

التعاون الدولي في مواجهة جرائم الإنترنت

المدرس المساعد

وسام الدين محمد العكلة

جامعة دمشق / كلية الحقوق

المستخلص

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 بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها ، فضلا عن 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 لابد 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 ومعاينة 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 .

International Cooperation in the Face of Internet Crimes

Abstract:

At the beginning of sixties, Internet has appeared to use for non-commercial purposes, and then it has developed dramatically in the recent years. In the past, it was just a small network and now it covers a millions of users around the world, and it turned from academic research network to an integrated environment for investment, business, production, media and access to information.

At the beginning of establishment of the network there was no interest in security matters inasmuch as attention of its structure and expanding of its activities, but after the availability of the network to the public, it began to appear the so-called "Information Crimes on the web or through it", these crimes are distinguished with modern style, speed of execution, ease to concealment, the ability to erase its effects and the multiplicity of its forms, in addition to its international capacity and crossing border. The development of internet and its wide and rapid spread was accompanied with numerous legal problems. It appeared in the legal field a new term called (Legal Vacuum of the Internet). For all of that it had to condensing the efforts of states to combat this novel type of crimes that are no longer concentrated in a particular country and doesn't go to a particular community but it cross the border in order to inflict damage in several states and communities taking advantage of the great development of modern technology means in communication, foster the cooperation between these states, take an effective measures to reduce it, eradicate it and punish its perpetrators.

In order to face the difficulties of international cooperation for combating crimes of Internet, it should to take a fast proceedings which appeared in the updating of national legislation in relation with Informatic and Internet crimes and made an (international, regional and bilateral) agreements in order to face shortcomings in legislation and current laws, and to processing the cases of conflict of laws and jurisdiction and to update the criminal investigative procedures which commensurate with the great development witnessed by information and communication technology and rehabilitation the employees who works at the boards of law in order to develop their knowledge about this type of novelty crimes.

((المبحث الأول))**ماهية جرائم الإنترنت****أولاً: مفهوم جرائم الإنترنت :**

إنَّ الجرائم التي ترتكب باستخدام شبكة الإنترنت كثيرة ومتنوعة ويصعب حصرها، لكنها بصفة عامة تشمل الدخول غير المشروع إلى مواقع الإنترنت^(١) أو إعاقة الوصول إلى الخدمة، وسرقة المعلومات والجرائم الجنسية كإنشاء المواقع الجنسية وجرائم الدعارة أو الدعاية للشواذ أو تجارة الأطفال جنسياً وجرائم ترويح المخدرات أو زراعتها، وتعليم الإجرام وصنع المتفجرات وتنفيذ العمليات الإرهابية، فضلاً عن جرائم الفيروسات واقتحام المواقع والإغراق بالرسائل المزعجة والاختراق والتجسس والقرصنة، وسرقة كلمات السر وانتحال الشخصية وتزوير البيانات وغسيل الأموال^(٢)، إلى جانب الأفعال التي تحرض على الكراهية والعنصرية والتمييز على أساس اللون أو الجنس أو الديانة أو الأصل القومي أو الاثني^(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.

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)^(٤).

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 بمحاولة التنصل من النشاط الإجرامي الإلكتروني المحدد، وتبعاً لذلك نجد أنَّ جرائم شبكة المعلومات الدولية " الإنترنت " تعد نوعاً فريداً من الجرائم المعلوماتية^(٥).

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 تبنى هذا التعريف الفقيه الألماني Ulrich Sieher^(١) .

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 واعتراض المعلومات، والاحتيال والاستعمال غير المشروع للبطاقات المصرفية وانتهاك حرمة الحياة الخاصة، إضافة إلى الأعمال الدعائية على شبكة الإنترنت لارتكاب الجرائم^(٢) .

وتتميز جرائم الإنترنت عن الجرائم التقليدية في القانون من حيث تميزها بوجود ركن مفترض هو استخدام الحاسوب^(٣) 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.

وقد أظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسب الآلي والإنترنت بأنّ (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 وتعد 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.

ثانياً : نشأة وتطور جرائم الإنترنت^(٩) :

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 .

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 بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها^(١٠)، فضلا عن اتصافها بالعالمية وعبورها للحدود.

فقد 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 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 أنّها تكون شبكة تصلح نفسها بنفسها، وقد عُرفت الشبكة التي صممت آنذاك بـ (ARPANET) Advanced Research Project Agency ، 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^(١١) .

ومع بداية عام ١٩٩٣ سُمح للشركات التجارية باستخدام الشبكة العالمية، وبدأ ظهور المتصفحات^(١٢) المسماة بـ Browser ولعبت هذه المتصفحات دوراً أساسياً في نشر الدعاية للشبكة^(١٣)، وبذلك أصبحت الشبكة ذات طابع دولي تتيح لجميع الأفراد والشركات في العالم إبرام الصفقات المختلفة وتبادل المعلومات والمراسلات الخاصة من خلالها.

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^(١٤)، 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 بحدائثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها، وتعدد صورها وأشكالها واتصافها بالعالمية وعبور الحدود.

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^(١٥)، وقد صاحب هذا التطور ظهور العديد من المشاكل القانونية فظهر على الساحة القانونية مصطلح جديد عرف باسم (الفراغ القانوني لشبكة الإنترنت)^(١٦).

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 بلد آخر فضلاً عن أن الضحايا لا يفصحون في الأغلب عما وقع عليهم من جرائم حرصاً على ثقة المتعاملين معهم فضلاً عن 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 الإجرامية التي تقع عن طريق المعلوماتية والإنترنت.

ثالثاً: خصائص جرائم الإنترنت:

حدد بعض الخبراء في سياق تحليلهم لجرائم الإنترنت وظروف ارتكابها أن لأفعالها خصائص متفردة لا تتوافر في أي من أفعال الجرائم التقليدية في أسلوبها وطريقة ارتكابها، وأهم هذه الخصائص^(١٧):

أولاً: الحاسب الآلي هو أداة ارتكاب جرائم الإنترنت، فلا يمكن تسمية جريمة مأو وصفها بجريمة الإنترنت دون استخدام الحاسب الآلي لأنه هو وسيلة الدخول إلى شبكة الإنترنت ومن ثم 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.

خامساً: هدف الجريمة، فمن المعروف أن 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 ودولاً بعينها وأخيراً أجهزة الكمبيوتر كهدف لها .

سادساً: تتسم بالخطورة البالغة، فالجرائم التي ترتكب بواسطة شبكة الإنترنت تتسم بالخطورة البالغة من عدة نواحي، الأولى جسامة 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^(١٨).

هذا فضلاً عن مجموعة من الخصائص الثانوية التي يمكن إيجازها بالآتي (إنَّها 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 المواقيت بين الدول) ،والمكاني (إمكانية تنفيذ الجريمة عن بعد) والقانوني (أي قانون يطبق؟) دوراً هاماً في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم).

رابعاً : أهداف ودوافع ارتكاب جرائم الإنترنت :

إنَّ 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. فضلاً عن ذلك فإنَّ 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^(١٩).

إنَّ 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 أنَّه يختلف بالنسبة للجريمة الواحدة من شخص لآخر، 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 أنَّه 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^(٢٠).

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 وأشد ضرراً على المجتمع المحلي أو المجتمعات الأخرى^(٢١).

ومن هذه المعوقات ما يتعلق بالجريمة ذاتها أو بالجهات المتضررة أو بجهات التحقيق، فالعوائق التي تتعلق بالجريمة تشمل خفاء الجريمة وغياب الدليل المرئي 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 ومن ثم 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^(٢٢) وذلك خشية 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^(٢٣).

سادساً : المتهمين بجرائم الإنترنت وخصائصهم:

لا شك أنّ نشطاء 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 .

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^(٢٣):

- 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 يغريهم 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 الجرام عبر دروب الإنترنت بحيث يمكنه الاختفاء تحت قناع فني يظهرهم في دول أخرى.

