر الباب السابع من القانون (المواد من ٢٤ إلى ٣٦).

^{٢٣} - جرائم الإنترنت، وجه من وجوه الشر المتعددة، مرجع سبق ذكره.

^{٢٤} - محمد محمد الألفي، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الإنترنت، ورقة مقدمة إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت" القاهرة خلال الفترة ٢ - ٤ حزيران/يونيو ٢٠٠٨، متوفرة على الرابط التالي: <http://www.f-law.net/law/showthread.php/28524>



التعاون الدولي في مواجهة جرائم الإنترنت

خامساً : هدف الجريمة ، فمن المعروف أنّ أغلبية جرائم الإنترنت يكون من ضمن أهدافها الأساسية هو الحصول على المعلومات الإلكترونية التي تكون إما محفوظة على أجهزة الحاسبات الآلية، وإما منقولة عبر شبكة الإنترنت وأخرى يكون هدفها الاستيلاء على الأموال، وقد تستهدف أفراداً أو جهات أو دولاً بعينها وأخيراً أجهزة الكمبيوتر كهدف لها .

سادساً : تتسم بالخطورة البالغة ، فالجرائم التي ترتكب بواسطة شبكة الإنترنت تتسم بالخطورة البالغة من عدة نواحي ، الأولى جسامه الخسائر الناجمة عنها قياساً بالجرائم التقليدية خاصة في جرائم الأموال، والثانية فهي ترتكب من فئات متعددة تجعل من التنبؤ بالمشتبه فيه أمراً صعباً، أما الثالثة فتتطوي على سلوكيات غير مألوفة^{٢٥} .

هذا فضلاً عن مجموعة من الخصائص الفرعية التي يمكن إيجازها بالآتي (أنّها جريمة لا تترك أثراً لها بعد ارتكابها، صعوبة الاحتفاظ الفني بآثارها إن وجدت، صعوبة التحقيق والتحري والمقاضاة ، تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها، إضافة إلى سهولة إخفاء معالم الجريمة ، وصعوبة تتبع مرتكبيها، كما يلعب البعد الزمني "اختلاف المواقف بين الدول" ، والمكاني " إمكانية تنفيذ الجريمة عن بعد " والقانوني " أي قانون يطبق؟" دوراً هاماً في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم) .

ثالثاً : أهداف جرائم الإنترنت

إنّ أهداف الجرائم التي ترتكب عبر الإنترنت تتحدد في الحصول على المعلومات أو تغييرها أو حذفها نهائياً والأغلب الأعم في هذه الحالات أن تكون جرائم اقتصادية للحصول على مزايا أو مكاسب مادية ، وقد يكون الهدف أجهزة الحاسب ذاتها وذلك بمحاولة تخريبها نهائياً أو على الأقل تعطيلها لأطول فترة ممكنة ، ومعظم تلك الجرائم تتم باستخدام الفيروسات الإلكترونية .

إضافة إلى ذلك فإنّ غالبية الجرائم التي ترتكب عبر شبكة الإنترنت تستهدف إما أشخاصاً أو جهات بعينها وقد ترتكب بطريقة مباشرة كالابتزاز والتهديد أو التشهير أو بطريقة غير مباشرة كالحصول على المعلومات الخاصة بتلك الجهات أو الأشخاص وذلك لاستخدامها في ارتكاب جرائم مباشرة^{٢٦} .

رابعاً : دوافع ارتكاب جرائم الإنترنت .

