إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية

م.م. حسين خليل مطر

نبذة عن الباحث :
جامعة البصرة- مركز دراسات البصرة والخليج العربي.

Abstract
This research studied the procedures for investigation and collect the evidence in the crimes electronic, as we found through the research that the world of information technology is world wide no bounded an end, and that means used in this crimes complex and varied.
This requires adeport onself by the legislator and the judiciary to take aset of reform stepes to confrontation this type of crimes.

الخلاصة :

تناولنا في هذا البحث دراسة اجراءات التحقيق وجمع الأدلة في الجرائم الألكترونية ، إذ وجدنا من خلال البحث إن عالم تقنية المعلومات عالم واسع لا يحده حد ، وان الوسائل المستعملة في ارتكاب الجريمة الالكترونية متشعبة ومتنوعة.
وهذا الامر يتطلب وقفة من قبل المشرع والقضاء لاتخاذ مجموعة من الخطوات الاصلاحية لمواجهة هذا النوع من الجرائم.

مقدمة

١) موضوع البحث:

إن أهم ما يُميز العصر الحالي عن غيره من العصور هو ما نشهده اليوم من تطور مثير في المجالات التكنولوجية ،الأمر الذي انعكس على مجمل مجالات الحياة، بحيث نستطيع القول بثقة بإنه لم يُعد هناك شأن يتصل بالحياة الانسانية إلا ناله نصيب من هذا التطور التكنولوجي المثير الذي أحدث ثورة أدخلت البشرية في عصر جديد.

وعلى الرغم من الايجابيات العديدة التي أحدثتها تقنية الانترنت في تسهيل نقل وتبادل المعلومات ،إلا إن هناك خشية متزايدة من تنامي الخروق والسلبيات والأعراض الجانبية لهذه الشبكة واستغلالها من قبل بعض الشركات والهيئات والعصابات والأفراد لارتكاب وتعميم أعمال وأفعال تتقاطع مع القوانين ومع الاعراف والأخلاق والآداب.

٢) أهمية البحث:

تكمن أهمية البحث في مدى الخطورة التي تُشكلها الجرائم الالكترونية إذ إنها تطال الحق في الحصول على المعلومات وتمس حرمة الحياة الخاصة للأفراد وتُهدد الأمن الوطني وتُؤدي إلى فقدان الثقة بالتقنية وغيرها من مفاصل الحياة العامة المختلفة.

٣) مشكلة البحث:

تتمثل مشكلة البحث في مدى الصعوبة التي تُواجهها إجراءات التحقيق في هذا النوع من الجرائم والمتمثلة في اخفاء الجريمة وسهولة وسرعة محو أو تدمير أدلة ومعالم الجريمة والضخامة البالغة لكمية البيانات المراد فحصها على الشبكة . وتبرز كذلك صعوبات في مسائل جمع الأدلة من المعاينة والتفتيش والضبط وغيرها من الاجراءات ،فضلاً عن الطابع العالمي الذي تمتاز به هذه الجرائم لكونها من الجرائم التي تتجاوز عنصري الزمان والمكان.

٤) منهجية البحث:

سنتناول في هذا البحث دراسة الجرائم الالكترونية في نطاق التحقيق الجنائي محاولين قدر الامكان وضع اليد على بعض الحلول الناجعة لمكافحة هذه الظاهرة الإجرامية،مستندين في ذلك إلى عرض وتحليل النصوص القانونية المتعلقة بهذا المجال .

٥) خطة البحث:

يقتضي إيفاء هذا الموضوع حقه تقسيمه إلى مبحثين ،إذ سيكون عنوان المبحث الأول (ماهية الجرائم الالكترونية) و يتضمن مطلبين ، سيُخصص المطلب الأول لبيان مفهوم الجرائم الالكترونية، بينما سيتم تخصيص المطلب الثاني للبحث في أهم الوسائل المستخدمة في ارتكاب الجريمة الالكترونية، بينما تخصص المبحث الثاني للبحث في كيفية إثبات الجريمة الالكترونية ،وذلك في مطلبين، متناولين كل من معوقات اثبات الجريمة الالكترونية واجراءات اثباتها .

وسوف ننهي البحث بخاتمة تتضمن أهم النتائج والتوصيات التي تبلورت من هذا البحث.

المبحث الأول :ماهية الجرائم الإلكترونية

لقد صاحب التطور التكنولوجي الهائل الذي أحدثته تقنية المعلومات ظهور بعض الفئات التي سعت إلى تحويل هذه التقنية إلى وسيلة لارتكاب الجرائم، وأصبح يُطلق عليها الجرائم الالكترونية ، سنحاول في هذا المبحث التعرف على ماهية هذه الجرائم من خلال توضيح مفهومها وخصائصها وأهم الوسائل المستخدمة في إرتكابها.

المطلب الأول :مفهوم الجرائم الالكترونية

تعتبر الجرائم الالكترونية هي النوع الشائع من الجرائم ،إذ إنها تتمتع بالكثير من المميزات للمجرمين تدفعهم إلى إرتكابها، وقد تكون هذه الدوافع ذات طبيعة ربحية بحيث يسعى الجاني من ورائها إلى الحصول على الأموال،أو يكون هدف الجاني هو الرغبة في إثبات الذات وتحقيق انتصار على

تقنية النظم المعلوماتية[١]،كما يُمكن أن يكون الدافع لارتكاب الجريمة تعرض الشخص للتهديد والضغط من الآخرين في مجالات الأعمال التجارية والأخرى الخاصة بالتجسس والمنافسة ، أو سعي بعض الموظفين إلى الإنتقام من المنشآت ، وقد يكون الهدف تهديد الشخص وابتزازه لحمله على القيام بفعل أو الإمتناع عنه،ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعين[٢] ،وقد يكون الدافع ذا طبيعة سياسية ،إذ تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم،كما إن الأفراد قد يتمكنون من إختراق الأجهزة الأمنية الحكومية ،كذلك أصبحت شبكة الإنترنت مجالاً خصباً لنشر أفكار العديد من الأفراد والمجموعات ووسيلة للترويج لأخبار وأمور أخرى قد تحمل في ثناياها مساساً بأمن الدولة أو بنظام الحكم أو قدحاً في رموز دولية أو سياسية والإساءة لها بالذم والتشهير[٣] ،كما إمتدت الجريمة الالكترونية لتشمل صور الجريمة المنظمة،حيث ظهر الإرهاب الإلكتروني على الشبكة، وأخذت الجماعات الإرهابية مواقع لها على الانترنت ، تمارس أعمالها من خلالها،كالتحريض على القتل،بالإضافة إلى تعليم صنع المتفجرات والقنابل،علاوة على نشر أفكارها الإرهابية،وأصبحت تقوم بشن عملياتها الإرهابية عبر الانترنت من خلال التلاعب بنظم وبيانات أنظمة خاصة.

لقد وردت مجموعة من التعريفات لهذا القسم من الجرائم،فيرى جانب من الفقه الألماني أنها (كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي)[٤].

ويختصر جانب من الفقه الجنائي جرائم الكمبيوتر بأنها (الاستخدام غير المشروع للحاسبات والتي تتخذ صورة فيروس يهدف إلى تدمير الثروة المعلوماتية)[٥].

يتضح من التعريفات التي ذكرناها إنها قد امتازت بالتعدد والاختلاف ضيقاً وأتساعا تبعاً للمعايير والمنطلقات المستندة إليها، فمنها ما اعتمد أصحابها على معيار الوسيلة المستخدمة في ارتكاب الجريمة، وآخرون اعتمدوا معيار موضوع الجريمة ذاتها،ومنهم من اعتمد معايير مختلطة جمعت بين المعيارين السابقين.