المبحث الثاني

الإجراءات الدولية لمواجهة جرائم الإنترنت

- ازدادت خلال السنوات الأخيرة جرائم الإنترنت وتعدد تصورها وأشكالها بعد توسع استخدام شبكة الإنترنت ودخول جميع فئات المجتمع إلى قائمة المستخدمين ، وفي محاولة للقضاء على هذه الظاهرة أو على الأقل الحد من انتشارها استحدثت (الاتحاد الدولي للاتصالات) دليلاً إلكترونيًا لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة على الإنترنت ، يعتمد على مفهوم أن تنهض جهة واحدة بذلك التتبع ، ما يمكن المعنيين من الرجوع إليها ومتابعتها بسهولة.
- ووصف الدليل بأنه (خريطة طريق) فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيا المعلومات والاتصالات حيث يستطيع أن يلاحق المعلومات من خلال أحدث المعايير الأمنية المتجددة باستمرار ، ثم يصبها في قاعدة بيانات تُفتح أمام المعنيين ، ما يُسهل مهمة البحث عن المعلومات المطلوبة.
- وتمّوضع الدليل بالتعاون المشترك بين (الاتحاد الدولي للاتصالات) و (الوكالة الأوروبية المختصة بأمن الشبكات والمعلومات) وأطراف دولية أخرى مهتمة بشؤون الأمن المعلوماتي على شبكة الإنترنت. ويعرض الدليل أسماء المنظمات المعنية بتطوير المعايير وما تنشره من صيغ خاصة بأمن الإنترنت ، ما يُجذب تكرار الجهود ، كما يسهل مهمة مهندسي أمن الشبكة الإلكترونية في كشف الثغرات التي تُمكن العابثين من تهديد أمنها ، ويضم الدليل خمسة أقسام تُحدّثُ بصفة مستمرة وتتناول منظمات تطوير المعايير الخاصة بتكنولوجيا المعلومات والاتصالات وأعمالها والصيغ المعتمدة لتلك المعايير وطرق إقرار الاتفاق على تلك المعايير ، والحاجات المستقبلية (٢٤) .

أولاً: الإجراءات المتخذة على المستوى العربي والعالمي لمكافحة جرائم الإنترنت :

إنّ أهم خطوة في مكافحة جرائم الإنترنت تتمثل أولاً في تحديد هذه الجرائم، ومن ثم تحديد الجهة التي يجب أن تتعامل معها والعمل على تأهيل القائمين على النظر فيها بما يتناسب وطبيعة هذه

الجرائم المستجدة، ومن ثم يجري التركيز على التعاون الدولي لمكافحة هذه الجرائم والحاجة إلى وجود تشريع دولي موحد في هذا المجال^(٢٥).

وقد أثبت الواقع العملي أنّ الدولة – أي دولة – لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت، حيث ظهرت أشكال جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت، التي باتت تشكل خطراً لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة^(٢٦)، ومع تميزها بالعالمية وبكونها عابرة للحدود فإنّ مكافحتها لا تتحقق إلا بوجود 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 المتعلقة بالإنترنت وتعميمها.

فعلى سبيل المثال في جرائم نشر الفيروسات الإلكترونية قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم من حواسيب موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة. فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاينة مرتكبيها، لذا فإنّ التحقيقات في الجرائم المتصلة بالحاسب الآلي وملاحقتها قضائياً تؤكد على أهمية المساعدة القانونية والأمنية المتبادلة بين الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأنّ جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها، بمعنى آخر أنّه متى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزاً عن ملاحقته^(٢٧).

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، فضلاً عن ما بات يعرف (بمشروع 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 في ٢٣/١١/٢٠٠١ بتوقيع (الاتفاقية المتعلقة بالجريمة الإلكترونية) في بودابست لمحاربة جرائم الإنترنت^(٢٨)، وهذه الاتفاقية هي أول اتفاقية توضع للتعاطي مع الطابع الدولي للجريمة السيبرانية، وقد دخلت حيز التنفيذ في تموز/يوليو ٢٠٠٤، وتناولت الاتفاقية كل ما يتعلق بجرائم الإنترنت سواء ما يقع ضد الشبكات والمعلومات أو الجرائم التقليدية التي تستخدم في ارتكابها الشبكات الرقمية، كما تناولت إجراءات البحث والتفتيش والضبط، وإجراءات التعاون الدولي لمكافحة الجريمة، والتعاون القضائي، واشتملت الاتفاقية على ٤٨ مادة موزعة على أربعة فصول. تناول الفصل الأول تعريف المصطلحات المستخدمة، وتناول الفصل الثاني الإجراءات الواجب اتخاذها على المستوى المحلي في مجال قانون العقوبات والإجراءات الجنائية وقواعد الاختصاص القضائي، ويهدف الفصل الثالث إلى تنظيم التعاون الدولي، ويضم الفصل الرابع والأخير الشروط الختامية.

وتحتوي الاتفاقية على عدة نقاط أساسية أهمها:

- المخالفات التي ترتكب ضد سرية وسلامة بيانات ونظم الحاسوب .
- المخالفات ذات الصلة بحقوق التأليف والنشر .
- حفظ وصيانة سلامة بيانات الحاسوب لفترة من الوقت تمتد حسب الضرورة ، وذلك لتمكين السلطات المختصة من طلب إشهارها .
- جمع بيانات الحاسوب في الزمن الحقيقي .
- الحماية الكافية لحقوق الإنسان والحريات .
- ضرورة اعتماد الدول الأطراف التدابير التشريعية وغيرها من التدابير الضرورية لفرض ولايتها القضائية على المخالفات التالية دون الإضرار بقانونها المحلي:
- عندما يحدث عن قصد النفاذ إلى كل أو جزء من النظام الحاسوبي بدون وجه حق.
- عندما يحدث عن قصد الاعتراض بدون وجه حق لعمليات إرسال البيانات غير العامة.

- عندما يحدث عن قصد إتلاف أو شطب أو تغيير أو كبت بيانات حاسوبية بدون وجه حق.
 - عندما تحدث عن قصد إعاقة خطيرة لأداء نظام بدون وجه حق.
 - ويتعين على كل طرف من الأطراف الموقعة على الاتفاقية أن يثبت ولايته القضائية على أي مخالفة تقترب داخل إقليمه أو على ظهر سفينة ترفع علم ذلك البلد، أو على يد أي من رعاياها إذا كانت المخالفة يعاقب عليها جنائياً في مكان ارتكابها، أو إذا ارتكبت المخالفة خارج الولاية القضائية الإقليمية لأي دولة .
 - كما تضمنت الاتفاقية قواعد التعاون الدولي المتصلة بتسليم المجرمين، والمساعدة المتبادلة لأغراض التحقيق، والإجراءات الخاصة بالأعمال الجنائية ذات الصلة بنظم الحاسوب والبيانات وجمع القرائن الإلكترونية للعمل الإجرامي، إضافة إلى إنشاء شبكة مساعدة متبادلة متوافرة على مدار الساعة طيلة أيام في الأسبوع ذات مراكز اتصال وطنية قادرة على تقديم المساعدة الفورية في حال وقوع المخالفة^(٢٩).
- وفي أيار/مايو ٢٠٠٢ عقد اجتماع لوزراء العدل والداخلية للدول الثماني الكبار في Mont-tremblant حيث أصدرت توصيات بمتابعة الاتصالات على الشبكات الدولية عبر الإنترنت لمكافحة الإرهاب والجرائم المنظمة، ومن بين الحلول المقترحة أن يتوافر لدى مؤدي الخدمات لشبكات الاتصال القدرات الفنية لإمداد رجال الشرطة بالدخول والوصول إلى المعلومات عن المستخدمين بموجب أمر لتسجيل وحفظ المعلومات.
- وقررت الدول الثماني الكبار إقامة نقطة مراقبة دائمة للإنترنت تعمل ٢٤ ساعة كل ٢٤ ساعة تقوم بإعطاء إنذار بمجرد تسرب أحد القرصنة إلى الشبكة وبمجرد إطلاق صفارة الإنذار يتحرك على الفور نخبة من خيرة الأخصائيين في عالم الإنترنت لتحديد مكان المشتبه فيه باتباع أثره الإلكتروني وفقاً لمجال نشاطه الإجرامي. ومن بين الأهداف التي يسعى مجلس التعاون الأوروبي لتحقيقها وضع نظام للتفتيش عن بعد TELEPERQUISITION حيث يستطيع ضابط الشرطة المعلوماتي تفتيش جهاز الكمبيوتر المشبوه عن بعد، وتوسيع مفهوم جريمة الإنترنت بحيث يجرم كل شخص يدخل دون ترخيص أي شبكة معلومات غير مخصصة للجمهور^(٣٠).

أما حالياً فتعكف دول الاتحاد الأوروبي على إعداد استراتيجيات تلامنا الإنترنت بسبب تزايد القلق من عمليات التسلل الجنائية والحروب الإلكترونية بين الدول، وقد اتفقت الدول الأعضاء في الاتحاد الأوروبي بتاريخ ١٠ حزيران/يونيو ٢٠١١ على تشديد العقوبات على منفيذيه جومات الإنترنت مثل تلك التي سجلت في الفترة الأخيرة ضد الحكومة الفرنسية ومؤسسات أوروبية ومجموعة (سيتي غروب) المصرفية.

