مجلة العلوم الإنسانية —— عدد 50 ديسمبر2018، المجلد أ، ص. ص 85-97 ——

معوقات مكافحة الجريمة المعلوماتية

بثينة حبيباتني
كلية الحقوق
جامعة الجزائر1

ملخص:
مما لا شك فيه أن الصعوبات التي تعترض سبل مكافحة الجريمة المعلوماتية متعددة، وكلها تنبع من كون هذه الجرائم تختلف جملة وتفصيلا عن الجرائم العادية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحتها، سواء أثناء إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمه للعدالة، أو خلال ملاحقة الجناة وكشف جرائمهم عبر الحدود.
لذلك تثور العديد من المشكلات والتي تقف عائقا أمام مكافحة الجريمة المعلوماتية، منها ما يتعلق بالكشف عن الجريمة والوصول إلى الجناة، وبعضها متعلق بإثبات الجريمة المعلوماتية، كما قد يبرز للوجود صعوبات متعلقة بالتعاون القضائي الدولي وتحديد قواعد الاختصاص.
الكلمات المفتاحية:
الجريمة المعلوماتية- صعوبات مواجهة الجريمة المعلوماتية- اكتشاف وإثبات الجريمة المعلوماتية-التعاون الدولي في مجال الجريمة المعلوماتية.

Abstract:
Undoubtedly, there are many problems hampering the process of fighting cybercrime. They are all due to the fact that these crimes are totally different from ordinary crimes. This raises some legal and operational challenges for the systems in charge of its fight. The challenges may intervene at the stage of gathering evidence and investigating through the virtual space to detect criminals and prosecute them, or at stage of tracking criminals and detecting their cross-border crimes.
Thus, many problems arise in the way of fighting cybercrimes, some of them are related to the detection of the crime and the identification of criminals and other are related to proving the cybercrime. Other problems may arise in relation to difficulties in the international judicial cooperation and the determination of jurisdictional rules.
Key words: Cyber criminality- difficulties in fighting cybercrimes- detection and confirmation of cybercrimes- international judicial cooperation in matters of cyber-criminality.

مقدّمة:

أدى التطور الكبير والانتشار الواسع والمتسارع للتقنية العالية والمتمثلة في الأنظمة المعلوماتية، إلى ظهور جملة من الجرائم تعددت صورها وأشكالها أطلق عليها الجرائم المعلوماتية.
فلم تعد الجريمة ترتكب بشكلها التقليدي بل تعدته إلى استعمال شبكة المعلومات إما كوسيلة لارتكاب العديد من الجرائم بعيد عن أعين الجهات الأمنية، أو أن تكون هي بيئة الجريمة، خاصة مع انتشار استعمال شبكة الويب العالمية (الانترنت)، والتي صنعت عالما افتراضيا لا يعترف بالحدود الجغرافية، فانتقلت الجريمة من صورتها المادية التقليدية إلى أخرى معنوية عابرة للدول والقارات، مما فرض على المجتمع الدولي البحث عن وسائل لمكافحة هذه الطائفة من الجرائم وذلك بإيجاد نظام عقابي لمرتكب جرائم المعلوماتية.

وعلى الرغم من أن مواجهة هذه الطائفة من الجرائم تتم بعدة اتجاهات، سواء بسن الدول لتشريعات جديدة أو تعديل تشريعاتها القائمة، إلا أن محاولات التصدي لها اصطدمت بعدة صعوبات، نظرا لخصوصية الجريمة المعلوماتية، والتي ترتكب في عالم رقمي لا يستغرق زمن ارتكابها سوى زمن بسيط، كما أن محو آثارها وإتلاف أدلتها عملية سهلة، وكشف هوية مرتكبها ليس بالأمر الهين، حيث يمكن للجاني تخزين البيانات المتعلقة بنشاطه الإجرامي في دولة أخرى، أو في مكان بعيد عن مكان ارتكاب الجريمة، ومع تمكنه من ترميز المعطيات الأمر الذي جعل إخفائها عن أجهزة العدالة أمرا بسيطا.

ولما كانت هذه الجرائم من طبيعة خاصة، فإن خطرها أو آثارها لم تعد محصورة في النطاق الإقليمي لدولة معينة، الأمر الذي بات يثير بعض التحديات أمام السلطات القضائية الدولية.

وعلى هدي هذه الأفكار، يمكننا طرح التساؤل التالي: **فيما تتمثل الصعوبات التي تعترض سبل مكافحة الجريمة المعلوماتية؟.** وبعبارة أخرى: **ما هي أهم المشكلات القانونية والفنية التي تواجه مكافحة الجريمة المعلوماتية؟.**

وسنجيب على هذا التساؤل وفقا لما يلي:

المبحث الأول: معوقات اكتشاف وإثبات الجريمة المعلوماتية

تحيط الجريمة المعلوماتية جملة من الصعوبات التي تقف أمام الكشف عنها والوصول إلى الجاني، نظرا للوسيلة المستعملة في ارتكابها وطبيعة المحل المعتدى عليه والمتمثل في معلومات معالجة آليا هذا من جهة، ومن جهة أخرى فإنه يصعب إثبات هذا النوع المستحدث من الإجرام وإسناد الجرم لفاعله لكون هذا الأخير يتميز بالذكاء والخبرات الفنية والعقلية، فيسعى إلى محو وإخفاء الدليل بشتى الطرق مما يجعل عملية إثباتها تعترضها العديد من العراقيل.

وعليه سنتناول في هذا المبحث معوقات اكتشاف الجريمة المعلوماتية من خلال المطلب الأول، ومن ثم نتعرض إلى معوقات إثبات الجريمة المعلوماتية من خلال المطلب الثاني.

