صعوبات الدليل الجنائي في الجرائم المعلوماتية

أ.م جاسم خريبط خلف

قسم القانون / كلية شط العرب الجامعة

الملخص

الاثبات هو اقامة الدليل على وقوع الجريمة ونسبتها الى المتهم وذلك وفق الطرق التي حددها القانون ، والاثبات في مجال الجرائم المعلوماتية ينطبق عليه المفهوم العام للأثبات وهو بذلك يواجه العديد من الصعوبات التي تتعلق بصعوبة الحصول على دليل ، فالجناة الذين يستخدمون الوسائل الالكترونية في ارتكاب جرائمهم يتميزون بالذكاء والاتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعة الفنية ، ولذلك فانهم يتمكنون من اخفاء الافعال غير المشروعة التي يقومون بها اثناء تشغيلهم لهذه الوسائل الالكترونية ويستخدمون في ذلك التلاعب غير المرئي في النبضات او الذبذبات الالكترونية التي يتم تسجيل البيانات عن طريقها .

ان الطبيعة غير المادية للبيانات المخزونة بالحاسب الالي والطبيعة المعنوية لوسائل نقل هذه البيانات تثير مشكلات عديدة في الاثبات الجنائي ويكون الدليل الناتج عن الجرائم التي تقع على العمليات الالكترونية غاية في الصعوبة ، كما ان الكم الهائل للبيانات التي يجري تداولها في الانظمة المعلوماتية تشكل احد الصعوبات التي تعوق التحقيق في الجرائم التي تقع عليها .

بالإضافة الى ذلك نجد ان نقص خبرة جهات التحري والتحقيق حيث يتطلب كشف الجرائم المعلوماتية والاهتداء الى مرتكبيها وملاحقتهم قضائياً استراتيجيات تحقيق وتدريب ومهارات خاصه تسمح بفهم ومواجهة تقنيات الحاسب الالكتروني المتطورة واساليب التلاعب المحاسبي المعقدة التي تستخدم عادة في ارتكاب هذه الجرائم ، يضاف الى ذلك ضعف التعاون الدولي في

مواجهة الجريمة المعلوماتية ، هذه المصادر كانت مواضيع بحثنا حول صعوبات الدليل الجنائي في الجرائم المعلوماتية .

Abstract

Evidence is to prove that a crime is committed and to relate it to a suspect according to legal procedures. The general concept of evidence also applies to cybercrimes. So, evidence encounters many problems as how to obtain proofs, as the criminals, who use electronic devices in their crimes, are both intelligent and accurate at what they do, and that is why they can hide their illegal activities when operating their devices which they use in their illegal manipulation of electronic vibrations or pulses through which data are saved.

The non-physical nature of data saved on computers and the nature of the transference techniques raise a number of problems in criminal evidence; the proof of crimes related to electronic processes is very hard. Also, the huge quantities of data used in information systems form one of the difficulties that hinder the investigation of related crimes. Additionally, we find that another reason is that investigators and detectives are not fully experienced at the time that revealing crimes, finding the criminals, and judicially chasing them all require investigation strategies,

training and skills that help understand and confront the advanced technologies of computers and the illegal manipulations which are usually used in such crimes. The weak international cooperation in combating cybercrimes is also discussed. These subjects constitute the core of our research on the difficulties of evidence.

المقدمـــــة

يشـهد العلـم منـذً منتصـف القـرن العشـرين ثـورة جديـدة اصـطلح علـى تسـميتها بـالثورة المعلوماتيـة وذلـك إشـارة إلـى الـدور البـارز الـذي أصـبحت تلعبـه المعلومـات فـــي الوقـت الـراهـــن ، فقـد أسسـت قـــوه لا يسـتهان بهـا فـــــي أيـدي الـدول والأفـراد ، وكـان التطـور الهائـل الـذي شـهده قطـاعي تكنولوجيـا المعلومـات والاتصـالات والانـدماج المـذهل الـذي حـدث بينهمـا فيما بعد هو المحور الأساسي الذي قامت علية هذه الثورة .

إن هـذا التقـدم مـع كـل مـا كـان يحملـه مـن ايجابيـات لحيـاة الإنسـان ألا انـه كـان فـي الوقـت ذاتـــه يحمـل فـي طياتـه بـذور الشـر التـي كانـت تنتظـر ممـن يســقيها ميــاه الحيــاة ، وســرعان مــا وجــدت ســاقيها المتمثــل بــالمجرم ألمعلومــاتي الــذي وجــد هــو الأخــر ضــالته التــي كــان يبحــث عنهــا فــي التكنولوجيـا الحديثـة التـي أتاحـت لـه فرصـة ارتكـاب الجريمـة والحصـول مـن ورائهـا علـى اكبـر قـدر ممكـن مـن الأمـوال وبأقـل قـدر ممكـن مـن الخسـارة والمخـاطرة ، معتمـداً فـي ذلـك علـى مـا يتمتـع بـه مـن مهـارة فنيـة تقنيه في هذا الصدد .

لـذلك ظهـرت عـدة جـرائم مرتبطـة بـالثورة المعلوماتيـة لـم يكـن لهـا وجـود مـن قبـل ومـن أمثلـه هـذه الجرائـم صناعـة ونشـر الفيروسـات والاختراقـات غيـر ألمشـروعه ، وتعطيـل أجهـزة الآخـرين ومضـايقة وملاحقـة الآخـرين المتعـاملين مـع الشـبكة وكـذلك اسـتخدام الانترنـت فـي النشـر والإعـلان عـن الصـور الإباحيـة والـدعوة لممارسـة الجـنس عبـر الشـبكة ، وكـذلك النصـب عـن طريـق الإعـلان عـن بيـع سـلع وهميـة عبـر الشبكة وغيرها الكثير من الجرائم التي تستجد كل يوم .

وبنـاءً علـى ذلـك فـان النمـوذج التقليـدي للتحقيـق الجنـائي واسـتخلاص ألا دلـه يعكـس مجمـوعـه خطـوات متتـاليـة يصاحبهـا الكثيـر مـن المشكـلات العمليـة ، و يكشـف التحليـل العميـق لهـذا النمـوذج أن هنـاك بعـض الخطـوات التـي يمكـن إلغاءهـا باسـتخدام نظـام يقـوم علـى تكنولوجيـا المعلومـات والاتصـالات ، بالإضـافة إلـى أهميـة إعـادة دورية ومراجعة بعض العمليات والإجراءات بهدف التسهيل والتبسيط .

وإذا كانت المحكمة تحكم في الدعوى بناءً على اقتناعها الذي تكون لديها من الأدلة المقدمة في أي دور من ادوار التحقيق أو المحاكمة وهي الإقرار وشهادة الشهود ومحاضر التحقيق والمحاضر والكشوف الرسمية الأخرى وتقارير الخبراء والفنيين والقرائن والأدلة الأخرى المقررة قانوناً .

فـإذا صـدق مـا سـبق بالنسـبة لجـرائم قـانون العقوبـات التقليـدي ، فـان قواعـد هـذا القـانون تبـدو قاصـرة إزاء ملاحقـة مرتكـب الجريمـة المعلوماتيـة ، ممـا يقـال بهـذا الصـدد بـان قواعـد قـانون العقوبـات التقليديـة تواجـه تحـديات إزاء مواجهـة الجريمـة المعلوماتيـة ، وتبـدو قاصـرة عـن مواجهـة العديـد مـن الأفعـال التـي تهـدد مصـالح اجتماعيـة واقتصـادية ارتبطت بظهور وانتشار جهاز الحاسب الآلي وشبكة الانترنت .

لـذلك كـان هـذا عـاملاً حاسـماً فـي قيـام كثيـر مـن الـدول بسـن تشـريعات جديـدة أو تعـديل تشـريعاتها القائمـة لمواجهـة الجريمـة المعلوماتيـة ، ألا أن المشـرع فـي البلـدان العربيـة لـم يتـدخل جـدياً بعـد لمواجهـة هـذا النـوع مـن الجـرائم بنصـوص خاصـة ، فضـلاً عـن أن القضـاء لـم يواجـه بعـد بمشـكلات قانونيـة تتعلـق بحمايـة المعلومـات والبـرامج التـي تخـص الكومبيوتر .

علية وجب تحديث الأساليب الإجرائية المتبعة لجمع الأدلة في الجرائم المعلوماتية ، وتحديثها على نحو يكفل استجابتها بشكل كافٍ، وبغير أن تتعرض حقوق الإفراد وحرياتهم للخطر عند الإثبات في مجال الجريمة المعلوماتية التي لا تعترف بالمكان من حيث أثارها ، وتستعصي على القواعد التقليدية في قانون الإجراءات الجنائية .