وبموجب القواعد الجديدة – التي لا يزال يتعين أن يقرها البرلمان الأوروبي – سيواجه المتسللون على الإنترنت عقوبة السجن خمس سنوات على الأقل إذا أدينوا بالتسبب في أضرار خطيرة لأنظمة تكنولوجيا المعلومات.

وستطبق عقوبات مشددة أيضاً على مدبري هجمات من خلال شبكات أجهزة كمبيوتر يتم برمجتها لتوجيه رسائل بريد إلكتروني غير مرغوب فيها ، وسوف تستهدف أيضاً سرقة الهويات ، وسيكون اعتراض البيانات بشكل غير قانوني جريمة جنائية في الاتحاد الأوروبي.

وكانت فرنسا قد تعرضت في شباط / فبراير ٢٠١١ لهجوم قبل اجتماع لوزراء مالية مجموعة العشرين في باريس ، كما استهدفت هجمات مؤسسات تابعة للاتحاد الأوروبي عشية قمة لزعماء أوروبيين في آذار/ مارس ٢٠١١، كما تمكن متسللون بداية حزيران/يونيو ٢٠١١ من الوصول إلى بيانات ٢٠٠ ألف حامل لبطاقات (سيتيغروب) بعد سلسلة هجمات استهدفت شركات بينها (غوغل) و(سونيكورب) و(نينتنندو) و(لوكهيدمارتن)^(٣١).

ورغم ذلك لا تزال الإنترنت كوسيلة إعلام دولية بمنأى عن القانون الدولي فلم تصدر حتى الآن اتفاقيات 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 وتبعها 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 وكندا وبريطانيا والسويد وماليزيا وسنغافورا، كما اهتمت بعض الدول الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت، بل إنَّها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم.

كما أصدرت اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) في عام ٢٠٠٧ مجموعة نماذج لتشريعات الفضاء السيبراني^(٣٢) في الدول الأعضاء بالإسكوا تضمنت توجيهات في مجالات التشريع والتنظيم والإدارة والأسس والخطوات المحددة التي يمكن أن تتخذها الدول والتوصيات والنصائح التي تمكن الدول الأعضاء من تقييم وضعها القانوني في هذه النواحي واستخراج النتائج^(٣٣) . إلا أنه لا يزال هناك نقص في التشريعات الرادعة لوضع حد لجرائم الإنترنت، لذا رأت منظمة الإسكوا إنّه من الضروري سن تشريعات وطنية تتوافق مع الاتفاقيات الدولية، وتشكيل فريق متخصص في صياغة التشريعات بعد مناقشتها مع الخبراء من الدولة أو من دول أخرى.

ومن هنا تأتي أهمية قيام الدولة بتوفير إطار قانوني يمكن من خلاله رفع آفاق المحققين في التحقيق فجرائم الحاسوب واتخاذ الإجراءات القانونية المناسبة التي تستند إلى آليات محددة تساعد في محاسبة المجرمين وإنزال العقوبات بهم، علماً أنّ القانون الوطني وحده غير كاف لردع المجرمين لأنه غالباً ما يكون إثبات أي جريمة أو اعتداء متوفر في دولة أخرى، ومن هنا علينا أن ندرك أهمية التعاون الدولي إذ إنّ التحقيق في أي جريمة لا يحتاج إلى خبراء من الدولة وحسب، بل يحتاج أيضاً إلى فريق دولي مدرب ومتخصص في كشف وإثبات جرائم الحاسوب والاتصالات في فترة زمنية معقولة .

لذلك يتوجب على كل دولة وضع خطة شاملة تتناول المواضيع التقنية والقانونية والسياسية وأن تضع أطر محددة وواضحة تبين أسس التعاون الإقليمي والدولي وتحسين طرق وسائل الاتصال واستمرار الحوار وتبادل المعلومات والآراء والخبرات والاستفادة من تجارب الآخرين والتدريب المستمر والحرص على إعداد الكفاءات ومراجعة الإجراءات المتخذة لمكافحة الجرائم التي ترتكب بواسطة شبكة الإنترنت.

وعلى المستوى العربي شهدت الدول العربية خلال السنوات الأخيرة تطورات متسارعة على صعيدي تكنولوجيا المعلومات والاتصالات واستخداماتها في المجالات كافة، كل ذلك في غياب تشريعات خاصة متكاملة لتنظيم هذا القطاع، لكن غياب هذه التشريعات لم يحل دون الاعتماد على هذا القطاع والاستفادة منه لا سيما في مجالي التجارة الإلكترونية والخدمات المصرفية والتي تطبق بشأنها الأحكام الجزائية العامة المعمول بها من جهة، ودون إقرار بعض الدول لقوانين خاصة لتنظيم استخدام شبكة الإنترنت من جهة ثانية^(٣٤) .

فقد بادرت الدول العربية على المستوى التشريعي إلى إصدار (قانون نموذجي) حول جرائم الإنترنت حيث أصدر مجلس وزراء الداخلية العرب مشروع قانون اطلق عليه (القانون العربي الموحد للإنترنت) ، وتمت المصادقة عليه في عام ٢٠٠٤، وهناك بعض الدول العربية أصدرت قوانين وطنية لتنظيم الإنترنت، فقد قامت مصر والسعودية^(٣٥) والبحرين والإمارات والأردن وتونس والمغرب والجزائر والكويت والسودان^(٣٦) بوضع قوانين خاصة بجرائم الحاسب الآلي والإنترنت، إلى جانب ذلك توجد مشاريع قوانين مماثلة في لبنان وسورية والعراق^(٣٧) بانتظار إقرارها من قبل الجهات المختصة.

وتركزت سياسات الدول العربية لمواجهة جرائم الإنترنت في مجال الإرهاب وغسيل الأموال والتجارة الإلكترونية والاعتداء على أنظمة الشبكة والحاسوب^(٣٨) ، فقد أنشأت وزارة الداخلية المصرية في نهاية عام ٢٠٠٢ (الإدارة العامة للتوثيق والمعلومات) التي تخصصت في مكافحة الجرائم المعلوماتية، و الشيء نفسه قامت به الحكومة المغربية عبر إنشاء (مكتب لمكافحة جرائم الإنترنت) في الإدارة العامة للأمن الوطني، كما أنشأت وزارة الداخلية العراقية (شعبة لمكافحة جرائم الإنترنت) في مقر وزارة الداخلية لمتابعة الجرائم التي ترتكب بواسطة الشبكة ومحاوله الحد من آثارها المتزايدة على المجتمع العراقي، 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، في حين تقوم وزارة الاتصالات والتقانة السورية بتنظيم (الملتقى الدولي السنوي لأمن المعلومات والاتصالات)^(٣٩) بحضور عدد كبير من خبراء الإنترنت والشركات العاملة في المجالات الإلكترونية والجامعات في عدد من الدول العربية والأوروبية، وغالباً ما يتناول هذا الملتقى البحث في أمن الشبكات والإنترنت والبريد الإلكتروني وتشفير البيانات وأمن الصيرفة الإلكترونية والجرائم التي ترتكب من خلال شبكة الإنترنت^(٤٠)، 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^(٤١).

وتجدر الإشارة إلى أن وضع القوانين والتشريعات التي تنظم استخدام شبكة الإنترنت لا يمكنها وحدها من القضاء على الجرائم التي ترتكب عبر هذه الشبكة أو من خلالها بل لا بد من نشر ثقافة

أمنية عالية بين مستخدمي الشبكة للحد من هذه الظاهرة، وفي هذا السياق نشرت منظمة التعاون والتنمية في الميدان الاقتصادي (OECD) مجموعة (مبادئ توجيهية لأمن شبكات ونظم المعلومات - نحو ثقافة أمنية) وتتضمن هذه المبادئ نشر الوعي والمسؤولية والتعاون والتنسيق لمنع واكتشاف الجرائم واحترام المصالح المشروعة للآخرين، وإجراء تقييمات للمخاطر وإدراج الأمن كعنصر أساسي في نظم وشبكات المعلومات، وإعادة تقييم أمن نظم وشبكات المعلومات وإدخال التعديلات المناسبة على السياسات العامة للأمن وممارساته وإجراءاته وتدابيره^(٤٢).