المطلب الأول: معوقات اكتشاف الجريمة المعلوماتية

إن مرد صعوبات اكتشاف الجريمة راجع لعدة اعتبارات منها ما هو متعلق بالإحجام عن إبلاغ السلطات المختصة، وكذلك نقص خبرة سلطات الاستدلال، ومنها ما هو راجع إلى فقدان الآثار التقليدية للجريمة، وكذلك فرض الجناة لتدابير الحماية.

الفرع الأول: إحجام الجهات المتضررة عن إبلاغ السلطات المختصة

إن عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات تعد إحدى معوقات اكتشاف الجريمة، إذ تحرص الجهات المجني عليها والتي غالبا ما تكون مصرفا، أو مؤسسة مالية، أو شركة، أو مشروعا صناعيا ضخما، على الإحجام عن الإبلاغ عن الجريمة بسبب الحفاظ على سمعة المؤسسات و مصداقيتها وثقة عملائها وعدم رغبتها في الظهور بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني، ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها[1]، الأمر الذي يجعلهم يفضلون الترضية المالية لعملائهم حتى لا يفقدوهم، ولا تتأثر سمعتهم المالية بدلا من البحث على الجناة، فهذه المؤسسات لا تكتفي في إطار ذلك بالإحجام عن الإبلاغ، وإنما إلى جانب ذلك تلجأ إلى الترضية الودية فيما بينها، وبين الجناة[2].

كما يكون الإحجام عن الإبلاغ عن هذا النوع من الجرائم من أجل إخفاء أساليب ارتكابها للحيلولة دون تقليد الآخرين للجناة ومحاكاتهم في جرائمهم، كما قد يتوخى بعض المجني عليهم من وراء العزوف عن الإبلاغ عدم إتاحة الفرصة للأجهزة الأمنية من الإطلاع على معلومات لم يجر الإبلاغ عنها، وربما يظهر ذلك بصورة أكبر في نطاق الجرائم التي تستهدف شركات التأمين أو البنوك رغبة في توقي الخسائر التي يتوقع تحققها نتيجة هذا الإبلاغ بسبب نقص ثقة العملاء في هذه المؤسسات[3].

الفرع الثاني: نقص خبرة سلطات الاستدلال

المعلوم أن متطلبات العدالة الجنائية تفرض على الأجهزة المسئولة عن تتبع الجرائم وضبطها والتحقيق فيها أن تتحمل مسؤوليتها نحو اكتشاف المجرمين وضبطهم ومحاكمتهم، ومثل هذا الأمر

يقتضي توفير الإمكانات التقنية اللازمة في عملية الكشف والاستدلال عن الجرائم، لاسيما بعد أن تطورت أساليب ارتكاب الجرائم وظهور أنماط مستحدثة من الجرائم ما كانت التشريعات لتعرفها من قبل، إلا بعد أن ظهرت وسائل متطورة تمكن المجرمين ارتكاب جرائمهم بأساليب وطرق غير معهودة لرجال السلطة العامة[4].

وعليه فإن توفير الإمكانات التقنية في الاستدلال والتحقيق عن هذه الجرائم سيكون أكثر حاجة فيها من غيرها من الجرائم، إذ أن القصور في توفير هذه الإمكانيات من شأنه أن يؤدي إلى صعوبة في اكتشاف هذه الجرائم، إذن ما يزيد من صعوبة اكتشاف هذه الجرائم هو قلة خبرة السلطات الاستدلالية، أو قلة الوسائل والإمكانيات لدى تلك الجهات إن توفر الكادر الفني، لذلك وفي سبيل تذليل هذه الصعوبة، هناك من يقترح ضرورة استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال للاستعانة به في التحقيق، وضرورة الاستعانة بالنخبة المتخصصة في أنظمة المعالجة الآلية لضبط هذه الجرائم واكتشافها، وتقديم أدلة الإدانة فيها، وتولي شرح هذه الأدلة وأبعادها أمام المحاكم[5].

فهناك جملة من الصعوبات تواجه عمل المحققين، وخاصة منهم غير المتخصصين أو غير ذوي الخبرة والدراية، والذين انحصرت معلوماتهم في جرائم قانون العقوبات التقليدية من قتل وسرقة، فمثل هؤلاء لن يكونوا قادرين على التعامل معها، كونها ترتكب بطريقة تقنية، حيث لا تتوفر لهم الدراية الفنية بهذا المجال، ولا التدريب والتقنية المطلوبين لكيفية التعامل مع أنظمة المعالجة الآلية[6]، الأمر الذي جعل بعض الدول تخصص وحدات وفرقا متخصصة في مجال البحث والتحري عن الجريمة المعلوماتية، إلا أنه من الغير الكافي أن يتم إنشاء أجهزة فنية متخصصة، بل لابد من إتباع إستراتيجية تدريبية وتكوين متعمق في ميدان تكنولوجيات الإعلام والاتصال[7].

كما أن بعض هذه المعوقات ترجع إلى شخصية المحقق، مثل التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الانترنت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية[8].

الفرع الثالث: فقدان الآثار التقليدية للجريمة

إذا كان من السهل على جهات التحري والتحقيق أن تتحرى على الجرائم التقليدية عن طريق المشاهدة أو التتبع أو سماع الشهود فإنه يصعب عليها ذلك في الجرائم المعلوماتية، إذ أن الجريمة تظل مجهولة ما لم يبلغ عنها للجهات المعنية بالاستدلالات والتحقيق الجنائي، وفي هذا الصدد تجدر الإشارة أن أهم الجرائم لا تصل إلى علم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، لكونها جرائم غير تقليدية لا تخلف أثار مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة[9]، ومشاهدة الجروح التي على المجني عليه، وعلامات التسمم التي ظهرت على المجني عليه نتيجة استخدام المواد السامة في جريمة القتل وكذلك التزوير والتزييف حيث يمكن مشاهدة النقود المزورة والمزيفة، وهذا كله يعود إلى طبيعة الجريمة المرتكبة، والوسيلة التي تستخدم في ارتكابها، أما الجريمة المعلوماتية فإن الأمر جدا مختلف، فمن حيث الوسيلة التي ترتكب بها مثل هذه الجرائم فإنها يتم ارتكابها عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي وشبكة الاتصالات العالمية بصورة آلية، وكما تنساب الكهرباء عبر الأسلاك، أو أن يتم نقلها بالإشعاعات، وغالبا ما يتم هذا عن طريق وحدات طرفية بعيدة، ربما تكون هذه الوحدات لا سلكية الاتصال مما يصعب ضبطها، بل أن هذه الجرائم يمكن ارتكابها عن طريق الهاتف إذ يمكن عن طريقه إصدار تعليماته للحاسب الآلي، ومن مسافات بعيدة قد تتعدى نطاق إقليم الدولة، مما يزيد من صعوبة اكتشافها[10].

