المسئولية الجنائية لوسطاء تقديم خدمات شبكة الإنترنت

محمد نصر*

مُنذ بدايات القرن الجديد ومع تزايد الاهتمام بالمعلوماتية، أطلق على العصر الراهن (العصر الرقمى)، ثار الجدل حول المركز القانونى لمقدمى الخدمات، ودورهم فى الوصول الأمثل لاستخدام الشبكة، وبخاصة أنهم المنوط بهم إما فتح نطاقات على شبكة المعلومات، أو مقدمى خدمات معلوماتية من خلال الشبكة، أو خالقين بيئة للتواصل الاجتماعى، وتذرَّع مقدمو الخدمات كثيرًا من أجل التخفيف من الالتزامات التى ألقاها القضاء- فى بداياته- على عاتقهم، وضغطوا، فى نفس الوقت، لإرساء نظامٍ خاصٍّ يُعفيهم من المسئولية، سواء عن إخلالهم بتقديم الخدمة أو عن عدم مشروعيَّة المضمون المعلوماتى المتداول عبر أجهزتهم، الأمر الذى أثار الكثير من الإشكاليات القانونية والفنية، تدخَّلت التشريعات المعاصرة، كالتشريعين الأوروبى والفرنسى، لحسم الجدل، ولوضعِ نظامٍ قانونىٍّ خاصٍّ بمقدمى خدمات الإنترنت، فحدَّدت، من خلاله بدقَّة، الالتزامات الملقاة على عاتقهم، والأحكام الخاصة بمسئوليتهم عمَّا يحدث من مخالفات عبر الشبكة[1].

ولاشك ان البلدان العربية، أضحت هدفا، كما أن تأثيرات تلك الأفعال غير المشروعة فاقت كل التصورات، كما كان لها أكبر الأثر على منظومة الاقتصاد، فثار التساؤل الهام حول مدى جدوى إعمال القواعد العامة، لإيجاد حلول متوازنة تتفق مع الطبيعة الخاصة لآلية عمل مقدمى خدمات الإنترنت.

مقدمة

مع نهايات القرن العشرين شهد العالم، وبشكل لم يسبق له مثيل، تطورًا هائلًا ومتسارعًا فى عالم الاتصالات وتكنولوجيا المعلومات، ونتيجة لهذه التطورات التكنولوجية وما صاحبها من تقدم فى صناعة الحاسبات الآلية، بدا العالم كقرية

* أستاذ القانون الجنائى المساعد، جامعة دار العلوم، المملكة العربية السعودية.

صغيرة ذابت فيه الحواجز، فتداخل وتشابك وارتبط سكانه بشبكة عنكبوتية عالمية يسبح فيها الجميع بحريَّة، فإذا بها ثورة المعلوماتية، انعكس آثارها على كافة الأصعدة والميادين ومنها الثقافية، والاقتصادية، والاجتماعية....[٢].

وأمام هذا التقدم العلمى والتكنولوجى، وفى ظلِّ غزوِ شبكة الإنترنت لكل مناحى الحياة، ولاشك أن ذلك كان له أكبر الأثر، وبخاصة ما حدث مؤخرا من أنه كان البيئة التى أثمرت هذا الربيع العربى، وبزغت بوادر الخير لفتحِ آفاقٍ جديدة لتقدم البشريَّة ولجنى ثمار التواصل والمعرفة، إلاَّ أنه، ظهرت فى نفس الوقت نوازع الشر لاستغلال هذا التقدم لتحقيق أغراضٍ شخصية على حساب قيم المجتمع[٣]، وحقوق الأفراد والجماعة وأمنهم، فما كان من أصحاب النفوس الضعيفة، أو من عصابات الجريمة المنظمة، أو من يستتر من خلالها لتحقيق أغراض مختلفة منها، ما هو سياسى أو أخلاقى..، إلاَّ أنهم تجرَّؤوا على استغلال شبكة الإنترنت فحولها إلى مسرحٍ يرتكبون فيه العديد من الجرائم والمخالفات: فقاموا بنشر الأخبار المزيَّفة[٤]، وبثوا الأفكار والممارسات المناهضة للأديان السماوية وللإنسانية، ونشروا الصور الفاضحة للصغار قبل الكبار، وانتهكوا حرمة الحياة الخاصة لأفراد المجتمع، وحملوا أو شهروا بالأشخاص أو قذفهوهم، وتعدُّوا على حقوق الملكية الفكرية... وما هذه إلاَّ نماذج من سلسلة مخالفات تُرتكب عبر الإنترنت يصعب حصرها.

أهمية البحث

يُثبت الواقع العملى أن تداول المعلومات عبر شبكة الإنترنت بحاجة إلى تظافر جهود الأشخاص القائمين على إدارتها[٥]، والذين تتنوَّع أدوارهم وأنشطتهم فى تشغيلها، فحتى يتمكن مستخدمو الإنترنت من الدخول إلى الشبكة، والإبحار فيها بحرِّية، والوصول إلى ما يصبون إليه من معلومات أو بثِّها، لا بُدَّ من وجود عدَّة أشخاص أو وسطاء، يُطلق عليهم عادةً مصطلح "مقدمى خدمات الإنترنت"، أو "الوسطاء فى خدمات

الإنترنت"، يتولُّون عملية إيواء المعلومات، وبثِّها، وعرضها[٦]، وهذا التنوُّع فى أدوارهم والتعدُّد فى أنشطتهم يجعل من اليسير عليهم تتبُّع النشاط المعلوماتى غير المشروع وكشفه، وبخاصة أنهم القائمون على إدارة ما يحدث من خلال المجال المتاح لجمهور المتعاملين، كما أن لديهم فى أحيان كثيرة القدرة على التعرض للخصوصية لطالبى الخدمة، إلاَّ أن تحقيق ذلك يبقى رهن وجود ضوابط قانونية تُحدِّد حقوق أطراف النشاط الإلكترونى والتزاماته فى مواجهة بعضهم البعض من جهة، وفى مواجهة المجتمع الذى يعيشون فيه من جهةٍ أُخرى، لذا بدت الحاجة ماسة لإيجاد تنظيم تشريعى متكامل يُحدد المركز القانونى لمقدمى خدمات الإنترنت، ويُبين فى نفس الوقت مسئولية كلٍّ منهم عمّا يُرتكب من مخالفات عبر الشبكة، الأمر الذى لا يُمكن تحقيقه إلا بتظافر جهود المشرِّعين على الصعيدين: الوطنى والدولى، وبخاصة فى عدم وجود جهة مرجعية لما يتم من خلال الشبكة المعلوماتية ككل.

ومن خلال التعرض لتوجهات البرلمان الأُوروبى الذى تبنَّى بالإجماع فى ٨ يونيو ٢٠٠٠م التوجيه رقم ٢٠٠٠/٣١، والمتعلِّق "ببعض الأوجه القانونية لخدمات شركات المعلومات، وبصفةٍ خاصَّة التجارة الإلكترونية، فى السوق الداخلى"[٧]، والذى تمَّ تخصيص القسم الرابع منه لتنظيم المركز القانونى للوسطاء فى خدمات الإنترنت، وذلك على غرار القانون الأمريكى الصادر فى ٢٨ أكتوبر ١٩٩٨م للحد من الاعتداءات على حقوق الملكية الفكرية فى نطاق الإنترنت والمسمَّى بـ Digital Millenium Copyright Act (DMCA)[٨]، والذى خصص الباب الثانى منه لتحديد مسئولية مقدمى خدمات الإنترنت عن التعدى على هذه الحقوق، وقد جاءت المادة (٢٢) من التوجيه الأُوروبى لتلزم الدول الأعضاء فى الإتِّحاد الأُوروبى على نقل أحكامه إلى تشريعاتهم الداخلية بحلول ١٧ يناير ٢٠٠٢. والتزامًا منها بذلك قدَّمت الحكومة الفرنسية فى ١٤ يونيو ٢٠٠١، كمحاولةٍ أُولى، مشروع قانونٍ حول "شركات المعلوماتية"، والذى حدَّدت فى قسمٍ منه المركز القانونى لمزودى خدمات

الإنترنت، إلا أن هذا المشروع أضحى لاغيًا بتغيُّر المشرِّع[٩]، فجاءت الحكومة الفرنسية من جديد فى ١٥ يناير ٢٠٠٣ بمشروع قانونٍ حول "الثقة فى الاقتصاد الرقمى"، والذى تمَّ الموافقة عليه من قِبل المشرِّع الفرنسى فى ٢١ يونيو ٢٠٠٤[١٠]، واعتبارا من هذا التاريخ أصبح لمقدمى خدمات الإنترنت فى فرنسا نظامهم القانونى الخاص.

مشكلة البحث

مع التقدم التكنولوجى الهائل، وتقدم تقنية الاتصالات، واكب ذلك زيادة تغيرات فى نشاطات العناصر الإجرامية، ولكن هناك تشابهًا بين الجريمة الإلكترونية مع الجريمة التقليدية فى أطراف الجريمة من مجرم ذى دافع لارتكاب الجريمة وضحية والذى قد يكون شخص طبيعى أو شخص اعتبارى وأداة ومكان الجريمة، وهنا يكمن الاختلاف الحقيقى بين نوعى الجريمة ففى الجريمة الإلكترونية الأداة ذات تقنية عالية وأيضا مكان الجريمة الذى لا يتطلب انتقال الجانى إليه انتقالا ماديا (إستاتيكيا) ولكن فى الكثير من تلك الجرائم فان الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجانى ومكان الجريمة، كما أن أدلة ثبوتها تحتاج إلى تحليل خاص، كما أنها تتميز بسهولة إخفاء معالمها.

هذا وتشير مجلة لوس انجلوس تايمز فى عددها الصادر فى ٢٢ مارس عام ٢٠٠٠ إلى أن خسارة الشركات الأميريكية وحدها من جراء الممارسات التى تتعرض لها والتى تندرج تحت بند الجريمة الإلكترونية بحوالى ١٠ مليارات دولار سنويا، وللتأكيد على جانب قد تغفله الكثير من مؤسسات الأعمال فإن نسبة ٦٢٪ من تلك الجرائم تحدث من خارج المؤسسة وعن طريق شبكة الإنترنت بينما تشكل النسبة الباقية (٣٨٪) من تلك الخسائر من ممارسات تحدث من داخل المؤسسات ذاتها.

مثال آخر حديث قد لا يتوقع أحد كم الخسائر الناجمة عنه وهو تلك الأعطال والخسائر فى البرامج والتطبيقات والملفات ونظم العمل الآلية وسرعة وكفاءة شبكات الاتصال والذى ينجم عن التعرض للفيروسات والديدان مثل ذلك الهجوم الأخير والذى تعرضت له الحواسب الآلية المتصلة بشبكة الإنترنت فى أغلب دول العالم من خلال فيروس يدعى (WS32.SOBIG) والذى أصاب تلك الأجهزة من خلال رسائل البريد الإلكترونى بصورة ذكية للغاية، حيث كان ذلك الفيروس يتخفى فى الوثيقة الملحقة بالبريد الإلكترونى (Attachment File) فى صورة ملف ذى اسم براق وعند محاولة فتح ذلك الملف فإن الفيروس ينشط ويصيب جهاز الحاسب ويبدأ فى إرسال المئات من رسائل البريد الإلكترونى من ذلك الجهاز المصاب مستخدما كل أسماء حسابات البريد الإلكترونى المخزنة عليه، الأمر الذى أدى إلى إصابة عدد هائل من الحواسب الشخصية للأفراد والشركات وملء خوادم البريد الإلكترونى بتلك الرسائل مثال على ذلك إصابة خوادم البريد الإلكترونى لشركة أميركا اون لاين بما يقارب ال ٢٠ مليون رسالة ملوثة وأدى ذلك أيضا إلى بطء شبكات وخطوط الاتصال[١١] بصورة كبيرة وأحيانا بالشلل التام، مما أدى لتعطل الكثير من الأعمال وتلف العديد من الملفات المهمة على تلك الحواسب وقد قدرت الخسائر الناجمة عن ذلك الفيروس بما يقارب ال ٥٠ مليون دولار أميريكى فى داخل الولايات المتحدة الأميريكية وحدها[١٢].

ومن الجرائم الأخرى ذات التأثيرات المختلفة سرقة بيانات بطاقات الائتمان الشخصية والدخول على الحسابات البنكية وتعديلها وسرقة الأسرار الشخصية والعملية الموجودة بصورة الكترونية وأيضا الدخول على المواقع وقواعد البيانات وتغيير أو سرقة[١٣] محتوياتها وأيضا بث الأفكار الهدامة أو المضادة لجماعات أو حكومات بعينها وأيضا السب والقذف والتشهير بالشخصيات العادية والعامة ورموز الدين والسياسة وخلافه.

وبالنظر فى نطاق القانون الجنائى، يعرف اتجاه فى الفقه[١٤] الجريمة "بأنها فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيرًا احترازيًا".

أما بالنسبة لجرائم الكمبيوتر (الحواسيب) والإنترنت، فقد تعددت التعريفات وفقا لمعايير متعددة سواء أكانت وفقا لمعيار شخصى من حيث توفر المعرفة والدراية بالتقنية أو وفقا لمعيار موضوع الجريمة، والمعايير المتعلقة بالبيئة المرتكب فيها الجريمة، وغيرها. ونلاحظ أن هذه الجرائم كانت تستهدف أنظمة بعينها، وصحيح أن ذلك يتم من خلال بيئة الشبكة المعلوماتية ككل، ولكن ما نرمى إليه بشكل جزئى لتحديد المسئولية الجنائية للوسطاء ومقدمى الخدمة، قاصرين ذلك على النطاق المعلوماتى الخاص بكل منهم، حتى نصل إلى إيجاد مرجعية عامة للشبكة المعلوماتية ككل.

وسنعرض لموقف الفقه الجنائى من تحديد لماهية العمل الغير المشروع والذى يتخذ البيئة المعلوماتية لتحقيق أهدافه.

فقد عرفتها الدكتورة هدى قشقوش بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[١٥]، وعرفها الأستاذ Rosenblatt بأنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التى تحول عن طريقه "، كما عرفها الفقيه Artar Solarz بأنها " أى نمط من أنماط الجرائم المعروف فى قانون العقوبات طالما كان مرتبط بتقنية المعلومات ". كذلك عرفها الأستاذ Eslie D.Ball بأنها " فعل إجرامى يستخدم الكمبيوتر فى ارتكابه كأداة رئيسية "، كما عرفتها وزارة العدل الأمريكية بأنها "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها"[١٦]، ويعرفها Sheldon بأنها "واقعة تتضمن تقنية الحاسب ومجنى عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب".

كما يعرفها خبراء منظمة التعاون الاقتصادn والتنمية OECD بأنها "كل سلوك غير مشروع أو غير أخلاقى أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها". ويعرفها الفقيه الفرنسى Vivant بأنها "مجموعة من الأفعال المرتبطة بالمعلوماتية والتى يمكن أن تكون جديرة بالعقاب[١٧]".

كما يعرفها الأستاذان Robert J.Lindquist، Jack Bologna بأنها "جريمة يستخدم فيها الحاسوب كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها".

أنواع الجريمة الإلكترونية

أولا: الجرائم التى تتم ضد الحواسب الآلية و نظم المعلومات[١٨]

١ – جرائم الإضرار بالبيانات

يعتبر هذا الفرع من الجرائم الإلكترونية من أشدها خطورة وتأثيرا وأكثرها حدوثا وتحقيقا للخسائر للأفراد والمؤسسات، ويشمل هذا الفرع كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة إلكترونية (Digital Form) على الحواسب الآلية المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها.

أبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أى تأثير سلبى عليها[١٩]، ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون ذوى القبعات البيضاء (White Hat Hackers)[٢٠] الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الإنترنت مستغلين بعض الثغرات فى تلك النظم مخترقين بذلك كل سياسات وإجراءات امن المعلومات التى يقوم بها مديرو تلك الأنظمة والشبكات (System and Network Administrators) ونتيجة عدم ارتباط ذلك النشاط بالشبكات

فاختراق الأمن بطريق مادى للاماكن التى توجد بها أجهزة الحاسب التى تحتوى على بيانات مهمة بالرغم من وجود إجراءات أمنية لمنع الوصول إليها وبمعنى آخر وصول شخص غير مصرح له وإمكانية دخوله إلى حجرة الحواسب المركزية بالمؤسسة ثم خروجه دون إحداث أى أضرار فإنه يعتبر خرقا لسياسة وإجراءات أمن المعلومات بتلك المؤسسة، ولا تعد الأخيرة تمثل صعوبة فى التحقق منها[٢١].