ولهذه الجرائم خصائص تميزها وتنفرد بها نوردها بالنقاط الآتية[١]:

١) إن جرائم الحاسوب ترتكب بعضها داخل أجهزة الحاسوب الشخصية في أي مكان حتى في غرف النوم أو داخل الأجهزة الرئيسية الكبيرة المحفوظة في أماكن مجهزة تجهيزاً آمناً.
٢) تتميز جرائم الحاسوب بوقت إرتكابها السريع للغاية، لهذا يجب أن يوضع في الاعتبار هذا العنصر الجوهري عند التخطيط لمواجهتها،وذلك نظراً لسرعة تنفيذ اجهزة الحاسوب الفائقة للتعليمات الصادرة إليها وفقاً للمعايير الزمنية للحاسوب.
٣) كما تتميز جرائم الحاسوب بأن الحواجز الجغرافية والمكانية لا تُمثل عوائق طبيعية أمام إرتكابها ، فمثلاً سرقة الأرصدة النقدية من البنوك باستخدام الحاسوب لا تُواجه العوائق المادية ككسر الأبواب واستخدام السلاح، وإنما يُمكن الدخول غير المشروع على شبكة معلومات البنك وإجراءات تحويلات غير مشروعة لأرصدة مالية ضخمة لحسابات الجاني أو الجناة في نفس البنك أو في بنوك أخرى،إذ إن أغلبية المؤسسات قد استغنت عن القيود والسجلات المادية بأخرى أكثر حداثة متمثلة بالمستندات الالكترونية والبصرية الموجودة بأنظمة الحاسوب.

المطلب الثاني :أهم الوسائل المستخدمة في ارتكاب الجرائم الالكترونية

إن الوسائل الفنية التي قد تستخدم لتدمير مكونات الحاسوب كثيرة ومعقدة في الوقت الحاضر، ولا يُمكن التنبؤ بالوسائل التي قد تستحدثها التكنولوجيا في هذا الشأن ،وبناءً على ذلك سوف نقوم بتناول أهم هذه الوسائل على النحو الآتي:

الفرع الأول :الفيروسات[٧]

تُعد الفيروسات من الوسائل كثيرة الخطورة على الحاسب الآلي يُمكن تعريفها على وفق ما حدده أحد التقارير الصادرة عن المركز القومي للحاسبات الآلية الأمريكي بأنها(برامج مهاجمة تُصيب أنظمة الحاسبات بأسلوب يُماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تُصيب الإنسان)[٨].

كما يُمكن أن يُعرف فيروس الكمبيوتر بأنه (برنامج يتكون من عدة أجزاء مكتوب بإحدى لغات البرمجة بطريقة خاصة تسمح له بالتحكم في البرامج الأخرى وقادر على تكرار نسخ نفسه،ويحتاج إلى برنامج وسيط (كعائل له) أو مساحة تنفيذية على الإسطوانة)[٩].

والفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي ولكنه مصمم بحيث يُمكنه التأثير على البرامج الأخرى الموجودة على الحاسب الآلي[١٠].

وتختلف أنواع الفيروسات من ناحية الحجم والنوع وطريقة التشغيل ومستوى الدمار الذي تُحدثه، وهذه الأنواع هي فيروس مُحاكاة الأخطاء ،فيروس الإبطاء، الفيروسات النائمة، التطورية، القاتلة، الفيروس الإسرائيلي، فيروس السرطان، فيروس الجنس وفيروس القردة، وفضلاً عن هذه الفيروسات هناك أنواع أخرى ظهرت بمناسبات معينة منها فيروس مايكل آنجلو الذي أطلق بمُناسبة ميلاد هذا الرسام ، وفيروس ناسا وفيروس الكرسماس،وغيرها يرتبط نشاطها بواقعة معينة مثل بدء تشغيل الجهاز كالفيروس الباكستاني[١١].

ويُلاحظ أن فيروس الحاسوب له من خصائص المجرم، فهو يختفي كخطوة أولى في وقت محدد ثم يبدأ في الظهور كخطوة ثانية ليُدمر في خطوة ثالثة، كالمجرم الذي يضع خطته لإرتكاب الجريمة، فأسلوب عمل وانتشار الفيروسات كثيرة، حيث تنتقل الفيروسات وتتكاثر من حاسوب إلى آخر عن طريق الأقراص الملوثة ،أو وصلات شبكة الحاسوب أو البرامج الملوثة،والأخطر من ذلك هو انتقالها عبر شبكة الانترنت ورسائل البريد الالكتروني، وقد يختص الفيروس بأحد البرامج وعندما يقوم المستخدم بتشغيل البرنامج ينتقل إلى القرص بداخل الحاسوب ويبدأ في أعماله التخريبية في تدمير المعلومات ومحوها أو تعديلها،وحين يظهر الفيروس فهو ينتقل مثل العدوى إلى البرامج الأخرى وينتشر بينها[١٢].

الفرع الثاني :الديدان

هي برامج صغيرة قائمة بذاتها وغير معتمدة على غيرها ،صُنعت للقيام بأعمال تدميرية أو بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم لشبكة الانترنت أو لإلحاق الضرر بهم أو بالمتصلين بهم ، وتلك الديدان تتميز بسرعة الانتشار وفي الوقت نفسه يصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة[١٣]،ومن شأن هذه البرامج استغلال أية فجوات في نظم التشغيل من أجل الانتقال من حاسب إلى آخر ومن شبكة إلى أخرى عبر الوصلات الرابطة بينها ،وتتكاثر أثناء إنتقالها كالبكتيريا بانتاج نسخ منها حتى تقوم بتغطية شبكة بأكملها ومن ثم تكون لها الامكانية لتعطيل أو ايقاف نظام الحاسب الآلي بصورة كاملة[١٤].

تختلف الديدان في طريقة عملها من نوع الى آخر ،فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة ،بينما بعضها يتخصص في البريد الالكتروني بحيث تقوم بارسال نفسها في رسائل إلى جميع من توجد عناوينهم في دفتر العناوين الموجود بالجهاز ، وأنواع أخرى من الديدان تقوم بإرسال رسائل قذرة الى بعض الموجودة عناوينهم في دفتر العناوين الموجود بالجهاز باسم مالك البريد مما يوقعه في حرج بالغ مع من تم ارسال تلك الرسائل اليهم[١٥].

الفرع الثالث :القنابل المنطقية أو الزمنية

هي عبارة عن برامج صغيرة يتم ادخالها بطرق غير مشروعة ومخفية مع برامج أخرى بهدف تدمير وتخريب وتغيير برامج ومعلومات وبيانات الحاسوب في لحظة محددة[١٦] .

ومن الممكن تعريف القنابل المنطقية بأنها برنامج أو جزء من برنامج ينفذ في لحظة معينة أو في كل فترة زمنية محددة بالساعة واليوم والسنة يتم ادخالها في برنامج وتنفذ في جزء من ثانية أو في ثوان أو دقائق وقد يتم ضبطها لتنفجر بعد عام[١٧].