وكما يرجع السبب في افتقاد الآثار التقليدية للجريمة المعلوماتية إلى ما لاحظه جانب من الفقه من أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها[11].

الفرع الرابع: فرض الجناة لتدابير أمنية

إن المتورطون في الجرائم المعلوماتية لديهم قدر كبير من الذكاء والتفوق يجعلهم يباشرون إجرامهم بدقة متناهية خشية افتضاح أمرهم وضبطهم، إذ غالبا ما يضرب المجرم المعلوماتي سياجا أمنيا على أفعاله غير المشروعة قبل ارتكابه لها، لكي لا يقعوا تحت طائلة العقاب، كما يزيد ذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه وذلك بالعمل على ترميز أو تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر شبكات الاتصال، بالإضافة إلى دس بعض التعليمات الخفية بين الأدلة لتصبح كالرمز، بحيث يستحيل على غيره الاطلاع عليها وفهم مقصودها ويتعذر على سلطات البحث والتحقيق الوصول إلى كشف أفعالهم غير المشروعة[12].

المطلب الثاني: معوقات إثبات الجريمة المعلوماتية

سبق وأن تناولنا بعض الصعاب التي تحيط بالجريمة المعلوماتية، وكان لابد لنا في هذا المقام من التطرق إلى باقي الصعوبات المتعلقة بإثبات الجريمة، من غياب الدليل المرئي وسهولة إخفاء الدليل وقصور إجراءات الحصول عليه، بالإضافة إلى تعقد الشبكة العنكبوتية وتشابكها وضخامة كم البيانات المتعين فحصها.

كل هذا كان من المعوقات التي تدخل في إطار إثبات الجريمة المعلوماتية، ولذلك كان لزاما علينا التطرق لمختلف هذه الصعوبات، وذلك من خلال الفروع الآتية:

الفرع الأول: غياب الدليل المرئي

إن هذه النوعية من الجرائم توجد في بيئة لا تعتمد التعاملات فيها على الوثائق والمستندات المكتوبة، بل على نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب، فالدليل في الجريمة التقليدية مرئي على العكس من الجريمة المعلوماتية التي تتم دون رؤية لدليل الإدانة[13].

وكما هو معلوم أن أغلب البيانات والمعلومات التي يتم تداولها من حاسب آلي إلى أخر تكون في هيئة رموز ونبضات وعادة تكون مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو فهمها إلا بواسطة الحاسب الآلي[14].

ولعل خفاء وعدم ظهوره في الجريمة المعلوماتية يجد سنده في أن هذه الجريمة قائمة على معلومة يتم سرقتها أو الاحتيال عن طريقها أو تزويرها، وبمعنى أخر أن هذه المعلومة هي الوسيلة لاقتران الجريمة والتي تخلف أثرا ماديا فيما بعد، لهذا يجد الفقه الجنائي صعوبة في التسليم بكونها موضوعا للسرقة واعتبارها من قبيل المال الذي يمكن سرقته، ذلك أن المعلومات ليست من الأشياء لأنها ليست من المنقولات، كما لا ترد عليها الحيازة ولا تنتقل بالاختلاس[15].

ولا يوجد شك في أن إثبات الجرائم التي تترك أثارا ملحوظة يكون سهلا ميسورا، على العكس في إثبات الجرائم التي تقع على الأمور المعنوية، لأن إثباتها يكون في منتهى الصعوبة، لكونها لا تترك ورائها أي أثر قد يدل أو يكشف عنها.

الفرع الثاني: سهولة إخفاء الدليل

من الصعوبات التي يمكن أن تعيق إثبات الجريمة المعلوماتية سهولة إخفاء الجناة لأدلة الإدانة أو محوها أو تدميرها، إذ يستخدمون في ذلك التلاعب غير المرئي في النبضات والذبذبات الالكترونية التي يتم تسجيل البيانات عن طريقها.

ومما يزيد من إمكانية وسهولة إخفاء هذا الدليل المتحصل من الوسائل الالكترونية، أنه يمكن محوه في زمن قصير جدا قد لا يستغرق أكثر من دقائق، وربما بعض أجزاء الدقيقة، بحيث لا تتجاوز تلك الفترة عدد من الثواني، وبشكل لا يمكن للسلطات اكتشاف الجريمة التي ارتكبها، إذا ما علمت هذه السلطات وقوع الجريمة، وبالتالي عدم استطاعة السلطات إقامة الدليل ضد الجاني[16].

ومن الوقائع العملية التي تؤيد ذلك ما قامت به عصابة محترفة في اختراق أنظمة الحاسب الآلي، وذلك من خلال تصميمها جهاز يمحو جميع أثار أي خطوات وتعاملات سابقة استخدمته في اختراق نظم لحاسبات خاصة بشركات معينة، وفي جميع أنحاء العالم، وكذلك ما قام به أحد الجناة بإدخال تعديل على الحاسب، حيث ضمنه، وفي نطاق التعليمات الأمنية لحماية ما فيه من معلومات

مخزنة، برنامج مهمته محو هذه المعلومات بشكل تلقائي، إذا ما تم اختراق المعلومات من قبل شخص غير مرخص له[17].