استخدام الشبكات وبصفة خاصة شبكة الإنترنت فى الدخول على قواعد البيانات أو مواقع الإنترنت والحصول على معلومات غير مسموح بها أو إمكانية السيطرة التامة على تلك الأنظمة بالرغم من وجود إجراءات حماية متعددة الدرجات من الحوائط النارية وأنظمة كشف ومنع الاختراق بالإضافة لآليات تشفير البيانات وكلمات السر المعقدة وبتخطى كل تلك الحواجز والدخول على الأنظمة المعلومات ثم الخروج دون إحداث أى تغيير أو إتلاف بها فإنه أبسط أنواع الاختراق الذى يعطى الإشارة الحمراء لمديرى النظم وأمن المعلومات بأن سياساتهم وإجراءاتهم التنفيذية لأمن المعلومات بحاجة إلى التعديل والتغيير وأنه يتعين عليهم البدء مرة أخرى فى عمل اختبار وتحليل للتهديدات ونقاط الضعف الموجودة بأنظمتهم (Risk Assessment) لإعادة بناء النظام الأمنى مرة أخرى وأيضا العمل على إجراء ذلك الاختبار بصورة دورية لمواكبة الأساليب الجديدة فى الاختراق.

أما بالنسبة إلى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل لنظم المعلومات فإن تلك الأنشطة تتم بواسطة أفراد هواه أو محترفين يطلق عليهم المخترقون ذوو القبعات السوداء (Black Hat Hackers) الذين قد يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانات والمعلومات التى يقومون بالاستيلاء عليها أو بغرض الإضرار بالجهة صاحبة تلك الأنظمة لوجود كره شخصى أو قبلى أو سياسى أو دينى أو القيام بذلك لحساب إحدى المؤسسات المنافسة مثال على ذلك ما ذكره مكتب التحقيقات الفيدرالية الأميريكى (FBI) فى السادس والعشرين

من سبتمبر عام ٢٠٠٢ من القبض على أحد عملائها ويدعى ماريو كاستللو ٣٦ عاما ومحاكمته بتهمة تخطى الحاجز الأمنى المسموح له به والدخول على أحد أجهزة المكتب ست مرات بغرض الحصول على بعض الأموال[٢٢]. فى التقرير السنوى الثامن لمكتب التحقيقات الفيدرالية الأميريكى الصادر عام ٢٠٠٣ بعنوان جرائم الحاسب فإن أكثر خسائر المؤسسات بالولايات المتحدة الأميريكية تأتى من الاستيلاء على المعلومات والتى تكبدتها خلال هذا العام خسائر تتعدى السبعين مليون دولار أميريكى ويأتى فى المركز الثانى نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز الخمسة وستين ونصف مليون دولار[٢٣].

تعطيل العمل والذى يطلق عليه ال (Denial of Service Attack) واختصارًا ال (Dos) والذى يعتمد على إغراق أجهزة الخوادم بالآف أو ملايين طلبات الحصول على معلومات، الأمر الذى لا تحتمله قدرة المكونات المادية (Hardware) أو نظم قواعد البيانات والتطبيقات والبرامج موجودة على تلك الخوادم التى تصاب بالشلل التام لعدم قدرتها على تلبية هذا الكم الهائل من الطلبات والتعامل معها، ويحتاج الأمر إلى ساعات عديدة حتى يتمكن مديرى النظم والشبكات للتعرف على مصادر الهجوم وعيوب النظم لديهم واستعادة العمل بصورة طبيعية، وبالطبع فإن هذه الساعات التى يكون فيها نظام المعلومات متعطلًا تكبد المؤسسة الخسائر المادية الجسيمة فضلا عن تعطيل مصالح المتعاملين مع تلك الأنظمة وفقدانهم الثقة فى تلك المؤسسة وهروب العملاء منها إلى مؤسسات منافسة كلما أمكن ذلك.

من صور الاعتداء الأخرى التى تمثل اعتداء على الملكية الفكرية للأسماء ما يحدث من اعتداءات على أسماء مواقع الإنترنت (Domain Names) حيث إن القاعدة العالمية فى تسجيل أسماء النطاقات (والتى تتم أيضا باستخدام بطاقات الائتمان من خلال شبكة الإنترنت)[٢٤] هى أن التسجيل بالأسبقية وليس بالأحقية (First Come First Served)، الأمر الذى

أحدث الكثير من المخالفات التى يتم تصعيدها إلى القضاء وبتدخل من منظمة الايكان التى تقوم بتخصيص عناوين وأسماء المواقع على شبكة الإنترنت ((ICANN) (Internet Corporation for Assigned Names and Numbers)) وذلك من أجل التنازل عن النطاق للجهة صاحبة الحق مع توقيع العقوبة أو الغرامة المناسبة.

يحدث أيضا فى تسجيل النطاقات عبر الإنترنت والتى يتم تسجيلها لمدد تتراوح من عام إلى تسعة أعوام أن لا تنتبه الجهة التى قامت بالتسجيل إلى انتهاء فترة تسجيل النطاق ووجوب التجديد، حيث توجد شركات يطلق عليها صائدو النطاقات[٢٥] (Domain Hunters) تقوم بتجديد النطاق لها ومساومة الشركة الأصلية فى التنازل عليه نظير آلاف الدولارات مستغلة اعتماد الشركة على هذا الاسم ومعرفة العملاء به لمدد طويلة هذا فضلا عن الحملات الدعائية له وكم المطبوعات الورقية التى أصدرتها الشركة وتحمل ذلك العنوان[٢٦]. من الجرائم الأخرى المتعلقة بأسماء النطاقات على شبكة الإنترنت ما يعرف بإعادة التوجيه (Redirection)، مثلما حدث لموقع شركة Nike فى شهر يونيو عام ٢٠٠٠، حيث قامت جماعة من المحترفين بالدخول على موقع شركة تسجيل النطاقات الشهيرة والمعروفة باسم (Network Solutions) وتغيير بيانات النطاق لضعف إجراءات أمن المعلومات بالشركة فى ذلك الحين وبذلك تم إعادة توجيه مستخدمى الإنترنت إلى موقع لشركة إنترنت فى اسكوتلاندا[٢٧]. أيضا قامت إحدى الجماعات بعمل موقع على شبكة الإنترنت تحت عنوان (http://www.gatt.org) مستخدمة شكل وتصميم الموقع الخاص بمنظمة التجارة العالمية (World Trade Organization) والذى يظهر كخامس نتيجة فى أغلب محركات البحث عن ال WTO وقد استخدمته للحصول على بيانات البريد الإلكترونى وباقى بيانات مستخدمى الإنترنت الذين كانوا فى الأصل يبغون زيارة موقع منظمة التجارة العالمية ومازالت القضية معلقة حتى الآن مع

المنظمـــة الدوليـــة لحمايـــة حقـوق الملكية الفكرية (World Intellectual Property Organization).

مشكلة البحث

حين يسعى المرء إلى جمع أدلة تتصل بجريمة ارتكبت مؤخرًا، وتصبح المهمة بالغة الصعوبة حين تتجاوز الواقعة أو الاختراق... إلخ، النطاق المكانى للولاية القضائية، كما تدعو الحاجة إلى وسائل متعددة ذات نظم مختلفة فى حفظ الأدلة، وهكذا لم تعد تكفى الوسائل التقليدية لإنفاذ القانون، كما أن بيئة التواصل الاجتماعى تسهم بشكل غير مباشر – مقدمى الخدمات الإلكترونية على الشبكة المعلوماتية– فى استخدامها فى بعض الجرائم المعلوماتية(٢٨).

إن بطء الإجراءات وعدم تحديدها، وكذا إيلاء جهة معينة السلطة أو مكنة الإدارة الرسمية لحفظ الأدلة الجنائية يجازف بفقدان الأدلة، وقد تكون بلدان متعددة متورطة فى الأمر، ولذا تشكل متابعة وحفظ سلسلة الأدلة تحديًا كبيرًا، بل حتى الجرائم "المحلية" قد يكون لها بعد دولى، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التى مرت الهجمة من خلالها(٢٩).

وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السلطات فى البلد الذى كان منشأ الجريمة، أو من السلطات فى البلد أو البلدان التى عبر من خلالها النشاط المجرَّم وهو فى طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، وهناك عنصران أساسيان للتعاون: المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة.

ولاشك أن أول الحلقات التى ينبغى غلقها، والمتمثلة فى نوادى الكومبيوتر، ومن خلال المنتديات، وعبر شبكات التواصل(٣٠).

وقد تكون المساعدة غير الرسمية أسرع إنجازًا، وهى الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أى أوامر تفتيش أو طلب تسليم المجرم). وهى تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية،

وتولد نتيجة الاتصالات التى جرت مع الوقت فى مسار المؤتمرات وزيارات المجاملة والتحقيقات المشتركة السابقة.

ومن ناحية أخرى فإن المساعدة الرسمية المتبادلة هى عملية أكثر إرهاقًا يتم اللجوء إليها عادة عملًا بترتيبات معاهدات بين البلدان المعنية وتشمل تبادل الوثائق الرسمية، وهى تشترط فى الغالب الأعم أن تكون الجريمة المعنية على درجة معينة من القسوة وأن تشكل جريمة فى كل من البلدان الطالبة والموجه إليها الطلب. ويشار إلى هذا الأمر الأخير باعتباره "تجريمًا مزدوجًا[٣١]".

منهج البحث

اعتمد البحث على المنهج الاستقرائى التحليلى، حيث إن جرائم المعلوماتية تتميز بالتطور الدائب والدائم، وبالرغم من الاهتمام المتزايد بها فإن التطور وإن كان محط اهتمام الباحثين، إلا أن تطبيقاته العملية محدودة، وبخاصة فى مجال العمل الشرطى والقضائى، ولاشك أن تحليل الأطر القانونية أو إيجاد عوامل أخرى مساعدة قد يكون له أبلغ الأثر فى الحد من تلك الجرائم[٣٢].

خطة البحث

وقد تعرضنا للمسئولية المفترضة لوسطاء تقديم خدمات الإنترنت والتزامهم بتحمل التبعة من خلال المحور الأول المسئولية المفترضة، ثم تعرضت للآلية الإجرائية لضبط الجريمة المعلوماتية من خلال المحور الثانى، ثم للتعاون الدولى من خلال المحور الثالث.

المحور الأول: المسئولية المفترضة

قد تنشأ المسئولية الجنائية نتيجة إسناد فعل ما لشخص، وقد تنشأ المسئولية الجنائية لأسباب أخرى، تتمثل فى الالتزام القانونى بتحمل التبعة فهى تنشأ تابعة لالتزام آخر وهو فى حقيقته واجب أصلى(٣٣).

فللمسئولية الجنائية ركنان أساسيان الأول هو الرابطة المادية بين الواقعة والنشاط المادى أى الإسناد المادى من جهة، والثانى هو الرابطة المعنوية بين الشخص والسلوك، فإذا كانت القاعدة العامة فى أساس المسئولية الجنائية شخصية، وكان كل إنسان لا يسأل إلا عن أعماله وسلوكه، فإن المشرع المصرى أسوة بغيره من مشرعى الأنظمة المقارنة، خرج عن هذه القاعدة وأخذ بالمسئولية الجنائية عن الغير فى مجال النشر فأخذ بالمسئولية الجنائية المفترضة على أساس تضامنى يتمثل فى افتراض علم رئيس التحرير بالمضمون المنشور فى الصحيفة واعتباره الفاعل الأصلى فى الجرائم المرتكبة بواسطة النشر، وهى المسئولية الجنائية المفترضة على أساس تضامنى استناد إلى علم رئيس التحرير بالمضمون المنشور فى الصحيفة واعتباره الفاعل الأصلى وكل من يسهم فيها بعد فاعلا أو شريكا حسب القواعد العامة بحيث لا يسأل شخص بينهم ما دام يوجد من قدمه عليه القانون فى ترتيب المسئولية الجنائية وهى ما تسمى بالمسئولية المتتابعة أو المسئولية المفترضة أو المسئولية الموضوعية...إلخ(٣٤).

وإن كان هناك اتجاه فى الفقه يسعى إلى إحلال الغرامات المالية كعقوبة أصلية بدلا عن العقوبات السالبة للحرية، وهو اتجاه محل نظر، لأننا لو استعرضنا الآثار السلبية التى ستلحق المجنى عليه سيفوق بكثير، أى غرامات مالية، مالم يطبق المشرع المسئولية الجنائية للشخص المعنوى.

ففكرة المسئولية المفترضة تقوم على ترتيب الأشخاص المسئولين جنائيا وحصرهم بحيث لا يسأل واحد منهم إلا إذا لم يوجد غيره ممن قدمه القانون عليه فى

الترتيب حتى نصل إلى دار النشر أو الطباعة وهو ما نص عليه المشرع المصرى[٣٥] فى المادة ١٧٨ مكررًا (١) إذا ارتكب الجرائم المنصوص عليها فى المادة السابقة عن طريق الصحف يكون رؤساء التحرير والناشرون مسئولين كفاعلين أصليين بمجرد النشر.

وفى جميع الأحوال التى لا يمكن فيها معرفة مرتكب الجريمة يعاقب بصفتهم فاعلين أصليين الطابعون والعارضون والموزعون.

ويجوز معاقبة المستوردين والمصدرين والوسطاء بصفتهم فاعلين أصلين إذا أسهموا عمدًا فى ارتكاب الجنح المنصوص عليها فى المادة السابقة متى وقعت بطريقة الصحافة[٣٦].

والسؤال المطروح فى هذا الصدد هو عن نوع المسئولية الجنائية لوسطاء تقديم خدمات شبكة الإنترنت فإذا كانت شبكة الإنترنت وسيلة من وسائل النشر والعلانية، مما لا تثور معه صعوبة فى إمكانية تطبيق الأحكام القانونية لجرائم السب والتشهير، فإن الجدل القانونى يثور بالنسبة لتحديد المسئولين جنائيا عن السلوك المرتكب فى الفضاء الإلكترونى وحصر المساهمين فيه، فمن هم الأشخاص القائمين على تشغيل الشبكة وخدماتها المتعددة؟ وبخاصة أن المشرع المصرى والعربى نص فقط على النشر بواسطة الصحف.

أصبحت الشبكة العالمية اليوم تضم مجموعة من الأنشطة والخدمات المختلفة فهى بنية تحتية للاتصالات أهم خدماتها البريد الإلكترونى e- mail والمنتديات News Group والناقل Transfere Protocol FTB لنقل الملفات بين أرجاء الشبكة ووسيلة المتصل Telnet وهو البرنامج الذى يتيح لأى شخص استخدام برامج ومميزات حاسوبية موجودة فى جهاز آخر بعيد ولا توجد فى جهاز المستخدم، أما شبكة المعلومات www فهى إحدى خدمات الشبكة من صفحات مصححة بلغة Html التى

تتيح إمكانية ربط الصفحات بالوسائط (Links) وهو سر تسميتها بالشبكة العنكبوتية[٣٧].

فالسؤال المطروح هنا هو من هم هؤلاء الوسطاء؟ ما الدور الذى يلعبه كل وسيط من علاقته بالمضمون المنشور على الشبكة؟.