ومن هنا يتضح لنا إن القنابل المنطقية تظل ساكنة ودون فاعلية وبالتالي غير مكتشفة لمدة قد تطول أو تقصر يحددها مؤشر موجود في برنامج القنبلة،وهذا المؤشر لا يقتصر على المدة الزمنية وانما قد يمتد الى ما يعرف بتوافر شروط منطقية معينة من داخل برنامج أو ملف معين،وذلك حسب الرمز الذي يحدده برنامج القنبلة ،فإذا حل الميعاد أو توافرت هذه الشروط ،بدأ البرنامج في القيام بمهامه التخريبية[١٨].

إن القنابل المنطقية أو الزمنية قد تم استخدامها على نطاق واسع لأنها تحقق أهدافاً يطمح لها الجاني ،ومن هذه الأهداف أو الميزات إنه يمكن القيام بتوقيت عملية الاتلاف بوقت معين وإن الأثر سوف يكون جسيماً[١٩].

ومن الأمثلة على القنابل المنطقية والزمنية في أنظمة الحاسوب هو قيام أحد المبرمجين الفرنسيين بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالجهة التي كان يعمل بها ، تتضمن أمراً بتفجيرها بعد ستة أشهر من تاريخ فصله مما ترتب عليه تدمير كافة بياناتها[٢٠] .

الفرع الرابع :تكنيك سلامي

ومن أساليب ارتكاب جرائم الكمبيوتر ما يُسمى بتكنيك سلامي،وهذه الطريقة عبارة عن خدعة تتم بواسطة سرقة كمية صغيرة جداً من مصادر كمية كبيرة للأموال حيث يتم اختلاس مبلغ بسيط جداً من مفردات العملة من حسابات مالية تتكون من عدة آلاف.

ومهارة المختلس في هذه الحالة تعتمد على قيامه بتغيير كمية هذه المفردات البسيطة باستمرار حتى لا تكشف ، ليظن المتعامل إنها كسور حسابية مهملة لا يفطن إليها طالما أن القليل في الكثير ربح،حيث تجمع هذه المبالغ البسيطة من حسابات آلاف العملاء ،وأخيراً تشكل مبلغاً كبيراً للمختلس ،حيث يقوم بتحويله مجمعاً على بعضه إلى شيك يتم صرفه بطريقة مشروعة[٢١].

الفرع الخامس :حصان طروادة

هو عبارة عن برمجية اختراق،وهو صفة لنوعية من الملفات التي لديها القابلية للانتشار عن طريق نسخ ذاته إلى الملفات الأخرى والدخول إلى الأماكن السرية والمشفرة،فينتشر فيها ليُحقق غرضه في التدمير والتخريب[٢٢].

صُمم هذا البرنامج في البداية بغرض حسن ومفيد هو معرفة مايقوم به الأبناء على جهاز الكمبيوتر في غياب الوالدين ،إلا إنه تم تطوير هذا البرنامج بعد ذلك تطويراً سيئاً،وتكمن خطورة هذا البرنامج في كونه يُتيح للمخترق أن يحصل على كلمة سر الدخول على الجهاز،بمعنى إنه يُتيح

للمخترق أن يتمكن من الدخول على الجهاز بطريقة لا تُثير أي ريبة أو شك نظراً لأنه يُمكنه من الدخول على جهاز الكمبيوتر باستخدام كلمة السر التي يستخدمها صاحب الجهاز[٢٣].

إن هذه الوسائل التي تعرضنا لها آنفاً يستخدمها الجناة عادةً لتحقيق عدة أغراض تختلف من شخص لآخر،ولعل من أهم هذه الغايات هو الإخلال بالآداب العامة وإثارة النعرات الطائفية والدينية والارهاب بمختلف أصنافه والتهديد والاحتيال.

المبحث الثاني :اثبات الجريمة الالكترونية

إن الجرائم الالكترونية عادةً ما يتم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها ،فضلاً عن الجرائم التي لم تُكتشف هي أكثر بكثير من تلك التي كُشف الستار عنها،فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم اكتشافه هو رقم خطير،وبعبارة أخرى فإن الفجوة بين عدد هذه الجرائم الحقيقي وماتم اكتشافه فجوة كبيرة، وهذا يرجع إلى عدة معطيات تدور حول واقع الجريمة الالكترونية ، وهذا ما سنتولى توضيحه في المطلبين الآتيين:

المطلب الأول :معوقات اثبات الجريمة الالكترونية

تتمحور هذه المعوقات حول كل متعلقات هذه الجريمة ،فمنها ماهو متصل بالجريمة ذاتها والجهات المتضررة، ومنها ماهو متعلق بالجهات التحقيقية والواقع التشريعي الخاص بهذا النوع من الجرائم ،وهذا ما سنأتي على بيانه في الفروع الآتية:

الفرع الأول :المعوقات المتعلقة بالجريمة

هناك أمور تُعيق سلطات التحقيق أثناء ممارستها لإجراءات التحقيق ،وتتمثل هذه الأمور بمايأتي:

١) اختفاء آثار الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه،إذ إن مرتكبي هذا النوع من الجرائم نادراً مايتركون آثاراً مادية ملموسة يمكن أن تُشكل طرف خيط يقود إليهم بفضل مهاراتهم في استخدام هذه التقنيات وبرامجها.

٢) صعوبة الوصول إلى الدليل لاحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع على محتواها أو استنساخها.

٣) سهولة محو الدليل أو تدميره في زمن قصير،فالجاني يُمكنه محو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جداً،بحيث يصعب على الجهات التحقيقية كشف الجريمة إذا علمت بها.

٤) الضخامة البالغة لحجم المعلومات والبيانات المتعين فحصها وامكانية خروجها عن نطاق اقليم الدولة[٢٤].

٥) لا يستخدم هؤلاء الجناة في دخولهم شبكة الانترنت أجهزتهم الخاصة في أغلب الأحيان،وإنما يلجأون إلى مقاهي الانترنت المنتشرة حالياً في معظم المدن والأحياء التي لا تتقيد بأي ضوابط أو أنظمة أمنية يُمكن من خلالها التعرف على مستخدمي أجهزة الحاسب الآلي المتعاقبين في حالة اكتشاف أفعال غير مشروعة مصدرها هذه الأجهزة.

٦) أغلب البيانات والمعلومات التي يتم تداولها عبر الحاسب الآلي وشبكة الانترنت هي عبارة عن رموز مخزنة على وسائط ممغنطة لا يُمكن الوصول إليها إلا بواسطة الحاسب الآلي ومن قبل أشخاص قادرين على التعامل مع هذه الأجهزة ونظمها[٢٥].

الفرع الثاني :المعوقات المتعلقة بالجهات المتضررة من الجريمة

تتمثل المعوقات المتعلقة بالجهات المتضررة بعدة جوانب نلخصها بمايأتي:

١) عدم ادراك خطورة الجرائم المعلوماتية من قبل المسؤولين بالمؤسسات ،وهذا يرجع الى اغفال جانب التوعية لإرشاد المستخدمين إلى خطورتها،وبالنظر الى بعض المؤسسات نجد أنها أسست نظم معلوماتها على تطبيقات خاصة من التقنية على أساس إنها تقدم لعملائها خدمات أسرع بدون عوائق ويكون ذلك على الجانب الأمني.

٢) الحفاظ على سمعة بعض المؤسسات والأفراد ، حيث يكون الإحجام عن الابلاغ عن هذا النوع من الجرائم بسبب عدم رغبة الجهات المتضررة في الظهور بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها،بما قد يترك انطباعاً باهمالها أو قلة خبرتها أو عدم وعيها الامني،ولم تتخذ الاحتياطات اللازمة لحماية معلوماتها.