الدافع أو الباعث هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام فهو عبارة عن قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو يختلف من جريمة إلى أخرى تبعاً لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك، كما أنّه يختلف بالنسبة للجريمة الواحدة من شخص لأخر، وفي الجرائم المتعلقة بالإنترنت ثمة دوافع عديدة ومتنوعة تحرك الجناة لارتكابها كالولع في جمع المعلومات وتعلمها والاستيلاء عليها وتغييرها أو إتلافها وحذفها نهائياً وقد يكون الدافع وراء ذلك التنافس أو الابتزاز أو تحقيق المكاسب أو الحصول على مزايا ومكاسب اقتصادية أو الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية ، حيث يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنّه مع ظهور أي تقنية جديدة يحاولون إيجاد الوسيلة المناسبة للتفوق على هذه التقنية وغالباً ما ينجحون في ذلك أو الحاق الأذى بأشخاص أو جهات بعينها ، إضافة إلى السعي وراء تحقيق أرباح أو مكاسب اقتصادية أو مادية، وقد يكون الدافع وراء ارتكاب مثل هذه الجرائم دوافع سياسية تتمثل في تهديد الأمن القومي والعسكري لدولة ما والحصول على معلومات غاية في الأهمية خصوصاً مع ظهور ما يعرف بحرب المعلومات والتجسس والإرهاب الإلكتروني^{٢٧} .

^{٢٥} - حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص ٣ .

^{٢٦} - محسن العبودي ، المواجهة الأمنية لجرائم الإنترنت ، مرجع سبق ذكره ، ص ٥ .

^{٢٧} - حسين بن سعيد الغافري ، جهود السلطنة في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ٤-٥ .



التعاون الدولي في مواجهة جرائم الإنترنت

خامساً : معوقات التحقيق في جرائم الإنترنت

يتسم التحقيق في جرائم الإنترنت وملاحقة مرتكبيها جنائياً بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق ، بل يمكن أن تؤدي إلى الخروج بنتائج سلبية تنعكس على المحقق ذاته بفقدانه الثقة في نفسه وفي أدائه ، كما تنعكس على المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون غير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها ، وانعكاساً أيضاً على المجرم نفسه حيث يشعر أنّ الجهات الأمنية غير قادرة على اكتشاف أمره وأنّ خبرة القائمين على المكافحة والتحقيق لا تجاري خبرته وعلمه ، الأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من هذه الجرائم التي قد تكون أكثر فداحة وأشدّ ضرراً على المجتمع المحلي أو المجتمعات الأخرى^{٢٨} .

ومن هذه المعوقات ما يتعلق بالجريمة ذاتها أو بالجهات المتضررة أو بجهات التحقيق ، فالعوائق التي تتعلق بالجريمة تشمل خفاء الجريمة وغياب الدليل المرني وافتقاد الآثار التقليدية للجريمة وصعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقع مرتكبيها أو ترميزها أو تشفيرها لإعاقة الوصول إليها ، إضافة إلى سهولة محو الدليل ضد الجاني أو تدميره في وقت قصير جداً وبالتالي تنصله من مسؤولية الفعل إلى جانب عدم معرفة بعض الأطراف المعنية بالجريمة المتعلقة بشبكة الإنترنت . أما العوائق المتعلقة بالجهات المتضررة فتشمل عدم إدراكها خطورة الجرائم المعلوماتية من قبل المسؤولين فيها وإغفال الجانب التوعوي لإرشاد المستخدمين إلى خطورة الجرائم المتعلقة بشبكة الإنترنت وعدم التركيز على الجانب الأمني ، والإحجام عن الإبلاغ عن الجرائم التي تتعرض لها بواسطة شبكة الإنترنت^{٢٩} وذلك خشيةً على سمعتها ومصداقيتها وظهورها بمظهر مشين أمام الآخرين أو احتجاز حواسيبها وتعطيل شبكاتها لفترة طويلة خلال عمليات التحقيق أو عدم معرفة الضحية بوجود جريمة أصلاً . أما العوائق التي تتعلق بالتحقيق ذاته فيمكن أن ترجع إلى شخصية المحقق كعدم مواكبته للتطورات في مجال الجرائم المعلوماتية أو تتعلق بالنواحي الفنية كنقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ونقص المهارة في استخدام الحاسب الآلي والإنترنت وقلة الخبرة في مجال التحقيق في جرائم الحاسب الآلي والإنترنت^{٣٠} .