أولاً: مقدمو الخدمة Internet Service Provider (I.S.P)

هو كل شخص يمد المستخدمين بالقدرة على الاتصال بواسطة أنظمة حاسب الآلى أو يقوم بمعالجة البيانات وتخزينها بالنيابة عن هؤلاء المستخدمين: وهو ما نصت عليه المادة (١) (٢) من اتفاقية بوداست ٢٠٠١ بشأن جرائم الإنترنت، فمزود الخدمة هو من يمكن المشتركين من الوصول إلى شبكة الإنترنت عن طريق مدهم بالوسائل الفنية اللازمة للوصول إلى الشبكة بمقتضى عقد توصيل الخدمة، فهو لا يقوم بتوريد المعلومة أو تأليفها[٣٨]، ولا يملك أى وسائل فنية لمراجعة مضمونها، لأن دوره فنى يتمثل فى نقل المعلومات على شكل حزم إلكترونية عن طريق حاسباته الخادمة، فهل يجوز اعتباره أحد المسئولين عن الجريمة المعلوماتية؟ هنا ظهر اتجاهان نعرض لهما تباعًا:

١ - الاتجاه القائل بعدم مسئولية المزود أو الوسيط أو الخادم

وقد استند هذا الاتجاه إلى أن مزود الخدمة لا يملك القدرة على التحكم فى أى مضمون يبث على الشبكة، والقول بتقرير مسئوليته هنا يماثل القول بمسائلة مدير مكتب البريد والهواتف على مدى مشروعية الخطابات والمكالمات التى تجرى عبر هذه الخطوط[٣٩] بل إن المسألة قد تنتهى بنا إلى تقرير مسئولية الجهات العامة على توفير محطات التقوية لبث القنوات الفضائية المرئية، فتقرير مسئولية مزود الخدمة يتطلب أن يكون دوره أكثر إيجابية فى بث المادة المجرمة بالإضافة إلى أنه لا يملك الوسائل الفنية التى تمكنه من مراقبة تلك المعلومات المتدفقة بأعداد تتجاوز الملايين[٤٠].

٢ - الاتجاه القائل بتقرير مسئولية مزود الخدمة

انقسم أنصار هذا الاتجاه إلى فريقين: الأول ينادى بتقرير المسئولية الجنائية طبقا لأحكام المسئولية المفترضة، والثانى يذهب إلى تقرير المسئولية طبقا للأحكام العامة للمسئولية الجنائية[٤١].

*** مساءلة مزود الخدمة طبقا لأحكام المسئولية المفترضة:**

يبدو لأول وهلة استجابة الدور الذى يقوم به مزود الخدمة لهذا النظام استنادا إلى مساهمته فى عملية النشر وتحقيق العلانية ووضعها فى متناول المستخدمين.

إلا أن المسئولية المتتابعة فى مجال النشر بالنسبة للمؤلف والناشر تقوم على أساس العلم المسبق بما تم إعلانه ونشره للآخرين، وهو ما يوجب التزام الناشر أو رئيس التحرر بالمراقبة مما لا يتوفر بالنسبة لمزود الخدمة، خاصة عند قيامه بالربط أثناء المنتديات المختلفة، حيث يقوم بتثبيت تلك المؤتمرات على جهازه الخادم وكل ما يصل لمزود الخدمة فى هذه الحالات هى حزم من البيانات المشفرة[٤٢].

وهو ما نصل معه إلى عدم قبول تطبيق أحكام المسئولية المتتابعة لأن مزود الخدمة لا يملك الوسائل الفنية والقانونية التى تمكن من مراقبة المضمون الذى ينشر ويتحرك على الشبكة.

*** مساءلة المزود طبقا للأحكام العامة للمسئولية الجنائية:**

يستند أصحاب هذا الرأى إلى أن مزود الخدمة لا يملك الوسائل الفنية اللازمة لمراقبة الصورة أو الكتابة إلا أنه يملك الوسائل الفنية اللازمة لمنع الدخول إلى هذه المواقع مما يؤدى إلى تقديم المساعدة لأصحاب تلك المواقع عن طريق مدهم بالزائرين وهو ما تتحقق به المساهمة الجنائية التبعية بالمساعدة[٤٣].

لكن يعد هذا الرأى أيضا محل نظر، لأن المساهمة الجنائية طبقًا لأحكام القانون الجنائى المصرى لا تكون إلا بالأعمال السابقة أو المعاصرة للسلوك الإجرامى

ولا تكون بالأعمال اللاحقة[٤٤]، أما مزود الخدمة فدوره يأتى لاحقا لارتكاب الجريمة التى تحققت بكامل عناصرها على الشبكة قبل أن يبدأ دور مزود الخدمة[٤٥].

هكذا نصل إلى صعوبة تطبيق فكرة العلم المسبق لأسباب فنية وقانونية، فالأسباب الفنية تتمثل فى عدم وجود الإمكانية لمراقبة المضمون المنشور قبل نشره أما الأسباب القانونية فترجع إلى عدم اختصاص مزود الخدمة بممارسة أى نوع من أنواع الرقابة التوجيهية على ما يتم نشره لما فى ذلك من تعارض والعديد من الضمانات الخاصة بحق المؤلف وحق الحياة الخاصة، ولا يمكن قبول قيامها بأى دور وقائى على الآخرين[٤٦].

إلا أننا نرى أنه فى حالة إنكار المسئولية عن مزودى الخدمة، والتى تمثل البيئة لاستقطاب المتطفلين أو من يسعون للإضرار بالآخرين من استخدام هذه البيئة، وبما يشكل خطرا على المجتمع بصفة عامة، ومن سيتم التعرض له،بصفة خاصة، وبأي وسيلة،وأيا كان حجم الضرر الذى سيتعرض له.

ثانياً: المسئولية الجنائية لمتعهد الإيواء أو المستضيف The Hoster

هو من يتولى إيواء صفحات معنية من الشبكة (web) على حساباته الخادمة (Server) مقابل أجر معين على الشبكة، حيث يقوم العميل وهو بمثابة المستأجر لتلك المساحة بكتابة المضمون الخاص عليها بطريقة مباشرة فيقوم بتخزين المادة المنشورة[٤٧] والمادة المعلوماتية لكى يتمكن العميل من الوصول إليها فى أى وقت[٤٨] كما يتولى مهمة تخزين وادارة المحتوى الذى قدمه له العميل فهو يسهم فى عملية النشر دون أن يكون بإمكانه السيطرة على المعلومة أو المضمون المنشور قبل عرضه على الإنترنت، فهو يساعد المستخدم فى الوصول إلى الموقع والتجول فيه.

وهنا يثور التساؤل حول مدى تقرير المسئولية الجنائية بالنسبة له.

١ – القول بعدم مسئولية مقدم الخدمة: يطلب عاملو الإيواء إعفاءهم من المسئولية الجنائية استنادا إلى أنهم يقومون بدور فنى يتمثل فى إيواء المعلومة وتخزينها

لتمكين الجمهور من الاطلاع عليها وهو ما أخذ به المشرع الفرنسى فى القانون رقم ٧١٩ الصادر سنة ٢٠٠٠ بتعديل قانون حرية الاتصالات، فنص التعديل على انتفاء المسئولية الجنائية والمدنية بالنسبة لكل الأشخاص الطبيعين أو المعنويين الذين يتعهدون بالتخزين المباشر أو المستمر من أجل أن يضعوا تحت تصرف الجمهور أشارات أو كتابات أو صور أو أغان أو رسائل، ولم يلزمهم هذا القانون إلا بضرورة التحقق من شخصية المساهم فى وضع المضمون أو كتابته ويستند أنصار هذا الاتجاه إلى أن دور التخزين الذى يقوم به عامل الإيواء لا يسمح بالسيطرة على المضمون[٤٩].

٢ - القول بمساءلة عامل الإيواء: واجه الرأى السابق نقدًا شديدًا وذهب رأى آخر إلى أن عامل الإيواء يجب أن يكون مسئولا[٥٠]، لأن بإمكانه رفض عملية الإيواء (مقدم الخدمة) إذا شعر بعدم مشروعية المضمون المنشور[٥١].

٣ - المساءلة طبقا للأحكام العامة المساهمة الجنائية: إذا كان عامل الإيواء يقوم باستضافة المعلومة أو المضمون المنشور على صفحاته دون أن يكون لديه أى سيطرة على المضمون، فسلطته على هذا الأخير وعلمه به يشبه مدى علم المؤجر بالجرائم التى يرتكبها المستأجر فى العين المؤجرة وفى هذه الحالة تنتفى المسئولية الجنائية لعامل الإيواء بمجرد ثبوت عدم علم عامل الإيواء بالمضمون غير المشروع، خاصة وأن البيانات والمعلومات تتدفق بين أرجاء الشبكة بسرعة كبيرة[٥٢]، وهو ما يتضح بصورة واضحة فى المنتديات ومجموعات المناقشة[٥٣]، أما بالنسبة لباقى الجرائم المرتكبة عبر صفحات (web) فإنها من الجرائم المستمرة إلى يستمر اراتكابها باستمرار عرضها على الصفحة ما يعنى إمكانية نشوء قرينة على العلم لها[٥٤]، وهنا يكون على المشرع المصرى عند صياغة الأحكام العامة للمسئولية الجنائية للمستضيف أن يقوم بأعمال الموازنة

بين التزامات هذا الأخير بعدم عرض المعلومات غير المشروعة من جهة حقوق المؤلف بالنسبة لصاحب المعلومة من جهة أخرى.

٤ – مساءلة عامل الإيواء طبقا لأحكام المسئولية المفترضة (المتتابعة)[٥٥]: نخلص من كل ما تقدم إلى صعوبة تطبيق الأحكام العام على أى من الوسيطين لصعوبة إثبات العلم بالمضمون المجرم مما تنتفى معه الوحدة المعنوية بين المساهمين أما أحكام المسئولية المتتابعة فلا يمكن تطبيقها أيضا لا لصعوبة مراقبة المضمون فحسب بل لاعتبار آخر لا يقل أهمية وهو أن أحكام المسئولية المفترضة (المتتابعة) استثناء من الأصل العام لا يجوز التوسع فيه.

فالمسئولية الجنائية يجب أن تتقرر بنص صريح ويجب أن ترتبط بإمكانية السيطرة على المعلومة فالوسيط فى تقديم هذه الخدمات سواءً كان مزود الخدمة أو عامل الإيواء، عبارة عن وسيط تجارى يقوم بأعمال الوسائط فى Cyber Space وهو ما يميزه عن الوسيط التقليدى الذى يكون قريبا من الأطراف وأكثر قدرة على تقييم تصرفاتهم بينما الوسيط المعلوماتى يقوم بدور الوسيط فى بيئة افتراضية تنعدم فيها الحدود الجغرافية اللازمة للاقتراب والتقييم كما تنعدم فيها النظم القانونية الحاكمة من جهة اخرى[٥٦].

وهو ما نصل معه إلى ضرورة التعرض إلى البعد الدولى للجريمة المعلوماتية والطبيعة اللامركزية للنطاق الذى ترتكب فيه هذه الجريمة، حيث تنعدم حدود الزمان والمكان الذى ترتكز عليه أسس القواعد الإجرائية التقليدية، فما هى التحديات الإجرائية للجرائم المعلوماتية وكيف يمكن مواجهتها[٥٧]؟

المحور الثانى: الآلية الإجرائية لضبط الجريمة المعلوماتية

من المعلوم أن الجريمة المعلوماتية ترتكب باستخدام التقنية المعلوماتية، مما يعنى أنها ترتكب فى فضاء افتراضى مفرغ Cyber Space، سواء ارتكبت عبر شبكة الإنترنت أم فى داخل نطاق ذات المؤسسة التى يتم الاعتداء عليها، أو ارتكاب الجريمة من خلالها، فضلا عن المشكلات الموضوعية التى تثيرها هذه الجرائم فى تطبيق القواعد التقليدية لقانون العقوبات الذى صيغت جل نصوصه ونظمه الأساسية لتواجه سلوكًا ماديًا يرتكب فى عالم مادى ملموس، فإذا كان ذلك هو حال القواعد الموضوعية للتجريم والعقاب، فما هو حال القواعد الإجرائية لهذا الفرع من القانون الجنائى؟ وهو ذلك الفرع الذى يتأسس فى كل النظم القانونية المختلفة على مبدأ دستورى هو الشرعية، أى شرعية التجريم والعقاب، الذى تنبثق عنها قاعدة الشرعية الإجرائية[٥٨]، وما يميز هذه الجريمة هو أنها ترتكب، فى نطاق رقمى يختلف كليًا عن النطاق التقليدى الذى ترتكب فيه الجريمة، حيث يتم الاستدلال عليها وضبطها وإثباتها بالوسائل التقليدية المتمثلة فى إجراءات الاستدلال والتحقيق، فهى إجراءات صيغت لضبط واثبات جرائم ترتكب فى عالم ملموس ماديًا، يلعب فيه السلوك المادى الدور الأكبر والأهم، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات جريمة ارتكبت فى عالم افتراضى غير ملموس؟ أما إذا ارتكبت الجريمة عبر الشبكة العنكبوتية الدولية[٥٩] (الإنترنت) تزداد العقبات القانونية صعوبة، فلا نكون أمام مشكلات إجرائية تخص ضبط الجريمة وإثباتها فحسب، بل نجد أنفسنا أمام مشكلة أكثر تعقيدًا تتمثل فى تحديد الاختصاص القضائى المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة، فقواعد الاختصاص القضائى التقليدية صيغت لكى تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكانى للجريمة، وهى قواعد ترتكز على مبدأ الإقليمية، وهو ما يرتبط بسيادة الدولة على إقليمها[٦٠]، فلا يكون الخروج عليه بقبول اختصاص قضائى أجنبى إلا فى حالات استثنائية يجب النص عليها صراحة،

وهنا تثور امامنا مدى إمكانية الاعتماد على هذه القواعد لتحديد الاختصاص القضائى لجريمة ترتكب فى مجال تنعدم فيه الحدود الجغرافية، وكثيرا ما يكون مرتكبوها فى بلاد مختلفة ومن جنسيات متعددة، وكثيرا أيضا ما يتعلق السلوك الإجرامى بأكثر من دولة: الدولة التى ارتكب فيها السلوك والدولة التى تم فيها القبض على الجانى وتلك التى حدثت فيها النتيجة الإجرامية وهو ما يتطلب منا التطرق إلى مشكلات ضبط الجريمة المعلوماتية واثباتها، ثم عن مشكلات الاختصاص بنظر الجريمة المعلوماتية، والأهم من ذلك تحديد المكان فى حالة الجرائم المستمرة.

أولاً: ضبط الجريمة المعلوماتية

يعتمد ضبط الجريمة واثباتها فى المقام الأول على جمع الأدلة التى حدد المشرع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التى يتم تجميعها عن تلك التى اعترف لها المشرع بالقيمة القانونية، وتتمثل فى وسائل الإثبات الرئيسية وفى المعاينة والخبرة والتفتيش وضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الإثبات كالاستجواب والمواجهة وسماع الشهود فهى مرحلة تالية من إجراءات التحقيق وجمع الأدلة، ولما كنا بصدد تناول الجريمة المعلوماتية وما تثيره من مشكلات إجرائية[٦١]، فسنتعرض للمشكلات القانونية التى يثيرها إثبات هذه الجرائم دون غيرها من الإجراءات كالاستجواب والمواجهة وسماع الشهود، لأن هذه الأخيرة تتم فى مواجهة البشر، أما المعاينة والخبرة والتفتيش، فهى إجراءات فنية محلها الأشياء لا الأفراد وهو ما يهمنا فى هذا الموضوع.

١ - حجية المخرجات الإلكترونية فى الإثبات

تخضع المحررات كغيرها من الأدلة التى تقدم أثناء نظر الدعوى إلى تقدير المحكمة حيث يسود مبدأ حرية القاضى فى تكوين عقيدته، وهو ما يختلف فيه القاضى المدنى

حيث يتقيد هذا الأخير بطرق معينة فى الإثبات، فالقاضى الجنائى له مطلق الحرية فى تقدير الدليل المطروح أمامه، وله أن يأخذ به أو يطرحه ولا يجوز تقييده بأى قرائن أو افتراضات(٦٢).

ولما كانت المحررات أحد الأدلة التى قد يلجأ إليها القاضى فى الإثبات فهى تخضع كغيرها من الأدلة لتقدير المحكمة، إلا إذا كان الإثبات متعلقًا بمواد غير جنائية، ففى هذه الحالة يكون على القاضى الجنائى أن يتقيد بطريق الإثبات المحددة فى ذلك الفرع من القانون مثال ذلك حق الملكية فى جريمة السرقة ، والعقود التى تثبت التصرف فى الحق فى جريمة خيانة الأمانة أو صفة التاجر فى جريمة التفالس بالتدليس(٦٣).