وهنا تظهر أهمية دراسة بحثنا هذا وهي صعوبات القيام بالاستدلالات واستخلاص الدليل في الجريمة المعلوماتية وهو ما سنبينه في مواضيع هذا البحث ، ذلك أن صعوبة استخلاص الدليل قد يكون سببها أمور تتعلق بالدليل ذاته مثل إخفاء هذا الدليل وعدم رؤيته ، وقد يكون سببها حجم وكم البيانات المتعلقة بهذه الجريمة من حيث ضخامتها ومن حيث سهولة تدميرها ، كذلك فان أجهزة الضبط القضائي وأجهزة التحقيق الجنائي قد تعيق التحقيق في هذه الجريمة متى ما انعدمت أو نقصت خبرتها بشأن الجريمة المعلوماتية ، لذلك وجب تأهيلهم وتدريبهم فضلاً عن الاستعانة بالخبراء في الحاسب الآلي.

كل هذه الأمور وغيرها سوف تترجم محاور بحثنا الذي تم تقسيمه كالأتي :-

المبحث الأول :- الصعوبات المتعلقة بالدليل ذاته

المطلب الأول :- عدم ظهور الدليل المادي

المطلب الثاني :- طبيعة المجني علية بالجرائم المعلوماتية

المطلب الثالث :- فقدان أثار الجريمة

المبحث الثاني :- الصعوبات المتعلقة بجهات التحقيق

المطلب الأول :- نقص المعرفة الفنية لدى سلطات التحقيق

المطلب الثاني :- الخبرة في الجرائم المعلوماتية

المطلب الثالث :- ضعف التعاون الدولي في مواجهة الجريمة المعلوماتية

المبحث الأول

الصعوبات المتعلقة بالدليل ذاته

الدليل هو أداة الإثبات عموماً ، ويقصد بهذا الإثبات القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه للوصول إلى حكم بشأن الواقعة محل الإثبات ، ويقتصر الإثبات على إثبات الوقائع لا بيان وجهة نظر المشرع وحقيقة قصده ، فالبحث في هذا يتعلق بتطبيق القانون وتفسيره وهو من عمل المحكمة ، وينقسم الإثبات إلى نوعين ، الإثبات بالأدلة المباشرة والتي هي الاعتراف والشهادة والخبرة والمعاينة لمسرح الواقعة ، والإثبات بالأدلة غير المباشرة والتي يصل القاضي إلى الحقيقة منها عن طريق الاستقراء والاستنتاج ، وهذا الإثبات في نوعية يخضع لمبدأ الإثبات الحر والذي يعتمد على حرية القاضي الجنائي في الإقناع ، فالدليل الجنائي معنى يدرك من مضمون واقعه تؤدي إلى ثبوت الإدانة أو ثبوت البراءة ، ويم ذلك باستخدام الأسلوب العقلي وأعمال المنطق في وزن وتقدير تلك الواقعة ، ليصبح المعنى المستمد منها أكثر دقه في الدلالة على الإدانة أو البراءة (١) .

فأهمية الدليل في المواد الجنائية أهمية عظيمة لأنه هو الذي يناصر الحقيقة ويبين مرتكبها ، وهو الذي يحول الشك إلى يقين ، فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بأن يكون أو لا يكون ، وهذا لا يتحقق إلا بالدليل بحسبان انه المعبر عن هذه الحقيقة ، وان إجراءات جمع الأدلة لم ترد في القانون على سبيل الحصر ، ولذلك يجوز للمحقق أن يباشر أي إجراء أخر يرى فيه فائدة للإثبات طالما انه لا يترتب على اتخاذه تقييد لحريات الإفراد أو مساس بحرمة مساكنهم (٢) .

على أية حال فان التطور الذي لحق بالوسائل الالكترونية قد اثر تأثيراً كبيراً على الأدلة المتحصلة منها وعلى إجراءات الحصول عليها فهذا التطور قد جعل أكثر هذه الأدلة يتميز بطبيعة غير مرئية بحيث يصعب الوصول إليها لأنها تكون نتاج تلاعب في رموز ونبضات والكترونيات .

كما انه قد زاد من صعوبة إجراءات الحصول عليها لأنه قد أمد الجناة بوسائل متطورة تمكنهم من إخفاء أفعالهم غير المشروعة كاستخدام كلمات السر والتشفير واستطاعة التلاعب في البيانات المخزونة ، بل وإتلافها في الوقت الذي يرونه مناسباً وفي ثوانٍ معدودة.

وعلى ضوء ذلك يمكن القول بأن الدليل المتحصل من الوسائل الالكترونية يستمد طبيعته من ذات العمليات الالكترونية التي نتج منها في حالة الاعتداء عليها بالأفعال غير المشروعة ، ولذلك فهو يتخذ أيضا طبيعة الكترونية بحيث تصعب على المحقق ألا بأتباع إجراءات معينه يكون الغالب منها ذو طبيعة فنية ، وليس أدل على ذلك من أن التلاعب في المستندات الالكترونية لا يمكن كشفه بالطرق

التقليدية وإنما قد يحتاج ذلك إلى أدلة الكترونية قد تتحصل من الوسائل الالكترونية ذاتها أو باستخدام التقنية العلمية المتقدمة التي يتعين إتباعها للوصول إليه (٣) .

عليه سوف نقسم هذا المبحث إلى ثلاثة مطالب على ضوء الصعوبات التي تواجه سلطة الاستدلال والتحقيق الجنائي في استخلاص الدليل ، وهي عدم ظهور الدليل المادي وطبيعة المجني عليه بالجرائم المعلوماتية وفقدان أثار الجريمة .

المطلب الأول

عدم ظهور الدليل المادي

إن من ابرز خصائص الجريمة المعلوماتية هو وقوعها في بيئة الكترونية وهذه الخاصية تترتب عليها جمله نتائج تصعب من مهمة اكتشاف هذه الجرائم لا بل وحتى التحقيق فيها .

وهذا عكس الجرائم التقليدية ، فرجل الشرطة الذي يقوم بجمع التحريات في واقعة سرقة حتى يصل المتهم ،ويستصدر امرأ بالقبض عليه وتتولى جهات التحقيق استجوابه وأحالتها إلى محكمة الموضوع ، فكل هذه وقائع خاضعة لسيطرة أجهزة العدالة ، والدليل فيها مرئي ومقروء ، عكس الجريمة المعلوماتية التي تتم دون رؤية لدليل الإدانة ، وحتى في حالة وجود الدليل يمكن للجاني طمس الدليل او محوه وفي حضور أجهزة العدالة غير المتخصصة ، ولذلك فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بطريق الإبلاغ عنها (٤).

لأنها لا تخلف في الغالب أية أثار مادية كتلك التي تخلفها الجرائم التقليدية ، حيث أنها لا تخلف لا سكيناً ولا سلاحاً ولا ظروفاً فارغة لطلقات نارية ولا بقعاً دموية أو غير ذلك من الآثار المادية (٥) .

كما أن اغلب الآثار المتخلفة عن هذه الجرائم هي أثار الكترونية وهذه الآثار بدورها أنما هي عبارة عن نبضات الكترونية غير مرئية بالعين المجردة (٦) ، فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة بحيث انه لا يمكن رؤيتها ألا من خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان .

إن ضخامة حجم وكم البيانات والملفات الالكترونية التي تتواجد في البيئة الالكترونية تصعب من أمكانية تحديد الملفات والبيانات الالكترونية المجرمة ، من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها ، وتؤدي في الغالب إلى اصطدام مهمة الاكتشاف بحق الأفراد في الخصوصية الشخصية .

أن البيئة المعلوماتية غالباً ما تكون مؤلفة من شبكات منتشرة في كافة أرجاء المعمورة ومرتبطة ببعضها البعض عن طريق شبكة الانترنيت ، بحيث تتيح الفرصة أمام مجرمي المعلوماتية للولوج عن بعد إلى البيانات الالكترونية المخزونة في أية بقعة من بقاع العالم(٧).

وعلى العكس من ذلك فأن سلطات الضبط القضائي والسلطات ألتحقيقيه لا يكون بإمكانها الولوج إلى تلك البيانات كونها تقع في الغالب خارج حدود اختصاص دولها ، بحيث تصطدم بسيادة الدول الأخرى (٨) .