سادساً : خصائص المتهمين بجرائم الإنترنت

لا شك أنّ نشاط الإنترنت يتمتعون بصفات وخصائص تميزهم عن غيرهم وهو انعكاس حتمي لما تتطلبه عمليات استخدام هذه الشبكة من قدرات تقنية وفنية ، بيد أنّ ذلك لا يعني حصر مرتكبي جرائم الإنترنت في طبقة أو فئة معينة أو جنس معين ، فمرتكب جريمة الإنترنت قد يكون من البالغين أو الأحداث، المتعلمين منهم أو المثقفين، الفقراء أو الأغنياء، الرجال أو النساء، كما لا يمكننا أن نحصر جرائم الإنترنت بنوع معين من الجرائم فقد تكون من الجرائم الماسة بأمن الدولة الداخلي أو الخارجي، وقد تكون من جرائم الاعتداء على الأشخاص أو الأموال .

^{٢٨} - عبد الرحمن بحر ، معوقات التحقيق في جرائم الإنترنت ، دراسة مسحية على ضباط الشرطة بدولة البحرين ، رسالة ماجستير جامعة نايف العربية للعلوم الأمنية ، الرياض ، ١٩٩٩ ، ص ٥١ ، كذلك أنظر حسين بن سعيد الغافري ، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت ، بحث منشور على شبكة الإنترنت من خلال الموقع www.eastlaws.com ، ص ١٩ .

^{٢٩} - (أظهرت دراسة أعدها معهد أمن الحاسوب CSI بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية أنّ نحو ٧٠% من الجرائم التي يتم اكتشافها لا يتم الإبلاغ عنها لسلطات تنفيذ القانون) ، أنظر حسين بن سعيد الغافري ، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت مرجع سبق ذكره ، ص ٢٠ .

^{٣٠} - سليمان بن مهجع العنزي ، وسائل التحقيق في نظم المعلومات ، رسالة ماجستير في العلوم الشرطية ، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية ، الرياض ، ٢٠٠٣ ، ص ٩٨ .



التعاون الدولي في مواجهة جرائم الإنترنت

ومن السمات العامة لمرتكبي جرائم الإنترنت الذين تتوفر لدى بعضهم أو معظمهم مجموعة من الخصائص التي تميزهم عن غيرهم من المتورطين في أشكال الانحراف والإجرام الأخرى، وأهم هذه الخصائص الآتي^{٣١}:

- السن: تتراوح أعمار مرتكبي جرائم الإنترنت عادة ما بين ١٨ و ٤٦ سنة والمتوسط العمري لهؤلاء هو ٢٥ سنة .
- المعرفة والقدرة الفنية الكبيرة ، حيث ينتمي مرتكب جرائم الإنترنت عادةً إلى الطبقة المتعلمة ومعظمهم يكونون من أصحاب التخصصات ومستخدمي شبكة الإنترنت ، فشعورهم بالأمن نتيجة الثقة الزائدة بالنفس وجهل الكثير بعلم وتقنيات الحاسب الآلي لا سيما استخدام الإنترنت يغيرهم بإمكانية ارتكاب الجريمة دون أن يتم اكتشافها .
- ارتفاع مستوى الذكاء والحرص الشديد وخشية الضبط وافتضاح الأمر .
- الحرفية الفنية العالية التي يتطلبها ارتكاب هذه الجرائم .
- تخفي مرتكبي هذه النوعية من الجرائم عبر دروب الإنترنت بحيث يمكنه الاختفاء تحت قناع فني يظهرهم في دول أخرى .

الفرع الثاني/ التعاون الدولي لمواجهة جرائم الإنترنت

أولاً : التعاون الأمني والقضائي بين الدول لمواجهة جرائم الإنترنت^{٣٢}

تقتضي فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالإنترنت تتبع النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات ، وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية لدولة ما فإن ذلك يتطلب وجود تعاون قضائي بين الدول لاستكمال التحقيق في الجريمة والقبض على مرتكبيها ، وهذا يتطلب بدوره وجود تعاون وتنسيق أمني وقضائي بين هذه الدول يسمح بالاتصال المباشر بين أجهزة الشرطة والأمن فيما بينها من خلال المنظمة الدولية للشرطة الجنائية " الإنتربول " أو من خلال إنشاء مكاتب متخصصة بجمع وتبادل المعلومات حول الجرائم المتعلقة بالإنترنت ومرتكبيها ، إضافة إلى تعقب مجرمي المعلوماتية بشكل عام وشبكة الإنترنت بشكل خاص وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثاً عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية ، إضافة إلى معاينة مواقع الإنترنت في الخارج وضبط الأقراص الصلبة أو تفتيش نظم الحاسب الآلي ، وهذا كله قد يصطدم بمشاكل الحدود والولايات القضائية وهو ما يتطلب تبادل المساعدة القانونية بين الدول من خلال تبادل المعلومات ونقل الإجراءات إلى إقليم دولة أخرى لمصلحة الدولة ذات المصلحة والإتابة القضائية وتسليم المجرمين .