وهنا تثور مشكلة مدى حجية المخرجات الإلكترونية فى الإثبات الجنائى فى هذه الحالات، فللمخرجات الإلكترونية أنواع مختلفة، فهى تتنوع بين مخرجات ورقية، ومخرجات لاورقية وهى المعلومات المسجلة على الأوعية الممغنطة كالأشرطة والإقراص المرنة Floppy Disk القرص الصلب Hard Disk وغيرها من الأوعية التى أصبحت فى تطور مستمر حتى وصلت إلى أقراص الـ Flash Discs التى أصبحت تتميز بسعات كبيرة للتخزين، خاصة أنه تواجهنا مشكلة أساسية تتعلق بصعوبة التمييز بين المحرر وصورته أو بين الأصل والصورة، ذلك لأننا نتعامل مع بيئة اليكترونية تعمل بالنبضات، والذبذبات والرموز والأرقام وهو ما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية(٦٤).

ولما كان المشرع المصرى لا يزال عازفًا عن التدخل التشريعى فى هذه المسألة فلا نجد بدًا من تطبيق القواعد العامة فى هذا الصدد، ولما كان ذلك، فالمشرع المصرى لا يزال يعتمد على مبدأ سيادة الدليل الكتابى على غيره من الأدلة ولا يجوز الاعتماد على الدليل غير الكتابى فى غير المسائل الجنائية، إلا على سبيل الاستئناس، ولا يخفى ما يؤدى ذلك من تقييد للقاضى الجنائى لأن الإثبات فى

المسائل الجنائية كثيرًا ما يعتمد على مسائل غير جنائية، وهو ما سبقت الإشارة إليه عند تناول جريمة التزوير فى هذا البحث التى اعتمدت على مدى اعتبار هذه الأوعية من قبيل المستندات أو المحررات موضوع جريمة التزوير، فمواجهة الجرائم المعلوماتية لا تتأتى إلا عن طريق نظام قانونى متكامل أهم عناصره التدخل لضبط المعاملات والتجارة الإلكترونية وإضفاء الحجية القانونية على المستندات الإلكترونية شأنها شأن المستندات الورقية فيما يتعلق بالإثبات الجنائى، وأن تكون دلالاتها يقينية للقاضى الجنائى، حتى يتاح للقاضى الجنائى الاعتماد عليها[٦٥]، كغيرها من الأدلة، وقد كان المشرع التونسى من السباقين بين أقرانه على المستوى العربى فى هذا المجال، حيث صدر فى تونس قانون التجارة والمعاملات الإلكترونية الذى اعترف للمستندات الإلكترونية سنة ٢٠٠٠ بحجيتها فى الإثبات، كما أصدرت إمارة دبى قانون التجارة الإلكترونية سنة ٢٠٠٢، وتبعهما بعد ذلك المشرع المصرى سنة ٢٠٠٤ الذى أصدر قانون نظم التوقيع إلكترونى، وتجدر الإشارة فى هذا الصدد إلى القانون العربى النموذجى السابق الإشارة إليه سنة ٢٠٠٣، وكل هذه القوانين أعطت للمستند الإلكترونى ذات الحجية التى يتمتع بها المحرر الورقى، تجدر الإشارة أيضا إلى أن لجنة الأمم المتحدة للقانون التجارى الدولى United Nation Commission on International Trade Law (UNCITRAL) على هذه الحجية وقد كان ذلك سنة ٢٠٠٠ أما القانون العربى النموذجى فنص فى المادة الأولى منه على تعريف الكتابة بأنها كل (عملية تسجيل للبيانات على وسيط لتخزينها)، والمقصود بالوسيط فى هذه الحالة هو الوسيط الإلكترونى لأن الوسيط الورقى المتمثل فى الأوراق التقليدية لا يحتاج إلى تعريف، وإن كنا نتحفظ على استخدام عبارة الوسيط دون تحديده بالإلكترونى، مادام الأمر متعلقًا بالتجريم والعقاب.

إذا كان المشرع التونسى يعد سباقًا إلى اللحاق بهذا التطور التشريعى فإن المشرع السنغافورى أصدر قانونا للإثبات أقر فيه حجية المستندات المعلوماتية فى الإثبات منذ سنة ١٩٩٧ وهو ما يبين مدى تأخر المشرع المصرى فى مواكبة هذا التطور(٦٦).

٢ - الخبرة والمعاينة فى الجرائم المعلوماتية

تعتبر كل من الخبرة والمعاينة أكبر العقبات التى تواجه الإثبات فى الجرائم المعلوماتية، فالمعاينة إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه، فيقوم بجمعها وجمع أى شىء يفيد فى كشف الحقيقة، وتقتضى المعاينة إثبات حالة الأشخاص والأشياء الموجودة بمكان الجريمة ورفع الآثار المتعلقة بها كالبصمات والدماء وغيرها، مما يفيد التحقيق، والمعاينة تكون شخصية إذا تعلقت بشخص المجنى عليه، أو مكانية إذا تعلقت بالمكان الذى تمت فيه الجريمة، ووضع الشهود والمتهم والمجنى عليه، أما المعاينة العينية فهى التى تتعلق بالأشياء أو الأدوات المستخدمة فى ارتكاب الجريمة وقد يقتضى الأمر الاستعانة بخبير للتعرف على طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأى المتخصص، وفى هذه الحالة يتم إرسال هذه الأشياء إلى الخبير لنكون أمام بصدد إجراء آخر من إجراءات التحقيق وهو الخبرة، فالخبرة هى أحد أهم وسائل جمع الأدلة، يلجأ إليها المحقق عند وجود واقعة مادية أو شىء مادى يحتاج التعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة فى الإثبات، أو ليس من الأجدر العمل على إقرار المسئولية الجنائية على الوسيط المعلوماتى بما يتيح التوصل إلى الفاعل الحقيقى ويمكن العمل على منح عفو من العقاب فى حالة الإدلاء بمعلومات تفيد فى الإدانة.

يثور التساؤل هنا عن مدى إمكانية معاينة الجريمة المعلوماتية[٦٧]، أما السلوك الإجرامى فى الجريمة المعلوماتية فهو عبارة عن بيانات مخزنة فى نظام معلوماتى يتطلب إثباته انتقال محقق متخصص، حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الأسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التى من شأنها أن تساعد التحقيق وأن يطلعوا زملاءهم عليها، مثل القيام بالبحث فى بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة، وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الإنترنت، ولكى ينجح المحققون فى عملهم يجب أن يقتفوا أثر الاتصالات من الحاسب المصدر إلى الحاسب أو المعدات الأخرى التى تملكها الضحية، مرورًا بمؤدى الخدمة والوساطة فى كل دولة، وهو ما يتطلب وجود محققين يتمتعون بخبرة فى هذا المجال، كما أن هناك ضرورة للتعاون الدولى، وأن تعمل الشرطة الدولية الإنتربول من إيجاد آلية للكشف عن هذه الجرائم.

كما يقتضى ذلك أيضا ان يعمل المحقق على الوصول إلى الملفات التاريخية التى تبين لحظات مختلف الاتصالات، من أين صدرت؟ ومن الذى يحتمل إجراؤها، بالإضافة إلى ضرورة إلمام المحقق بالحالات التى يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الأسطوانة الصلبة للحاسب، والأوقات التى يستخدم فيها برامج استعادة المعلومات التى تم إلغاؤها[٦٨].

فالمحقق الذى يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملمًا بمهرات هذه التقنية، مثل القدرة على استخدام برامج Time Stamp وهى البرامج التى يمكن عن طريقها تحديد الزمن الذى تم فيه السلوك الإجرامى، لأن ذلك لا يكون متاحًا فى جميع الأنظمة المعلوماتية، أما الخبير ففى هذه الحالة يجب أن يكون ملمًا بمهارات

تحليل البيانات ومهارات التشفير التى تتيح له فك الرموز واستعادة البيانات الملغية[٦٩].

ولما كانت الجرائم ترتكب عبر الشبكة الدولية فقد نصت المادة ٢٣ على أن (تتعاون كل الأطراف، وفقًا لنصوص هذا الفصل، على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولى فى المجال الجنائى والترتيبات التى تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلى على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذلك بشأن الحصول على الأدلة فى الشكل الإلكترونى لمثل هذه الجرائم) كما نصت المادة ٣٠ من الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على: أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقًا لما هو وارد فى المادة ٢٩ فإن الطرف المساند إذا اكتشف وجود مؤدى خدمة فى بلد آخر قد شارك فى نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة[٧٠] حتى يمكن تحديد هوية مؤدى الخدمة هذا والطريق الذى تم الاتصال من خلاله، كما أشارت المادة ٣١ إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأى طرف أن يطلب من أى طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكانى لذلك الطرف والتى يدخل فيها أيضا البيانات المحفوظة وفقًا للمادة ٢٩ من الاتفاقية.

وهو ما نصل معه إلى حقيقة مؤداها أننا نواجه اليوم اخطر مظاهر العولمة، فالتعاون الدولى فى المجال الجنائى لم يعد مقتصرًا على نظام الإنتربول، فأصبح على الدولة أن تستخدم بروتوكولات موحدة لنظم التخزين والحماية المعلوماتية كما حدث

على مستوى الاتصالات الهاتفية، لأن التعاون بين دولة وأخرى سوف يتم بين أجهزة الخبرة الجنائية بشكل مباشر وبطريقة متشابكة، وهو ما نصل معه إلى أن تطوير البنية التحتية المعلوماتية لأى دولة اليوم أصبح ضرورة ملحة، ومطلبًا أساسيًا قد يترتب على غيابه انعزال الدولة وصيرورة نظامها المعلوماتى – إذا كان متواضعًا – مباحًا لمجرمى المعلوماتية[٧١].

نخلص من كل ما تقدم إلى أن الخبرة والمعاينة الجنائية فى الجرائم المعلوماتية اليوم تحتاج إلى إدارة خاصة يعمل بها متخصصون فى أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية، وهو ما يتطلب إنشاء إدارة خاصة للخبرة والمعاينة فى الجرائم المعلوماتية، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية، أما رجال القضاء والنيابة والضبطية القضائية فلا شك أنهم يحتاجون للتدريب على استخدام مهارات الحاسب الآلى والموسوعات القانونية التى تتطلب ربط كل المؤسسات القضائية بقواعد بيانات قانونية مثل أحكام المحاكم والقوانين المختلفة، لتوفير إمكانية استخدام موسوعات القوانين ومجموعات الأحكام القانونية العربية المختلفة وتعليمات النائب العام، لرفع مستوى الكفاءة القانونية لدى رجال القضاء والنيابة العامة[٧٢].

ثانياً: قواعد الاختصاص

خلصنا إلى عدم كفاية القواعد التقليدية للخبرة والمعاينة، وعدم ملاءمتها لإثبات الجرائم المعلوماتية، فهل تستجيب القواعد الخاصة بتحديد نطاق تطبيق القانون من حيث المكان، فكيف يمكن تحديد مكان وقوع الجريمة المعلوماتية؟ وإذا كانت هذه الجريمة ترتكب فى مجال افتراضى غير محدد جغرافيًا فهل يمكن ربط هذه الجريمة بدولة ما دون أخرى، فإن ذلك يتطلب ضرورة الحديث عن لامركزية الفضاء المعلوماتى، قبل تناول التعاون الدولى لملاحقة الجريمة المعلوماتية[٧٣]، وهل سيقتصر

العلم بالجريمة، بما يتم الإبلاغ عنه، وبخاصة فى حالة أن معرفة حجم الضرر أمر يعتمد على مدى خبرة المضرور نتيجة العمل غير المشروع من جانب المجرم المعلوماتى، والتى تعتمد فى أفعالها على المنتديات، أو على المواقع التى تقدم خدمات، بمعنى أدق من خلال مقدمى خدمات المعلوماتية أو وسطاء الخدمة.

١ - عالمية الجريمة المعلوماتية

لم تعد للحدود الجغرافية أى أثر فى الفضاء الشبكى أو الآلى، فهو لا يعترف بالحدود الجغرافية حيث يتم تبادل البيانات فى شكل حزم الكترونية توجه إلى عنوان افتراضى ليس له صلة بالمكان الجغرافى، فهو فضاء ذو طبيعة لا مركزية ويمكن إجمال أهم خصائصه فى عدم التبعية لأى سلطة حاكمة[٧٤]، فالفضاء الآلى: نظام إلكترونى معقد لأنه عبارة عن شبكة اتصال لا متناهية غير مجسدة وغير مرئية، ومتاحة لأى شخص حول العالم وغير تابعة لأى سلطة يمكن أن تحدد نطاقها أو مسلكها، فالفعل المرتكب فيها يتجاوز الأماكن بمعناه االتقليدى وله وجود حقيقى وواقعى لكنه غير محدد المكان لكنه حقيقة واقعة.

فالشبكة عالمية النشاط والخدمات لا تخضع لأى قوة مهيمنة إلا فى بدايتها حيث كان تمويل هذه الشبكة حكوميا يعتمد على المؤسسة العسكرية الأمريكية، أما الآن فقد أصبح التمويل يأتى من القطاع الخاص، حيث الشركات الإقليمية ذات الغرض التجارى التى تبحث عن كل السبل للاستفادة من خدماتها بمقابل مالى[٧٥].

والجريمة المرتكبة عبر شبكة الإنترنت جريمة تعبر الحدود والقارات، وهو ما يدرجها ضمن موضوعات القانون الجنائى الدولى.

وقد ازدادت أهمية القانون الجنائى الدولى بعدما تطورت الجريمة المنظمة فى وقت تقلص فيه المفهوم التقليدى للسيادة، حيث اتسع نظام المعاهدات الدولية لمكافحة الجرائم العابرة للحدود فالجانب الدولى للجريمة المعلوماتية لا يعد عنصرا من عناصرها كما هو الحال فى الجريمة الدولية بل يعد هو نطاقها المكانى.

إن القواعد العامة التى تحكم نطاق تطبيق النصوص الجنائية – التى تتمثل فى مبدأ إقليمية النص الجنائى والاستثناءات الواردة عليه – تقتضى تطبيق النص الجنائى على كل الجرائم الواقعة فى إقليمية.

٢ - النطاق المكانى

يعتمد النظام القانونى على جريمة ترتكب فى مكان قابل للتحديد الجغرافى، أما الجريمة المعلوماتية فهى جريمة ترتكب فى نطاق غير قابل للتحديد الجغرافى، إلا أنه يضم أكبر تجمع إنسانى يتميز بارتباط وتشابك معقد، وتتمثل أهم خصائصه فى خلق آليات خاصة لفرض الالتزامات والإذعان لها مثل قطع الاتصال على مخترقى بعض القواعد أو طردهم من المنتديات، لكن هذا التجمع الانسانى الضخم يفتقر إلى المعايير الأخلاقية المشتركة(٧٦).

وهو ما حدا المجلس الأوروبى إلى عقد اتفاقية بوداست السابق الإشارة إليها، والتى قدمت صورا لمكافحة هذه الجرائم ونصت المادة ٢٢ منها على "أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التى يراها لازمة لكى يحدد اختصاصه بالنسبة لكل جريمة تقع وفقًا لما هو وارد فى المواد من ٢ إلى ١١ من الاتفاقية الحالية عندما تقع الجريمة(٧٧):

أ- داخل النطاق المحلى للدولة.

ب- على ظهر سفينة تحمل علم تلك الدولة.

ج- على متن طائرة مسجلة فى هذه الدولة.

د- بواسطة أحد رعاياها، إذا كانت الجريمة معاقبًا عليها جنائيًا فى المكان الذى ارتكبت فيه أو إذا كانت الجريمة لا تدخل فى أى اختصاص مكانى لأى دولة أخرى.

ولكل طرف أن يحتفظ لنفسه بالحق فى عدم تطبيق، أو عدم التطبيق إلا فى حالات وفى ظل شروط خاصة، قواعد الاختصاص المنصوص عليها فى الفقرة الأولى (ب و د) من هذه المادة أو فى أى جزء من هذه الفقرات.

وتنص الفقرة ٤ من المادة على عدم استبعاد أى اختصاص ينعقد للقضاء الوطنى طبقا للقانون المحلى الفقرة ٥ تنص على أنه فى حالة حدوث تنازع فى الاختصاص فإنه يجب أن يتم حله بالتشاور بين الدول الأطراف حول المكان الأكثر ملائمة، كما أفردت الاتفاقية بندا خاصا لضرورة التعاون بين الدول.