ولصعوبة استخلاص الدليل في مثل هذه الجريمة يرى المختصين في جرائم الحاسب الآلي ، أن هذا الجهاز وما يقع علية من جرائم معلوماتية يعد تحدياً هائلاً لرجال الأمن ، ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادراً على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية (٩)

وإذا كانت المصادفة من الأمور التي يعول عليها في كشف الجريمة المعلوماتية فأن وجود أجهزة الرقابة أو التدقيق داخل جهة الإدارة ، سواء كانت حكومية ، أو خاصة أو شركة من الشركات ، سوف يؤدي إلى كشف وقوع هذه الجريمة ، ومن ثم إظهار الدليل الخفي الذي تتسم به مثل هذه الجرائم ، شريطة

أن يكون الجهاز الذي يتولى هذه الرقابة ذا تخصص وخبرة عالية في التعامل مع أجهزة الحاسب الآلي وبرامجها ، وعالماً بأحداثها وطرق التعامل معها ، سيما وان المجرم في هذه الجريمة لدية الخبرة الفنية والمعرفة الكافية التي تمكنه من اقتراف جريمته .

ونؤكد ما ذكرناه بأن الجريمة التقليدية يكون الدليل فيها مرئياً ، من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب وكذلك المادة السامة التي استعملت في القتل ، أو المحرر ذاته الذي تم تزويره أو النقود التي زيفت وأدوات تزييفها ، حيث يستطيع عضو الضبط القضائي أو سلطة التحقيق رؤية الدليل المادي وملامسته بإحدى الحواس .

بينما في الجرائم المعلوماتية تكون البيانات والمعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام ألمعلوماتي مما تجعل أمر طمس الدليل ومحوه كلياً من قبل الفاعل أمراً في غاية السهولة (١٠) .

لذلك يرى جانب من الفقه الجنائي أن متطلبات العدالة الجنائية تفرض على الأجهزة الحكومية أن تتحمل كامل مسؤولياتها نحو اكتشاف الجرائم وضبط المجرمين ومحاكمتهم ، وهذا يقتضي توفير الإمكانيات التقنية اللازمة لتحقيق الجرائم المعلوماتية ، وبمعنى أخر يتعين استقطاب وجذب الكفاءات المهنية المتخصصة في هذا المجال ، للاستعانة بها في تحقيق هذه الجرائم ، ويتعين عدم التذرع بالميزانيات المالية كسبب يحول دون قيام الدولة بواجباتها نحو تحقيق العدالة الجنائية ، وحتى يتم ذلك يرى هذا الجانب ضرورة الاستعانة بالنبضة المتخصصة في الحاسب الآلي حال تحقيق الجرائم المعلوماتية وذلك لضبط هذه الجرائم واكتشافها ، وتقديم أدله الادانه فيها وشرح هذه الادله وإبعادها أمام المحاكم ، ويجب أن يتم ذلك في أطار القانون الجنائي وخصوصاً قواعد الخبرة أمام المحاكم الجنائية والتي ينظمها قانون الإجراءات الجنائية (١١) .

وتجدر الإشارة إلى أن انتحال الشخصية ، وكذلك التسلسل الإلكتروني من ابرز أمثلة السلوك الإجرامي في الجريمة المعلوماتية ، وذلك كدليل على عدم رؤية دليل الجريمة ، فكلاهما يستخدم أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية الكترونياً أو الوصول إلى مراكز الحاسب الآلي والدخول إلى قواعد المعلومات .

المطلب الثاني

طبيعة المجني عليه بالجرائم المعلوماتية

تتطلب الجرائم المعلوماتية على غرار الجرائم التقليدية حرفية عالية سواء عند ارتكابها أو عند العمل على اكتشافها من الشخص الذي يرتكبها ، أي يجب ان يكون ذلك الشخص خبيراً بالقدر اللازم والكافي بأمور الحوسبة والانترنت ولذلك نجد ان معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي ، وأن الشرطة تبحث أول ما تبحث عن خبراء الكومبيوتر عند ارتكاب هذا النوع من الجرائم (١٢) .

لذلك يعمد الجاني إلى تشفير الملفات أو البيانات الالكترونية التي تتضمن محتوى غير مشروع بغية منع الغير من الاطلاع عليها واكتشافها ، كما هو الحال في حالة نقل البيانات المتعلقة بجرائم غسيل الأموال عبر الانترنت بعد تشفيرها (١٣).

ويحرص الجاني بعد ارتكابه لجريمته على محو أثارها التي تدل على وقوعها ، وذلك من خلال التوسل بتقنيات معدة لهذا الغرض مع الأخذ بنظر الاعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الالكترونية التي يمكن القيام بها في أزمان قياسية متناهية القصر تقاس باللحظات والثواني(١٤) .

بناءً على ذلك كثيراً ما يكون ضحايا الجرائم المعلوماتية هم السبب في تصعيب اكتشاف هذه الجرائم لعدة أسباب وهي :

١- نقص الخبرة الفنية التقنية :

ان البيئة الالكترونية عموماً وعلى وجه الخصوص على شبكة الانترنيت توفر مناخاً مثالياً لاجتماع الفرائس بصياديها في بودقه واحدة ، خصوصاً وان اغلب مستخدمي هذه الشبكة لا تتوفر لديهم المعرفة التقنية اللازمة للتعرف على هذه الجرائم وأساليب ارتكابها ، مما يجعلهم عرضة للاقتناص من قبل مجرمي المعلوماتية من دون ان يشعروا بذلك ، فمثلاً قد يرسل الجاني رسالة متضمنة لفيروس أو ملف تجسس خفي الى الضحية

والتي تظهر في الغالب كرسالة ، بحيث انه بمجرد قيام الأخير بفتح الرسالة ، فأنه يتم إدخال الفيروس أو الملف ألتجسسي تلقائياً إلى كمبيوتر الضحية ومن دون أن يشعر الأخير بذلك ، كونه لا يعرف معنى الرسائل تلك ليقوم الفيروس في النهاية بإتلاف نظام الكومبيوتر أو أن يقوم الجاني بالولوج إلى كومبيوتر الضحية مـــن خـــلال ملف التجسس ، ومن دون أن يتمكن المجني عليه من اكتشاف ذلك ، وحتى ولو اكتشفه فأن ذلك غالباً بعد مرور زمن طويل من وقوع الجريمة وبالتالي بعد فوات الأوان وبعد زوال أغلب أثارها (١٥) .

٢- عدم اتخاذ الحيطة والحذر :

الكثير من ضحايا الجرائم المعلوماتية لا يتخذون الحيطة والحذر اللازمين لاكتشاف مثل هذه الجرائم في حال وقوعها فأغلب الإفراد من مستخدمي شبكة الانترنت لا يستخدمون برامج وتقنيات للحمايـة ضـد الاختراق والتجسس والوقاية مـــن الفيروسات ، ما يترتب على ذلك عدم أمكان اكتشافهم للجريمة الواقعة لحظة ارتكابها وقد يكتشفونها بعد مرور مدة طويلة

وقد لا يكتشفونها أبدا أن هذا الأمر يشمل حتى المؤسسات والشركات المالية والتجارية (١٦) ، فهي لا تقوم بمراجعة حساباتها المالية والتجارية يومياً ولا حتى شهرياً لتكتشف مثل هذه الجرائم قبل فوات الأوان ، وحتى ولو قامت بمثل هذه المراجعة فأنها غالباً ما تعتبر المفارقات الحاصلة في حساباتها مجرد مفارقات عادية ناجمة عن خسائرها الاعتيادية أو عن عمليات دفع أجله .

كما وان هذه المؤسسات غالباً ما تتسابق مع بعضها البعض في توفير خدماتها للعملاء بأكبر قدر ممكن من التسهيلات بحيث توجه اهتمامها إلى تحسين وتسهيل الحصول على خدماتها على حساب نظامها الأمني (١٧) ، مما ينجم عنه بالتالي سهولة اختراق نظامها الأمني وفي الغالب من دون أن يكتشف أمر الاختراق .

٣- الامتناع عن الإخبار :

تبقى الجريمة المعلوماتية مستترة ما لم يتم الإبلاغ عنها ، فالجريمة في صورتها التقليدية تصل إلى علم سلطات التحقيق عن طريق الشكوى أو الأخبار والتي يجب على عضو الضبط القضائي قبولها متى وردت في شأن جريمة ويحرر بها محضراً يرسله فوراً إلى قاضي التحقيق ، حتى يتسنى مراقبة مشروعية أعمال التحري ، والشكوى كالإخبار ، ألا أنها توجه ضد شخص معين وتقدم من المجني عليه أو المضرور من الجريمة ، بينما الأخبار يقدم من غيرهما أو يخلو من تعيين أسم من تنسب إليه الجريمة(١٨) .