٣) تعد التقنية المستخدمة في نظم المعلومات مجال استثمار،ولذا تتسابق الشركات في تبسيط الاجراءات وتسهيل استخدام البرامج والاجهزة وملحقاتها،وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الامني،على سبيل المثال مستخدمو شبكة الانترنت عبر مزودي الخدمة وبطاقات الانترنت المدفوعة ليسوا مطالبين بتحديد هويتهم عند الاشتراك في خدمة الانترنت،أي ان مزود الخدمة لا يعرف هوية مستخدم الخدمة[٢٦].

٤) خشية بعض الجهات المتضررة من الحرمان من الخدمة،اذ ان الافصاح عن التعرض لجريمة معلوماتية من شانه حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتي،فقد يحرم الموظف في الجهة من خدمات معينة على الانترنت او قد يحرم من خدمات الانترنت عموماً،حيث يتعرض لجريمة معلوماتية ناجمة عن الاختراق او زيارته لأماكن غير مأمونة او غير مسموح بزيارتها، وقد يكون سبب عدم الابلاغ عن الجريمة عدم معرفة الضحية بوجود جريمة اصلاً،وعدم القناعة انها ممكن ان تحدث في مؤسسته[٢٧].

الفرع الثالث :المعوقات المتعلقة بالجهات التحقيقية

هناك معوقات للتحقيق في جرائم الحاسوب والانترنت تتعلق بالسلطات القائمة بالتحقيق وترجع لعدة اسباب ، والاسباب سوف نذكرها كما يلي:

١) بعض هذه المعوقات ترجع الى شخصية المحقق ،مثل التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الانترنت ،بالاضافة الى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الالكترونية ،بينما في المقابل نجد أن مرتكبي هذه الجرائم يتابعون كل جديد ويعملون على تطوير سبل اخفاء أدلة جرائمهم،فضلاً عن ذلك إن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة اصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم،وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات وهي لغة جديدة ومتطورة.

٢) وكذلك من اهم معوقات التحقيق تلك المتعلقة بأساليب المكافحة ،مثل عدم توفر الاجهزة والبرامج المناسبة للتحقيق وعدم التنسيق بين المحققين في هيئات التحقيق والعاملين في مجال المعلومات والانظمة الالكترونية والحاسوب.

لكل ما ذكرناه انفاً تبدو الحاجة ملحة الى انشاء وحدة متخصصة للتحقيق في الجرائم الالكترونية تتكون من محققين وطاقم من ذوي الاختصاص في مجال تقنية المعلومات[٢٨]،وتبريرنا لهذا هو إن عالم تقنية المعلومات عالم لا حدود له وفي تطور متسارع بشكل مذهل،ففي كل يوم يرفدنا بابتكارات جديدة،ولهذا لابد من توفر مجموعة خاصة بهذه المسائل لكي تكون على اطلاع

دائم على هذا العالم اللامتناهي، فضلاً عن ان وجود مثل هكذا وحدة سيساهم بشكل فعال برفد الجهات التشريعية بكل مستجد في مجال تقنية المعلومات لكي تعمل بدورها على سد اية ثغرة في مجال التشريعات الالكترونية ،بالاضافة الى دورها التوعوي للمجتمع في مجال تقنية المعلومات واحاطته بكل ما يحويه من مخاطر[٢٩].

الفرع الرابع :المعوقات التشريعية

ثمة مجموعة نقاط جوهرية تدور في هذا الاطار نستعرضها عبر نقطتين:

أولاً: على الصعيد الوطني:

يتصدى قانون العقوبات للظواهر الاجرامية فيُحدد الافعال الجرمية ويضع العقوبات الرادعة لكل منها،وغايته انزال العقاب بالمجرمين وحماية المجتمع من شرورهم وردع غيرهم عن الاقتداء بهم،وهذا يُمثل الشق الأول من المعادلة التشريعية الجزائية،أما الشق الثاني فيتمثل في قانون أصول المحاكمات الجزائية الذي يحدد القواعد الاجرائية والضمانات التي ينبغي أن تسير على هديها الجهات المعنية بانفاذ القانون في مراحلها المختلفة بدءاً بمرحلة الاستدلال وانتهاءا بالمحاكمة، فالقانونان إذن يُكملان بعضهما .

وكما هو الحال في المعوقات المرتبطة بالجريمة ذاتها أو الجهات المتضررة من الجريمة ، كذلك تبرز ذات المشكلة بالنسبة للنصوص المتعلقة بهذه الجرائم،بمعنى آخر هل إن إبقاء الحال كما هو عليه في النصوص التقليدية يكفي لتغطية كل ماهو حديث يفرزه لنا التطور المتسارع ،أم إن هناك حاجة لوضع نصوص وقواعد جديدة لتدارك النواقص؟

فبالنسبة لمحور بحثنا برزت لنا بعض الأمور نذكر من ذلك على سبيل المثال ،إن المعلومات التي تُشكل عصب الجرائم الالكترونية إذا وقعت عليها جريمة السرقة،فالمشكلة هنا إن أحد أركان جريمة السرقة هو وقوعها على مال منقول لغير الجاني عمداً،فهل إن وصف المنقول ينطبق على المعلومات (مادة الجريمة الالكترونية) وذلك على اعتبار إن جرائم الأموال تتحقق بخروج المال من حيازة المجني عليه إلى حيازة الجاني،بينما جريمة النترنت لا يُشترط في تحققها خروج المعلومات من حيازة المجني عليه وإنما تتحقق الجريمة حتى ولو بقيت المعلومات في حيازة المجني عليه كاستنساخ المعلومات والاستفادة منها لاحقاً.

مثال آخر إن مفهوم الجريمة المشهودة كما أوضحه المشرع في أصول المحاكمات الجزائية قائمة على معطيات مادية وحسية لا ينسجم مع طبيعة الجريمة الالكترونية التي عادة لا يظهر منها أية إشارات أو معطيات مادية أو حسية[٣٠].

من أجل كل هذا وغيره وفي سبيل وضع معالجات لكل المشاكل المتعلقة بتقنية المعلومات اتجه المشرع في العديد من الدول إلى اتجاهات عدة نوضحها في النقاط الآتية[٣١]:

١)الإتجاه الأول: تعديل نصوص الجرائم التقليدية وذلك بإضافة (المعلوماتية) إلى محل الجريمة ليشملها السلوك الاجرامي ،أي تطبق النصوص التقليدية على الجرائم الالكترونية بعد تعديل محل الفعل الاجرامي.

٢)الاتجاه الثاني: إضافة نصوص جديدة بعد النصوص التقليدية لتشمل كافة الجرائم الالكترونية كل في موقعه ،كإضافة نص جريمة الاحتيال بواسطة الانترنت بعد نصوص جريمة الاحتيال التقليدية واضافة نص جريمة السرقة بواسطة الانترنت بعد نصوص جريمة السرقة التقليدية وهكذا،وقد أخذ بهذا الاتجاه معظم الدول الأوربية ،كما في كندا والنمسا.

٣)الإتجاه الثالث:استحداث قسم جديد للجرائم الالكترونية على غرار الأقسام التقليدية كقسم جرائم الأموال،وإضافة نصوص جديدة إليه لتمثل الجرائم الالكترونية كافة أو تجميع ما يتعلق بالجريمة المعلوماتية في تشريع مستقل يُوضح الطبيعة الخاصة للجريمة المعلوماتية،وقد أخذت الولايات المتحدة بهذا الإتجاه وبريطانيا.