^{٣١} - محمد محمد صالح الألفي ، أنماط جرائم الإنترنت ، مرجع سبق ذكره ، ص ٢ .

^{٣٢} - حسين بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مرجع سبق ذكره ، ص ٣ .



التعاون الدولي في مواجهة جرائم الإنترنت

ثانياً : التعاون الدولي في مجال التدريب على مواجهة الجرائم المتعلقة بجرائم الإنترنت إن التقدم المتواصل والسريع في تكنولوجيا الحاسب الآلي والإنترنت يفرض على جهات تنفيذ القانون أن تسير في خطوات متساقطة مع التطورات السريعة التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومواجهتها . وهذا يتطلب من هذه الجهات أن تكون على درجة كبيرة من الكفاءة والمعرفة والقدرة على كشف غموض تلك الجرائم والتعرف على مرتكبيها بسرعة ودقة متناهيتين ، وهذا لن يتحقق إلا بتدريب وتأهيل القائمين على هذه الأجهزة بالتعاون والتنسيق مع غيرها من الأجهزة في الدول الأخرى بهدف كسب الخبرة الفنية في مجال الجريمة المعلوماتية وتكنولوجيا المعلومات والبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي^{٣٣} .

ومن المفيد أن يتضمن المنهج التدريبي بيان المخاطر والتهديدات ونقاط الضعف وأماكن الاختراق لشبكة المعلومات وأجهزة الحاسب الآلي ومعالجة البيانات وتحديد نوعية وأنماط الجرائم المعلوماتية وصفات المجرم المعلوماتي والدوافع وراء ارتكاب الجرائم المعلوماتية ، إضافة إلى إجراءات التحقيق وجمع المعلومات وتحليلها وأساليب المواجهة والاستجواب ومراجعة النظم الفنية للبيانات وأساليب العمل الجنائي وخوض تجارب عملية من خلال عينات من الجرائم المعلوماتية التي سبق التحقيق فيها^{٣٤} .

وتعد الولايات المتحدة الأمريكية من أكثر الدول المتقدمة والمتطورة تقنياً في مجال مكافحة الجرائم المعلوماتية وجرائم الشبكات ، ورغم ذلك فهي تدرك أنه ما من دولة وإن كانت متقدمة يمكنها التصدي بمفردها لأخطار هذه الأنماط المستحدثة من الجرائم ، لذلك تحرص على تقديم المساعدة التقنية والتدريب لرفع قدرات العدالة الجنائية لدى الحكومات الأخرى ومساعدة ما لديها من أجهزة شرطة ومسؤولي الادعاء العام والقضاة ليصبحوا أكثر فعالية في مكافحة جرائم الإنترنت لدى هذه الدول قبل أن يمتد أثرها ليتجاوز حدود بلدانها ويوجد حالياً في الولايات المتحدة مكتب للمساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج تابع لوزارة العدل الأمريكية ، إضافة إلى البرنامج الدولي للمساعدة والتدريب على التحقيق الجنائي (ICITAP) الذي يعمل مع مكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج وتوفير مساعدات لأجهزة الشرطة في البلدان النامية حول العالم^{٣٥} .