وتنطبق نفس الأحكام في الجرائم المعلوماتية ، لكن المجني عليه في كثير من الأحيان يفضل عدم التبليغ عن الإصابة بفيروس وخاصة إذا كان المجني عليه مؤسسة مالية كبيرة كالبنوك ، وذلك حتى لا تهتز ثقة المتعاملين معها ويترتب على ذلك سحب ودائعهم واستثماراتهم فيها (١٩) ، وكذلك تدخل هذه

المؤسسات في اعتباراتها أن الإبلاغ عن الجرائم المعلوماتية التي وقعت ضدها ربما يؤدي إلى إحاطة المجرمين علماً بنقاط الضعف في أنظمتها .

ولذلك يبدو لنا من الملائم لدى سلطات الأمن في الجرائم المعلوماتية واكتشافها ان ترصد ميدانياً حركة المعاملات التجارية داخل المؤسسات المالية وحولها ، وذلك عن طريق جمع المعلومات السرية عن حركة السوق وتداول الأموال والممتلكات والتغيرات الاجتماعية والسلوكية للموظفين وصغار رجال الأعمال الذين يرتبطون بمؤسسات الجريمة المنظمة ، سيما وأن جرائم الحاسب الآلي هي من أدوات وأسلحة هذه الجريمة ، حيث يجري استقطاب صغار الموظفين وذوي القدرات الفنية والذين هم على مقربة من أسرار برامج الحاسب الآلي للمؤسسات المالية والشركات التجارية ويرتبط ذلك بضرورة تطوير ثقافة الحاسب الآلي في وسط رجال الأمن ، وربط تلك الثقافة بالثقافة الأمنية في صورها التقليدية ، وهو ما يضمن نجاحاً للأجهزة الأمنية في مواكبة ظاهرة الجرائم المعلوماتية (٢٠) .

٤- عدم أدراك خطورة الجرائم المعلوماتية (٢١) :

إن كثيراً من ضحايا الجرائم المعلوماتية لا يدركون خطورة هذه الجرائم ، لا بل وان بعضهم لا يتصور أمكانية وقوع مثل هذه الجرائم .

ويبدو أن معالجة هذه الأمور تتوقف عموماً على قيام ألدوله ممثلة بمؤسساتها التعليمية والقانونية و الإعلامية بنشر الثقافة القانونية بين مواطنيها ومؤسسات المجتمع المختلفة ، وتحذيرهم بخصوص خطورة الجرائم عموماً والجرائم المعلوماتية خصوصاً وكذلك أرشادهم إلى ضرورة اتخاذ كافة الاحتياطات اللازمة والكفيلة بضمان عدم وقوعهم ضحايا لمثل هذه الجرائم .

ومثل هذا الأمر يعد في الحقيقة من الواجبات المفروضة على الدولة تجاه الإفراد في المجتمع في سبيل حماية أموالهم و أنفسهم وأعرافهم من مخاطر الجرائم عموماً ولها في سبيل ذلك أن تستعين بكافة الوسائل المتاحة والمشروعة ، على أن واجب الدولة هنا لا يقتصر على مجرد التوعية ، بل ينبغي عليها ان تقوم بتجريم الأفعال التي يقتضي واقع الحال تجريمها (٢٢) .

المطلب الثالث

فقـدان آثـــار الجريمـــة

المشكلة التي تواجه أجهزة العدالة الجنائية ان الجرائم المعلوماتية لاتصل لعلم السلطات المعنية بطريقة اعتياديــة كباقي جرائم قانون العقوبات ، فهي جرائم غير تقليدية ، لا تخلق اثأرا مادية كتلك التي تخلفها الجريمة العادية مثل الكسر فـــي جريمة السرقة ، وجثة المجني عليه في القتل ، واختلاس المال من المجني عليه في السرقة وغيرها ، ويرجع السبب في فقدان الآثار التقليدية للجريمة المعلوماتية إلى 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 ، كما لو كان البرنامج معداً ومخزناً على جهاز الحاسب ، ويتوافر أمام المتعامل عدة اختيارات ، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد فتكتمل حلقة الأمر المطلوب تنفيذه ، كما في المعاملات المالية في البنوك أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى حيث يتم ترصيد الأشياء المخزونة أو حسابات العملاء ، أو نقلها من مكان لأخر بطريقة إليه وحسب الأوامر المعطاة لجهاز الحاسب الآلي (٢٣) .

ويمكن في الفروض السابقة ارتكاب بعض أنواع الجرائم كالاختلاس أو التزوير وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكومبيوتر ، وتكون بالنتيجة مخرجات على هوى مستعمل الجهاز الذي ادخل البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات ورقية ، وبالتالي تفقد الجريمة أثارها التقليدية (٢٤) .

كما وان هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الوسائل الالكترونية ويكون أمرها حكراً عليهم كالتجسس على ملفات البيانات المختزنة والوقوف على ما بها من أسرار ، كما أنهم قد ينسخون هذه الملفات ويتحصلون على نسخ منها بقصد استعمالها تحقيقاً لمصالحهم الخاصة ، كذلك فانه قد يقوم باختراق قواعد البيانات والتغيير في محتوياتها تحقيقاً لمأرب خاصة وقد يخربون الأنظمة تخريباً منطقياً بحيث يمكن تمويهه ، كما لو كان مصدره خطأ في البرنامج أو في الأجهزة أو في أنظمة التشغيل أو التصميم الكلي للنظام المعالج أليا للمعلومات ، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب أو يعدلون برامجه أو يحرفون البيانات المخزنة بداخله دون ان يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل .

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الالكترونية انه يمكن محو الدليل في زمن قصير ، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جداً .

بحيث لا تتمكن السلطات مـن كشف جـرائمه إذا مـا علمت بها ، وفي الحالة التي قد تعلم بها فأنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات أقامة الدليل ضده(٢٥) .

لذلك يجد أعضاء الضبط القضائي ، أحيانا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم فضلاً عن صعوبة أجراء التحريات السرية وتتبع مسار العمليات الالكترونية العابرة للحدود (٢٦).

ومن المسائل التي أثيرت كذلك بمناسبة تعذر الحصول على الدليل في الجريمة المعلوماتية بطرق تقليدية نظراً لخصوصية هذا النوع من الجرائم ، هو مدى سريان الحماية المعول بها للاطلاع غير المصرح به على الأوراق المختومة أو المغلقة ، لتمتد إلى نظام المعالجة الآلية للبيانات والمحمي فنياً ضد الاختراق ، حيث يجب عدم المساس بمبدأ المشروعية (٢٧) .

إن السبب في حظر الاطلاع على الأوراق المغلقة ، والمغلقة والمختومة هو رغبة صاحبها في عدم اطلاع الغير عليها، بدليل انه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها ، بدليل إغلاق هذه الأوراق أو تغليفها بأي طريقة وذات العلة تتوافر في البيانات المعالجة أليا ، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو كلمة المرور الدخول إلى نظام هذه البيانات ، وبذلك يكون صاحب ذلك النظام قد رفض مسبقاً عمليات الاطلاع غير المصرح به ما لم يكن الراغب في الاطلاع مصرحاً له عن طريق أعطائه مفتاح المرور إلى هذه البيانات وذلك لا يتوافر فـي حالة عضو الضبط القضائي القائم بالتفتيش موضوع الحديث ، إن هذا التوجه يهدف أولا وأخيرا إلى إيجاد مظلة حماية قانونية لنظام البيانات المعالجة أليا والتي لا يصرح للغير بالاطلاع عليها (٢٨) .

وقبل الانتهاء من هذا المبحث لا يفوتنا أن نتطرق إلى المعاينة في الجريمة المعلوماتية كوسيلة للحصول على الدليل ، فالمعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة حيث يقوم عضو الضبط القضائي بمعاينة الآثار المادية للجريمة ويعمل في المحافظة عليها (٢٩).

إن معاينة الجرائم التقليدية والاطلاع على مسرح الجريمة فيها يكون ذو أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف وملابسات ارتكابها وتوفير الأدلة المادية التي يمكن تجميعها عن طريق هذه المعاينة ، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبها .

ويرجع السبب في ذلك أن الجريمة التقليدية غالباً لها مسرح تجري عليه الإحداث التي تخلف اثأرا مادية تترتب عليها الأدلة ، وهذا المسرح يعطي المجال أمام سلطة الاستدلال والتحقيق الجنائي في الكشف عن الجريمة والأدلة وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة ، لكن فكرة مسرح الجريمة في الجريمة المعلوماتية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة ، والسبب في ذلك أن الجريمة المعلوماتية قلما تخلف اثأرا مادية ، كما أن الجناة يغيروا أو يتلفوا أو يعبثوا بالآثار المادية للجريمة أن وجدت .

على أي حال عند معاينة مسرح الجريمة المعلوماتية يجب مراعاة عدة ضوابط وهي (٣٠) :

١- تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكة اتصالات يجب البحث عن خادم

الملف ، وذلك لتعطيل الاتصالات لمنع تخريب الادله الموجودة أو محوها ، ويراعى تصوير الأجهزة الموجودة ، خاصة الأجزاء الخلفية منها .

٢- وضع حراسة كافية على مكان المعاينة ، ومراقبة التحركات داخل مسرح الجريمة بل ورصد الاتصالات الهاتفية من والى مكان مسرح الجريمة .

٣- ملاحظة الطريقة المعد بها النظام ألمعلوماتي والآثار التي يخلفها ،ومعرفة السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار .

٤- عدم نقل المواد المعلوماتية خارج مسرح الجريمة ألا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات الممرات المغناطيسية التي قد تتسبب في محو البيانات .

٥- التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقه وشرائط وأقراص ممغنطة وغير سليمة أو محطمة ورفع البصمات التي قد تكون عليها .

٦- قصر المعاينة على الباحثين والمحققين الذين لديهم كفاءة علمية وخبرة فنية في مجال الحاسبات والشبكات واسترجاع المعلومات وان يكونوا قد تلقوا تدريبا جيداً على ذلك .

نخلص مما تقدم أن الانتقال والمعاينة في الجرائم المعلوماتية تستوجب على القائم بالتحقيق أن يتعامل مع مكان وقوعها على انه يتكون من مكانين احدهما تقليدي والأخر افتراضي والأول مثل غير من أماكن وقوع الجريمة التقليدية يتكون بشكل أساسي من مكونات مادية ملموسة مثل أجهزة الكومبيوتر وشاشاتها وملحقاتها ، والذي يمكن أن يترك الجاني فيه الكثير من الآثار المادية

كبصمات أصابعه أو بعضا من مقتنياته الشخصية ، وهو بصورة عامة يقع خارج البيئة الالكترونية ، تنطبق عليه كافة القواعد المتبعة في معاينة مكان وقوع الجريمة التقليدية ، أما الثاني فانه يقع داخل البيئة الالكترونية ويتكون من بيانات رقمية (الكترونية) موجودة في داخل كمبيوترات أو على شبكة الانترنت وهو الذي يثير الجانب الأكبر من المشاكل في مجال التحقيق في الجرائم المعلوماتية .

المبحث الثاني

الصعوبات المتعلقة بجهات التحقيق

إن اكتشاف الجرائم عموماً ومن ضمنها الجرائم المعلوماتية بعد وقوعها يدخل ضمن المفهوم العام للتحريات التي بدورها من إجراءات الاستدلال ، التي تدخل ضمن مهام أعضاء الضبط القضائي المكلفون قانوناً بعدة واجبات من ضمنها التحري عن الجرائم والكشف عنها (٣١) ، بكافة الوسائل المتاحة والمشروعة وهذا الواجب يشمل أيضا محاولة اكتشاف أية جريمة يمكن أن تكون قد وقعت (٣٢) .

فهم عين العدالة وإذنها في التنقيب عن الجرائم عموماً ، وأخرجها من وراء الاستره ، ووضع مرتكبها تحت تصرف القضاء ، ألا أن مهمتهم هذه ليست بالسهلة ، وإنما تكتنفها صعوبات عده وهذا ما نسبيه في ثلاث مطالب ، نتناول في المطلب الأول نقص المعرفة الفنية لدى سلطات التحقيق ، والثاني الخبرة في الجرائم المعلوماتية ، أما المطلب الثالث فنتناول به ضعف التعاون الدولي في مواجهة الجريمة المعلوماتية .

المطلب الأول

نقص المعرفة الفنية لدى سلطات التحقيق

من الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة المعلوماتية نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة ، وكذلك لدى أجهزة العدالة الجنائية ممثله في سلطات الاتهام والتحقيق الجنائي ، وذلك فيما يتعلق بثقافة الحاسب الآلي وكيفية التعامل معها ، وذلك على الأقل في البلدان العربية ، نظراً لان تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخراً عن أوربا والولايات المتحدة ، فقد اثبت الوقائع بان بعضاً من أعضاء الضبط القضائي قد أعانوا مجرمي المعلوماتية على ارتكاب جرائمهم عن جهل ومن دون قصد ، بدلاً من ضبطهم وذلك بالنظر لعدم امتلاكهم المعرفة اللازمة للتعرف على مثل هذه الجرائم ووسائل ارتكابها (٣٣) .

كما أن هذا الأمر قد أدى بهم في كثير من الأحيان إلى التسبب بإتلاف أثار الجريمة المعلوماتية وتدميرها عن غير عمد نتيجة الإهمال أو الخطأ أو لعدم التعامل مع هذه الآثار بصوره مهنية ، فاكتشاف الجرائم المعلوماتية تتطلب عموماً استراتيجيات ومهارات فنية وتدريبات خاصة لتفهم تقنيات المعلوماتية ونظمها وأساليب ارتكاب جرائمها ، وهي ما لا تتوافر لدى اغلب جهات الضبط القضائي التقليدية .

إن جهات الضبط القضائي التقليدية تعاني عموماً من ضعف الثقافة القانونية اللازمة للتعرف على الجرائم المعلوماتية وتقدير خطورتها ، ومثل هذه الإشكالية تتضاعف أضعافا مضاعفة في الدول التي لا تملك قانوناً خاصاً بمكافحة الجرائم المعلوماتية ، فوجود الأخير ضرورة لا

غنى عنها لتعريف المجتمع عموماً وجهات الضبط القضائي خصوصاً بخطورة هذه الجرائم ، وكذا لتحديد الأفعال التي تشكل هذه الجرائم من عدمها (٣٤) .

إن المشكلة هي ليست في منح الموظفين ذوي العلاقة بجرائم الحاسب الآلي صفة عضو الضبط القضائي .. مع أننا من المؤيدين لذلك .. ذلك أن مأموري الضبط القائمين بالفعل وسلطات التحقيق الجنائي تنقصها الخبرة في الجريمة المعلوماتية ، وان اكتشاف هذه الجرائم والتوصل إلى فاعليها وملاحقتهم قضائياً ، لا يتطلب فقط الإلمام بأصول البحث الجنائي أو قواعد التحقيق القانونية ، فذلك مفترض باعتبار انه أعمالا لقاعدة الشرعية التي تحكم الإجراءات الجنائية ، ولكن يجب الإلمام بأصول التحقيق الجنائي الفني في الجرائم التقليدية فضلاً عن مهارات خاصة تسمح باستيعاب تقنيات الحاسب الآلي من حيث برامجه ، أنظمته ، طبيعة الجريمة الواقعة عليه ومفرداتها، من احتيال الالكتروني وقرصنه واختراق وحماية ، وكيفية كسر جدار الحماية وفيروسات الكومبيوتر ، ونظم استعمال ومعلومات دولية وغيرها من مصطلحات يمكنه عن طريقها التعامل مع هذه الجريمة المتفردة في خصوصيتها ، وكذلك التعامل مع المجرم ألمعلوماتي وهو مجرم ذات طبيعة خاصة يتعين فهم كيفية التعامل معه .

ويزيد من التحدي الذي تواجهه أجهزة العدالة الجنائية في جرائم الحاسب الآلي وجرائم الانترنت ، أن الجناة في هذه الجرائم لهم المفردات والمصطلحات الخاصة بهم ، لدرجه أنهم يطلقون على أنفسهم اسم (النخبة) بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاته المتميزة ، ويطلق على رجال الشرطة والنيابة والقضاء صفة الضعفاء (٣٥) .

يبدو لنا ان هذا القصور الفني والمعرفي لدى سلطات التحقيق يتطلب ابتداء تفعيل عدة أمور لمكافحة الجرائم المعلوماتية وإمكانية ضبط الأدلة الجنائية أن وجدت ويمكن أن نورد أهمها :-

١. تفعيل دور الضبط الإداري :-

يعد الضبط الإداري أو البوليس الإداري من أهم وظائف الإدارة ، ويهدف إلى المحافظة على النظام العام في الأماكن العامة عن طريق إصدار القرارات اللائحية والفردية واستخدام القوة المادية ، مع ما يتبع ذلك من فرض قيود على الحريات الفردية ، يستلزمها انتظام أمر الحياة في المجتمع (٣٦) .