ولم ينص القانون العربى النموذجى بشأن الجرائم المعلوماتية على أى قواعد لتحديد الاختصاص بنظر هذه الجرائم، فإن كان الفقه الجنائى اليوم قبل فكرة تطبيق القانون الأجنبى لمواجهة الجريمة عبر الوطنية ما أظهر ضرورة تجاوز فكرة تلازم الاختصاص الجنائى القضائى والتشريعى فيلزم من باب أولى قبول هذه الفكرة والتوسع فيها بالنسبة لجرائم ترتكب فى الفضاء الإلكترونى الذى يتجاوز الحدود والقارات، وبذلك نصل إلى ضرورة التفكير فى وضع ضوابط إسناد جنائية لتحديد الاختصاص الموضوعى والإجرامى بعد أن تصنف إلى فئات مختلفة تشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائيا على المستوى العالمى لوضع ضوابط إسناد تشير إلى القانون الواجب التطبيق[٧٨].

إلا أن هذه القواعد يجب أن تتم صياغتها فى إطار اتفاقات دولية لأن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولى، وهو أهم ما جاء فى اتفاقية بودابست بشكل يسمح بتبادل التعاون سواء كان ذلك على مستوى جمع الأدلة أو تسليم المجرمين وهو ما يعنى أن المجتمع الدولى مقبل على توسع فى مجال التعاون القضائي الذى يتوقع أن يتم بين الأجهزة القضائية، والامنية بشكل مباشر نظرًا لأن عامل الوقت فى حفظ الأدلة المعلوماتية سوف يكون حرجًا ومتطلبًا لسرعة الإنجاز[٧٩].

ولعلنا لا نكون مغالين إذا أعطينا الاختصاص لأكثر من دولة، ولكن الصعوبة تكمن فى تحديد أولوية الاختصاص عند التنازع، أسوة بما هو عليه العمل فى جرائم التدخل غير المشروع على متن الطائرات للارتباط، والمتمثل فى مرور وسيلة النقل الجوي بأجواء أكثر من دولة.

المحور الثالث: التعاون الدولى

فى عالم تشغل المعلومات والبيانات أهمية بالغة سواء للتبادل التجارى، أو للتواصل الاجتماعى، من مناطق متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا، ويتاح فى ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرارا فادحة، يغدو عندها التعاون الدولى واسع المدى فى مكافحة الجرائم المعلوماتية ومن بينها جرائم الإنترنت أمرا محتما.

ومع ضرورة هذا التعاون، إلا أنه ثمة صعوبات ومعوقات تقف دون تحققه وتجعله صعب المنال، سنعرض لأبرز تلك الصعوبات أو المعوقات، وكيفية مواجهتها(٨٠).

أولًا: الصعوبات التى تواجه التعاون الدولى

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدرٍ من الأمن والنظام، وتشكل الجريمة إحدى القضايا الرئيسية فى الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء، ولقد أثبت الواقع العملى أن الدولة – أى دولة – لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل فى كل ميادين الحياة، فنتيجة للتطور الملموس والمذهل فى الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهى نوعٌ من الجرائم المعلوماتية، التى باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة(٨١).

إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه أهمها:

١ – عدم وجود أنموذج موحد للنشاط الإجرامى[٨٢]

بنظرة متأنية للأنظمة القانونية فى التشريعات العربية لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا فى أحد الأنظمة قد يكون مجرّما وغير مباح فى نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالى اختلاف السياسة التشريعية من مجتمع لآخر[٨٣].

٢ – تنوع واختلاف النظم القانونية الإجرائية

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحرى والتحقيق والمحاكمة التى تثبت فائدتها وفاعليتها فى دولة ما قد تكون عديمة الفائدة فى دولة أخرى أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية فى دولة معينة، قد تكون ذات الطريقة غير مشروعة فى دولة أخرى، وبالتالى فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنقاذ القانون فى الدولة الأخرى على استخدام ما تعتبره هى أنه أداة فعّالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أى دليل إثبات جرى الحصول عليه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه بناء على اختصاص قضائى وبشكل مشروع.

٣ - عدم وجود قنوات اتصال[٨٤]

لعل التعاون الدولى فى مجال مكافحة الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعنى عدم القدرة على جمع الأدلة والمعلومات العملية التى غالبا ما تكون مفيدة فى التصدى لجرائم معينة ولمجرمين معينين، وبالتالى تنعدم الفائدة من هذا التعاون.

٤ - مشكلة الاختصاص

الجرائم المتعلقة بالإنترنت من أكبر الجرائم التى تثير مسألة الاختصاص على المستوى المحلى، أو الدولى ولا توجد أى مشكلة بالنسبة للاختصاص على المستوى الوطنى أو المحلى، حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك[٨٥].

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولى حيث اختلاف التشريعات والنظم القانونية والتى قد ينجم عنها تنازع فى الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التى تتميز بكونها عابرة للحدود، فقد يحدث أن ترتكب الجريمة فى إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائى للدولة الأولى استنادا إلى مبدأ الإقليمية[٨٦]، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصى فى جانبيه، وقد تكون هذه الجريمة من الجرائم التى تهدد أمن وسلامة دولة أخرى فتدخل عندئذ فى اختصاصها استنادا إلى مبدأ العينية[٨٧]، كما تثار فكرة تنازع الاختصاص القضائى فى حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجانى ببث الصور الخليعة ذات الطابع الإباحى من إقليم دولة معينة وتم الإطلاع عليها فى دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التى مستها الجريمة[٨٨].

٥ – التجريم المزدوج

التجريم المزدوج من أهم الشروط الخاصة للاستجابة لأى طلب لتسليم المجرمين، فهو منصوص عليه فى أغلب التشريعات الوطنية والمواثيق الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته تلك[٨٩]، نجده عقبة أمام التعاون الدولى فى مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، سيما وأن بعض الدول قد تجرم بعض الأفعال دون تجريم الأفعال التى تتم عن طريق البيئة المعلوماتية، والخاضعة للرقابة والإشراف من قبل مقدمى خدمات الإنترنت، بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أو لا، الأمر الذى يعوق تطبيق الاتفاقيات الدولية فى مجال تسليم المجرمين، ويحول بالتالى دون جمع الأدلة ومحاكمة مرتكبى الجرائم المتعلقة بالإنترنت[٩٠].

٦ – المساعدات القضائية

نعلم أن أول الطرق التى يمكن من خلالها كشف الحقيقة وبخاصة أن الكثير من الدول لا تسمح بالكشف عن الخصوصية المعلوماتية، إلا بإذن قضائى، وبالنسبة لطلبات الإنابة القضائية الدولية والتى تعد من أهم صور المساعدات القضائية الدولية فى المجال الجنائى أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذى يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، وهو الأمر الذى انعكس على الجرائم المتعلقة بالإنترنت[٩١].

٧ – التدريب

تتمثل فى عدم الاهتمام من جانب القيادات الإدارية فى بعض الدول للتدريب لاعتقادهم بارتفاع التكلفة، كما أن تطوير العمل من خلال تطبيق ما تعلمه المتدربون فى الدورات التدريبية وما اكتسبوه من خبرات لن يعود صداه على جهات العمل، ومن التى قد تهدد التعاون فى مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين

وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين، سيما فى مجال تكنولوجيا المعلومات وشبكات الاتصال، حيث إنه يوجد بعض الأشخاص ممن لا يعى فى هذا المجال شيئا، وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة فى هذا المجال[٩٢].

بالإضافة إلى أن الجريمة المعلوماتية تتطور وتحتاج إلى جهات ترصد هذا التطور، كما أن الجهات المعنية لا تشمل الجهات الشرطية أو القضائية، بل تمتد لتشمل جميع القطاعات والأفراد التى تتعامل مع التقنية المعلوماتية – ولاشك أن تفعيل ذلك لا يكون إلا من خلال التدريب المشترك – كما أن كثير من الدول ترى أن استكشاف هذا العالم، بمثابة قدس الأقداس، ومن ثم فهو لا يمس، وبالطبع نسف التعاون الدولى فى هذا المجال[٩٣].

أيضا من الصعوبات التى قد تؤثر على العملية التدريبية وعلى التعاون الدولى فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملى لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التى سيؤديها المتدربون فى بيئة العمل الطبيعية.

ثانياً: مواجهة الصعوبات التى تواجه التعاون الدولى

فيما يتعلق بالعقبة الأولى المتمثلة فى عدم وجود نموذج موحد للنشاط الإجرامى فإن الأمر يقتضى توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولى يتفق مع طبيعة هذا النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلة، وتتمثل هذه الوسيلة فى تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم[٩٤]، وأن تتم مراجعة لهذه الاتفاقيات بصفة دورية.

وبالنسبة للمعوق الثانى والخاصة بتنوع واختلاف النظم القانونية الإجرائية نجد أن المواثيق الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشىء الذى يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولى فعّال، فمثلا المادة ٢٠ من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير فى هذا الصدد إلى التسليم المراقب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة[٩٥]، والتى تعتبر من أهم التقنيات المستخدمة فى التصدى للجماعات الإجرامية المنظمة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد فى الملاحقات القضائية المحلية منها أو الدولية فى دول أطراف فى سياق نظم المساعدة القانونية المتبادلة[٩٦].

وهذا ما أكدت عليه الاتفاقية الأوروبية للإجرام المعلوماتى حيث نصت المادة ٢٩ على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكانى لذلك الطرف الآخر والتى ينوي الطرف طالب المساعدة أن يقدم طلبًا للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها.

كما أكدت المادة ٣٠ من ذات الاتفاقية على الكشف السريع عن البيانات المحفوظة، حيث نصت على: أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقًا لما هو وارد فى المادة ٢٩ فإن الطرف المساند إذا اكتشف وجود مؤدى خدمة فى بلد آخر قد شارك فى نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدى الخدمة، وهذا الطريق الذى تم الاتصال من خلاله[٩٧].

كما أشارت المادة ٣١ من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأى طرف أن يطلب من أى طرف آخر أن يقوم بالتفتيش أو أن يدخل بأى طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكانى لذلك الطرف والتى يدخل فيها أيضا البيانات المحفوظة وفقًا للمادة ٢٩، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن فى الحالات الآتية:

- إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر الفقد أو التعديل.
- أو أن الوسائل والاتفاقات والتشريعات الواردة فى الفقرة ٢ تستلزم تعاونًا سريعًا.

فى حين نجد أن المادة ٣٢ من ذات الاتفاقية سمحت بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور[٩٨].

أيضا نصت المادة ٣٣على تعاون الدول الأطراف فيما بينها لجمع البيانات فى الوقت الحقيقى عن التجارة غير المشروعة، والمرتبطة باتصالات خاصة على أرضها تتم بواسطة شبكة معلومات، وفى إطار ما هو منصوص عليه فى الفقرة الثانية. وينظم هذا التعاون الشروط والإجراءات المنصوص عليها فى القانون الداخلى. ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التى يكون جمع المعلومات بشأنها فى الوقت الحقيقى متوافر فى الأمور المشابهة على المستوى المحلى.

وهناك أيضا المادة ٣٤ من ذات الاتفاقية والتى نصت على التعاون فى مجال التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التى تتم عن طريق إحدى شبكات المعلومات.

ونلاحظ مما سبق أن الاتفاقية الأوروبية للإجرام المعلوماتى أوجدت بعض الحلول التى من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولى لمواجهة الجرائم المتعلقة بشبكة الإنترنت.

وللحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلاحظ أنه غالبا ما تشجع المواثيق الدولية، الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير فى الحصول على هذه المعلومات وتبادلها[٩٩]، ومن الأمثلة على هذه المواثيق الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية فى المادة ٢٧ منها، والمادة ٩ من اتفاقية ١٩٨٨، والمادة ٤٨ من اتفاقية الأمم المتحدة لمكافحة الفساد، والبند الثانى من المادة ٢٧ من الاتفاقية الأوروبية بشأن الإجرام المعلوماتى، والمادة ٣٥ من ذات الاتفاقية الأوروبية والتى أوجبت على الدول الأطرف فيها ضرورة تحديد نقطة اتصال تعمل لمدة ٢٤ ساعة يوميًا طوال أيام الأسبوع لكى تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكترونى، وهذه المساعدة تشمل تسهيل أو إذا سمحت الممارسات والقوانين الداخلية بذلك، تطبيق الإجراءات التالية بصفة مباشرة أولا: إسداء النصيحة الفنية. ثانيا: حفظ البيانات وفقًا للمواد ٢٩، ٣٠، ثالثا: جمع الأدلة وإعطاء المعلومات ذات الطابع القضائي وتحديد أماكن المشتبه فيهم[١٠٠].

كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر، وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربين القادرين على تسهيل عمل الشبكة.

أما بالنسبة لمشكلة الاختصاص فى الجرائم التى تتم عبر الشبكة العنكبوتية فثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائى خاصة بالنسبة للجرائم

المتعلقة بالإنترنت[١٠١]، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التى تشهده تكنولوجيا المعلومات والاتصالات.

ولأجل القضاء على مشكلة التجريم المزدوج والذى يعد من أهم الشروط الخاصة بنظام تسليم المجرمين ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة فى المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال والتى تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضى قوانين الدولتين معا أو بمجرد السماح بالتسليم لأى سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة فى كل دولة[١٠٢].

وفيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ فى الرد فإننا نجد الحاجة ملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختص فى نظر مثل هذه الطلبات لنقضى على مشكلة البطء والتعقيد فى تسليم طلبات الإنابة[١٠٣]، وهذا بالفعل ما أوصى به مؤتمر الأمم المتحدة الحادى عشر لمنع الجريمة والعدالة الجنائية والذى انعقد فى بانكوك فى الفترة من ١٨-٢٥/٤/٢٠٠٥، حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة فى أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات فى الوقت المناسب[١٠٤]، ونفس الشىء نجده فى البند الثانى من المادة ٢٧ من الاتفاقية الأوروبية بشأن الإجرام المعلوماتى، والمادة ٣٥ من ذات الاتفاقية الأوروبية والتى أوجبت على الدول الأطرف فيها ضرورة تحديد نقطة اتصال تعمل لمدة ٢٤ ساعة يوميًا طوال أيام الأسبوع لكى تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو الاستقبال الأدلة فى الشكل الإلكترونى عن الجرائم. كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر، وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربون القادرون على تسهيل عمل الشبكة.

أما بالنسبة للرد على طلبات التماس المساعدة فإنه من الضرورة بمكان الاستجابة الفورية والسريعة على هذه الطلبات،لأجل ذلك تنص غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة، وهذا ما أكدت عليه الفقرة الثالثة من المادة ٢٥ من الاتفاقية الأوروبية للإجرام المعلوماتى حيث نصت على أنه "يمكن لكل طرف، فى الحالات الطارئة أن يوجه طلبًا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكترونى على أن تستوفى هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها (ويدخل ضمن ذلك الكتابة السرية إذا لزم الأمر) مع تأكيد رسمى لاحق إذا اقتضت الدولة المطلوب منها المساعدة فى ذلك. وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريعة[١٠٥].

أما فيما يتعلق بالصعوبات الفنية التى تواجه التعاون الدولى فى مجال التدريب فإنه يمكن التغلب عليها بإجراء المزيد من البرامج التى تعمل على بيان مخاطر الجرائم المعلوماتية والأضرار التى تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبمزيد من التنسيق بن الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية مشتركة تناسب جميع الفئات، كما يتعين الاهتمام بالمساعدين القضائيين، ومنهم رجال الأدلة الجنائيين، وما تم استحداثه مؤخرا من وظيفة وهى محلل جنائى، وتظهر أهميته فى جرائم المعلوماتية.