الفرع الثالث: ضخامة البيانات المتعين فحصها

يشكل الكم الهائل للبيانات والمعلومات والتي هي بحاجة إلى فحص ودراسة لاستخلاص دليل الجريمة منها، أحد مصادر الصعوبات التي تعيق عملية الإثبات في الجرائم المعلوماتية، حيث أن طباعة كل ما هو موجود في الدعامات الممغنطة قد يتطلب مئات الآلاف من الصفحات، وفي نفس الوقت قد لا تقدم هذه الأخير أي فائدة للتحقيق، ولذلك على السلطات القائمة بالضبط والتحقيق أن لا تتمتع بالخبرة الفنية في مجال الحاسب الآلي فحسب، وإنما لابد أن تمتلك هذه السلطات أيضا القدرة على فحص الكم الهائل من المعلومات والبيانات المخزنة على أنظمة المعالجة الآلية[18].

ويسلك المحقق غير المدرب لمواجهة هذه الصعوبة أحد السبيلين:

إما حجز البيانات الالكترونية بقدر يفوق قدرة البشرية على مراجعتها أو التغاضي عن هذه البيانات كلها على أمل الحصول على اعتراف بالجريمة من المتهم[19].

لذلك وفي ظل تواضع القدرات التي يتمتع بها رجال الضبط والتحقيق، كان لزاما لهذه الجهات أن تستعين بالخبراء التي تقوم على التمييز بين ما هو مفيد للتحقيق وبين ما هو خارج عن إطار التحقيق وما من شأنه تعطيل سير العدالة، حيث أن الاستعانة بالخبراء خاصة في هذا الإطار قد يضع المحقق في دائرة مغلقة من المعلومات وكم هائل من البيانات، قد لا يستطيع الخروج منها، خاصة إن لم يكن مسلحا بالتقنية والقدرة والخبرة المعلوماتية[20].

فتواجد البيانات والمعلومات في الجريمة المعلوماتية يعد عائقا أمام جهات التحقيق والتي تسعى للوصول إلى دليل الإثبات في هذا النوع من الجرائم ونسبتها إلى الفاعل، فكلما كانت هناك بيانات ومعلومات أكثر في جهاز الحاسب الآلي كلما ازداد الأمر تعقيدا للوصول إلى الدليل.

الفرع الرابع: لا محدودية شبكة الانترنت

من الصعوبات التي تواجه سير الإثبات في الجرائم المعلوماتية، هو أن شبكة الانترنت ليس لها حدود دولية، فهي لا تعترف بتلك الحدود القائمة بين الدول، كما أنها ليست مملوكة لأحد، وبالتالي فليس هناك جهاز رقابي عليها ولا سلطة مركزية تتحكم فيها، فالانترنت ظاهرة دولية تنعدم مركزيتها وتتساوى أمامها الدول الكبيرة والصغيرة دون المساس بسيادة الدول، ما يخلق صعوبة كبيرة أمام الجهات التي تقوم بتعقب دليل الإثبات عبر هذه الشبكة[21].

فنظرا لانتشار الشبكات على مستوى العالم فإنه يستحيل الحصول على دليل في حالة توزيع مسرح الجريمة بين أكثر من دولة، بسبب تعقيد الإجراءات ووجود مشاكل عملية وتشريعية في بعض الدول مما يحول دون الحصول على دليل رقمي، كما أن سرعة مرور البيانات الرقمية عبر الشبكات في أقل من ثانية له تأثير عكسي على دليل الإدانة أو البراءة[22].

المبحث الثاني:المعوقات المتعلقة بالجانب القضائي

يتزايد عدد الجرائم المعلوماتية ذات البعد الدولي، ولاسيما لأن وجود مرتكبي هذه الجرائم في مكان وجود الضحية لم يعد لازما في كثير من الأحيان بالنظر إلى أنهم يرتكبون جرائمهم من خلال شبكة الانترنت عبر الوطنية، لهذا أصبح من الضروري أن تتعاون السلطات القضائية دوليا وأن تساعد الدولة صاحبة الاختصاص القضائي.

وعلى الرغم من كون التعاون الدولي الفعال له أهمية بارزة في مجال مكافحة الجريمة المعلوماتية، وذلك بعد أن أصبحت الأخيرة تتخطى حدود الدول، إلا أن الملاحظ في الواقع قصور هذا التعاون مقارنة بتطور هذا النوع المستحدث من الإجرام.

فالتعاون الدولي قد يكون صعبا بسبب الاختلافات القائمة في التشريعات والممارسات بين الدول وكذلك بسبب العدد المحدود نسبيا من المعاهدات والاتفاقات المتاحة للدول بشأن التعاون الدولي[23].

ومن جانب آخر فإنه يتزامن مع ظهور الجرائم المعلوماتية العديد من المشكلات الخاصة بتحديد القانون الواجب التطبيق والقضاء المختص بنظر تلك الجرائم.

وعليه سنتعرض في هذا المبحث إلى المعوقات المتعلقة بالتعاون الدولي من خلال المطلب الأول، والمعوقات المتعلقة بالقانون الواجب التطبيق والاختصاص القضائي من خلال المطلب الثاني.

المطلب الأول: المعوقات المتعلقة بالتعاون الدولي

على الرغم من كون التعاون بين أعضاء المجتمع الدولي يتقدم وبشكل مشجع بشأن مكافحة الجرائم، إلا أنه لم يصل إلى درجة تسمح بإيجاد نظام جنائي فعال يوازي التقدم التكنولوجي الذي شهده العالم، حيث أن الوسائل والتدابير المتخذة في هذا المجال وعلى الرغم من جديتها إلا أنها لا ترتقي إلى مستوى التحدي التي تفرضه الجريمة العابرة لحدود الدولة.