ويقوم الضبط الإداري بدور فعال في مكافحة الجرائم المعلوماتية ، وذلك من خلال اتخاذ كافة الإجراءات والوسائل للحيلولة دون وقوع تلك الأخيرة ، عن طريق حفظ النظام بعناصره الثلاث (الأمن العام والسكينة العامة والصحة العامة) ، ولما كانت هناك إمكانية الجمع بين أعمال الضبط القضائي والإداري معاً ، كتلك الحالة التي يتم فيها تفتيش الحقائب عبر المنافذ الكمر كية ، فيتم اكتشاف جريمة إثناء هذا التفتيش ، كان من المنطقي أن يكون هناك محل للضبط الإداري في العالم الافتراضي ، إذا انه وفي وقتنا هذا والذي يشهد تطوراً تكنولوجياً فريداً من نوعه ، وضعت هناك أجهزة للشرطة مسخرة للقيام بدوريات في غرف الدردشة لمراقبه ما يحدث فيها .

ولها في ذلك جميع الصلاحيات اللازمة للوقاية من كافة صور الإجرام ، ومن بين تلك الصلاحيات التفتيش الذي يقوم به عضو الضبط القضائي على أجهزة الحاسب الآلي في مقاهي الانترنت أو في أحدى المؤسسات بقصد التأكد من صلاحية

البرمجيات وإذا به يكتشف عدم صلاحيتها مع وجود برمجيات أو صور إباحية (٣٧) .

هذا من جهة و من جهة أخرى فان بعض العاملين في بيئة الانترنت يتمتعون بصفة الضبطية الإدارية ، كمزودي الدخول وخدمات الانترنت ، إذ تبعاً لا عمالهم ووفقاً للقانون فهم يمنحون الصلاحية في الرقابة عبر المزود عن سير حركة العمل ومدى الخضوع للنظام والقانون من قبل العاملين والمتعاملين مع الانترنت ، حيث إذ حدث ووجدت الجريمة باكتشافها بهذا الأسلوب ، فانه ليس لرجل الضبط الإداري سوى التحفظ على أدلة الجريمة إلى حين حضور رجال الضبط القضائي (٣٨) .

والى جانب الإجراءات التي يتخذها رجال الضبط الإداري لمواجهة جرائم الانترنت مبكراً ،و بالتالي منع وقوعها ، هناك إجراءات يقوم بها العاملون بالمنشآت الحيوية ، يطلق عليها ،امن المعلومات ،، وهي عبارة عن احتياطات وإجراءات تتخذها الإدارات الحديثة لمنع وقوع الجريمة ، وذلك من خلال تحديد المعلومات الهامة ، ثم تحليل المخاطر والتهديدات والقابلية للعدوان ، ثم تطبق الإجراءات المضادة لتصل إلى مرحلة التقييم (٣٩) .

٢. التدريب التخصصي لجهات التحقيق :-

ان التحقيق في الجرائم المعلوماتية في حاجة إلى خبرة ومهارات خاصة لا تتأتى دون تدريب تخصصي يراعى فيه عدة عناصر تتعلق بشخص المتدرب ومنهج التدريب ، وصفته ما أن كان رسمياً ام غير رسمي وكذلك أسلوب التدريب وجهة التدريب.

فبخصوص المتدرب ، لابد أن يكون الشخص مؤهلاً لذلك سواء من رجال الشرطة أو سلطات التحقيق الجنائي ، وهــذا يتطلب قدرات ذهنية ونفسية خاصـــة لتلقي هذا التدريب ، ألا أن تدريب المتخصصين في معالجة البيانات ونظم التشغيل يؤتى ثماره وبسرعة عن أولئك المنتمين لأجهزة العدالة كما في الشرطة والتحقيق الجنائي ، ويتعين توافر الخبرة لدى متلقي برنامج التدريب (٤٠) .

أما عن منهج الدورة التدريبية يتعين أن يكون علمياً من الناحية النظرية العملية ويشتمل على المخاطر والتهديدات وأماكــن الاختراق لشبكة المعلومات وأجهزة الحاســب التي يمكـن تعرضه لها ،وكذلك مفاهيم معالجة البيانات سواء ما تعلق منها بالبرامج أو الأجهزة ، ونوعيات الجريمة المعلوماتية ، ويضاف لذلك موضوعات أخرى مثل التفتيش والضبط واستخدام الحاسب كوسيلة في الحصول على أدله الاتهام ، والتعاون الدولي المشترك في ملاحقة هذه الجرائم .

والتدرب قد يكون بصفة رسمية أو غير ذلك ، والتدريب غير الرسمي يكون بتكليف المتدرب بالعمل مع شخص لديه خبرة في تحقيق الجرائم المعلوماتية ، أما التدريب الرسمي فيكون من خلال حلقات دراسية أو حلقات نقاش وهو ما يسمى (بورش العمل) ، وذلك حول جرائم الحاسب الآلي وشبكات المعلومات وإساءة استخدامها (٤١).

نخلص مما تقدم انه يجب على كافة أجهزة العدالة الجنائية وكذلك جهاز الشرطة مواكبة المتغيرات التكنلوجية في مجال الحاسبات والمعلوماتية لمواجهة الجريمة المعلوماتية والمجرم ألمعلوماتي وذلك من خلال برامج طموحة للتدريب ، وإدارات متخصصة للاستدلال في الجريمة المعلوماتية وأجهزة تحقيق متخصصة في مثل هذه الجرائم .

ويكفي للتدليل على أهمية هذا التدريب واكتساب الخبرة في مجال الجريمة المعلوماتية أن رجل الضبط وكذلك المحقق لن يمكنهما القيام بعملهما في الاستدلال والتحقيق ألا عن طريق الإلمام بتقنية الحاسب الآلي .

المطلب الثاني

الخبرة في الجرائم المعلوماتية

ان الفلسفة العامة التي تسود الإثبات الجنائي انه يعتمد على القناعة الوجدانية ، وذلك أن الإثبات ينصب على واقعه طواها الزمن ويتعين أعادة تركيب صورتها كما وقعت حتى تنطبق الحقيقة القانونية مع الحقيقة الواقعية ، وصعوبة ذلك تبرر اعتماد كل وسائل الإثبات المتاحة دون تقيد ، خصوصاً وان محل الإثبات يتسع ليشمل كل العناصر التكوينية للجريمة وما يلابسها من ظروف نفسية ويواكبها من أسباب الإعفاء أو الإباحة وما إلى ذلك . ومن ثم كان على القاضي أن يقوم بدور ايجابي فليس دوره فقط الموازنة بين الأدلة المقدمة من هذا الفريق أو ذاك بالإدانة أو البرائة ، وإنما عليه اتخاذ كل الإجراءات الضرورية والتحقق من صدق أية وسيلة تثار في سبيل الكشف عن الحقيقة وتكوين قناعته.

لقد كان اللجوء إلى الخبرة في الماضي استثنائياً غير أن أمرها تعاظم نتيجة الطفرة التي عرفتها مختلف العلوم واطراد توسع دائرة التقنية خلال القرن الحالي ، الأمر الذي نتج عنه تزايد الأفعال الممنوعة قانوناً بكيفية لم تكن متوقعه كما بينا .

تعرف الخبرة بأنها إجراء يتعلق بموضوع يتطلب الماماً بمعلومات فنية لا مكان استخلاص الدليل منه ، أو أنها الاستشارات الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقرير المسائل الفنية التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوفر لدى القضاة بحكم العمل أو الثقافة .

كما عرفها الفقه الجنائي (٤٢) بأنها « تقدير مادي أو ذهني يبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها بمعلوماته الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أو بجسم الجريمة أو المواد المستعملة في ارتكابها أو أثارها » .

أن انتداب الخبراء أجراء من إجراءات التحقيق تختص به سلطة التحقيق (القاضي أو المحقق) (٤٣) .

غير أن هذا لا يمنع عضو الضبط القضائي من استدعاء أهل الخبرة بشأن الجريمة التي يباشر فيها التحقيق سواء تعلقت الخبرة بجسم الجريمة أو موادها وأثارها .

على أن المشروع لم ينص صراحة على حق سلطة الضبط القضائي باستدعاء الخبراء كما فعل المشرع المصري (٤٤) .