الخاتمة

أصبح واقعًا ملحًا ضرورة إيلاء النظر إلى المسئولية الجنائية لمقدمى الخدمات المعلوماتية، وإلى ضرورة التدخل الأمنى والتشريعى لتنظيم التعاملات الإلكترونية بصفة عامة، فضلا عن ضرورة وضع أطر تدريبية كفيلة باستجلاء العلم بالاختراقات الأمنية، وكذا حصر الاعتداءات التى تتم، لأنه لا توجد إحصائيات شاملة لما يحدث

فعليا من اعتداءات عبر الشبكة المعلوماتية، قبل إصدار القوانين اللازمة لمواجهة الجرائم المعلوماتية، لأن المعاملات الإلكترونية اليوم أصبحت تغطى معظم التعاملات اليومية، وفى مختلف المجالات، فهى بالتالى ليست جرائم إنترنت بالمعنى الفنى وإن كان يطلق عليها الجرائم الإلكترونية إلا أنها يمكن أن ترتكب دون استخدام الحاسب الآلى، أما الجرائم المعلوماتية بالمعنى الفنى القانونى فهى الجرائم التى لا يتصور ارتكابها دون استخدام التقنية المعلوماتى لأن هذه الأخيرة تشكل عنصرًا من عناصرها، مثل الاختراق وتدمير الشبكات وتحريف البيانات أو التلاعب بها وإساءة استخدام بنوك المعلومات.

وقد تعرضت الجريمة المعلوماتية للاعتداء على الحياة الخاصة، حيث أفرزت لنا هذه التقنية الحديثة عناصر جديدة للحياة الخاصة لم تعرفها القوانين التى حصرت حمايتها الجنائية فيما تصورت أنه يغطى جميع عناصر الحياة الخاصة للإنسان، فقصرت هذه الحماية على المسكن والمحادثات الهاتفية، دون أن تشمل تلك البيانات المتدفقة عبر الشبكة العنكبوتية الدولية، وليس المقصود هنا ما يتم حفظه فى أرشيف الدولة الإلكترونى، أو تلك المخزنة فى النظم المعلوماتية للمؤسسات العامة، ولكن الخطورة تكمن فى ما يتم اختزانه فى المؤسسات الخاصة وبخاصة فيما ينتج من منتديات أو شبكات التواصل الاجتماعية التى تتعامل مع الجمهور من جهة أخرى، وكثيرًا ما يتم الاعتداء فى وقت يكون فيه المتهم بعيدًا عن موقع الجريمة أو مكانها، انتقل البحث بعد ذلك لتناول المشكلات القانونية التى تثيرها الجرائم المعلوماتية من حيث المسئولية الجنائية، بالنسبة لوسطاء تشغيل الشبكة التى ترتكب عن طريقها الجريمة المعلوماتية، فهذه الأخيرة يتدخل لتشغيلها العديد من الأفراد أو الجهات العامة منها و الخاصة فالشبكة لا تعمل إلا عن طريق مزود الخدمة الذى يمد العميل بالوسيلة الفنية التى توصله بالشبكة، أما متعهد الوصول فهو من يوفر لمالك الموقع المساحة فى الفضاء الإلكترونى لكى يمكنه من استخدامها وتحميلها بالمضمون أو

بالبيانات، وهنا تثور إشكالية حول إمكانية تطبيق الأحكام العامة للمسئولية الجنائية مما يستدعى التدخل التشريعيى لحسم هذه المشكلة، إذا ما ارتكبت عن طريق الشبكة أى من جرائم السب أو التشهير، والنظر إلى البعد الدولى للجرائم المعلوماتية موضحًا أن الجانب الدولى لهذه الجرائم يشكل نطاقها المكانى، وليس عنصرًا فيها كما هو الحال بالنسبة للجريمة الدولية، لأن الجريمة المعلوماتية شأنها شأن الجرائم المنظمة عبر الوطنية التى يمكن ارتكابها داخل حدود دولة واحدة، إلا أن عناصرها المادية تمتد لأكثر من دولة واحدة، كما يتعين إعتبار جرائم المعلوماتية التى تتم عبر الحدود جريمة دولية لأن هذه الأخيرة، يشكل العنصر الدولى فيها عنصرًا من عناصرها، لذلك فإن دراسة الجانب الدولى فى هذه الجرائم يجب أن يكون فى محاولة لتجاوز القواعد التقليدية لتحديد مبدأ الإقليمية الذى تتأسس عليه قواعد الاختصاص القضائى والقانونى لملاحقة الجرائم التى ترتكب عبر أكثر من دولة.

الإجراءات الوقائية

١ – منع انتحال أرقام الإنترنت أو ما يعرف بـ (IP-Spoofing) والتى يقوم خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقة غير مشروعة، والنص على عقوبة مشددة، حتى ولو كان باتخاذ برنامج لإخفاء IP.

٢ – منع إساءة استخدام البريد الإلكترونى أو ما يعرف بـ (E-mail Spamming) سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحا باسم البريد المهمل والذى ينتشر بشكل كبير فى الدول المتقدمة، وما يتم فى الدول العربية من المغالاة فى البرامج الدعائية بما يسبب تعطيل للشبكة، دون وجود تنظيم، مستغلين البيانات المخزنة لدى مقدمى خدمات الإنترنت.

٣ – الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين (Dialup-Server) وسجل استخدام البروكسى (Proxy) لمدة لا تقل عن (٦) أشهر، عمل رقابة على مقدمى برامج الكومبيوتر.

٤ – الحصول على خدمة الوقت (NTP) عن طريق وحدة البروكسى ومزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.

٥ – تحديث سجلات منظمة رايب (www.ripe.com) الخاصة بمقدمى الخدمة.

٦ – ضرورة تنفيذ ما تتوصل إليه وحدات مكافحة جرائم المعلوماتية، وأيا كانت مسمياتها على المستوى العربى أو الدولى، بخصوص متابعة ومعاقبة المخالفات الأمنية، وعمل إستراتيجيات للوقاية من تلك الجرائم.

التوصيات

١ – أهمية تظافر الجهود الدولية من أجل سن القوانين والتشريعات الدولية لمكافحة جرائم الإنترنت، وبخاصة النص على المسئولية الجنائية المفترضة لوسطاء الخدمة، وإلزام كل دول العالم بتطبيق تلك القوانين لضمان القضاء أو التخفيف من هذه الجرائم على شبكة الإنترنت.

٢ – حماية صناعة التقنية المعلوماتية والبرمجيات، وذلك لضمان منع عمليات التجسس والقرصنة والاحتيال المالى، وإيلاء متخصصين محترفين لصياغة آليات لهذه المواجهة.

٣ – تشديد العقوبات المتعلقة بالإرهاب المعلوماتى لما يمثله من خطر داهم على سلامة وأمن الوطن والمواطن، وبخاصة المستتر خلف وسطاء مقدمى خدمة الإنترنت.

٤ – وضع الضوابط التى تمنع الغزو الثقافى المتمثل بالأفكار المنحرفة والمواقع الإباحية التى تستهدف الشباب وتسعى إلى تدميره والتأثير على معتقداته وإرادته.

٥ – اعتبار القرصنة على البرامج بمثابة جريمة مشددة وبخاصة إذا كان الهدف منها إخفاء مرتكب هذه الجرائم، مثلها مثل أى سلعة أخرى.

٦ – نشر الوعى بأهمية الاستخدام القانونى للبرامج، وإيجاد حلول وقائية فعالة.

٧ – العمل على إنشاء محاكم للقضايا الافتراضية على شبكة الإنترنت لتتمكن من التعامل مع هذه الأنواع المستحدثة من الجرائم، وتدريب جهاز الخدمة المعاونة ومساعدى مأمورى الضبط القضائى.

٨ – التوعية الإعلامية المستمرة للمخاطر الناتجة عن سوء استخدام شبكة الإنترنت وما قد تلحقه من أضرار جسيمة على أمن واقتصاد الأوطان والمجتمعات والأفراد.

٩ – تطوير القدرات التقنية على شبكة الإنترنت، وإنشاء شرطة الإنترنت للقبض المباشر على مرتكبى الجرائم حال دخولهم على الشبكة من خلال التتبع الفنى للجهاز أو الخط الهاتفى الذى ارتكبت منه الجريمة.

المراجع

1-Vacca, John, 1996, Internet Security Secrets. USA: IDG Book. Worldwide Inc. Wilson, c. Holding Management Accountable: A new policy for Protect Against Computer Crime. Proceedings of the National Aerospace and Electronics Conference, USA, 2000, pp. 272-281.

2-Adsit, C. Kristin., 1999, Internet Pornography Addiction.[Online].

- Available: http://www.chemistry.vt.edu/chem-dept/ dessy/honors /papers99/adsit.htm [9.3.2001].

- Highley, Reid, 1999, Viruses: The Internet's Illness.[Online]. Available:http://www.chemistry.vt.edu/chem-dept/dessy/honors/papers99/highleh.htm [9.3.2001].

3 - Koerner, B. I., Only You Can Prevent Computer Intrusions. U.S. News and World Report, 127, 1999, p. 50.

Morningstar, Steve, 1998, Internet Crime and Criminal Procedures. [Online]. Available: http://www.prevent-abuse-now.com/index.html [13.10.2001].

٤ – فى المسئولية الإلكترونية بشكلٍ عام عن المخالفات المرتكبة عبر الإنترنت، راجع، محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، الطبعة الأولى، ٢٠٠٣.

٥ – تعتبر الصين ثانى أكبر سوق للإنترنت فى العالم وذلك بوجود نحو ٨٤٣ ألف موقع إلكترونى، ويصل مستخدمو الإنترنت فيها إلى نحو ١٤٠ مليون شخص، راجع سناء عيسى، مقال بعنوان فيروسات جديدة تستهدف أنظمة مايكروسوفت، مجلة العالم الرقمى، العدد ٣٨ بتاريخ ٢٠٠٣/٠٩/١٤ منشورة على الموقع الإلكترونى www.al-jazirah.com

٦ – فى تعدُّد أشخاص القائمين على خدمات الإنترنت، انظر: عبد الفتاح بيومى حجازى، النظام القانونى لحماية الحكومة الإلكترونية، الكتاب الثانى، دار الفكر الجامعى، الإسكندرية، الطبعة الأولى، ٢٠٠٣، ص ٣٣٩ وما بعدها، محمد حسين منصور، ص ١٩٦ وما بعدها،

- Lionel Thoumyre, "Hyper dossier sur les acteurs de l'Internet en France", juriscom.net, 22 juin 2004, disponible à l'adresse www.juriscom.net /pro/ visu. php? ID= 485.

– القانون الفرنسى رقم ٢٠٠٤/٥٧٥ حول "الثقة فى الاقتصاد الرقمى"،

- Loi n° 2004/575 du 21 juin 2004 sur la Confiance dans l'économie numérique, JO, 22 juin 2004, p.11168.

٧ – التوجيه الأوروبى رقم ٢٠٠٠/٣١ والمتعلِّق "ببعض الأوجه القانونية لخدمات شركات المعلومات، وبصفةٍ خاصَّة التجارة الإلكترونية، فى السوق الداخلى"،

Directive n° 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000 relative "à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur", JOCE, n° L 178,17 juillet 2000, p.1 ets.

٨ - القانـــون الأمريكـــى الصـادر فـى ٢٨ تشرين الأول ١٩٩٨ والمسمَّى Digital Millenium Copyright Act (DMCA) (Public Law n° 105-304, 112 sat, 2860, 28 oct. 1998.)، يُمكن أيضا الإطِّلاع على نصوص هذا القانون على الموقع الإلكترونى للمكتب الأمريكى لحقوق النشر وذلك على العنوان التالى http://lcweb.loc.gov/copyright.

9 - Luc Grynbaum, "Une immunité relative des prestataires de services Internet", Communication- Commerce électronique, Études, Septembre 2004, n° 28, p. 36.

- القانون الفرنسى رقم ٢٠٠٤/٥٧٥ حول "الثقة فى الاقتصاد الرقمى"،

Loi n° 2004/575 du 21 juin 2004 sur la Confiance dans l'économie numérique, JO, 22 juin 2004, p.11168.

١٠ - التوجيـه الأوروبـى رقـم ٢٠٠٠/٣١ والمتعلِّـق "بـبعض الأوجـه القانونيـة لخـدمات شـركات المعلومات، وبصفةٍ خاصَّة التجارة الإلكترونية، فى السوق الداخلى"،

- Directive n° 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative "à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur", JOCE, n° L 178,17 juillet 2000, p.1 ets.

١١ - يمكنـك ملاحظـــة وجود الفيروس فى جهازك إذا ما كان الحاسب الآلى يحتاج لوقت أكثر من اللازم لتحميل أو تنفيـذ البرامـــج، أو تغيّر فى حجم الذاكرة، أو اختفاء بعض الملفات، أو ظهور رسائل غير اعتيادية على الشاشـة، أو وجـود إشـارات غير عادية أو أصوات غيـر عاديـة تطلـق مـن جهـاز الحاسـوب وقـد تكـون هـذه الإشـارات لأسـباب أخـرى غيـر الفيروسات.

12 - Feraud, H. E.Schlanilz, la cooperatation policiere international, R.I.D.P,1974, pp. 477-478.

١٣ - قد يقوم الفيروس بحذف الجزء الأول من الملف التنفيذى وكتابة نفسه فى هذا المكان، الأمر الذى يؤدى إلى توقف عمل هذا الملف بشكل جزئى ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة الفوقية، وقد يقوم الفيروس بنسخ نفسه فى الجزء الأخير من الملف التنفيذى ويعرف هذا النوع من الفيروسات باسم فيروسات الكتابة غير الفوقية. وهناك فيروس الكتابة المباشرة حيث يقوم بكتابة نفسه مباشرة على الأسطوانة الصلبة فى مكان محدد، فيؤدى إلى عدم قدرة نظام التشغيل على التعامل مع الملفات بالرغم من أن هذه الملفات مازالت موجودة على القرص الصلب ولم يتم حذفها ومن أشهر هذه الفيروسات فيروس تشرنوبل.

- ولقد ظهرت هذه النوعية من البرامج الضارة لأول مرة فى عام ١٩٨٨ على يد الطالب الأمريكى Roper Tappan Morris وهى ما عرفت بدودة موريس Morris، ومن أشهرها دودة الحب " Love Bug" والتى ظهرت عام ٢٠٠٠ وتسببت فى خسائر تقدر بملايين الدولارات، راجع مقال جريمة إتلاف وتدمير المعطيات والبيانات بواسطة الإنترنت، المرجع السابق.

١٤ - محمد بوشيبة، "حماية برامج الحاسوب طبقا لقانون ٢٠٠٠ المنظم لحقوق الملؤف والحقوق المجاورة"، مجلة القضاء والقانون، عدد. ص ٨٤.

١٥ - محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة للنشر الإسكندرية - طبعة ٢٠٠٣- ص ٢٩٤.

16 - Philippe Jougledx, droit des médias, faculté de droit d'aix- Marseille, dans le thème: «la criminalité dans le cuber- espace », 1999, p. 25 et suivants.

١٧ - فى هذا الإطار فقد قام أحد المسئولين الإعلاميين بإحدى الشركات بعد فصله عن العمل بزرع قنبلة منطقية زمنية فى برنامج الشركة أدى إلى انهيار النظام كاملا لمدة شهر كامل مما كبد الشركة خسائر كبيرة. انظر بهذا العدد: Mohammed Bozobar انظر المرجع السابق ص ٥٢٣.

18 - Nanoart, 2000, [Online]. Available: http://www.nanoart.f2s.com/hack/ [15.11.2000] NUA Internet Surveys. (1998,June). How Many Online? [Online]. Available: http://www.nua.ie/surveys/howmayonline/index.html [26.10.2000].

١٩ - تجرم بعض التشريعات العربية حتى مجرد الاستخدام دون تحقيق أية غاية نفعية طالما تحقق الضرر حتى ولو كان محتملا "الشاب مرتضى (...) حكم بثلاث سنوات سجنا نافذا وغرامة ١٠٠٠٠٠ درهما (حوالى ٩٧٠ يورو) بتهمة انتحال صفة بعد انخراطه فى موقع "فيس بوك" ببروفايل سماه "الأمير مولاى رشيد" بدون أية غاية نفعية أو إجرامية ودون حتى إرسال أية رسالة منه.