وإن كان التعاون الدولي في مجال مكافحة الجرائم المعلوماتية يعد مطلبا تسعى إلى تحقيقه أغلب الدول، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه سنتعرض إليها فيما يلي:

الفرع الأول: عدم وجود نموذج موحد للنشاط الإجرامي

فمن بين الصعوبات التي تقف أمام التعاون الدولي بشأن مكافحة الجريمة المعلوماتية هو غموض المفاهيم القانونية أو اختلافها، والسبب في ذلك هو عدم الاتفاق على مفهوم موحد للجريمة المعلوماتية، حيث أن الاختلاف في تعريف الفعل المجرم يعد سببا في فشل الجهود الدولية في مكافحة هذا النوع من الإجرام المستحدث.

وعلى الرغم من إصدار العديد من الدول التشريعات التي تكافح الجريمة المعلوماتية، إلا أنه لا يمكن اعتبارها جامعة مانعة والدليل على ذلك أن المؤسسات المحلية في فرنسا والولايات المتحدة الأمريكية وكندا، تطالب في كل عام بإضافة صور وأشكال جديدة من السلوك المعلوماتي والتي لم ينص عليها في التشريعات العقابية المعمول بها في هذا المجال، وبهذا يتبين عدم وجود اتفاق عام مشترك بين الدول حول صور الجريمة المعلوماتية.

فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام آخر، ويرجع السبب في ذلك إلى طبيعة النظام القانوني السائد في الدولة أو إلى اختلاف العادات والتقاليد والأديان والثقافات من دولة إلى أخرى بل من مجتمع إلى آخر وبالتالي اختلاف السياسة التشريعية، ولعل هذا الاختلاف قد أتاح الفرصة لمرتكبي الجرائم المعلوماتية على تنظيم أنفسهم وارتكاب الجرائم بشكل عابر للحدود الجغرافية[24].

ثانيا: تنوع واختلاف النظم القانونية الإجرائية

إن اختلاف النظم الإجرائية التي يتم إتباعها في البحث والتحري والتحقيق في الجرائم المعلوماتية يعد أحد المعوقات التي تقف أمام التعاون الدولي، والسبب راجع لكون الإجراءات التي يثبت فائدتها وفعاليتها في دولة ما قد تكون غير ذي فائدة في دولة أخرى، وقد لا يسمح للجهات المختصة بالتحقيق بإجرائها أصلا، كما هو الحال بالنسبة للتنصت، والمراقبة الالكترونية، والتسليم المراقب، وغيرها من الإجراءات الشبيهة.

فإذا ارتكبت الجريمة المعلوماتية بين أكثر من دولة، فإن الدولة الأولى ستصاب بالإحباط لعدم قدرة السلطات المختصة القيام بالإجراءات اللازمة في الدولة الثانية، كما قد تمنع السلطة القضائية في الدولة الثانية قبول الدليل الذي يساعد في إثبات الجريمة لأنها ترى بأن الطريقة التي تم استحصاله من خلالها غير مشروعة[25].

الفرع ثالث: التجريم المزدوج

إن اختلاف النظم القانونية والتشريعات العقابية لها دور بارز في مجال وضع العوائق أمام تحقيق التعاون الدولي في مجال الجرائم المعلوماتية، حيث أن اشتراط تجريم ذات الفعل في التشريعات الوطنية هو من أهم الشروط، خاصة في نطاق تسليم المجرمين والذي تشترطه أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين[26].

إلا أنه من جانب أخر، نجد أن معظم الدول لم تصدر التشريعات التي تعالج أو تضع الآلية المناسبة لمحاربة الجريمة المعلوماتية، وهنا كان من الصعوبة أن يتم تحديد ما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم، يمكن أن تطبق على الجرائم المعلوماتية أم لا، وهذا بالطبع

الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، وهذا الأمر الأخير ينعكس بشكل سلبي على إجراءات جمع الأدلة وملاحقة ومحاكمة الجناة في الجرائم المعلوماتية[27].

الفرع الرابع: الصعوبات الخاصة بالمساعدات القضائية

من صور التعاون الدولي في المجال القضائي، هو طلب المساعدات القضائية الدولية، ومنها على سبيل المثال الإنابة القضائية والتي تعتبر من أهم صور التعاون الدولي في المجال الجنائي، إلا أنها عادة ما تتم بين الدول بالطرق الدبلوماسية ما يجعلها تتسم بالبطء في إجراءاتها بالإضافة إلى تعقيدها.

إن من الصعوبات الكبيرة التي تواجه المساعدات القضائية الدولية هي التباطؤ في الرد، إذ أن الدولة التي تتلقى طلب المساعدة عادة ما تكون متباطئة في الرد على هذا المطلب، والسبب يعود في ذلك، إما إلى نقص عدد الموظفين المربين أو صعوبات لغوية أو الاختلاف في كيفية الإجراءات بين الدولتين[28].

الفرع الخامس: عدم وجود قنوات اتصال

أهم الأهداف المرجوة من التعاون الدولي في مجال 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 يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين، وبالتالي تنعدم الفائدة منه[29].

المطلب الثاني: المعوقات المتعلقة بالمحكمة المختصة والقانون الواجب التطبيق

إن صعوبة تحديد الاختصاص القضائي للمحكمة التي تنظر في القضية المتعلقة بالجريمة المعلوماتية وعلى وجه الخصوص المتعلق منها بالانترنت، يعد إحدى أهم المشكلات التي تعرقل عملية مكافحة الجريمة المعلوماتية، حيث أن هذا النوع من الجرائم هو الأكثر إثارة لموضوع الاختصاص على المستوى الوطني والدولي نتيجة الترابط في شبكة الانترنت.