ثالثاً: الصعوبات التي تواجه التعاون الدولي في مكافحة جرائم الإنترنت

إن التعاون الدولي في مجال مكافحة الجرائم المتعلقة بشبكة الإنترنت وإن كان يعد مطلباً تسعى إلى تحقيقه أغلب الدول - إن لم يكن كلها - إلا أن ثمة صعوبات ومعوقات تحول دون تحقيقه في كثير من الأحيان أهمها :

- عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مجرماً في نظام ما قد يكون مباحاً وغير مجرم في نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والأديان والثقافات من مجتمع إلى آخر، وبالتالي اختلاف السياسات التشريعية من مجتمع إلى آخر^{٣٦} .

^{٣٣} - هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة في الفترة ١-٣/٥/٢٠٠٠ ، المجلد الثاني، الطبعة الثالثة ٢٠٠٤، ص ٤٩٦ .

^{٣٤} - حسين بن سعيد الغافري ، الجهود الدولية في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ٢١ .

^{٣٥} - حسين بن سعيد الغافري ، الجهود الدولية في مواجهة جرائم الإنترنت ن مرجع سبق ذكره ، ص ٢٣ .

^{٣٦} - جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، مرجع سبق ذكره ، ص ٧٢ .



التعاون الدولي في مواجهة جرائم الإنترنت

- تنوع واختلاف النظم القانونية الإجرائية بين الدول، فطرق التحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الإلكترونية والتسليم المراقب والعمليات المستترة وغيرها من الإجراءات الشبيهة ، وإذا ما اعتبرت طريقة ما من طرق جمع الأدلة والتحقيق أنها قانونية في دولة معينة أنها قد تكون غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى ستشعر بخيبة الأمل لعدم قدرة سلطات تنفيذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها غير مشروعة حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع^{٣٧} .

- إلى جانب الصعوبات التي تواجه المساعدات القضائية بين الدول والتعاون في مجال تدريب الكوادر الفنية وعدم وجود قنوات اتصال بين بعض الدول لتبادل المعلومات وجمع الأدلة حول جرائم الإنترنت إضافة إلى مشكلة تنازع الاختصاص حول هذه الجرائم ، وتعتبر جرائم الإنترنت من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي ولا توجد أي مشكلة بالنسبة للاختصاص الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانوناً لذلك ، لكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية التي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود^{٣٨} .

- رغم أن التجريم المزدوج للفعل يعتبر أهم شروط تسليم المجرمين إلا أنه يشكل أحياناً عقبة أمام التعاون الدولي في تسليم المتهمين بارتكاب جرائم عبر شبكة الإنترنت سيما وأن بعض الدول لا تجرم أنواع معينة من هذه الجرائم بالإضافة إلى أنه من الصعوبة تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أم لا ؟ الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالإنترنت^{٣٩} .

^{٣٧} - حسين بن سعيد الغافري ، الجهود الدولية في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ٢٥ .

^{٣٨} - جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠١ ، ص ٧٣ .

^{٣٩} - حسين بن سعيد الغافري ، الجهود الدولية في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ٢٦ ، أنظر أيضاً جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، مرجع سبق ذكره ، ص ٩١ .



التعاون الدولي في مواجهة جرائم الإنترنت

الخاتمة والتوصيات

على الرغم من الخصائص التي تتميز بها جرائم الإنترنت وتنفرد بها عن غيرها من الجرائم التقليدية إلا أن ذلك لا يغير من طبيعة تلك الجرائم سواء في أوصافها أو أركانها ، ووجه الخلاف قد يكون في أداة أو وسيلة ارتكابها ، لذلك فإنه من الناحية العملية يمكن تطبيق أحكام قانون العقوبات التقليدي في حال غياب تشريع خاص يحكم هذه الجرائم ، خصوصاً الجرائم المتعلقة بالنشر والقذف والسب والجرائم المخلة بالأداب والاعتداء على حرمة الحياة الخاصة على ذات الجرائم التي تتم عبر شبكة الإنترنت ، ولمواجهة الصعوبات التي تواجه التعاون الدولي في مكافحة جرائم الإنترنت لا بد من اتخاذ إجراءات تتمثل بالآتي :