- ونطق الحكم من طرف المحكمة الابتدائية بالدار البيضاء مساء يوم الجمعة ٢٢ فبراير ٢٠٠٨ فى محاكمة غابت فيها كل شروط وضمانات المحاكمة العادلة"، يقول بلاغ الجمعية، من جهتها، أنشأت أسرة فؤاد موقعا على الإنترنت خاصا بالتضامن معه، زوار الموقع تجاوز عددهم ٧١ ألف شخص خلال أقل من ثلاث أسابيع، كما بلغ عدد التوقيعات على العريضة التضامنية ٧٠٠٠ توقيع. فى نفس الوقت، أنشأ عدد من مستعملى "فيس بوك" صفحة تضامنية مع فؤاد بلغ عدد أعضائها ٤٠٠٠ شخص، فيما وضع العشرات من مستعملى "فيس بوك" صورة فؤاد بدل صورتهم على صفحاتهم الخاصة فى الموقع.

٢٠ - برنامج (Back Orific): ثاني أشهر البرامج وأقدمها يعطى المستخدم قدرة كاملة على جهاز الضحية تم الإعلان عنه من قبل جهة تدعى بجمعية البقرة الميتة (Cult of Dead Cow) والإصدارة التى صدرت فى عام ١٩٩٩ باسم بـ (BO2K).

21 - Bouchaib Rmall, la criminalité informatique, criminalité a double dimension: internationale, thèse pour l'obtention du grade de ducteur en droit privé- option: droit des affaires, faculté des sciences juridiques, économiques et sociales- fés, 2005, p: 82.

٢٢ - تركى محمد الوطيان، جرائم الحاسب الآلى: دراسة نفسية تحليلية، هذا المقال موجود على الموقع/ www.minshawi.COM.PDR other/oteyom

٢٣ - برنامج (Sub Seven): أخطر برامج الاختراق يسمى فى منطقة الخليج (الباكدور جى) ويطلق عليه البعض اسم القنبلة. تتركز خطورته فى أنه يتميز بمخادعة الشخص الذى يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفه ويعتبر أقوى برنامج اختراق للأجهزة الشخصية وفى إصدارته الأخيرة يمكنه أن يخترق سيرفر لقنوات المحادثة (Mirc) كما يمكنه اختراق جهاز أى شخص بمجرد معرفة اسمه فى (ICQ) كما يمكنه اختراق مزودات البريد (smtp/pop3) يعتبر الاختراق به صعب نسبيا وذلك لعدم انتشار ملف التجسس الخاص به فى أجهزة المستخدمين إلا أنه قائما حاليا على الانتشار بصورة مذهلة ويتوقع أنه بحلول منتصف عام ٢٠٠١ سوف تكون نسبة الأجهزة المصابة بملف السيرفر الخاص به (٤٠-٥٥٪) من مستخدمى الإنترنت حول العالم وهذه نسبة مخيفة جدا إذا تحققت فعلا وهذا البرنامج خطير للغاية فهو يمكن المخترق من السيطرة الكاملة على الجهاز وكأنه جالس على الجهاز الخاص به حيث يحتوى البرنامج على أوامر كثيرة تمكنه من السيطرة على جهاز الضحية بل يستطيع أحيانا الحصول على أشياء لا يستطيع مستخدم الجهاز نفسه الحصول عليها مثل كلمات المرور فالمخترق من هذا البرنامج يستطيع الحصول على جميع كلمات المرور التى يستخدمها صاحب الجهاز!!! ومن أهم أعراض الإصابة بهذا البرنامج ظهور رسالة "قام هذا البرنامج بأداء عملية غير شرعية" وتظهر هذه الرسالة عند ترك الكمبيوتر بدون تحريك الماوس أو النقر على لوحة المفاتيح حيث يقوم البرنامج بعمل تغييرات فى حافظة الشاشة وتظهر هذه الرسائل عادة عندما تقوم بإزالة ادخالات البرنامج فى ملف (system.ini).

24 - Rapalus, P., 2000 May, Ninety Percent of Survey Respondents Detect Cyber Attacks. Computer Security Institute. [Online]. Available: http://www.gocsi.com/prelen_000321.htm [11.10.2001]

- Reuvid, Jonathan, 1998, The Regulation and Prevention of Economic Crime, London: Kogan, 14.

25 - Philippe Jougledx, droit des médias, faculté de droit d'aix- Marseille, dans le thème: « la criminalité dans le cuber- espace », 1999, p. 25 et suivants.

٢٦ – برنامج (Net bus): أشهر البرامج وأكثرها انتشارا وقد يكون سبب انتشاره أنه من أوائل البرامج التى ظهرت لهذا الغرض، ولسهولة استخدامه لقى رواجا كبيرا وعلى الرغم من أنه لم يكمل العامين من عمره فإنه يوجد العديد من الإصدارات التى تتحسن وتزداد خطورة فى كل إصدارة عن سابقتها. (Nanoart, 2000)

27 - Skinner, W. F. and Fream, A. M., November, 1997, A social Learning Theory Analysis of Computer Crime Among College Students. Journal of Research in Crime and Delinquency, 34 (4), 495-519. Staff. (2000, April 2). The Business of Technology.
- Available:http://www.redherring.com/mag/issue7/news-security.html [11.10.2001].
- Thomas, P., 2000, February 23, Insufficient computer security threatens doing business

٢٨ – العلمى عبد الواحد "المبادئ العامة لقانون الجنائى الغربى" مطبعة النجاح الجديدة، طبعة ١٩٩٨، ص ٢٧٦.

٢٩ – محمد بوشيبة، مقالة بعنوان حماية برامج الحاسوب طبقا لقانون ٢٠٠٠ المنظم لحقوق المؤلف والحقوق المجاورة، منشورة بمجلة القضاء والقانون العدد ١٥٠ سنة ٢٠٠٤.

٣٠ – محمد أمين الرومى، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، طبعه ٢٠٠٣، ص ١٠٢.

٣١ – حسين بن سعيد الغافرى – جرائم الحاسب الآلى – ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجى لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية "الإنترنت" الأول والذى انعقد بمقر الأمانة العامة بالرياض خلال الفترة من ٤-٥/٤/٢٠٠٤.

32 - Thomas, P., 2000, February 23, Insufficient Computer Security Threatens Doing Business.
-Available:http://www.cnn.com/2000/TECK/computing/02/23/credir.card.thefts/index.html [11.11.2001].
-Thompson, R., February, Chasing after petty computer crime. IEEE Potentials, 18 (1), 1999, pp. 20-22.

٣٣ – عبدالله عبدالعزيز اليوسف، التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، ١٤٢٠هـ، ص ص ١٩٥- ٢٣٣.

٣٤ – محمد محمود مندورة، الجرائم الحاسب الآلية، دورة فيروس الحاسب الآلى، مكتب الآفاق المتحدة: الرياض، ١٤١٠هـ، ص ص ١٩ – ٢٦؛ عبدالمجيد سيد احمد منصور، السلوك الاجرامى والتفسير الاسلامى، الرياض، مركز أبحاث الجريمة.

٣٥ – من القانون الليبى فى المادة ٦٤ ع.ل على أنه (مع مراعاة مسئولية المؤلف وباستثناء حالات الاشتراك إذا ارتكبت أحدى الجرائم عن طريق الصحافة الدورية يعاقب حسب الأحكام الاتية: المدير أو المحرر المسئول الذى لا يمنع النشر عندما لا تتوفر الموانع الناتجة عن القوة القاهرة أو الحادث الطارئ أو الاكراه المادى أو المعنوى الذى لا يمكن دفعه إذا كون الفعل جناية أو جنحة تتوفر فيها النية الإجرامية وتطبق العقوبة المقررة للجريمة المرتكبة مع خصمها إلى حد النصف وإذا كون الفعل جريمة خطيئة أو مخالفة فتطبق العقوبة المقرر لها) ونصت المادة ٣١ من قانون المطبوعات الليبى رقم ٧٦ الصادر سنة ١٩٧٢ على المسئولية المتتابعة بالنسبة للجرائم المرتكبة بواسطة المطبوعات غير الدورية أو شبة الدورية.

٣٦ – عادل ريان محمد، جرائم الحاسب الآلى وأمن البيانات، العربى، (٤٤٠)، ١٩٩٥، ص ص ٧٣ – ٧٧.

٣٧ – فهد بن عبدالله اللحيدان، الإنترنت، شبكة المعلومات العالمية، الطبعة الأولى، الناشر غير معروف، ١٩٩٦، ص٥١ وما بعدها.

٣٨ – محمد فتحى عيد، الإجرام المعاصر، الرياض: أكاديمية نايف العربية للعلوم الأمنية، ١٤١٩هـ، ص ١٢.

٣٩ – جميل عبد الباقى الصغير، الإنترنت والقانون الجنائى، دار النهضة العربية، ١٩٩٢، ص ١١٩.

٤٠ – مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ص ٥٧–٦٩؛ محمد عبد الطاهر حسين، المسئولية القانونية فى مجال شبكات الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢، ص ٣٨.

٤١ – هلالى عبداللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة فى ٢٣ نوفمبر ٢٠٠١)، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٦، ص١٦٠؛ عبدالفتاح بيومى حجازى، الدليل الجنائى والتزوير فى جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٢، ص١٣.

42 - V. dr. Mohammed Buzubar, "la Criminalite informatique sur L'internet", Journal of law, (Kwait University), No.1, Vol.26, March 2002, p. 21 et s.

- جميل عبدالباقى الصغير، القانون الجنائى والتكنولوجيا الحديثة، الكتاب الأول: الجرائم الناشئة عن استخدام الحاسب الآلى، دار النهضة العربية، القاهرة، ١٩٩٢، ص ص ٤ - ٥؛ محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، ١٩٩٨، ص٣؛ عبدالله العلوى البلغيثى: "الإجرام المعاصر، أسبابه وأساليب مواجهته"، ورقة مقدمة ضمن أشغال المناظرة الوطنية حول (السياسة الجنائية بالمغرب: واقع وآفاق)، التى نظمتها وزارة العدل بمكناس خلال الفترة من ٩ - ١١ ديسمبر ٢٠٠٤، المجلد الأول، (الأعمال التحضيرية)، الطبعة الثانية، منشورات جمعية نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية، العدد (٣)، ٢٠٠٤، ص٢٢٢.

٤٣ - ذياب البداينة، المنظور الاقتصادى والتقنى والجريمة المنظمة، ضمن أبحاث حلقة علمية حول الجريمة المنظمة وأساليب مكافحتها، التى نظمتها أكاديمية نايف العربية للعلوم الأمنية، ١٤ - ١٨ نوفمبر ١٩٩٨، مركز الدراسات والبحوث، الرياض، ١٩٩٩، ص٢٠٩ وما بعدها؛ كذلك انظر بالخصوص بحثنا السابق، ص٨١؛ بحثنا الموسوم بالإرهاب والإنترنت، مقدم إلى المؤتمر الدولى لجامعة الحسين بن طلال بعنوان: الإرهاب فى العصر الرقمى، المنعقد بمدينة معان، الأردن، خلال الفترة ١٠ - ٢٠٠٨/٧/١٣، ص١ وما يليها؛ جميل الصغير، المرجع السابق، ص٥ وما بعدها؛ حسنين المحمودى بوادى، إرهاب الإنترنت، الخطر القادم، الطبعة الأولى، دار الفكر العربى، الإسكندرية، ٢٠٠٦، ص ٤٩ وما بعدها؛ محمد أمين الرومى، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٤، ص٧.

٤٤ - جميل عبد الباقى الصغير، الإنترنت والقانون الجنائى، دار النهضة العربية، ٢٠٠١، ص ١٢٩.

- أحمد السيد عفيفى، الأحكام العامة للعلانية فى قانون العقوبات، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠١ - ٢٠٠٢، ص ص ٥٥١ - ٥٥٢.

٤٥ - جميل عبد الباقى الصغير، الإنترنت والقانون الجنائى، مرجع سابق، ص ص ١٣٢-١٣٤.

٤٦ - ينص الفصل ٥٧٥ من القانون الجنائى المغربى (من طبع فى المملكة كلا أو بعضا من الكتب أو التصانيف الموسيقية أو الرسوم أو الصور الفنية أو أى إنتاج أخر مطبوع أو منقوش، مخالف بذلك القوانين والنظم المتعلقة بملكية مؤلفيها،يعد مرتكبا لجريمة التقليد،

ويعاقب بغرامة من مائتين إلى عشرة آلاف درهم، سواء نشرت هذه المؤلفات فى المغرب أو فى الخارج.

- ويعاقب بنفس العقوبة من يعرض هذه المؤلفات المقلدة للبيع أو يوزعها أو يصدرها أو يستوردها) انظر فى هذا المعنى بصدد جريمة السرقة، محمود نجيب حسنى: جرائم الاعتداء على الأموال فى قانون العقوبات اللبنانى، دار النهضة العربية، بيروت، ١٩٦٩، ص ص ٦٣-٦٤، عبد الفتاح الصيفى: قانون العقوبات اللبنانى جرائم الاعتداء على أمن الدولة وعلى الأموال دار النهضة العربية، بيروت، ١٩٧٢، ص ٢٥٦.

٤٧ - أحمد السيد عفيفى، المرجع السابق، ص ٥٥٤.

٤٨ - محمد حسن منصور، المسئولية الإلكترونية، دار الجامعة، للنشر، الإسكندرية، ٢٠٠٣، ص ٢٠٢.

٤٩ - جميل عبد الباقى الصغير، المرجع السابق، ص ص ١٣٧-١٣٨.

٥٠ - المادة الأولى من القانون المغربى رقم٠٠- ٢ بشأن حماية حق المؤلف والحقوق المجاورة. ويقصد بمصطلح برنامج الحاسوب وفق المادة الأولى من القانون المغربى المتعلق بحقوق المؤلف والحقوق المجاورة (كل مجموعة من التعليمات المعبر عنها بكلمات أو برموز أو برسوم أو بأى طريقة أخرى تمكن - حينما تدمج فى دعامة قابلة لفك رموزها بواسطة آلة - أن تنجز أو تحقق مهمة محددة، أو تحصل على نتيجة بواسطة حاسوب أو بأى طريقة إلكترونية قادرة على معالجة المعلومات) المادة ١-٦٤.

٥١ - جميل عبدالباقى الصغير، المرجع السابق، ص ١٣٥.

٥٢ - هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢، ص٥.

٥٣ - عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٤، ص٧٨٥ وما بعدها؛ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية . دراسة مقارنة، مكتبة الآلات الحديثة . أسيوط، ١٩٩٤، ص٥ وما يليها؛ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت فى مرحلة جمع الاستدلالات. دراسة مقارنة، (رسالة ماجستير)، دار الفكر الجامعى، الإسكندرية، ص٣٥ وما بعدها.

٥٤ - جميل عبدالباقى الصغير، مرجع سابق، ص١٤٢.

٥٥ – إن القانون رقم ٧٣ لسنة ١٩٧٢ بشان المطبوعات الليبى ينص فى المادة ٣١ على أن المطبوعات تشمل الكتابات والصور والرسوم، ولما كان ما يبث على الشبكة يعد من الكتابات، فإن اعتبار عامل الإيواء هنا قائما بدور رئيس التحرير تواجهه عقبة فنية تتمثل فى عدم قدرته على مراقبة المضمون

56 - Chriss Reed, Internet Law- 2004 - Campridge University Press, p.89.

٥٧ – أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلى والإنترنت – دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر . عمان . الأردن، ٢٠٠٠، ص١٠٥ ؛ بحثنا السابق السياسة الجنائية فى مواجهة جرائم الإنترنت Cyber Crimes، ص٩٠.

٥٨ – هشام رستم، ص ١٨؛ أسامة أحمد المناعسة وآخرون، ص٢٨٩؛ جميل عبدالباقى الصغير، أدلة الإثبات الجنائى والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، ٢٠٠٢، ص١١٣ وما بعدها.

٥٩ – عطية عثمان محمد بوحويش، حجية الدليل الرقمى فى إثبات جرائم المعلوماتية، رسالة التخصص العالى (الماجستير)، مقدمة إلى أكاديمية الدراسات العليا/ فرع بنغازى، للعام الجامعى ٢٠٠٩، ص٧٠.