وليس هذا فحسب، وإنما تبرز صعوبة أخرى تكمن في إشكالية تحديد القانون الواجب التطبيق، وذلك نظرا لعدم وجود قانون جنائي موحد يحكم الجريمة المعلوماتية، إذ أن هناك العديد من القوانين المحددة للجرائم والمتعددة بتعدد الدول والتي تختلف باختلاف الأنظمة القانونية السائدة في تلك الدول.

الفرع الأول: إشكالية القضاء المختص بنظر الجرائم المعلوماتية

لقد ثار خلاف بين الفقه حول تحديد المحكمة المختصة في نظر هذه الجرائم، فذهب الجانب الأول منه إلى أن الاختصاص ينعقد في الجرائم المعلوماتية إلى محاكم الدولة التي تم فيها تحميل البيانات، كون عملية جمع الأدلة والبيانات تكون سهلة لكونها دولة المصدر، كما أن بنك معلومات محل التحميل يكون أكثر ثباتا.

وقد وجهت العديد من الانتقادات لأصحاب هذا الجانب يتمثل أهمها في أن بعض الأفعال قد لا يكون معاقب عليها في دولة التحميل وبالتالي يكون فعلا مباحا ولا يعاقب عليه القانون، لذلك ظهر جانب آخر من الفقه يتجه لإعطاء الاختصاص لمكان وقوع النتيجة الإجرامية لتعدد دول التحميل مما يعقد الاختصاص لأكثر من دولة مما يؤدي لضياع المسؤولية خصوصا إذا كانت دولة التحميل لا تعاقب على مثل هذه الأفعال، ولكن كان على هذا الرأي مآخذ أيضا حيث لم تضع في الحسبان مصلحة المتهم بأن تطبق عليه قوانين غير قانون الدولة التي يحمل جنسيتها مما يزيد من تكلفة المحاكمات في هذه الجرائم، وزيادة مدة واجل المحاكمة[30].

كل هذه المبررات استدعت نشأت اتجاه ثالث يرى بانعقاد الاختصاص القضائي لمكان المعتدى عليه فهو المكان الذي تحققت فيه النتيجة الإجرامية ومرتبط بشخص المعتدى عليه[31].

وقد حسم المشرع الجزائري موضوع الاختصاص القضائي بأن منح القضاء الجزائري صلاحية نظر الجرائم المعلوماتية المرتكبة في الجزائر وعلى إقليميها، إذ ينعقد الاختصاص إما لمكان ارتكاب الجريمة أو محل إقامة المتهم، أو مكان القبض عليه.

وينعقد الاختصاص وفقا لمعيار من المعايير المشار إليها بحسب السبق للمحكمة التي دخلت الدعوى الجزائية حوزتها قبل غيرها، فإذا نظرت القضية محكمة محل ارتكاب الجريمة فإنها بالتالي تكون هي المختصة دون غيرها، ويكون من حقها تمديد اختصاصها بشان اتخاذ أي إجراء من إجراءات المحاكمة وهو ما نصت عليه المادة (47) والمادة (80) والمادة (329) من قانون الإجراءات الجزائية.

الفرع الثاني: إشكالية تحديد القانون الواجب التطبيق

إن الجرائم المعلوماتية لا ترتبط بحدود إقليمية لدولة ما، بل على العكس من ذلك، فهي جريمة عابرة للحدود، بالإضافة إلى اختلاف التشريعات والنظم القانونية من دولة إلى أخرى في مواجهة تلك الجرائم، لهذا وجدت العديد من المبادئ التي تحدد القانون الواجب التطبيق.

وعليه سنبحث على معيار يتلاءم وطبيعة الجريمة المعلوماتية

-أولا: مبدأ إقليمية النص الجنائي:

إن القاعدة العامة المطبقة في أغلب الدول هي مبدأ الإقليمية، بمعنى أن القانون الجنائي يطبق على كافة الجرائم التي ترتكب في إقليميها أو جزء من إقليميها بغض النظر عن جنسية فاعلها أو مرتكبها.

وتأخذ بهذا المبدأ أغلب التشريعات على غرار المشرع الجزائري من خلال نص المادة (3) من قانون العقوبات والتي نصت على أن: "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية".

وتطبيقا لهذا المبدأ، فإن الجرائم المعلوماتية العابرة للحدود تخضع في كثير من الأحيان لأكثر من قانون، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة تحققت في نطاق بلد آخر، فإن كلا البلدين يكون قانونه واجب التطبيق على الواقعة، بمعنى أنه يتم تطبيق قانون كل دولة تحقق في نطاقها أحد عناصر الركن المادي للجريمة.

كما قد يثير إشكالية ازدواجية الاختصاص حيث يختص بها القانون الأجنبي في نفس الوقت الذي تدخل في اختصاص القانون الوطني، وذلك قد يؤدي إلى الإحاطة بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة[32].

كما يترتب على تطبيق هذا المبدأ عدم اهتمام الدولة إلا بالجرائم التي تقع على إقليمها، فلا يمتد إلى ما يرتكب خارجه من جرائم ولو كان مرتكبوها من رعايا هذه الدولة، كما أن هذا المبدأ لا يتفق مع جرائم الانترنت نظرا للبعد العالمي لشبكة الانترنت وانتقال المعلومات من خلالها الشيء الذي يخلق إشكالا كبيرا في القانون الواجب التطبيق خاصة في ظل اختلاف تشريعات هذه الدول، وعدم وجود اتفاقات فيما بينها.

وعليه يبدو أن مبدأ الإقليمية غير ملائما للجريمة المعلوماتية، وهذا بالنظر لطبيعيتها الغير مادية وكذلك صعوبة اكتشافها وتحديد زمان ومكان وقوعها بدقة.

ثانيا: مبدأ شخصية النص الجنائي

يأخذ هذا المبدأ وجه ايجابي ووجه سلبي، فالوجه الايجابي يعني تطبيق القانون الجنائي على كل من يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليميها، أما الوجه السلبي فيعني تطبيق القانون الجنائي على جريمة يكون فيها المجني عليه ينتمي إلى جنسية الدولة ولو كان الجاني أجنبيا وارتكب الجريمة خارج إقليم الدولة.