ثانياً: التعاون القضائي بين الدول لمواجهة جرائم الإنترنت :

إذا كانت هناك جريمة من جرائم الإنترنت تستحق التحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة. إلا أنّ المساعدة الرسمية المتبادلة هي عملية أكثر تعقيداً يتم اللجوء إليها عادة عملاً باتفاقيات بين البلدان المعنية ونصوص قانونية داخلية، وهي تشترط في الغالب الأعم أن تكون الجريمة على درجة معينة من الخطورة، وأن يكون الفعل مجرماً في كل من الدول الطالبة والموجه إليها الطلب، ويشار إلى هذا الأمر الأخير باعتباره (تجريماً مزدوجاً) .

كما أنّ فعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالإنترنت غالباً ما تقتضي تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة .

ولتحديد مصدر الجريمة غالباً ما يتعين على أجهزة تطبيق القانون الاعتماد على السجلات التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها، وفي أحيان أخرى قد يتطلب تطبيق القانون تتبع أثر التوصيل ووقت إجرائه، وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالباً فإن أجهزة تطبيق القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى، بمعنى الحاجة إلى ما يسمى التعاون القضائي الدولي^(٤٣)، أي التعاون بين الدول لاستكمال التحقيق في الجريمة والقبض على مرتكبيها، وهذا يتطلب بدوره وجود

تعاون وتنسيق أمني 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. ومن استقراء النصوص القانونية ونصوص الاتفاقيات الدولية بهذا الصدد يمكننا القول إنَّ أوجه التعاون القضائي الدولي في مكافحة الإجرام عموماً وجرائم الإنترنت على وجه الخصوص تتحدد في المجالين الآتيين:

- التعاون القضائي في مجال الإنابة القضائية .
- التعاون القضائي الدولي في مجال تسليم المجرمين.

التعاون القضائي الدولي في مجال الإنابة القضائية:

تعني الإنابة القضائية (طلب من السلطة القضائية المنبئة من السلطة المنابة قضائية كانت أم دبلوماسية أساسه التبادل باتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة في الخارج، وكذا أي إجراء قضائي آخر يلزم اتخاذه للفصل في المسألة المثارة أو المحتمل إثارتها في المستقبل أمام القاضي المنيب ليس في مقدوره القيام به في نطاق دائرة اختصاصه)^(٤٤).

وتبدو الحاجة إلى الإنابة القضائية الدولية حين يقتضي الأمر الخروج عن قواعد الاختصاص الإقليمي، فالأصل هو أن تقوم الجهة القضائية بدراسة الدعوى التي ترفع إليها والتحقيق فيها واتخاذ كافة الإجراءات بشأنها إلى حين إصدار الحكم فيها، إلا إنَّه قد تعجز الجهة عن القيام بالتحقيق اللازم أو استقصاء الأدلة في شأن المنازعة محل الدعوى القضائية المنظورة أمامها، ومن ذلك أن يكون الشهود المطلوب سماعهم أو محل الجريمة المراد معاينته أو الخصم المراد استجوابه أو تحليفه اليمين القانونية في دولة أخرى^(٤٥).

وقد حرصت الدول على تنظيم مجموعة من الإجراءات التي تنظم الإنابة القضائية منها اتفاقية الرياض للتعاون القضائي بين الدول العربية الموقعة عام ١٩٨٣، واتفاقية تسليم المجرمين وتنفيذ الأحكام والإنابات القضائية التي وافق عليها مجلس الدول العربية بتاريخ ١٤/٩/١٩٥٢ ودخلت حيز النفاذ عام ١٩٥٣، والاتفاقية الخاصة بتنفيذ الأحكام والإنابات والإعلانات القضائية بين دول مجلس التعاون الخليجي لعام ١٩٩٥، واتفاقية التعاون القانوني والقضائي بين دول مجلس التعاون العربي الموقعة في بغداد عام ١٩٨٦^(٤٦)، والاتفاقية العربية لمكافحة الإرهاب التي تمّ التوقيع عليها في القاهرة عام ١٩٩٨، ودخلت حيز النفاذ عام ١٩٩٩.

وللإنابة القضائية أربعة أركان هي: (الهيئة القضائية المنبئة، والهيئة القضائية المنابة، وموضوع الطلب ويتمثل بالإجراء المطلوب القيام به، وصيغة الطلب)، والقاعدة هي أن تصدر الإنابة عن جهة قضائية إلى جهة قضائية أخرى، وتبلغ الإنابة إما بالطريق القضائي المباشر بين الجهات القضائية، أو عن طريق وزارتي العدل بين البلدين، أو بالطرق الدبلوماسية، أو عن طريق الخصم نفسه.

وتجدر الإشارة إلى أنّ الإجراء الذي يتم بطريق الإنابة القضائية وفقاً للمبادئ العامة وما تقضي به الاتفاقيات الدولية ومن ذلك المادة (٢٠) من اتفاقية الرياض الأثر القانوني ذاته كما لو تمّ أمام الجهة المختصة لدى الطرف المنيب.

وقد نصت المادة (١٤) من اتفاقية الرياض على أنّه (لكل طرف متعاقد أن يطلب إلى أي طرف متعاقد آخر أن يقوم في إقليمه نيابة عنه بأي إجراء قضائي متعلق بدعوى قائمة وبصفة خاصة بسماع الشهود وتلقي تقارير الخبراء ومناقشتهم وإجراء المعاينة وطلب تحليف اليمين)^(٤٧).

التعاون في مجال تسليم المجرمين:

تسليم المجرمين أو استردادهم هو عملية قانونية اتفاقية تتم بين دولتين، تطلب إحداها من الأخرى تسليمها شخصاً يقيم على أراضيها لتحاكمه، أي الدولة الطالبة، عن جريمة من اختصاص محاكمها، ويعاقب عليها قانونها، أو لتنفيذ فيه حكماً صادراً عن هذه المحاكم، واسترداد المجرمين هو نوع من أنواع التعاون بين الدول لمكافحة الإجرام، بإلقاء القبض على المجرمين الفارين، ومحاكمتهم، وتنفيذ العقوبة بهم.

وتتفق أكثر التشريعات العربية والأجنبية، والاتفاقيات الدولية، على أن الاسترداد لا يمكن أن يتم إلا إذا تحققت فيه شروط معينة أهمها:

١- أن يكون التجريم مزدوجاً: ومعنى هذا الشرط أن يكون الفعل موضوع الاسترداد مجرماً في قانون الدولتين: طالبة الاسترداد، والمطلوب منها التسليم.

٢- أن تكون الجريمة على قدر معين من الأهمية: وهذا الشرط تفرضه اعتبارات عملية، تتعلق بإجراءات الاسترداد الطويلة والمعقدة والباهظة التكاليف، فالاسترداد لا يمكن اللجوء إليه إلا من أجل الجرائم المهمة والخطيرة، لكي لا تشغل أجهزة الدولة في جرائم قليلة الأهمية، كالمخالفات والجنح البسيطة.

٣- ألا تكون الجريمة مما يحظر التسليم فيها قانوناً أو عرفاً: كالجرائم السياسية والعسكرية. وقد أجمعت الدول العربية في اتفاقية الرياض لسنة ١٩٨٣ (المادة ٤١ / الفقرة أ) على عدم جواز التسليم (إذا كانت الجريمة المطلوب من أجلها التسليم تُعدّ بمقتضى القواعد القانونية النافذة لدى الطرف المتعاقد المطلوب إليه التسليم جريمة لها صبغة سياسية) .

٤- أن يكون الاختصاص القضائي منعقداً للدولة طالبة الاسترداد: وهذا الشرط نتيجة منطقية لطبيعة مؤسسة الاسترداد، فطلب الاسترداد يعني قبل كل شيء، أن الدولة طالبة هي صاحبة الحق قبل غيرها من الدول الأخرى، بملاحقة الشخص المطلوب استرداده، ومحاكمته، وإنزال العقاب المستحق به، أما إذا كان قضاء هذه الدولة غير مختص في الأصل بالنظر في الجريمة المرتكبة، فإن طلب الاسترداد يفقد مسوغه ومعناه.