- تحديث التشريعات الوطنية المتعلقة بالجرائم المعلوماتية وجرائم الإنترنت وإبرام اتفاقيات (دولية، إقليمية ثنائية) لمواجهة القصور في التشريعات والقوانين الحالية ومعالجة هذا النوع من الجرائم والسماح باستخدام بعض تقنيات التحقيق الخاصة في حالات الضرورة كالمراقبة الإلكترونية وغيرها من أشكال المراقبة لاستكمال جمع الأدلة حول هذه الجرائم ومعالجة حالات تنازع القوانين والاختصاص القضائي وتحديد الإجراءات التحقيقية الجنائية بما يتناسب مع التطور الكبير الذي تشهده تكنولوجيا المعلومات والاتصالات^{٤٠} .
- تأهيل القانمين على أجهزة إنفاذ القانون لتطوير معلوماتهم في مجال تكنولوجيا المعلومات ، من خلال تدريب وتأهيل القانمين بالضبط والخبراء وسلطات التحقيق والقضاة ، وتنمية قدرات مأموري الضبط والخبراء وسلطات التحقيق وتكوين مهاراتهم حتى تتكون لديهم درجة من المعرفة الفنية تتناسب مع حجم المتغيرات والتطورات المتلاحقة في مجال جرائم تقنية المعلومات والإنترنت خاصة جرائم الإرهاب عبر الإنترنت، مع تطوير أساليب البحث عن الأدلة وتقديمها لتواكب هذه التطورات عن طريق عقد دورات تدريبية متصلة عن كيفية التعامل مع هذا النوع من الجرائم والتدريب على دراسة وتحليل الأدلة.
- فرض رقابة كافية وليست شاملة من قبل الحكومات عن كل ما يقدم من خلال الشبكة لمنع الدخول والترويج لبعض المواقع التي تدعو لعادات لا تتناسب مع مجتمعاتنا ، إضافة إلى المواقع التي تبث الأفكار الإرهابية والتكفيرية التي تتنافى مع المبادئ الدينية الداعية للسلام والتسامح بين الشعوب .
- التنسيق وتبادل المعلومات والخبرات بين الأجهزة المعنية في كافة دول العالم ، ونقل التقنيات التي تستخدم في الدول المتقدمة في مكافحة جرائم الإنترنت إلى الدول التي لا تتوفر فيها هذه التقنيات .
- تعزيز التعاون والتنسيق بين المنظمات والمؤسسات الدولية المعنية بمواجهة كافة أشكال الجرائم عبر الإنترنت وتطوير وتحسين الآليات التقليدية للتعاون الدولي على المستوى الجنائي حتى تتلاءم مع اتساع شبكات الاتصالات والابتعاد عن البطء وكثرة الإجراءات والتعقيدات غير الملائمة لطبيعة هذه الطائفة من الجرائم .
- حث الدول للإسراع والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم المعلوماتية والإنترنت^{٤١} .
- عقد الندوات والدورات وإعداد الدراسات والبحوث بهدف نشر الوعي والتنبيه بمخاطر هذه الجرائم ، إضافة إلى التنسيق والتعاون بين السلطات المختصة بين الدول والهيئات والمنظمات الدولية والإقليمية من أجل تبادل الخبرات في مجال مكافحة هذا النوع المستحدث من الجرائم ، وتنمية الوعي الأمني من خلال إطلاق حملات التوعية الإعلامية والأمنية لتجنب الوقوع في مثل هذه الجرائم أو التعرض لها وتفادي أثارها السلبية وتبصير الجمهور بالمعارف الأمنية وترسيخ قناعاتهم بأبعاد مسؤولياتهم الأمنية وكسب مساندتهم في مواجهة الجريمة وكشف مظاهر الانحراف^{٤٢} .

^{٤٠} - حسين بن سعيد الغافري ، الجهود الدولية في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ٢٧ .
^{٤١} - محمد محمد الألفي ، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الإنترنت ، ورقة مقدمة إلى المؤتمر الدولي الأول حول " حماية أمن المعلومات والخصوصية في قانون الإنترنت " مرجع سبق ذكره .
^{٤٢} - حسين بن سعيد الغافري ، جهود السلطنة في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ١٢-١٣ .