وقد أخذ المشرع بمبدأ الشخصية في شقه الايجابي وذلك من خلال نص المادتين 582-583 من قانون الإجراءات الجزائية، ولا يعترف بمبدأ الشخصية في الوجه السلبي.

غير أن هذا المبدأ وردت عليه قيود بصفة عامة وبالتالي فإن الاختصاص لا ينعقد في المحاكم الوطنية بشكل تلقائي بالنسبة للجرائم التي تقع في الخارج، بل لابد من علم النيابة العامة بها.

والملاحظ أن هذا المبدأ يعتمد بصفة أساسية على الجاني من حيث الكشف على هويته ومن ثم التعرف على جنسيته، وهذه المعلومات تعد صعبة وعسيرة في الجرائم المعلوماتية أين يستعمل الأسماء المستعارة والتشفير بالإضافة إلى اللغة الصعبة والمعقدة في كشفها والتعامل معها.

ومن مخاطر تطبيق القانون الجنائي الوطني على الجرائم التي تقع في الخارج والتي يختص بها القانون الأجنبي في ذات الوقت أنها تؤدي إلى المساس بمبدأ عدم جواز محاكمة الشخص عن نفس الفعل الواحد مرتين[33].

ثالثا: مبدأ العينية

طبقا لهذا المبدأ يطبق القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بغض النظر عن جنسية مرتكبها، ويرجع هذا المبدأ إلى المساس بسيادة الدولة.

وقد نص القانون الجزائري على هذا المبدأ من خلال نص المادة 566 من قانون الإجراءات الجزائية، كما نص القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على هذا المبدأ وذلك من خلال المادة 15 حيث ورد النص كالتالي" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

وعلى هذا الأساس قد يطبق هذا المبدأ على الجرائم المعلوماتية إذا كانت تمس مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

غير أن هذا المبدأ في الواقع يصادف تطبيقه العديد من المشكلات التي تعيق التنفيذ، ومنها مشكلة تعارض تطبيق القانون الجنائي وفقا لمبدأ العينية مع تطبيق القانون وفقا لمبدأ الإقليمية في حالة أن تكون الجريمة المرتكبة وفقا لمبدأ العينية مجرمة في قانون الدولة الأخرى التي اقترفت فيها، فهنا تثار مسألة تنازع الاختصاص والقانون الواجب التطبيق بين الدولة المقترفة فيها الجريمة وفقا لمبدأ الإقليمية والدول الأخرى التي تعد الجريمة من الجرائم التي يناط بقضائها نظرها وفقا لمبدأ العينية، وبالتالي فقد يحاكم الشخص على فعله مرتين.

الخاتمة:

أظهرت الدراسة وجود العديد من المعوقات التي تعترض سبل مكافحة الجرائم المعلوماتية، منها ما هو متعلق بالكشف عن الجريمة من حيث إحجام المجني عليهم عن الإبلاغ حرصا على ثقة العملاء أو لصعوبة اكتشافها من قبل الأشخاص العاديين، فضلا عن نقص خبرة سلطات الاستدلال والتحقيق وفرض الجناة لتدابير أمنية، ومنها ما هو متعلق بإثبات الجريمة المعلوماتية، إذ يثير الدليل الالكتروني صعوبات تتعلق بعدم ظهوره بشكل مرئي، بالإضافة إلى قدرة الجاني على إتلاف وتشويه الدليل في وقت قصير كما يمكن في أقل من ثانية العبث به أو محوه بالكامل فضلا عن استحالة الحصول على الدليل الالكتروني في حالة توزيع مسرح الجريمة على أكثر من دولة.

كما يبرز للوجود مسألة صعوبة التعاون القضائي الدولي وتحديد قواعد الاختصاص، حيث أن التباين الموجود بين قوانين الدول المختلفة جعل من بعض الأفعال مجرمة في دولة وغير مجرمة في دولة أخرى، بالإضافة إلى اختلاف وتنوع النظم الإجرائية، كما أن تعدد المعايير واختلافها من دولة إلى أخرى يثير إشكالية تحديد المحكمة المختصة والقانون الواجب التطبيق الأمر الذي يمنح الفرصة للجاني للإفلات من المتابعة والعقاب.

وللتصدي لهذه الصعوبات يجب اتخاذ ما يلي:

-ضرورة تأهيل وتكوين رجال الضبطية القضائية على الأساليب التقنية والحديثة المستخدمة في هذه الجرائم، وتدريبهم على التدابير الواجب اتخاذها في هذا المجال، للإسراع في الكشف عن الجريمة وتعقبها، من أجل عدم ضياع الدليل.

-إعطاء الضبطية القضائية المزيد من الوسائل التقنية المتطورة مع ضرورة الاستعانة بذوي الخبرة.

-ضرورة العمل على توحيد الجهود الدولية من أجل صياغة قانون موحد لمواجهة الجرائم المعلوماتية.

-ضرورة تأهيل وتكوين قضاة متخصصين للنظر في هذا النوع من الجرائم.
-ضرورة تعزيز التعاون الدولي من خلال إبرام المزيد من الاتفاقيات على المستوى الإقليمي والدولي.
-الحاجة إلى المزيد من التعاون الدولي في مجال التحقيق وتسليم المجرمين وتنفيذ الأحكام القضائية.
-توعية مستخدمي الحاسب الآلي والانترنت حول خطورة هذه الجرائم، وأهمية الإبلاغ عنها والإرشاد عن مرتكبيها.