٥- ألا يكون الاختصاص القضائي منعقداً للدولة المطلوب إليها التسليم: فللدولة المطلوب إليها التسليم أن ترفض طلب الاسترداد إذا كانت محاكمها مختصة بالنظر في الجريمة موضوع التسليم اختصاصاً إقليمياً أو عينياً أو شخصياً، ورفض التسليم لا يعني ترك الشخص المطلوب استرداده من دون محاكمة، بل يجب على الدولة الراضة أن تحاكمه أمام محاكمها في حدود اختصاصها، ولكي يكتمل التعاون الدولي في هذه الحالة، فإن على الدولة طالبة الاسترداد أن تزود الدولة التي قررت محاكمة الشخص المطلوب أمام محاكمها، بما لديها من وثائق ومستندات ومعلومات وأشياء تثبت جريمته، وعلى الدولة التي حاكمته أن تعلم بالمقابل الدولة طالبة الاسترداد بنتيجة المحاكمة عند انتهائها.

٦- ألا تكون الدعوى العامة أو العقوبة قد سقطت بأحد أسباب السقوط: كالنقادم أو العفو العام أو العفو الخاص، وألا يكون قد قضي بالجريمة قضاء مبرماً في الدولة المطلوب إليها التسليم : وهذا الشرط تتمسك به الدول استناداً إلى مبدأ السيادة ، فتسليم شخص إلى دولة أخرى لمحاكمته بعد أن تكون محاكم الدولة المطلوب إليها التسليم قد حاكمته وحكمت عليه بصورة نهائية، فيه مساس بهيبتها وقدرة قضائها على تحقيق العدالة الجنائية.

وتبدأ إجراءات الاسترداد في أكثر الدول العربية بعد أن تأخذ النيابة العامة علماً بوقوع الجريمة، وبفرار مرتكبها إلى دولة أجنبية معينة، حيث ترفع في هذه الحالة كتاباً إلى وزير العدل، الذي يرفعه إلى (لجنة تسليم المجرمين) (بمقتضى التشريع السوري)، وهي الجهة المختصة بتقديم طلب الاسترداد، وبالنظر في طلبات الاسترداد التي تصل إلى سورية من دولة أجنبية، ويعود إليها أمر البت في طلبات الاسترداد سلباً أو إيجاباً بقرارات معللة غير خاضعة للطعن، ومتى قررت الجهة المختصة في أي دولة عربية تقديم طلب الاسترداد، فإنَّ عليها أن تعد طلبها كتابة، وترسله إلى الجهة المختصة في الدولة المطلوب إليها التسليم، مصحوباً بالوثائق الثبوتية اللازمة^(٤٨) . ويجوز في أحوال الاستعجال أن تطلب الدولة طالبة الاسترداد القبض على الشخص المطلوب وتوقيفه مؤقتاً، وذلك إلى حين وصول طلب الاسترداد والمستندات اللازمة.

وتلعب المنظمة الدولية للشرطة الجنائية (الإنتربول)^(٤٩) دوراً مهماً في استرداد المجرمين الفارين، فعندما يفر المجرم إلى خارج البلاد في أي دولة منتسبة إلى (الإنتربول) - ومنها الدول العربية - يطلب المرجع القضائي المختص بطلب الاسترداد مباشرة، أو عن طريق قيادة قوى الأمن الداخلي، إلى المكتب الوطني للشرطة الجنائية الدولية في بلده، أن يبلغ المنظمة في مركزها بباريس بالأمر، فتقوم هذه على الفور بإذاعة بحث على الصعيد الدولي عن المجرم الفار، وإذا كان الطلب متفقاً مع دستور (الإنتربول) ، يصدر الأمين العام للمنظمة مذكرة فردية ذات شارة حمراء، تعمم على جميع المكاتب الوطنية للشرطة الجنائية الدولية في بلدان العالم، ويطلب فيها التحري عن المجرم الفار، وإلقاء القبض عليه، وتوقيفه احتياطياً، كما تنشر المنظمة في كل شهر جدولاً يحتوي على المذكرات الخاصة بالأشخاص المطلوبين، وفي الحالات الاستثنائية الطارئة، تستعمل شبكة البث السلكي أو اللاسلكي أو البريد الإلكتروني التي تربط قيادة المنظمة بالمكاتب الوطنية في دول

العالم، لإذاعة البحث عن هؤلاء الأشخاص. وإذا ما تعددت طلبات الاسترداد من دول مختلفة عن جريمة واحدة، فتكون الأولوية في التسليم وفق أحكام اتفاقية الرياض، بحسب التسلسل التالي:

- الدولة التي أضرت الجريمة بمصالحها (الاختصاص العيني)،
- ثم الدولة التي ارتكبت الجريمة في إقليمها (الاختصاص الإقليمي).
- ثم الدولة التي ينتمي إليها الشخص المطلوب استرداده بجنسيته عند ارتكاب الجريمة (الاختصاص الشخصي).

أما إذا اتحدت الظروف، فتفضل الدولة التي هي أسبق في طلب الاسترداد، وإذا كانت طلبات الاسترداد عن جرائم متعددة، فيكون الترجيح بينها بحسب ظروف الجريمة وخطورتها والمكان الذي ارتكبت فيه، ومع ذلك فقد تركت اتفاقية الرياض للدولة المطلوب إليها التسليم حق الفصل في الطلبات المقدمة إليها من مختلف الأطراف المتعاقدة بمطلق حريتها، مراعية في ذلك جميع الظروف. وإذا تمَّ استرداد الشخص المطلوب، فيجب أن يشمل الاسترداد الأشياء والوثائق والنقود والأدوات الجرمية التي ضبطت حين إلقاء القبض عليه، والتي صودرت منه أو من غيره، لصلتها بالجريمة المقترفة^(٥٠).

ثالثاً: التعاون الدولي في مجال التدريب على مواجهة الجرائم المتعلقة بجرائم الإنترنت.

إنَّ التقدم المتواصل والسريع في تكنولوجيا الحاسب الآلي والإنترنت يفرض على جهات تنفيذ القانون أن تسيّر في خطوات متناسقة 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 وإدارة الشبكات وعمليات الحاسب الآلي^(٥١).

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^(٥٢).

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 الجزائي (ICITAP) الذي يعمل مع مكتب المساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج وتوفير مساعدات لأجهزة الشرطة في البلدان النامية حول العالم^(٥٣).

رابعاً: الصعوبات التي تواجه التعاون الدولي في مكافحة جرائم الإنترنت .

لمواجهة الصعوبات التي تواجه التعاون الدولي في مكافحة جرائم الإنترنت كان لا بد من اتخاذ إجراءات سريعة تتمثل في تحديث التشريعات الوطنية المتعلقة بجرائم الإنترنت وإبرام اتفاقيات (دولية، إقليمية، ثنائية) لمواجهة القصور في التشريعات 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.

إنَّ التعاون الدولي في مجال مكافحة جرائم شبكة الإنترنت وإن كان يعد مطلباً تسعى إلى تحقيقه أغلب الدول - إن لم يكن كلها - إلا أنَّ 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 مُجرماً في نظام ما قد يكون مباحاً وغير مُجرّم 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^(٥٤).
- 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 أنّها قانونية في دولة معينة أنّها قد تكون غير مشروعة في دولة أخرى، وبالتالي فإنّ الدولة الأولى ستشعر بخيبة الأمل لعدم قدرة سلطات تنفيذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنّه أداة فعالة، بالإضافة إلى أنّ السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنّها غير مشروعة حتى وإن كان هذا الدليل تمّ الحصول عليه في اختصاص قضائي وبشكل مشروع^(٥٥).
- 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 تُثار 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^(٥٦).
- رغم أنّ التجريم المزدوج للفعل يعتبر أهم شروط تسليم المجرمين إلا أنّه يشكل أحياناً عقبة أمام التعاون الدولي في تسليم المتهمين بارتكاب جرائم عبر شبكة الإنترنت سيما وأنّ بعض الدول لا تجرم أنواع معينة من هذه الجرائم بالإضافة إلى أنّه 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^(٥٧).

الخاتمة والتوصيات:

أدى تطور شبكة الإنترنت إلى إحداث طفرة عميقة في عقلية الجيل العربي الجديد من جهة، وفي طبيعة الإعلام العربي من جهة أخرى، حيث استطاعت الشبكة إزالة كافة العراقيل والرقابة الحكومية لتنتج في نقل الخبر من السر إلى العلن وفضح الممارسات التي ترتكبها بعض الأنظمة العربية ضد شعوبها.