إلا انه ذكر بأن لعضو الضبط القضائي عند تحقيقه في الجريمة المشهودة ان يحضر في الحال كل شخص يمكن الحصول منه على إيضاحات (٤٥) .

كما ان ندب الخبراء يستهدف منه اكتشاف الجريمة ومرتكبيها وهو عمل يعتبر بحقيقة الأمر من صميم سلطة الضبط القضائي .

لم يبين قانون أصول المحاكمات الجزائية العراقي الكيفية التي يجري انتداب الخبير بواسطتها غير أن المحاكم تلجأ عادة للاستعانة بأحد الخبراء المقيدين في الجدول المعد وفق أحكام قانون الخبراء أمام القضاء رقم (٦٣) لسنة (١٩٧٤) أو أي قانون يحل محله .

او من بين خبراء الدولة ومؤسساتها الرسمية وشبه الرسمية أو من بين مؤسسات القطاع الاشتراكي أو المنظمات المهنية ، كما أنها أن احتاجت إلى خبير من غير هؤلاء والذين اشرنا إليهم فأنها تستطيع استدعائه وتكليفه بالمهمة ، علماً بأن الخبراء المسجلين في الجدول لا يمارسون أعمالهم لأول مرة ألا بعد حلفهم اليمين بأن يؤدوا خبرتهم بأمانة وإخلاص ، أما الخبير الذي يستعين به القائم بالتحقيق من غير المسجلين في الجدول فأنه يحلف اليمين في كل مرة يكلف بها في قضية ، ويستطيع القائم بالتحقيق استبدال الخبير متى ما وجد ان الامر يستدعي ذلك كما يستطيع القائم بالتحقيق مناقشته وتوجيه الأسئلة إليه بحضور ذوي العلاقة ، كما أن رأي الخبير غير ملزم على ما يبدو طالما يستطيع القائم بالتحقيق استبداله (٤٦).

وإذا كانت هذه هي قواعد الخبرة في المسائل الجنائية والتي نظمتها قوانين الإجراءات الجنائية لتحكم مهمة الخبير في أدائه لمأموريته وذلك أمام سلطة التحقيق أو محكمة الموضوع على السواء ، فأنه يجب مراعاة ضرورة مشروعية الدليل المترتب على أعمال الخبرة ، وذلك أن هذه الأعمال تهدف أولا وأخيرا إلى الفصل في مسألة فنية علمية لا دراية لسلطة التحقيق او المحكمة بها ، وهذا لا يخل بقاعدة أن المحكمة

هي الخبير الا على في الدعوى ، ألا ان لسلطات التحقيق والمحكمة أذا رأت بان لا وجه لا قامة الدعوى الجنائية عليها أن تفند الدليل العلمي المستمد من أعمال الخبير بدليل علمي أخر ، حتى لا تهدر دليلاً ذا قيمة في الإثبات .

ومشروعية الدليل العلمي المستمد من أعمال الخبرة متفق على وجوب مشروعيته في كافة النظم القانونية ومنها الأدلة المستمدة من عمليات سحب وتحليل عينات الدم وعينات البول وعينات الكتابة والصوت (٤٧) .

أما الخبرة في مجال الجرائم المعلوماتية لا تشمل تلك النوعية من الخبرة التي تتحصل من الدراسة ، فدراسات الحاسب الآلي والانترنت لا ترتبط بمنهج دراسي او بحثي معين او حتى مدة زمنية يقضيها المرء دارساً في الجامعات والمدارس المتخصصة .

وإنما ترتبط بمهارات خاصة وبموهبة استعمال الحاسوب والانترنيت والتعامل مع تقنية المعلومات ،آذ أن أمهر مبرمجي نظام التشغيل لم يكن تحصيله العلمي يتجاوز المرحلة الثانوية ، وذات الأمر ينطبق على عتاة الهكرة ومخترقي الأنظمة فأن أعمارهم لا تتجاوز مرحلة التعليم الثانوي والسنوات الجامعية الأولى في أحسن الأحوال .

ومن هذا المنطلق تتميز الخبرة في مجال تكنلوجيا المعلومات عن الخبرة في أي فرع أخر من الفروع التي يمكن ان تكون محلاً للخبرة أمام القضاء .

والخبرة في مجال الحاسب الآلي والانترنت أنواع عديدة (٤٨) ، منها الخبرة الخاصة وهذه تعد اقوي أنواع الخبرات على الإطلاق

لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسه حقيقية بين المنظمات الخاصة ، والى جوار الإفراد توجد المنظمات الخاصة في كافة المجالات والتي يكون لها السبق في مجال الخبرة ، وتختلف المنظمات الخاصة مابين منظمات أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الالكترونية وبين نوعيه من المنظمات تسعى إلى فك طلاسم العالم الافتراضي على أسس تجارية .

وهنالك المؤسسات التعليمية ، وهي تعد أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة في العالم الافتراضي ، فهذه تعد مصدر دعم متكامل لمؤسسات الدولة ككل ، وبالتالي ليس هناك أفضل من التقنيين في المعلوماتية لفك سر الجريمة عبر الانترنت.

كما شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الجرائم المعلوماتية وعلى رأس تلك الدول الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الانتربول .

وبعد ذلك يتعين على المحقق أن يحدد للخبير ألمعلوماتي دوره في المسألة المنتدب فيها على وجه ألدقه ، وهذا يعود بنا إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق في الجرائم المعلوماتية لنجاح تحقيق مثل هذه الجرائم ، ودرءاً لما ينأى به البعض من انه يمكن للخبير نفسه أن يحدد أطار مهمته ، إذ ان ذلك سوف يقوض دور المحقق والقاضي في الدعوى الجزائية في مثل هذه الجرائم المعلوماتية (٤٩) .

وعلى ضوء ذلك هناك أسلوبان لعمل الخبير في الجرائم المعلوماتية (٥٠) ، هما :

١- القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كما هو الشأن في التهديد أو النصب أو السب أو جرائم النسخ وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق ودعارة الأطفال وغيرها ، ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها الى مسارها الذي أعدت فيه ، وتحديد عناصر حركتها ، وكيف تم التوصل الى معرفتها ، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت الذي ينسب الى جهاز الحاسوب الذي صدر عنه هذا الموقع .

٢- القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته ، وإنما تؤدي حال تتبع موضوعاتها إلى قيام الإفراد بارتكاب جرائم كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية التي تناسب وزن الإنسان بادعاء انه إذا تتبع التعليمات الواردة فيها فلن يصاب الشخص بحالة إدمان ، وأيضا كيفية زراعة المخدرات بعيداً عن أعين الغير ، وكيفية أعداد القنابل وتخزينها ، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها ، وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بالدخول من مكان ثابت ، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكبي الجريمة مشتركاً لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها ويقوم بالولوج الى الانترنت من محل أقامته .

وحيث أن أسلوب عمل الخبير يكون بهذه الصورة لذلك يتعين التنسيق مابين الخبير ألمعلوماتي والمحقق الجنائي قبل محاكمة الجاني في الجريمة المعلوماتية ، على أن يشمل اللقاء كافة الخبراء الذين

ساهموا من سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط أو التفتيش أو فحص البرامج وجمع الأدلة الجنائية ، على أن يتم في هذا اللقاء حصر الأدلة المتوفرة وترتيبها وفقاً لأهمية كل دليل أو بينة أو قرينة ، كما يجب على المحقق الجنائي أن يشرح لهؤلاء الخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة المقام عنها الدعوى الجزائية ضد المتهم (٥١) .

وبالتالي يمكن تحديد الخبرة في الموضوعات الآتية :

١- الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية المحلقة به ، وكلمات المرور أو السر واكواد التشفير .
٢- طبيعة البيئة التي يعمل في ضلها الحاسب من حيث تنظيم ومن تذكير أو توزيع عمل المعالجة الإلية - وتحديد أماكن التخزين والوسائل المستخدمة في ذلك .
٣- قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك إعطاب أو تخريب الادله المتحصلة من الوسائل الالكترونية .
٤- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدله مقروءة و المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير تعطيل أو إتلاف ، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة .

ونشير إلى انه من الإعمال ذات المحظورة الخاصة في عمل الخبير التقني هي الدراسات التاريخية التي يقوم بها الخبير ، بهدف تحديد أسلوب مرتكب الجريمة ، وهي دراسات محاطة

بالسرية المطلقة في هذا المجال لكونها تؤدي إلى فتح سجلات وملفات انتهى موضوعها ، أو أنها تجعل الخبير يطلع على محاضر تحقيقات قد ينص في التشريعات على حضر اطلاع غير سلطات التحقيق عليها ، سيما في الحالات التي يكون فيها الخبير خبيراً في قضية أخرى ليست ذات علاقة بموضوع القضية التي يقوم بتحقيقها .