الهوامش:

1- خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2010، ص68.
2- محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، ط1، دار المناهج، الأردن، 2005، ص218.
3- موسى مسعود أرحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28-2009/10/29، ص6.
4- محمد حماد مرهج الهيتي، المرجع السابق، ص215.
5- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، القاهرة، 2002، ص37.
6- محمد حماد مرهج الهيتي، المرجع السابق، ص216.
7- فرنسا مثلا قامت بإنشاء عدة وحدات متخصصة وغير متخصصة ضمن جهازي الشرطة والدرك لمكافحة هذا الإجرام المستحدث بجميع صوره ومن ذلك المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات، بالإضافة إلى قسم الانترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف اختصارا (STRTD)، والقسم الالكتروني التابع لمعهد البحوث الجزائية التابع للدرك الوطني المعروف اختصارا ب (IRCGN) وكذا وحدات أقسام الاستعلامات والتحقيقات القضائية المعروف اختصارا ب (BDRIJ).

Myriam QUEMENER et joel FERRY, cybercriminalité défi mondial, 2 édition, 2009, p214.

وفي الجزائر فإنه بالإضافة إلى مصالح الضبطية القضائية فإنه بموجب المرسوم الرئاسي رقم 183/04 المؤرخ في 2004/06/26 تم إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام تحت وصاية القيادة العامة للدرك الوطني، ويحتوي هذا المعهد على قسم الإعلام الآلي يختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية، والى جانب ذلك يوجد مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية تابع أيضا لقيادة الدرك الوطني، أما على مستوى المديرية العامة للأمن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية ومن الفروع التقنية التي تتضمنها هذه المخابر، خلية الإعلام الآلي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية، وحتى تكتمل قدرات تلك الأجهزة في هذا المجال فقد تم إنشاء الهيأة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

8- خالد ممدوح إبراهيم، المرجع السابق، ص69. لينا محمد الأسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، ط1، دار الحامد، الأردن، 2015، ص246.
9- عبد الفتاح بيومي حجازي، المرجع السابق، ص41.
10- محمد حماد مرهج الهيتي، المرجع السابق، ص214.

11-عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص.83
12- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، ص20، مقال منشور على شبكة الانترنت: www.arablawinfo.com تاريخ الدخول إلى الموقع 2016./09/05
13- ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق،المجلد 18، العدد2، كانون الثاني، جامعة النهرين، 2016، ص215. مقال منشور على شبكة الانترنت:http://www.mlawnahrain.org/issue.php?i=58 ، تاريخ الدخول إلى الموقع 2016./09/06
14- عبد الرحمن محمد بحر، معوقات التحقيق في جرائم الانترنت (دراسة مسحية على ضباط الشرطة في دولة البحرين)، رسالة مقدمة إلى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، 1999، ص27.
15- ميسون خلف حمد الحمداني، المرجع السابق، ص.216
16- لينا محمد الأسدي، المرجع السابق، ص.269
17- محمد حماد مرهج الهيتي، المرجع السابق، ص.213
18- لينا محمد الأسدي، المرجع السابق، ص.273
19- عبد الله حسين علي محمود، سرقة المعلومات الخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002، ص.359
20- ميسون خلف حمد الحمداني، المرجع السابق، ص.227
21- لينا محمد الأسدي، المرجع السابق، ص.273
22- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، 12-2007/11/14، ص.32
23- فريق الخبراء المعني بالجريمة السيبرانية، مشروع المواضيع المطروحة للنظر في إطار دراسة شاملة بشأن تأثير الجريمة السيبرانية وتدابير التصدي لها، فينا 21/17/يناير/2011، ص.16
24- لينا محمد الأسدي، المرجع السابق، ص.253
25- براء منذر كمال عبد اللطيف، ناظر أحمد منديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009، ص11.
26- لينا محمد الأسدي، المرجع السابق، ص.256
27- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 1998، ص.91
28- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، ص55، مقال منشور على شبكة الانترنت:
http://www.minshawi.com/vb/attachment.php?attachmentid=337&d=12005
80014 ، تاريخ الدخول إلى الموقع 2016./09/19
29- حسين بن سعيد بن يوسف الغافري، المرجع نفسه، ص.53
30- أسامة أحمد مناعسة، جلال محمد، صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، ط1، دار وائل للنشر، 2001، ص.211،210
31- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، 2014، ص.374

32- موسى مسعود أرحومة، المرجع السابق، ص18.

قائمة المراجع:

أولا: الكتب

1- أسامة أحمد مناعسة، جلال محمد، صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، ط1، دار وائل للنشر، الأردن، 2001.

2- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 1998.

3- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، 2014.

4- خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2010.

5- عبد الله حسين علي محمود، سرقة المعلومات الخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002.

6- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، القاهرة، 2002.

7- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، 2006.

8- لينا محمد الأسدي، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دراسة مقارنة، ط1، دار الحامد، الأردن، 2015.

9- محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، ط1، دار المناهج، الأردن، 2005.

10- Myriam QUEMENER et joel FERRY, cybercriminalité défi mondial, 2 édition, 2009

ثانيا: الرسائل

1- عبد الرحمن محمد بحر، معوقات التحقيق في جرائم الانترنت (دراسة مسحية على ضباط الشرطة في دولة البحرين)، رسالة مقدمة إلى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، 1999.

ثالثا: المقالات

1- براء منذر كمال عبد اللطيف، ناظر أحمد منديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009.

2- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الانترنت، مقال منشور على شبكة الانترنت:
http://www.minshawi.com/vb/attachment.php?attachmentid=337&d=1200580014 ، تاريخ الدخول إلى الموقع 2016/09/19.

3- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، 12-2007/11/14.

4- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، مقال منشور على شبكة الانترنت: www.arablawinfo.com تاريخ الدخول إلى الموقع 2016/09/05.

5- موسى مسعود أرحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28-2009/10/29.
6- ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق،المجلد 18، العدد2، كانون الثاني، جامعة النهرين، 2016. مقال منشور على شبكة الانترنت:http://www.mlawnahrain.org/issue.php?i=58 .