فقد لعبت شبكة الإنترنت (من خلال أشكال التعامل معها: مواقع، منتديات، صحف إلكترونية، مدونات، مواقع اجتماعية، بريد إلكتروني) دوراً أساسياً في تحرر الشعوب العربية وتمكينها من تحدي الأنظمة الدكتاتورية وفي تأمين الاتصال الجماهيري بين النشطاء على الشبكة ومواقع التواصل الاجتماعي^(٥٨) خلال ما سمي بـ (ربيع الثورات العربية) التي اجتاحت المنطقة العربية خلال الفترة الأخيرة، واستطاعت قلب موازين القوى وفسح المجال أمام فضاءات أكثر فعالية وأمناً للتعبير عن الرأي، وقد تجلّى ذلك في الحراك الشعبي والسياسي الذي عم البلاد العربية وبفضلها استطاع المواطن العربي نقل معاناته وحيثيات الثورة عبر معلومة عادل وزنها أحياناً من حيث التأثير، وزن المادة الإعلامية العالية المستوى^(٥٩).

فالיום نعيش في عصر جديد، من أبرز صفاته ثلاثي الحدود الجغرافية، الأرضية والفضائية، الفاصلة بين الدول، إنّه عصر الإنترنت والتواصل السريع بين البشر، عصر تستطيع فيه دولة صغيرة حجماً وسكاناً أن تلعب بواسطة قناة تلفزيونية دوراً سياسياً مهماً في توجيه الرأي العام في دول أكبر منها، عشر أو عشرين مرة حجماً وقوة عسكرية.

هذا العصر الجديد هو الذي يفسر ارتباك الدول الكبرى أمام ما حدث وتناقض مواقفها، وهو ما يبرر نجاح الانتفاضة الشعبية هنا وفشلها هناك وتعثرها هناك^(٦٠)، ذلك أنّ العوامل التي أطلقت وشجعت وحسمت هذه الانتفاضات عديدة ومتنوعة: من تدخلات دولية ووسائل إعلامية حديثة واندفاع الأجيال الطالعة ومواقف القوى المسلحة، بالإضافة إلى تردّي الأوضاع الاقتصادية والعطش إلى

الحرية والكرامة، وما كانت كل تلك العوامل لتتلاقى وتتفاعل لو لم نكن نعيش في عصر الإنترنت^(٦١).

وعلى الجانب الآخر لاستخدام شبكة الإنترنت نجد أنّ هناك عددا هائلا من الجرائم التي ترتكب بواسطة هذه الشبكة ضد الأشخاص والدول والأموال والشركات والمؤسسات والبنوك العامة والخاصة، وتتميز هذه الجرائم بخصائص وميزات خاصة تنفرد بها عن غيرها من الجرائم التقليدية إلا أنّ ذلك لا يغير من طبيعة تلك الجرائم سواء في أوصافها أو أركانها، ووجه الخلاف قد يكون في أداة أو وسيلة ارتكابها، لذلك فإثمه من الناحية العملية يمكن تطبيق أحكام قانون العقوبات التقليدي في حال غياب تشريع خاص يحكم هذه الجرائم، خصوصا 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 :

- الإسراع في تنظيم وتقنين هذا القطاع الهام من جرائم المعلوماتية من خلال إقرار تشريعات خاصة متكاملة من شأنها تنظيم تبادل ونقل المعلومات عبر الشبكات الدولية وتعميم تداولها بشكل ميسر ومحاسبة مرتكبي الجرائم التي ترتكب بواسطتها،حث الدول للإسراع والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم المعلوماتية والإنترنت^(٦٢).
- 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^(٦٣).
- تأهيل القائمين على أجهزة إنفاذ القانون لتطوير معلوماتهم في مجال تكنولوجيا المعلومات، من خلال تدريب وتأهيل القائمين 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، 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 دول العالم، ونقل التقنيات التي تستخدم في الدول المتقدمة في مجال مكافحة جرائم الإنترنت إلى الدول التي لا تتوفر فيها هذه التقنيات .
 - تعزيز التعاون والتنسيق بين المنظمات الدولية المعنية بمواجهة كافة أشكال الجرائم عبر الإنترنت وتطوير الآليات التقليدية للتعاون الدولي على المستوى الجنائي حتى تتلاءم مع اتساع شبكات الاتصالات والابتعاد عن البطء وكثرة الإجراءات والتعقيدات غير الملائمة لطبيعة هذه الجرائم .
 - عقد الندوات والدورات وإعداد الدراسات والبحوث بهدف نشر الوعي والتنبية بمخاطر هذه الجرائم، فضلا عن 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^(٦٤) .
 - إنشاء وحدات تحقيق خاصة في الدول تتولى مهمة التحقيق في جرائم الإنترنت والادعاء فيها، والاهتمام بتدريب وتأهيل كوادرها بصورة مستمرة وإيجاد قضاء متخصص متدرب للنظر في هذه الجرائم المستحدثة، وتعزيز وتنشيط تبادل المعلومات بين الأجهزة الأمنية وخبراء نظم المعلومات^(٦٥)
 - وضع سياسات خاصة بالأمن والحماية على المستوى الوطني، ومراقبة تنفيذها بشكل دوري وإنشاء هيئات وإدارات تعنى بتنفيذها، وتنظيم دورات تدريبية عالية المستوى في الحماية والأمن للمتخصصين في تكنولوجيا الاتصالات والمعلومات.

(الهوامش)

- (١) نصت المادة (٣) من مشروع قانون مكافحة الجرائم الإلكترونية السوري (تم إقراره من اللجنة الوزارية المشتركة نهاية عام ٢٠١٠) على أنه (يعاقب بالحبس من شهر إلى ثلاثة أشهر والغرامة من عشرة آلاف إلى خمسين ألف ليرة سورية أو بإحدى هاتين العقوبتين كل من دخل قصداً إلى موقع على الإنترنت أو نظام معلوماتي بشكل غير مشروع. وتصبح العقوبة الحبس من ثلاثة أشهر إلى سنة، والغرامة من خمسين ألف ليرة إلى ثلاثمائة ألف ليرة سورية، إذا حصل الفاعل على بيانات أو معلومات، وقام بإلغائها أو حذفها أو تدميرها أو تغييرها أو الإضافة عليها أو إعادة نشرها. ولا تقل العقوبة عن ستة أشهر والغرامة عن مائة وخمسين ألف ليرة سورية لكل من ارتكب أو سهل ذلك للغير أيّاً من الجرائم المنصوص عليها في البند السابق من هذه المادة مستغلاً عمله).
- (٢) محمد محمد صالح الألفي، أنماط جرائم الإنترنت، دراسة منشورة على شبكة الإنترنت من خلال الموقع www.eastlaws.com.
- (٣) بتاريخ ٢٨/١/٢٠٠٣ أقر مجلس أوروبا البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر. انظر: مجلس أوروبا، سلسلة المعاهدات الأوروبية، رقم ١٨٩، البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، ستراسبورغ، ٢٨/١/٢٠٠٣.
- (٤) محسن العبودي، المواجهة الأمنية لجرائم الإنترنت، دراسة منشورة على شبكة الإنترنت من خلال الموقع WWW.EASTLAWS.COM، ص ٤.
- (٥) أحمد صلاح الدين إبراهيم، ومضات في جرائم الإنترنت (الأنماط – المسؤولية الجنائية – استراتيجية المواجهة)، مرجع سبق ذكره، ص ٦ .
- (٦) شبكة النبا المعلوماتية، جرائم الإنترنت، وجه من وجوه الشر المتعددة، دراسة منشورة على شبكة الإنترنت بتاريخ ٢٢ أيار/مايو ٢٠٠٨، متوفرة على الرابط التالي :
<http://www.annabaa.org/nbanews/70/260.htm>.
- (٧) دانيا لاركين، محاربة جرائم الإنترنت، مقالة منشورة بتاريخ ١٧ أيار/مايو ٢٠٠٨، متوفرة على الرابط التالي:

<http://www.america.gov/st/democracyarabic/2008/May/20081117124454snmasabla0.2601086.html>

(٨) عرّف نظام التعاملات الإلكترونية السعودي (الحاسب الآلي) في المادة الأولى بأنّه (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 عبدالغني محمد عطاالله، 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/crifor.aspx>

(٩) 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 ١/١١/١٤٢٣ هـ، ص ٤ .

- (١٠) أحمد صلاح الدين إبراهيم، مرجع سبق ذكره، ص ١-٢ .
- (١١) أبرز هذه المتصفحات هي Google , Firefox , Opera , Microsoft Internet Explorer .
- (١٢) أحمد صلاح الدين إبراهيم، مرجع سبق ذكره، ص ٢ .
- (١٣) شبكة النبا المعلوماتية، جرائم الإنترنت، وجه من وجوه الشر المتعددة، مرجع سبق ذكره .
- (١٤) محسن العبودي، مرجع سبق ذكره، ص ٤ .
- (١٥) حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الإنترنت، بحث منشور على شبكة الإنترنت من خلال الموقع www.eastlaws.com، ص ١٦ .
- (١٦) 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>

- (١٧) حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص ٣ .
- (١٨) محسن العبودي، مرجع سبق ذكره ، ص ٥ .