٤)الإتجاه الرابع: ويسمى بالإتجاه المختلط،حيث يتم اختيار أسلوب من الأساليب أعلاه لغرض وضع تشريع للجرائم الالكترونية ،وهذا معمول به في السويد ،حيث بدأت في استحداث قسم جديد للجرائم الالكترونية ضم العديد من الجرائم المستحدثة كجريمة الدخول غير المشروع إلى المواقع الخاصة أو استنساخ البيانات غير المشروعة من مختلف مواقع الانترنت ،ثم إضافة نصوص جديدة بعد النصوص القديمة للجرائم التقليدية،أي إنها جمعت بين الإتجاه الثاني والثالث،وأخذت بهذا الإتجاه ألمانيا والسويد وهولندا.

وتأسيساً على ما تقدم فإننا ندعو المشرع العراقي إلى إصدار تشريع خاص ومستقل للجرائم الإلكترونية يُوضح فيه الطبيعة الخاصة للجريمة الألكترونية ووضع عقوبات خاصة لهذه الجريمة تتلاءم وإياها،فضلاً عن وضع إجراءات جنائية تنسجم مع طبيعة هذا النمط من الجرائم.

ثانياً: على الصعيد الدولي:

تُعد جرائم تقنية المعلومات من أكثر الجرائم التي تُثير مشاكل تتعلق بالإختصاص على المستوى الدولي، وذلك بسبب الطبيعة الخاصة لهذا النوع من الجرائم التي تمتاز بقدرتها على التحرك في مجال فضائي واسع لا توقفه حدود الدول وسيادتها الاقليمية،حيث يُمكن لجريمة تقنية المعلومات أن تقع في مكان وتُنتج آثارها في مكان أو أماكن أخرى خارج الدول،وهذا الأمر يدعو إلى التعاون بين الدول من خلال الإتفاق على معايير محدودة ،وإن من أبرز المعوقات التي تُواجه الدول لتنظيم موضوع الجرائم الالكترونية هو تفاوت الدول في تحديد مفهوم الجرائم الالكترونية وأساليب التعامل معها ،وهذا راجع الى ان كل دولة تعمل على تنظيم موضوع التقنيات الالكترونية ضمن حدود قيمها السياسية والقانونية والاخلاقية والثقافية .

تعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الالكتروني،وقد أسست مجموعات عمل لوضع استراتيجيات لمكافحة الجرائم الالكترونية ،وأبرز هذه المجموعات والمنظمات الدولية التي عملت في موضوع الجرائم الالكترونية هو الاتحاد الدولي للاتصالات، ويُمثل هذا الاتحاد الذي يضم اكثر من (١٩٢) دولة وأكثر من (٧٠٠) شركة من القطاع الخاص والمؤسسات والاكاديمية منبراً إستراتيجياً للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة ،ويعمل الاتحاد على مساعدة الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات ،وقد وضع الاتحاد الدولي للاتصالات مخططاً لتعزيز الأمن الالكتروني العالمي يتكون من سبعة أهداف رئيسة وهذه الأهداف هي :

١)وضع أستراتيجيات لتطوير نموذج التشريعات الالكترونية يكون قابلا للتطبيق محلياً وعالمياً بالتوازي مع التدابير القانونية والوطنية والدولية المعتمدة .

٢)وضع استراتيجيات لتهيئة الارضية الوطنية والاقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلقة بالجرائم الالكترونية.

٣)وضع استراتيجيات لتحديد الحد الادنى المقبول عالمياًفي موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.

٤)وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.
٥)وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه ،وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للافراد عبر الحدود الجغرافية.
٦)تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي المجالات المعلوماتية جميعها.
٧)تقديم المشورة بشان امكانية اعتماد اطار استراتيجي عالمي لاصحاب المصلحة من اجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها[٣٢].

وتأسيساً على ماسبق يجب على العراق تصعيد نشاطه لازالة كافة العقبات فيما يتعلق بموضوع الجرائم الالكترونية من خلال عقد الاتفاقيات الثنائية أو الإنضمام الى الاتفاقيات الجماعية ذات العلاقة بالجرائم الالكترونية او الاتفاقيات الخاصة بالمساعدة القضائية بشكل عام على أن يكون مرجعهم في كل هذا المبادئ التي وضعها الاتحاد الدولي للاتصالات باعتباره الجهة المختصة ونقطة المحور الذي تعود اليه كافة حكومات الدول عند الاتفاق على كل متعلقات موضوع تقنية المعلومات .

المطلب الثاني :اجراءات الإثبات

إن المحققين يُواجهون العديد من الصعوبات عند ممارسة وظائفهم في اثبات الجرائم الالكترونية وهو ما يتطلب مجهوداً إضافياً وتدريباً وتعاوناً من الجهات ذات العلاقة لإثبات هذا النوع من الجرائم.

الفرع الأول : التحري وجمع الأدلة في الجرائم الالكترونية

عادةً ما تبقى الجريمة مستترة حتى يصل خبرها إلى السلطات المختصة،هذا الوضع ينطبق على الجرائم كافة دون استثناء ، لكنه يتجلى وضوحاً بالنسبة لجرائم تقنية المعلومات نظراً لطبيعتها،حيث يصعب على الأشخاص العاديين الإبلاغ عنها لما تتطلبه من مهارات فنية غير متوافرة سوى لفئات مهنية أو تخصصية في مجال الحاسب الآلي ونظم تقنية المعلومات،وفي الأحوال جميعها فإن أي إخبار عن جريمة سواء كان فاعلها مجهولاً أم معلوماً ينبغي أن يتضمن على الأقل معلومات أولية عن الجريمة مثل تحديد محل الجريمة ومكان وقوعها ونوعها،إذ تُعد هذه العناصر مهمة وضرورية لمساعدة رجال الضبط القضائي في أي إخبار متعلق بجرائم تقنية المعلومات،بحيث تُمكنهم من تحديد معالم الجريمة ووضع خطة للتعامل معها من الناحيتين الفنية والقانونية.

هذا ويتم الكشف عن الجرائم الالكترونية بوضع برمجيات حاسوبية معينة خصوصاً فيما يخص جرائم القرصنة أو نشر المواد الإباحية.

إن استحداث الأدوات البرمجية الحاسوبية التي من خلالها يُمكن التعرف على الأنماط الإجرامية تعد مسألة لا غنى عنها في كشف الجريمة بالنظر لضخامة حجم المعلومات المتوافرة في شبكة الانترنت،وهناك وسيلتان لأعضاء الضبط القضائي لغرض الحصول على البيانات المتعلقة بارتكاب الجريمة من نظام حاسوب ،وهما تستندان إلى معايير تقنية وقانونية، وتتمثل بما يأتي:

١) يتم الحصول على المعلومات من الموقع نفسه الذي تم من خلاله ارتكاب الجريمة بعد أن يتم إكتشافه باستخدام البرمجيات الحديثة.
٢) يتم الحصول على المعلومات عن طريق إعتراض أو رصد البيانات المنقولة من الموقع أو إليه أو في إطاره[٣٣].

أما إذا كانت الجريمة مشهودة كما لو تم ضبط الفاعل وهو يستخدم موقع الانترنت لارتكاب إحدى الجرائم ،فعلى عضو الضبط القضائي إخبار قاضي التحقيق والادعاء العام بوقوع الجريمة وينتقل فوراً إلى محل الحادثة ويسأل المتهم عن التهمة المُسندة إليه ويضبط كل ما يظهر إنه استعمل في إرتكاب الجريمة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الأشياء التي يُعتقد إن لها صلة بالجريمة ويسمع أقوال من يُمكن الحصول منه على معلومات وإيضاحات في شأن الحادثة ومرتكبها ويُنظم محضراً بذلك(٣٤).