التعاون الدولي في مواجهة جرائم الإنترنت

- إنشاء وحدات تحقيق خاصة في الدول تتولى مهمة التحقيق في الجرائم المعلوماتية ومنها الجرائم المتعلقة بالإنترنت والادعاء فيها ، والاهتمام بتدريب وتأهيل كوادرها بصورة مستمرة وإيجاد قضاء متخصص متدرب للنظر في هذه الجرائم المستحدثة ، وتعزيز وتنشيط تبادل المعلومات بين الأجهزة الأمنية المنوط بها تنفيذ القانون وخبراء نظم المعلومات^{٤٣} .

المراجع

- ١- أحمد صلاح الدين إبراهيم، ومضات في جرائم الإنترنت (الأنماط - المسؤولية الجنائية - استراتيجية المواجهة) بحث منشور على شبكة الإنترنت من خلال الموقع www.eastlaws.com .
- ٢- جرائم الإنترنت، وجه من وجوه الشر المتعددة ، شبكة النبا المعلوماتية، دراسة منشورة بتاريخ ٢٢ أيار/ ٢٠٠٨ متوفرة على الرابط التالي: <http://www.annabaa.org/nbanews/70/260.htm>
- ٣- جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائي ، دار النهضة العربية ، ٢٠٠٢ .
- ٤- حسين بن سعيد الغافري ، جهود السلطنة في مواجهة جرائم الإنترنت ، بحث منشور على شبكة الإنترنت من خلال الموقع www.eastlaws.com .
- ٥- حسين بن سعيد الغافري ، الجهود الدولية في مواجهة جرائم الإنترنت ، دراسة منشورة على شبكة الإنترنت من خلال الموقع <http://www.eastlaws.com> .
- ٦- دانيال لاركين ، محاربة جرائم الإنترنت ، مقالة منشورة بتاريخ ١٧ أيار/مايو ٢٠٠٨ ، متوفرة على الرابط التالي:
<http://www.america.gov/st/democracyarabic/2008/May/20081117124454snm-assabla0.2601086.html>
- ٧- سليمان بن مهجع العنزي ، وسائل التحقيق في نظم المعلومات ، رسالة ماجستير في العلوم الشرطية كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ٢٠٠٣ .
- ٨- شيماء عبد الغني محمد عطا الله ، مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقا لنظام مكافحة جرائم المعلوماتية الصادر في ٧ / ٣ / ١٤٢٨ هـ الموافق ٢٦ / ٣ / ٢٠٠٧ ، متوفر على الرابط التالي : <http://faculty.ksu.edu.sa/shaimaatalla/Pages/crifor.aspx>
- ٩- عبد الله المنشاوي ، جرائم الإنترنت من منظور شرعي وقانوني ، بحث منشور على شبكة الإنترنت من خلال موقع الدراسات والبحوث WWW.MINHAWL.COM ، مكة المكرمة بتاريخ ١١/١/١٤٢٣ هـ .
- ١٠- عبد الرحمن بحر ، معوقات التحقيق في جرائم الإنترنت ، دراسة مسحية على ضباط الشرطة بدولة البحرين ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ١٩٩٩ .
- ١١- محسن العبودي ، المواجهة الأمنية لجرائم الإنترنت ، دراسة منشورة على شبكة الإنترنت من خلال الموقع www.eastlaws.com .
- ١٢- محمد محمد صالح الألفي ، أنماط جرائم الإنترنت ، دراسة منشورة على شبكة الإنترنت من خلال الموقع www.eastlaws.com .
- ١٣- محمد محمد الألفي، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الإنترنت ، ورقة مقدمة إلى المؤتمر الدولي الأول حول " حماية أمن المعلومات والخصوصية في قانون الإنترنت " القاهرة خلال الفترة ٢- ٤ حزيران/ يونيو ٢٠٠٨ ، متوفرة على الرابط التالي: <http://www.f-law.net/law/showthread.php/28524>
- ١٤- هشام محمد فريد رستم ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة في الفترة ١-٣/٥/٢٠٠٠ ، المجلد الثاني، الطبعة الثالثة ٢٠٠٤ .

^{٤٣} - حسين بن سعيد الغافري ، جهود السلطنة في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ١٧ .