- (١٩) حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص ٤-٥.
- (٢٠) 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.
- (٢١) (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 .
- (٢٢) سليمان بن مهجع العنزي، وسائل التحقيق في نظم المعلومات، رسالة ماجستير في العلوم الشرعية ، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣ ، ص ٩٨ .
- (٢٣) محمد محمد صالح الألفي، أنماط جرائم الإنترنت، مرجع سبق ذكره، ص ٢.
- (٢٤) الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، وحدة الاستراتيجيات الإلكترونية، سويسرا، جنيف، ٢٠٠٦.
- (٢٥) توجد تشريعات وطنية تختص بجرائم الحاسب الآلي بشكل عام في كثير من بلدان العالم، كما يوجد ما بين ٥٠-٦٠ بلداً لديها قوانين تختص بجرائم الإنترنت طبقاً لمركز أبحاث جرائم الحاسب (Computer Crime Research Center) .
- (٢٦) تدابير مكافحة الجرائم المتصلة بالحواسيب - مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة ١٨-٢٥/٤/٢٠٠٥م - وثيقة رقم. A/CONF.203/14.
- (٢٧) 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)، ص ٦.
- (٢٨) مجلس أوروبا، سلسلة المعاهدات الأوروبية، رقم ١٨٥، الاتفاقية المتعلقة بالجريمة الإلكترونية، بودابست، ٢٣/١١/٢٠٠١.
- (٢٩) مجلس أوروبا، سلسلة المعاهدات الأوروبية، رقم ١٨٥، الاتفاقية المتعلقة بالجريمة الإلكترونية، بودابست، ٢٣/١١/٢٠٠١.

- (٣٠) الاتحاد الدولي للاتصالات، مرجع سبق ذكره، ص ١٩-٢٠.
- (٣١) صالح أحمد البربري، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٣/١١/٢٠٠١، الدليل الإلكتروني للقانون العربي، ص ١٨.
- (٣٢) وكالات الأنباء، بتاريخ ١١/٦/٢٠١١.
- (٣٣) الفضاء السيبراني له معنيان: المعنى الواسع هو الفضاء المتعلق بشبكات الحاسوب والإنترنت، وهو فضاء عالمي لا يرتبط بأي نطاق محدد جغرافياً، ولا تتوافر عليه أية صلاحية قانونية وطنية. والمعنى الضيق المعرف بشبكة حواسيب معينة أو قاعدة معلومات سواء كانت هذه الشبكة على المستوى الوطني أو مؤسسة ما داخلية أو شبكة محلية، انظر: الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا، منشورات الأمم المتحدة، نيويورك، رقم الوثيقة E/ESCWA/ICTD/2008/8 تاريخ ٢٧ حزيران/يونيو ٢٠٠٧، ص ١.
- (٣٤) الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا، منشورات الأمم المتحدة، نيويورك، رقم الوثيقة E/ESCWA/ICTD/2008/8 تاريخ ٢٧ حزيران/يونيو ٢٠٠٧.
- (٣٥) بتاريخ ٢١/١/٢٠١١ وقع وزراء الداخلية والعدل العرب في اجتماعهم المشترك الذي عقد بمقر جامعة الدول العربية على خمس اتفاقيات بهدف تعزيز التعاون العربي، إحدى هذه الاتفاقيات هي (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات)، وتتكون الاتفاقية من ٤٣ مادة، وتحدد مجالات جريمة استخدام وسائل المعلومات، ومنها جرائم الاحتيال، والإباحية وجرائم أخرى مثل تزوير العملات، والاستغلال الجنسي، وحرمة الاعتداء على الحياة الخاصة، وما يتعلق بالإرهاب، والجريمة المنظمة.
- (٣٦) فرضت السعودية عقوبات بالحبس لمدة عام واحد وغرامات تصل إلى ما يعادل ١٣٣ ألف دولار لجرائم القرصنة المرتبطة بالإنترنت.
- (٣٧) قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧.
- (٣٨) بتاريخ ٢٠/٤/٢٠١١ أعلن علي الدباغ وزير الدولة والناطق الرسمي باسم الحكومة العراقية بأن مجلس الوزراء قرر الموافقة على مشروع قانون (جرائم المعلوماتية) المُدقّق

من قبل مجلس شورى الدولة وإحالته إلى مجلس النواب استناداً إلى أحكام المادتين (٦١/البند أولاً و٨٠/البند ثانياً) من الدستور مع الأخذ بنظر الاعتبار رأي اللجنة القانونية في الأمانة العامة لمجلس الوزراء والملاحظات المطروحة من قبل الوزراء، وأشار الدباغ إلى أنّ الموافقة على مشروع قانون جرائم المعلوماتية يأتي حرصاً من الحكومة على الارتقاء بالمستوى الرقابي واحتواء وتقويض جرائم المعلوماتية ونظم الحاسوب.

(٣٩) شبكة النّبأ المعلوماتية، جرائم الإنترنت ، وجه من وجوه الشر المتعددة ، مرجع سبق ذكره .

(٤٠) آخر ملتقى تمّ تنظيمه هو (الملتقى الدولي السادس لأمن المعلومات والاتصالات) خلال الفترة من ١١/١٠/٢٠١٠ - ١٣/١٠/٢٠١٠.

(٤١) 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، وقد تضمن القانون عقوبات صارمة تصل في بعض الحالات إلى الحبس ثلاث سنوات والغرامة إلى مليون ليرة ومضاعفة العقوبة في حال التكرار، انظر الباب السابع من القانون (المواد من ٢٤ إلى ٣٦).

(٤٢) شبكة النّبأ المعلوماتية، جرائم الإنترنت، وجه من وجوه الشر المتعددة، مرجع سبق ذكره.

(٤٣) الاتحاد الدولي للاتصالات، مرجع سبق ذكره، ص ٢١.

(٤٤) براء منذر كمال عبد اللطيف، ناظر أحمد منديل، التعاون القضائي الدولي في مواجهة جرائم الإنترنت، بحث مقدم إلى المؤتمر العلمي الأول لكلية القانون/ جامعة تكريت (تحولات القانون العام في مطلع الألفية الثالثة) ، ٢٠٠٩، ص ٢.

(٤٥) شائف علي محمد الشيباني، مرجع سبق ذكره، ص ٤.

(٤٦) نص قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ المعدل على الإنابة القضائية وتسليم المجرمين في المواد من ٣٥٢-٣٦٨، وحددت النصوص أنّ الإجراءات المتبعة في الإنابة القضائية وتسليم الأشخاص سواء كانوا من المتهمين الذين لم تزل قضاياهم قيد التحقيق أو المحكوم عليهم من الذين صدرت بحقهم أحكام من المحاكم العراقية إلى الدول الأجنبية يجب أن تراعى الأحكام والنصوص المذكورة في قضايا تسليمهم، والإنابة القضائية

فيما يخصهم، مع مراعاة أحكام المعاهدات والاتفاقيات الدولية وقواعد القانون الدولي العام، إضافة إلى مبدأ المعاملة بالمثل الذي يجب مراعاته والعمل بموجبه مع تلك الدول.

(٤٧) المادة ١٤ من اتفاقية الرياض للتعاون القضائي بين الدول العربية الموقعة عام ١٩٨٣.

(٤٨) المادة ٤٢ من اتفاقية الرياض للتعاون القضائي بين الدول العربية الموقعة عام ١٩٨٣.