٦٠ – جميل عبدالباقى الصغير، أدلة الإثبات الجنائى والتكنولوجيا الحديثة، ص١١٥؛ عطية بوحويش، ص٧٣ وما بعدها.

٦١ – أسامة أحمد المناعسة وآخرون، ص٢٨٠ وما بعدها؛ هلالى عبداللاه أحمد، تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى. دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٧، ص٧٧ وبما بعدها.

٦٢ – مأمون سلامة، الإجراءات الجنائية فى التشريع الليبى، ج ٢ط٢٠٠٠، منشورات المكتبة الجامعة، ص١٥١.

٦٣ – مأمون سلامة، المرجع السابق، ص١٦٠.

٦٤ – أحمد شرف الدين، حجية الرسائل الإلكترونية فى الإثبات، شبكة المعلومات القانونية العربية، East Law.com، ٢٠٠٧.

٦٥ – عمر بن يونس، الإجراءات الجنائية عبر الإنترنت فى القانون الأمريكى "المرشد الفيدرالى الأمريكى لتفتيش وضبط الحواسيب وصولًا إلى الدليل الإلكترونى فى التحقيقات الجنائية"، الطبعة الأولى، ٢٠٠٤ - ٢٠٠٥، ص ص٢٠١ – ٢٠٤.

٦٦ – على أحمد راشد، المدخل وأصول النظرية العامة، ١٩٧٤، ص١٨٥؛ عدنان الخطيب، موجز القانون الجزائى، الكتاب الأول، المبادئ العامة فى قانون العقوبات، مطبعة جامعة دمشق، ١٩٦٣، ص٧٩؛ موسى مسعود ارحومة، الأحكام العامة لقانون العقوبات الليبى، الجزء الأول، النظرية العامة للجريمة، الطبعة الأولى، منشورات جامعة قاريونس، بنغازى، ٢٠٠٩، ص١١٠ وما يليها.

- R. Vouin et J. Léauté, droit pénal et procédure pénale, 2 me éd., Paris, 65, P. 19; Mohieddine Amzazi, Présis de droit Criminel, 1 ère éd.,1994, 4, Dar Nachr Al Maarifa, Rabat, p. 62.

٦٧ – وإذا كانت المادة ٧٤ إجراءات جنائية ليبى تنص على انتقال المحقق لأى مكان ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديًا، فهل يكون للجريمة المعلوماتية وجود مادى، يمكن للمحقق الليبى معاينته؟ نجد فى هذه المادة أن المشرع سن هذا النص لضبط جريمة لها وجود مادى محسوس فى العالم الخارجى، وما يؤكد ذلك هو أن المادة ٤٤ من ذات القانون تنص على أن (توضع الأشياء والأوراق التى تضبط فى حرز مغلق وتربط كلما أمكن) فالحرز المغلق الذى يتم ربطه هو الإجراء العام الذى تخضع له كل الأشياء المضبوطة، وهنا نصطدم بالعقبة الأساسية أمام معاينة الجريمة المعلوماتية التى ترتكب داخل الفضاء المعلوماتي أو السيبرانى، فالمحقق فى هذه الحالة يتعامل مع بيئة مليئة بالنبضات الاليكترومغناطيسية والبيانات المخزنة داخل نظام معلوماتية شديدة الحساسية ولا يتعامل مع أوراق أو أسلحة أو أشياء قابلة للربط وهو ما يؤكد القواعد الإجرائية التقليدية سنت لتواجه سلوكًا ماديا يرتكب بواسطة الات وأدوات قابلة للربط والتحريز.

68 - Recommandations sur le dépistage des communications électroniques transfrontalière dans le cadre des enquêtes sur les activités criminelles www G8 Mont tremblant Canada 21 mai 2002.

أشار إليه صالح أحمد البربرى دور الشرطة فى مكافحة جرائم الإنترنت فى إطار الاتفاقية الأوروبية، الموقعة فى بودابست فى ٢٠٠١/١١/٣ – www.arablawinfo.com

69 - P. Wilhem, "La hiérarchie des responsabilité sur Internet", précité, p. 4.

٧٠ – موسى مسعود أرحومة، تحديد النطاق المكانى لجرائم تلويث البيئة البحرية والقانون الواجب التطبيق، ورقة مقدمة إلى المؤتمر العلمى الخامس لكلية الشريعة والقانون/ جامعة إربد الأهلية بعنوان: البيئة فى ضوء الشريعة والقانون – واقع وتطلعات، الأردن، خلال الفترة ١٢ – ١٣ يوليو، ٢٠٠٦، ص٥ وما بعدها.

٧١ – ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائى، دار النهضة العربية، القاهرة، ١٩٨٣، ص ٢٠٧؛ أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة ١٩٩٤، ص ٤٨.

٧٢ – صالح أحمد البربرى، دور الشرطة فى مكافحة جرائم الإنترنت فى إطار الاتفاقية الأوروبية، الموقعة فى بودابست فى ٢٠٠١/١١/٢٣ –www.arablawinfo.com، ص ٢.

٧٣ – كمال أنور محمد القاضى، تطبيق قانون العقوبات من حيث المكان، رسالة دكتوراه، مقدمة إلى كلية الحقوق، جامعة القاهرة، ٢٢ إبريل، دار مطابع الشعب، ١٩٦٥، ص٩٠ وما يليها.

٧٤ – أحمد عبدالكريم سلامة، قانون حماية البيئة، دراسة تأصيلية فى الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود، السعودية، ١٤١٨هـ، ١٩٩٧، ص٥٣٥.

٧٥ – منير الجنبهى، ممدوح الجنبهى، صراخ الإنترنت وسائل مكافحتها، المرجع السابق، ص ٩. فتوح الشاذلى، القانون الدولى الجنائى، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠١، ص ٣٤.

٧٦ – سالم محمد سليمان الأوجلى: أحكام المسئولية الجنائية عن الجرائم الدولية فى التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٩٩٧، ص ٤٢٥

77 - USA V. Thomas, no. cr – 94 – 20019 – 9 (w. d. tenn. 1994).

مشار إليها عند: عمر محمد بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص٩٠٨.

٧٨ – جميل عبد الباقى الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٨، ص ٧٥.

٧٩ – تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادى عشر لمنع الجريمة والعدالة الجنائية، المنعقد فى بانكوك فى الفترة ١٨-٢٥/٤/٢٠٠٥ – وثيقة رقم A/CONF.203/14. ص ٥.

٨٠ – جميل عبد الباقى الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة ١٩٩٨، ص ٧٥.

٨١ – تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادى عشر لمنع الجريمة والعدالة الجنائية، المنعقد فى بانكوك فى الفترة ١٨-٢٥/٤/٢٠٠٥، وثيقة رقم A/CONF.203/14.

٨٢ – عبد الفتاح بيومى حجازى: الدليل الجنائى والتزوير فى جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٢، ص١٠٢.

٨٣ – جميل عبد الباقى الصغير، الجوانب الإجرائية، المرجع السابق، ص ٧٢.

٨٤ – عبدالله محمد صالح الشهرى، المعوقات الإدارية فى التعامل الأمنى مع جرائم الحاسب الآلى: دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، رسالة ماجستير غير منشورة، جامعة الملك سعود، الرياض، المملكة العربية السعودية، ١٤٢٢هـ.

٨٥ – هذه المعايير الثلاثة هى مكان القبض على المتهم، مكان وقوع الجريمة أو محل إقامة المتهم

86 - Floret latrive:41 pays contre les pirates.disponible sur:www. liberation.com/multi/actu/20000424/20000427chtml

٨٧ – جميل عبد الباقي الصغير، الجوانب الإجرائية، مرجع سابق ص ٧٣.

88 - www.cybercrime.gov/coepress.html

- قبل وضع هذا المشروع كان المجلس الأوروبى قد وافق على التوصية رقم R٨٩-٩ وتتضمن هذه التوصية قائمتين بالجرائم التى تقع فى مجال الحاسب الآلى، الأولى تحتوى على الحد الأدنى من الجرائم الواجب النص عليها فى التشريعات الوطنية للدول المختلفة (ومنها الدخول غير المشروع لنظام الحاسب الآلى أو لشبكة المعلومات)، فى حين أن القائمة الثانية اختيارية وتضع مجموعة من الجرائم مثل إتلاف المعلومات وبرامج الحاسب الآلى.
- للمزيد حول هذه التوصية انظر مقال محمد أبو العلا عقيدة: مواجهة الجرائم الناشئة عن استخدام الحاسب الآلى، مجموعة أعمال مؤتمر حول الكمبيوتر والقانون المنعقدة، بالفيوم من ٢٩ يناير إلى ١ فبراير ١٩٩٤، ص ص ١١٩ – ١٢٠، جامعة عين شمس.

٨٩ – ينص الفصل ٤٠ من مجموعة القانون الجنائى المغربى على ما يلى:

- "يجوز للمحاكم فى الحالات التى يحددها القانون إذا حكمت بعقوبة جنحية أن تحرم المحكوم عليه لمدة تتراوح بين سنة وعشر سنوات، من ممارسة حق أو عدة حقوق من الحقوق الوطنية أو المدنية أو العائلية المنصوص عليها فى الفصل ٢٦.
- يجوز أيضا للمحاكم تطبيق مقتضيات الفقرة الأولى من هذا الفصل إذا حكمت بعقوبة جنحية من اجل جريمة إرهابية.

٩٠ – جميل عبد الباقى الصغير، الجوانب الإجرائية، المرجع السابق، ص ٩١.

٩١ - ينص الفصل ٢٦ من مجموعة القانون الجنائى المغربى على ما يلى: التجريد من الحقوق الرسمية يشمل:

- عزل المحكوم عليه وطرده من جميع الوظائف وكل الخدمات والأعمال العمومية.
- حرمان المحكوم عليه من أن يكون ناخبا أو منتخبا وحرمانه بصفة عامة من سائر الحقوق الوطنية ومن حق التحلى بأى وسام.
- عدم الأهلية للقيام بمهمة محلف أو خبير وعدم الأهلية لأداء الشهادة فى أى رسم من الرسوم أو الشهادة أمام القضاء إلا على سبيل الإخبار فقط.
- عدم أهلية المحكوم عليه بان يكون وصيا أو مشرفا على غير أولاده.
- الحرمان من حق حمل السلاح ومن الخدمة فى الجيش والقيام بالتعليم أو إدارة مدرسة أو العمل فى مؤسسة للتعليم كأستاذ أو مدرس أو مراقب.
- والتجريد من الحقوق الوطنية عندما يكون عقوبة أصلية يحكم به لزجر الجنايات السياسية ولمدة تتراوح بين سنتين وعشر سنوات ما لم تنص مقتضيات خاصة على خلاف ذلك.

٩٢ - ينص الفصل ٢-٢١٨ (يعاقب بالحبس من سنتين إلى ست سنوات وبغرامة تتراوح بين ١٠٠٠٠و٢٠٠٠٠٠ درهم كل من أشاد بأفعال تكون جريمة إرهابية بواسطة الخطب أو الصياح أو التهديدات المفوه بها فى الأماكن أو الاجتماعات العمومية أو بواسطة المكتوبات والمطبوعات المبيعة أو الموزعة أو المعروضة للبيع أو المعروضة فى الأماكن أو الاجتماعات العمومية أو بواسطة الملصقات المعروضة على أنظار العموم بواسطة مختلف وسائل الإعلام السمعية البصرية والالكترونية).

93 - Office fédéral de la justice, le nouveau media interroge le droit, rapport d un groupe intertemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscité par Internet, Berne, mai 1996. voir cet article sur le site: www.ofg.admin.ch.

- انظر فى هذا الصدد البحث المقدم من د. محمد أبو العلا عقيدة: الحماية الجنائية للتجارة الإلكترونية، ندوة مركز بحوث الشرطة بأكاديمية الشرطة حول المردودات الأمنية لنظام التجارة الإلكترونية، أكاديمية الشرطة، ٢٩ أبريل٢٠٠٢، ص ٥.
- حسام شوقى، حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة، ٢٠٠٣، ص ١٣٦.

٩٤ – من الأمثلة على التشريعات المعنية بالجرائم المعلوماتية: حماية البيانات والخصوصية، القانون الجنائى، حماية الملكية الفكرية، الحماية من المضمون الضار، قانون الإجراءات الجزائية، التشفير والتوثيقات الرقمية. أنظر:

Ulrich Sieber, Legal Aspects of Computer- Related Crime in the Information Society.Com crime Study. 1/01/1998

٩٥ – انظر أيضا المادة ١١ من اتفاقية ١٩٨٨ بشأن التسليم المراقب، والمادة ٥٠ من اتفاقية الأمم المتحدة لمكافحة الفساد.

٩٦ – راجع فى ذلك الأدلة التشريعية لتنفيذ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبرتوكولات الملحقة بها (منشورات الأمم المتحدة رقم المبيع (E.O.5.V2) الجزء الأول – الفقرة ٣٨٤.

٩٧ – عبد الكريم غالى، الحماية القانونية للإنسان من مخاطر المعلوميات، رسالة دكتوراة، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط، ١٩٩٥، ص١٨.

98 – Guidelines Concerning Computerized Personal Data Files. Adopted by the General Assembly on 14 December 1990:Francesco Miani: le cadre réglementaire des traitements de données personnelles effectues au sein de l'union européenne, revue trimestrielle de droit européen, Dalloz, No.2, 2000, p. 283.

٩٩ – أنظر ما جاء بتوصية المجلس الأوربى رقم (R95)13 الصادرة فى ١٩٩٩/٠٩/١١م بشأن مشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات

100 - Charlotte-Marie pitrat-Laurent le veneux: Protection du consommateur et des données personnelles. voir le site: www.finance.gouv.fr,Tierry Leonard: E.Marketing et protection des données à caractère personnel. voir le site: www.droit-technologie.org

١٠١ – على سبيل المثال ٢٢ من الاتفاقية الأوروبية بشأن الإجرام المعلوماتى.

١٠٢ – أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، ١٩٨٨، ص ٨٥.

١٠٣ – مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، ط١، ٢٠٠١، ص ٧٧.

١٠٤ – تعزيز التعاون الدولى فى إنفاذ القانون، مرجع سابق، ص ٢٦.

١٠٥ – كانت هذه الحماية مثار جدل كبير فى فرنسا قبل تدخل المشرع الفرنسى بالنص عليها صراحة القانون رقم ٨٥–٦٦٠ الصادر فى ٣ يوليه ١٩٨٥، وكان الفقه والقضاء هناك منقسمين حول امتداد حماية حق المؤلف إلى برامج الحاسب الآلى بسبب الاختلاف حول توافر شروط المصنف المحمى فى برامج الحاسب الآلى: انظر على سبيل المثال.

- Lucas, A., Les programmes d'ordinateurs comme objets de droits intellectuelles, JCP, 1982,1,Doc,3081.
- Huet, J., La modification du droit sous l'influence de l informatique, aspect de droit privé, JCP, 1983, 1, Doc, 3095.
- Goutal, J. L., La protection juridique du logiciel, D.1984, Chron, p. 197.
- Vivant, M., Informatique et propriété intellectuelle, JCP, 1984,1 Doc,3081.
- انظر فى عرض هذا الخلاف بالتفصيل محمد حسام لطفى، الحماية القانونية لبرامج الحاسب الآلى، القاهرة، دار الثقافة للطباعة والنشر، ١٩٨٧، ص ٨٧ وما بعدها.

THE CRIMINAL RESPONSIBILITY OF THE MEDIATORS OF INTERNET SERVICES

Mohamed Nasr

Ever since the internet existed, there has been a legal argument on the status of Internet Service Providers (ISP) and their role in achieving the best use of the World Wide Web.

Most often the ISP had pleaded to mitigate the legal obligations that case law has strained them with, and at the same time they practiced pressure to build a special legal system that aims to relief them from the responsibility whether pertaining to their breach in providing the service or the illegality of the data that is being processed on their servers.

Such as the French and the European legislations put an end to this controversy by adopting a special legal system for the ISP. Accordingly their legal obligations have been set clearly and unique provisions for determining their responsibility for any contravention on the Internet have been set.

Laws of some countries, like the Jordanian law, did not adopt such a legal system, and this raises an important question relating to the efficiency of applying the general rules to find balanced solutions that meet the special nature of the ISP work.