وبشكل عام على المكلفين بمعاينة مسرح الجريمة اتباع جملة من الارشادات التي قد تسهم بإزالة الغموض المحيط بملابسات ارتكاب الجريمة(٣٥):

١)التحفظ على الأجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الاشياء التي يعتقد ان لها صلة بالجريمة.

٢)اثبات الطريقة التي تم بواسطتها اعداد النظام والعمليات الالكترونية ،وخاصة ماتحتويه السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام.

٣)عدم نقل أي مادة متحفظ عليها من مسرح الجريمة قبل التأكد من خلو المحيط الخارجي بموقع الحاسب الآلي من أي مجالات لقوة مغناطيسية يُمكن أن تسبب في محو البيانات المسجلة عليها.

٤)اثبات حالة التوصيلات والكبلات المتصلة بمكونات النظام كله،وذلك لاجراء مقارنة لدى عرض الأمر على القضاء.

الفرع الثاني : التحقيق الابتدائي في الجرائم الالكترونية

ثمة مجموعة من الاجراءات يجب إتباعها في هذا الإطار لاستحصال الدليل على الجريمة ،وسنتناول في هذا الفرع التفتيش والخبرة فقط لكونهما أكثر الإجراءات تماساً وأهمية في نطاق الجريمة الإلكترونية :

أولاً: التفتيش: يُقصد بالتفتيش البحث عن جسم الجريمة والأداة التي استخدمت في إرتكابها وكل ماله علاقة بها أو بفاعلها(٣٦).

إن عالم تقنية المعلومات يتكون بطبيعة الحال من شقين هما الكيانات المادية والكيانات المعنوية ،وتبعاً لذلك فإن التفتيش باعتباره اجراء من اجراءات التحقيق الابتدائي يختلف في كلا الشقين،وعلى ذلك لا بُد من التفريق بين تفتيش الكيانات المادية وتفتيش الكيانات المعنوية وذلك في النقطتين الآتيتين:

أ) **تفتيش الكيانات المادية:** إن التفتيش المتعلق بالكيانات المادية في نطاق الجرائم الالكترونية يسهل إجراؤه وتنطبق عليه القواعد التقليدية للتفتيش،إذ لاخلاف على إن الولوج إلى المكونات المادية للكمبيوتر بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يُفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للاجراءات القانونية الخاصة بالتفتيش،بمعنى إن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الأماكن العامة أو من الأماكن الخاصة،حيث إن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش،فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حرمة ،فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها التفتيش وبنفس الاجراءات المقررة قانوناً في التشريعات المختلفة،مع مراعاة التمييز بين ما إذا كانت مكونات الكمبيوتر المراد

تفتيشها منعزلة عن غيرها من أجهزة الكمبيوتر الأخرى ،أم إنها متصلة بكمبيوتر آخر أو بنهاية طرفية في مكان آخر كمسكن غير المتهم مثلاً،فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود التي يستلزمها المشرع لتفتيش هذه الأماكن،أما إذا وجد شخص يحمل مكونات الكمبيوتر المادية أو كان مسيطراً عليها أو حائزاً لها في مكان ما من الأماكن العامة سواء كانت عامة بطبيعتها كالطرق العامة والميادين والشوارع،أم كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة،فإن تفتيشها لا يكون الا في الحالة التي يجوز فيها تفتيش الاشخاص وبنفس القيود المنصوص عليها في هذا المجال[٣٧].

ب)**تفتيش الكيانات المعنوية:** أثار تفتيش الكيانات المعنوية خلافاً كبيراً في الفقه،فذهب رأي في الفقه إلى جواز تفتيش وضبط البيانات الالكترونية بمختلف أشكالها،ويستند هذا الرأي في ذلك إلى القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي شيء)،فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة،بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة،ولذلك فإنه يقترح أصحاب هذا الرأي على مواجهة هذا القصور التشريعي بالنص صراحةً على جواز تفتيش المكونات المعنوية للكمبيوتر[٣٨].

وإذا ما تصفحنا المواد الخاصة بالتفتيش في قانون أصول المحاكمات الجزائية العراقي سنجد إن المشرع قد ذكر كلمة (أشياء)على إطلاقها في أكثر من موضع في هذه المواد،وهذا يعني إن التفتيش في نطاق الجرائم الالكترونية من الجائز أن يمتد للكيانات المادية والمعنوية على حد سواء ضمن ضوابط يجب مراعاتها عند اجراء التفتيش على هذه الكيانات[٣٩] .

وقد أكد على المفهوم ذاته مجموعة من التشريعات منها قانون الإجراءات الجزائية الإتحادي الإماراتي،حيث أشارت نصوص القانون إلى إن التفتيش يقع على الأشياء المتعلقة بالجريمة أو التي تكون لازمة للتحقيق فيها، وقد تكررت كلمة (أشياء) دون أن تُحدد ماهية هذه الأشياء،إن كانت مادية أو معنوية[٤٠].

ثانياً: الخبرة : يقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة وفاعلها باتخاذ الاجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه،ومن ضمن هذه الاجراءات هي الاستعانة بأهل الخبرة وذلك تحقيقاً لمبدأ هام وهو مبدأ التخصص نظراً لكون الخبرة هي تقدير مادي أو ذهني يُبديه أصحاب الفن أو الإختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها وبمعلوماته الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أم بجسم الجريمة أم المواد المستعملة في ارتكابها أم آثارها[٤١].

وإن تشكيل فريق متخصص بالتحقيق في الجرائم بشكل عام قد يعد أمراً ضرورياً،ومرجع تقدير ذلك للجهة التحقيقية ،أما على مستوى الجرائم الالكترونية فالأمر مختلف،إذ يُعد تشكيل مثل هكذا فريق من الاعتبارات التي لا مناص منها وله أهمية خاصة نظراً للطبيعة الخاصة التي تتميز بها الجرائم الالكترونية عن غيرها من الجرائم، وذلك لأن هذه الجرائم مرتبطة بمسائل فنية وعلمية بحتة،إذاً يصبح لزاماً على القائم بالتحقيق الاستعانة بالخبراء والمختصين،لأن تصدي المحقق لفحص شيء وإبداء الرأي فيه دون أن تتوافر لديه المعرفة اللازمة يجعل قراره معيباً يضر بمصلحة التحقيق ويعوق الوصول إلى الحقيقة،وكل هذا يصب في أهمية التقارير التي يُنجزها خبراء تقنية المعلومات في مجال الجرائم الالكترونية ويُعطيها مكانة متميزة من حيث الإلزام.

إن إختيار الخبير في الجرائم الالكترونية يتوقف على نوع الجريمة المرتكبة ومجال الخبرة المطلوبة وطبيعتها الفنية ،فلا يكفي حصول الخبير على درجة علمية معينة،وإنما ينبغي أن تكون لديه خبرة علمية تخصصية وكفاءة فنية عالية في حقل أو أكثر من حقول تقنية المعلومات ونظمها ووسائلها ،فقد تكون الجريمة المرتكبة تزوير مستندات أو تلاعباً في البيانات أو الغش أثناء نقل أو بث البيانات أو إطلاق الفيروسات أو قرصنة أو إعتداء على حرمة الحياة الخاصة أو التجسس[٤٢].