(٤٩) البدايات الأولى للتعاون الدولي الشرطي ترجع إلى عام ١٩٠٤ عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ ١٨/٥/١٩٠٤، ولم تمر سنة على إبرام هذه الاتفاقية إلا وكانت سبع دول من الدول المتعاقدة تنشي مثل تلك الأجهزة وتتبادل من خلالها المعلومات والبيانات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج من أجل القضاء على هذه الجريمة في أقاليمها. بعد ذلك أخذ التعاون الشرطي الدولي يأخذ صورة المؤتمرات الدولية أولها وأسبقها تاريخياً كان مؤتمر موناكو (١٤-١٨/٤/١٩١٤) والذي ضم رجال الشرطة والقضاء والقانون من ١٤ دولة، وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية، خاصة ما يتعلق بمدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين، إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية تذكر. وبنهاية عام ١٩٢٣ نجح الدكتور (جوهانو سويرا) مدير شرطة فيينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية وذلك في الفترة ٣-٧/٩/١٩٢٣، ضم مندوبي تسعة عشر دولة وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية (International Criminal Police Commission (ICPO) يكون مقرها فيينا، وتعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة، إلا أن اندلاع الحرب العالمية الثانية أوقف اللجنة عن أعمالها، حتى وضعت الحرب أوزارها عام ١٩٤٦، حيث عقد في بروكسل في الفترة ٦-٩/٦/١٩٤٦ مؤتمر دولي بهدف إحياء مبادئ التعاون الأمني ووضعها موضع التنفيذ بدعوة من المفتش العام للشرطة البلجيكية (Louvage)، وانتهى الاجتماع إلى إحياء اللجنة الدولية للشرطة الجنائية (ICPO) ونقل مقرها إلى باريس، وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية (International Criminal Police Organization (Interpol). وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة، من تجميع 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، ومدّها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت.

(٥٠) عبود السراج، استرداد وتسليم المجرمين شروطه وإجراءاته وآثاره في القانون السوري، مقالة منشورة على الرابط التالي:

<http://law-uni.net/la/showthread.php?t=32461>

(٥١) 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 .

(٥٢) حسين بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص ٢١.

(٥٣) حسين بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص ٢٣.

(٥٤) جميل عبد الباقي الصغير ، الانترنت والقانون الجنائي ، الانترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، ٢٠٠٢ ، ص ٧٢ .

(٥٥) حسين بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت ، مرجع سبق ذكره ، ص ٢٥ .

(٥٦) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٧٣ .

(٥٧) 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.

(٥٨) كان لموقع التواصل الاجتماعي (الفيسبوك) دور كبير في الثورات العربية حيث وصل

عدد المشتركين الجدد في الفيسبوك خلال عام ٢٠١٠ إلى ٢٥٠ مليون شخص وإجمالي عددا

لمشتركين في الموقع هو ٥٠٠ مليون شخص، ٧٠% من مستخدمي الفيسبوك هم من خارج

الولايات المتحدة الأمريكية، تعتبر مصر هي الأولى في الشرق الأوسط استخداماً للفيسبوك،

كان عدد مستخدمي الفيسبوك قبل ثورة ٢٥ كانون الأول/يناير ٤.٢ مليون شخص، لكنه ارتفع

٢٣.٨ بالمئة بعد الثورة إلى ٥.٢ مليون. أما بقية الدول العربية الأخرى فلا تقل عن مصر في

زيادة نسبة الإقبال على استخدام الإنترنت فيها، إذ بلغ عدد مستخدمي الإنترنت في السعودية ٩.٨٠٠.٠٠٠ مستخدم أي ٣٨.١% من تعداد السكان، وفي الجزائر بلغ عدد مستخدمي الإنترنت ٤.٧٠٠.٠٠٠ مستخدم أي ١٣.٦% من تعداد السكان، وفي سوريا بلغ عدد مستخدمي الإنترنت ٣.٩٣٥.٠٠٠ مستخدم أي ١٧.٧% من تعداد السكان، وفي تونس بلغ عدد مستخدمي الإنترنت ٣.٦٠٠.٠٠٠ مستخدم أي ٣٤.٠% من تعداد السكان.

(٥٩) سفيان الرامي، الثورات العربية وسوسيولوجيا الإنترنت، تقرير لقناة فرانس ٢٤ بتاريخ ٢٠١١/٧/١٣، متوفر على الرابط التالي:

<http://www.france24.com/ar/20110713-arabic-egypt-syria-internet-facebook-twitter-tunisie-protests-sociology>

(٦٠) بتاريخ ٢١ حزيران/يونيو ٢٠١١ أصدر اتحاد كتاب الإنترنت العرب بياناً حياً فيه الثورات والحركات الاحتجاجية في الدول العربية وأكد تضامنه مع الثوار ومشروعهم الوطني من أجل القضاء على الأنظمة الدكتاتورية وبناء أوطان تتسع لمفاهيم الديمقراطية وحقوق الإنسان وحرية التعبير والتوزيع العادل للثروات، ودعا الاتحاد المثقفين والكتاب العرب إلى استثمار الوسائط الجديدة من أجل فضح الجرائم والمجازر التي ترتكب في حق الشعوب العربية في البلدان التي شهدت حركات احتجاجية.

(٦١) باسم الجسر، الثورات العربية في عصر العولمة والإنترنت، مقالة منشورة في صحيفة الشرق الأوسط، العدد ١١٨١٩، تاريخ ٨ نيسان/أبريل ٢٠١١.

(٦٢) 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.

(٦٣) حسين بن سعيد الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص ٢٧.

(٦٤) حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الإنترنت، مرجع سبق ذكره، ص ١٢-١٣.

(٦٥) المرجع السابق، ص ١٧.

(المصادر)

١. الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية، وحدة الاستراتيجيات الإلكترونية، سويسرا، جنيف، ٢٠٠٦.
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.
٣. الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا، منشورات الأمم المتحدة، نيويورك، رقم الوثيقة E/ESCWA/ICTD/2008/8 تاريخ ٢٧ حزيران/يونيو ٢٠٠٧.
٤. براء منذر كمال عبداللطيف، ناظر أحمد منديل، التعاون القضائي الدولي في مواجهة جرائم الإنترنت، بحث مقدم إلى المؤتمر العلمي الأول لكلية القانون/ جامعة تكريت (تحولات القانون العام في مطلع الألفية الثالثة) ٢٠٠٩.
٥. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١.
٦. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، ٢٠٠٢.
٧. حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الإنترنت، بحث منشور على شبكة الإنترنت من خلال الموقع www.eastlaws.com.
٨. 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).
٩. دانيال لاركين، محاربة جرائم الإنترنت، مقالة منشورة بتاريخ ١٧ أيار/مايو ٢٠٠٨، متوفرة على الرابط التالي:
<http://www.america.gov/st/democracyarabic/2008/May/20081117124454snmassabla0.2601086.html>
١٠. سليمان بن مهجع العنزي ، وسائل التحقيق في نظم المعلومات ، رسالة ماجستير في العلوم الشرطية كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ٢٠٠٣.
١١. شائف علي محمد الشيباني، الإنابة القضائية الدولية في القانون اليمني (دراسة مقارنة) ، دائرة التدريب والتأهيل في مكتب النائب العام اليمني، ٢٠٠٦.
١٢. شبكة النبا المعلوماتية، جرائم الإنترنت، وجه من وجوه الشر المتعددة، دراسة منشورة بتاريخ ٢٢ أيار/ ٢٠٠٨ متوفرة على الرابط التالي

<http://www.annabaa.org/nbanews/70/260.htm>

١٣. شيماء عبدالغني محمد عطاالله ، 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>

١٤. صالح أحمد البربري، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية الموقعة في بودابست في ٢٣/١١/٢٠٠١، الدليل الإلكتروني للقانون العربي.

١٥. 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 ١/١١/١٤٢٣ هـ .

١٦. عبد الرحمن بحر ، معوقات التحقيق في جرائم الإنترنت ، دراسة مسحية على ضباط الشرطة بدولة البحرين ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، ١٩٩٩ .

١٧. عبود السراج، استرداد وتسليم المجرمين شروطه وإجراءاته وأثاره في القانون السوري، مقالة

منشورة على الرابط التالي: <http://law-uni.net/la/showthread.php?t=32461>

١٨. مجلس أوروبا، سلسلة المعاهدات الأوروبية، رقم ١٨٩، البروتوكول الإضافي لاتفاقية

الجريمة الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكرهية الأجانب التي

ترتكب عن طريق أنظمة الكمبيوتر، ستراسبورغ، ٢٨/١/٢٠٠٣.

١٩. مجلس أوروبا، سلسلة المعاهدات الأوروبية، رقم ١٨٥، الاتفاقية المتعلقة بالجريمة

الإلكترونية، بودابست، ٢٣/١١/٢٠٠١.

٢٠. محسن العبودي، المواجهة الأمنية لجرائم الإنترنت، دراسة منشورة على شبكة الإنترنت من

خلال الموقع www.eastlaws.com.

٢١. محمد صالح الألفي، أنماط جرائم الإنترنت، دراسة منشورة على شبكة الإنترنت من

خلال الموقع www.eastlaws.com.

٢٢. 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>

٢٣. 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 .