الخاتمة:

أولاً: النتائج:

١) اتضح لنا في نطاق مفهوم الجرائم الالكترونية أن التعريفات التي أوردها الفقه قد امتازت بالتعدد والاختلاف ضيقاً وإتساعاً تبعاً للمعايير والمنطلقات المستندة إليها، فمنها ما اعتمد أصحابها على معيار الوسيلة المستخدمة في ارتكاب الجريمة، وآخرون اعتمدوا معيار موضوع الجريمة ذاتها،ومنهم من اعتمد معايير مختلطة جمعت بين المعيارين السابقين.

٢) إن عالم تقنية المعلومات عالم لا حدود له وفي تطور متسارع بشكل مذهل،ففي كل يوم يرفدنا بابتكارات جديدة.

٣) إن الوسائل الفنية التي قد تستخدم لتدمير مكونات الحاسوب كثيرة ومعقدة في الوقت الحاضر، ولا يُمكن التنبؤ بالوسائل التي قد تستحدثها التكنولوجيا في هذا الشأن.

٤) أتضح لنا وجود العديد من المعوقات تعتري اثبات الجريمة الالكترونية، منها ماهو متعلق بالجريمة ذاتها أو الجهات المتضررة من الجريمة أو الجهات التي تتولى التحقيق في هذه الجرائم بالاضافة الى المعوقات التشريعية،وهذا الأمر يتطلب إتخاذ مجموعة من الخطوات الإصلاحية في هذا الصدد.

٥) إن للجرائم الالكترونية طبيعة خاصة،إذ تمتاز بقدرتها على التحرك في مجال فضائي واسع لا توقفه حدود الدول وسيادتها الاقليمية،حيث يُمكن لجريمة تقنية المعلومات أن تقع في مكان وتُنتج آثارها في مكان أو أماكن أخرى خارج الدول.

ثانياً :التوصيات:

١) ندعو مجلس القضاء الأعلى الى انشاء هيئة متخصصة للتحقيق في الجرائم الالكترونية تتكون من محققين وطاقم من ذوي الاختصاص في مجال تقنية المعلومات، إذ ان وجود مثل هكذا هيئة سيساهم بشكل فعال برفد الجهات التشريعية بكل مستجد في مجال تقنية المعلومات لكي تعمل بدورها على سد اية ثغرة في مجال التشريعات الالكترونية ،بالاضافة الى دورها التوعوي للمجتمع في مجال تقنية المعلومات واحاطته بكل ما يحويه من مخاطر.

٢) ندعو المشرع العراقي إلى إصدار تشريع خاص ومستقل للجرائم الإلكترونية يُوضح فيه الطبيعة الخاصة للجريمة الإلكترونية ووضع عقوبات خاصة لهذه الجريمة بحيث تتلاءم وإياها،فضلاً عن وضع إجراءات جنائية تنسجم مع طبيعة هذا النمط من الجرائم.

٣) يجب على العراق تصعيد نشاطه لإزالة العقبات فيما يتعلق بموضوع الجرائم الالكترونية من خلال عقد الاتفاقيات الثنائية أو الإنضمام الى الاتفاقيات الجماعية ذات العلاقة بالجرائم الالكترونية او الاتفاقيات الخاصة بالمساعدة القضائية بشكل عام على أن يكون مرجعهم في كل هذا المبادئ التي وضعها الاتحاد الدولي للاتصالات باعتباره الجهة المختصة ونقطة المحور الذي تعود اليه حكومات الدول عند الاتفاق على متعلقات موضوع تقنية المعلومات.

الهوامش:

١) د. ناصر بن محمد البقمي/مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية/سلسلة محاضرات الامارات تصدر عن مركز الامارات للدراسات والبحوث الاستراتيجية /العدد ١١٦/٢٠٠٨ /ص١٠.
٢) أحمد خليفة الملط/الجرائم المعلوماتية/دار الفكر الجامعي/الاسكندرية/٢٠٠٥/ص ١٠٢.
٣) د.ناصر بن محمد البقمي/مصدر سابق/ص١١.
٤) راشد بشير ابراهيم/التحقيق الجنائي في جرائم تقنية المعلومات (دراسة تطبيقية على امارة ابو ظبي)/بحث منشور في مجلة دراسات استراتيجية/مركز الامارات للدراسات والبحوث الاستراتيجية/العدد ١٣١/٢٠٠٨/ص٢٣.
٥) د. عبد الفتاح بيومي حجازي/مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي/ط١/دار الفكر الجامعي/الاسكندرية/٢٠٠٦/ص٢١.
٦) د.جمال ابراهيم الحيدري/الجرائم الالكترونية وسبل معالجتها/ط١/مكتبة السنهوري/بغداد/٢٠١٢/ص٣٠.
٧) سمي (الفيروس) هذا الاسم لتشابه آلية عمله مع تلك الفيروسات التي تصيب الكائنات الحية بعدد من الخصائص كخاصية الانتقال بالعدوى وكونه كائناً غريباً يقوم بتغيير حالة الكائن المصاب اضافة إلى ان الضرر الذي يسبب فيه يجب أن يتم العلاج بازالته،انظر في هذا الصدد : منير محمد الجنيهي،ممدوح محمد الجنيهي/جرائم الانترنت والحاسب الآلي ووسائل مكافحتها /دار الفكر الجامعي /الاسكندرية/٢٠٠٦/ص٧١.
٨) د.حسن حماد حميد الحماد/الإتلاف المعلوماتي/بحث منشور في كتاب (نحو معالجات لبعض المستجدات في القانون الجنائي{مجموعة أبحاث معمقة})/ط١/منشورات الحلبي الحقوقية/بيروت/٢٠١٣/ص١٣٥.
٩) د.عبد الفتاح مراد/شرح جرائم الكمبيوتر والانترنت /د.ن/د.م/د.ت/ص٦٤.
١٠) منير محمد الجنيهي،ممدوح محمد الجنيهي/مصدر سابق/ص٦٨.
١١) د.حسن حماد حميد الحماد/مصدر سابق/ص١٣٦.
١٢) خالد عياد الحلبي/إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت/ط١/دار الثقافة للنشر والتوزيع/الأردن/٢٠١١/ص٧٧.
١٣) منير محمد الجنيهي،ممدوح محمد الجنيهي/مصدر سابق/ص٨٢.
١٤) د.حسن حماد حميد الحماد/مصدر سابق/ص١٣٨.
١٥) منير محمد الجنيهي،ممدوح محمد الجنيهي/مصدر سابق/ص٨٢.
١٦) خالد عياد الحلبي/مصدر سابق/ص٨٦.
١٧) د.حسن حماد حميد الحماد/مصدر سابق/ص١٣٩.
١٨) خالد عياد الحلبي/مصدر سابق/ص٨٦-٨٧.
١٩) د.حسن حماد حميد الحماد/مصدر سابق/ص١٤٠.
٢٠) خالد عياد الحلبي/مصدر سابق/ص٨٧.
٢١) د.عبد الفتاح مراد/مصدر سابق/ص٧٦.
٢٢) د.محمد طارق الخن/الجريمة المعلوماتية/د.ن/د.م/٢٠١٢/ص٤٠.
٢٣) منير محمد الجنيهي،ممدوح محمد الجنيهي/مصدر سابق/٥٦.
٢٤) خالد عياد الحلبي/مصدر سابق/ص٢٢٣.
٢٥) راشد بشير ابراهيم/مصدر سابق/ص٩٠.
٢٦) خالد عياد الحلبي/مصدر سابق/ص٢٢٣.
٢٧) د.خالد ممدوح ابراهيم/فن التحقيق الجنائي في الجرائم الالكترونية/دار الفكر الجامعي/الاسكندرية/٢٠١٠/ص٦٧-٦٨.
٢٨) في الولايات المتحدة الامريكية تم انشاء وحدة متخصصة للمكافحة والتحقيق في هذه الجرائم من ضمن مكتب التحقيقات الفيدرالي،ويكون تدريب هذه الوحدة مستمراً ليُواكب تطور جرائم الحاسوب والانترنت،وفي المملكة الأردنية الهاشمية

أنشأت مديرية الأمن قسماً خاصاً بجرائم الحاسوب والانترنت منذ عام ١٩٩٨، يتولى إجراءات المكافحة والاستدلال والتحقيق في الجرائم الالكترونية ،وتم رفد هذا القسم بمختصين في مجال علوم وهندسة الحاسوب،وزود بما يلزم من أجهزة ومعدات وبرمجيات تساعد في اجراءات التحقيق،وفي فحص الأجهزة المضبوطة في الجريمة والمحافظة على الأدلة ،أنظر في هذا الصدد : خالد عياد الحلبي/مصدر سابق/ص٢٢٥.

٢٩) وإن إنشاء وحدات تحقيقية متخصصة في صنف معين من الجرائم في العراق ليس بالأمر الجديد أو المستغرب،فقد سبق وأن تم انشاء وحدة تحقيقية متخصصة بجرائم الفساد الاداري والمالي ألا وهي هيئة النزاهة العراقية.

٣٠) حيث نصت الفقرة (ب) من المادة (١) من قانون أصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة (١٩٧١) على مايلي:(تكون الجريمة مشهودة اذا شوهدت حال ارتكابها أو عقب ارتكابها ببرهة يسيرة أو إذا تبلغ المجني عليه مرتكبها أثر وقوعها أو تبعه الجمهور مع الصياح أو إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملاً آلات أو أسلحة أو أمتعة أو أوراقا أو أشياء أخرى يستدل منها على انه فاعل أو شريك فيها أو إذا وجدت به في ذلك آثار أو علامات تدل على ذلك).

٣١) د. جمال ابراهيم الحيدري/مصدر سابق/ص٣٨.

٣٢) دراسة بعنوان (المعاهدات الدولية للانترنت:حقائق وتحديات)للدكتور(جورج لبكي) منشورة على الموقع الالكتروني (www.groups.google.com).

٣٣) د.جمال ابراهيم الحيدري/مصدر سابق/ص٧٦.

٣٤) نصت المادة (٤٣) من قانون أصول المحاكمات الجزائية على مايلي:(على عضو الضبط القضائي ... إذا أخبر عن جريمة مشهودة أو اتصل علمه بها أن يخبر قاضي التحقيق والادعاء العام بوقوعها وينتقل فوراً إلى محل الحادثة وبدون إفادة المجني عليه ويسأل المتهم عن التهمة المسندة اليهم شفوياً ويضبط الأسلحة وكل ما يظهر أنه استعمل في ارتكاب الجريمة ويعاين آثارها المادية ويحافظ عليها ويثبت حالة الأشخاص والأماكن وكل ما يُفيد في اكتشاف الجريمة ويسمع أقوال من كان حاضراً أو يُمكن الحصول منه على إيضاحات في شأن الحادثة ومرتكبها ويُنظم محضراً بذلك.

٣٥) راشد بشير ابراهيم /مصدر سابق/ص٥٢.

٣٦) د.سلطان الشاوي/أصول التحقيق الإجرامي/د.ن/د.م/د.ت/ص٨١.

٣٧) أنظر المواد من (٧٢) إلى (٨٦) من قانون أصول المحاكمات الجزائية.

٣٨) خالد ممدوح ابراهيم/مصدر سابق/ص١٩٧.

٣٩) أنظر المواد (٧٤،٧٥،٧٨،٧٩) من قانون أصول المحاكمات الجزائية .

٤٠) المواد (٥١،٥٣،٥٥،٥٧) من قانون الإجراءات الجزائية الإتحادي الإماراتي رقم (٣٥) لسنة (١٩٩٢).

٤١) أ. عبد الأمير العكيلي ، د.سليم حربة/ شرح قانون أصول المحاكمات الجزائية/ ج١/د.ن/بيروت/٢٠٠٩/ص١٢٦.

٤٢) راشد بشير ابراهيم /مصدر سابق/ ص٦٩.

المصادر:

أولاً: الكتب:

١) **أحمد خليفة الملط/الجرائم المعلوماتية/دار الفكر الجامعي/الاسكندرية/٢٠٠٥.**

٢) **د.جمال ابراهيم الحيدري/الجرائم الالكترونية وسبل معالجتها/ط١/مكتبة السنهوري/بغداد/٢٠١٢.**

٣) **خالد عياد الحلبي/إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت/ط١/دار الثقافة للنشر والتوزيع/الأردن/٢٠١١.**

٤) **د.خالد ممدوح ابراهيم/فن التحقيق الجنائي في الجرائم الالكترونية/دار الفكر الجامعي/الاسكندرية/٢٠١٠.**

٥) **د.سلطان الشاوي/أصول التحقيق الإجرامي/د.ن/د.م/د.ت.**

٦) أ. عبد الأمير العكيلي ، د.سليم حربة/ شرح قانون أصول المحاكمات الجزائية/ ج١/د.ن/بيروت/٢٠٠٩.
٧) د. عبد الفتاح بيومي حجازي/مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي/ط١/دار الفكر الجامعي/الاسكندرية/٢٠٠٦.
٨) د.عبد الفتاح مراد/شرح جرائم الكمبيوتر والانترنت /د.ن/د.م/د.ت.
٩) د.محمد طارق الخن/الجريمة المعلوماتية/د.ن/د.م/٢٠١٢.
١٠) منير محمد الجنيبهي،ممدوح محمد الجنيبهي/جرائم الانترنت والحاسب الآلي ووسائل مكافحتها /دار الفكر الجامعي /الاسكندرية/٢٠٠٦.

ثانياً : البحوث والدراسات:

١)د. جورج لبكي / دراسة بعنوان (المعاهدات الدولية للانترنت:حقائق وتحديات) منشورة على الموقع الالكتروني (www.groups.google.com).
٢)د.حسن حماد حميد الحماد/الإتلاف المعلوماتي/بحث منشور في كتاب (نحو معالجات لبعض المستجدات في القانون الجنائي(مجموعة أبحاث معمقة))/ط١/منشورات الحلبي الحقوقية/بيروت/٢٠١٣.
٣)راشد بشير ابراهيم/التحقيق الجنائي في جرائم تقنية المعلومات (دراسة تطبيقية على امارة ابو ظبي)/بحث منشور في مجلة دراسات استراتيجية/مركز الامارات للدراسات والبحوث الاستراتيجية/العدد ١٣١/٢٠٠٨.
٤)د. ناصر بن محمد البقمي/مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية/سلسلة محاضرات الامارات تصدر عن مركز الامارات للدراسات والبحوث الاستراتيجية /العدد ١١٦/٢٠٠٨.

ثالثاً: القوانين:

١) قانون أصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة (١٩٧١).
٢) من قانون الإجراءات الجزائية الإتحادي الإماراتي رقم (٣٥) لسنة (١٩٩٢).