وتجدر الإشارة ألا انه وان كان المقرر أن المحكمة تملك سلطة تقديرية بالنسبة لتقرير الخبير الذي يرد إليها ، ألا أن ذلك لا يمتد إلى المسائل الفنية ولا يجوز لها تنفيذها إلا بأساليب فنية تخضع للتقدير المطلق لمحكمة الموضوع ، ومن ثم فلا تستطيع المحكمة أن تنفذها وترد عليها بأساليب فنية قد يصعب عليها أن تشق طريقها فيها ألا عن طريق خبره فنية أخرى .

لذلك يبدو لنا صعوبة الخبرة في اكتشاف الدليل الجنائي في الجرائم المعلوماتية على ضوء الأمور التي تم ذكرها لنقص الخبراء والفنيين عند وقوع الجريمة المعلوماتية والذين يشمل عملهم المراجعة والتدقيق عند وقوع الجريمة المعلوماتية لجمع البيانات الإلية والبرامجيات ، لذلك نرى وجوب تشكيل فريق من الخبراء من قطاعات مختلفة بالدولة حكومية وغير حكومية والجهات المعنية بالجريمة المعلوماتية ، يعمل هذا الفريق على تقييم الخبرة المكتسبة في مجال هذه الجرائم في ضوء التشريعات القائمة وما يمكن عمله في المستقبل .

المطلب الثالث

ضعف التعاون الدولي في مواجهة الجريمة المعلوماتية

غالباً ما تكون المعلومة ذاتها مملوكة لبعض الإفراد أو الشركات أو المؤسسات والدول في بعض الأحيان الأخرى ، وتتأتى صعوبة مكافحة الجريمة المعلوماتية من أن مالكي المعلومات أو حائزيها يحاولون اتخاذ إجراءات الحماية اللازمة بصفة مستقلة ومنفردة ، فالأفراد من ناحية والمؤسسات والدول أيضا من ناحية أخرى يحاولون تسخير إمكانياتهم من اجل حماية الأنظمة المعلوماتية الخاصة بهم دون تكاتف أو تعاون مشترك بهدف حماية المعلومات بشكل عام ، فغياب التعاون والتنسيق بين الإفراد والشركات والدول يلعب دوراً رئيساً ومؤثراً في عدم انحسار مد الجريمة المعلوماتية وبالتالي صعوبة إثباتها (٥٢) .

ومن ناحية أخرى فان غياب سياسة التعاون الدولي والتنسيق بين الدول في مقاومة الجريمة المعلوماتية يقابله في ذات الوقت تعاون واضح بين محترفي الإجرام ألمعلوماتي ، ففضلاً عن البرامج التي يستعين بها القراصنة في أنشطتهم الإجرامية ، فأنهم يتعاونون فيما بينهم ويتبادلون النصائح والخبرات فيما يتعلق بأنشطتهم مما يزيد من فاعلية وخطورة هجومهم وخصوصاً في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة والمنفردة ضد الجريمة المعلوماتية (٥٣) .

ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية ، ألا أن هناك عوائق تحول دون ذلك ، وتجعل هذا التعاون صعباً وأهمها :-

١. عدم وجود نموذج موحد للنشاط الإجرامي :-

فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الـواجب تجريمها ، فما يكون مباحاً في احد الأنظمة قد يكون مجرماً وغير مباح في نظام أخر ، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف

البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر ، وبالتالي اختلاف السياسة التشريعية من مجتمع لأخر(٥٤) .

ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة على صور موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على تنظيم أنفسهم وارتكاب جرائم دون تقيد بالحدود الجغرافية الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة .

٢. اختلاف النظم القانونية الإجرائية :-

بسبب تنوع واختلاف النظم القانونية الإجرائية ، نجد أن طرق التحري والتحقيق والمحاكمة التي ثبت فائدتها وفاعليتها في دولة مـــا قـد تكون عديمة الفائدة في دوله أخرى أو قد لا يسمح بأجـــرائهـا ، كمـا هـــو الحـــال بالنسبة للمراقبـــة الالكترونيـــة ، والتسليم المـــراقـــب ، والعمليات المستترة ، وغيرها من الإجراءات الشبيهة ، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دوله معينة قد تكون ذات الطريقة غير مشروعه في دوله أخرى ، وبالتالي فان الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنقاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي انه أداة فعالة ، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعه ، حتى وان كان هذا الدليل تم الحصول علية في اختصاص قضائي وبشكل مشروع (٥٥) .

٣. عدم وجود معاهدات ثنائية أو جماعية بين الدول :- (٥٦)

وحتى في حال وجود هذه المعاهدات فأنها قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الانترنت ، ومن ثم تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول ، وبعدها يظهر الأثر السلبي في التعاون الدولي .

٤. مشكلة الاختصاص في جرائم الانترنت :-

الجرائم المتعلقة بالانترنت من اكبر الجرائم التي تثير مسألة الاختصاص على المستوى المحلى أو الدولي وعند وجود أي مشكله بالنسبة للاختصاص على المستوى الوطني أو المحلي يتم الرجوع إلى القواعد الإجرائية المحددة قانوناً لذلك (٥٧) .

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية والتي ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالانترنت التي تتميز بكونها عابره للحدود ، وكذلك اعتبرت من الجرائم الدولية(٥٨) .

فيحدث أن ترتكب داخل إقليم دوله ألا أنها تمتد إلى خارج إقليم تلك الأخيرة ، مما يعني خضوعها لا كثر من قانون جنائي كما هو الشأن في جرائم المخدرات والإرهاب والتجسس الاقتصادي وغسيل الأموال .

٥. عدم وجود قنوات اتصال :-

أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين ، الحصول على المعلومات والبيانات المتعلقة بهم ، ولتحقيق هذا الهدف كان لازماً أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع أدله معينة أو معلومات مهمة ، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العلمية التي غالباً ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون (٥٩) .

بناءً على ما تقدم أصبح أمـــر التعاون الدولي في مكافحة الجريمة المعلوماتية أمرا حتمياً ، ويجب اتخاذ خطوات جادة في هذا الصـــدد أو استكمال مـــا بدأ ، أو تعـــزيز فاعليته ، وان نقطة البداية التي يجب أن يفطن إليها المجتمع الدولي فـــي سبيل مكـــافحته للجريمة المعلوماتية ، هي ضرورة رسم سياسة جنائية

متناسقة من اجل الأجرام ألمعلوماتي عن طريق التدخل بالتقويم للأنشطة الإجرامية المعلوماتية ، مع الأخذ في الاعتبار أهمية الاتفاق على ماهية الأنشطة التي يضفى عليها التجريم ألمعلوماتي حتى يؤدي هذا التجريم ثماره وتسد الثغرات في وجه المجرمين المعلوماتيين ، وعلى ذلك ينبغي القضاء على التناقضات الموجودة في سياسة التجريم ، فإذا لم يتم التنسيق الدولي في هذا الإطار فسينتهي الأمر إلى جعل المعلوماتية بمثابة مكان ترفيهي للقراصنة على غرار ما يحدث في مجال غسيل الأموال والتهرب الضريبي ، حيث سيجد القراصنة مأوى يلجأون إلية في سبيل تحقيق ما يريدون دون الوقوع تحت طائلة القانون ، ولا شك أن محور الارتكاز بالنسبة للتعاون الدولي هنا يستند إلى ضرورة الموازنة بين واجب حماية الحق في الإعلام والاتصال من ناحية وأهمية مقاومة الأجرام ألمعلوماتي والقضاء علية من ناحية أخرى .

وقد لقي هــذا الموضوع الأخير اهتماماً من العديد من الدول والمنظمات والهيئات الدولية ، ومنها المؤتمر الدولي لمكافحة استغلال الأطفال في الجنس على الانترنت (٦٠).

والذي دعا إلى ضرورة تنسيق وتدعيم التعاون الدولي في مكافحة هذه الأنشطة الإجرامية ووضع بعض القواعد الذاتية المتعلقة بموردي خدمة الانترنت وتشجيع أنشاء وتدعيم قنوات اتصال سهلة مُيسره تسمح للمواطنين بالإبلاغ عن المواقع الإباحية للأطفال عبر الانترنت .

وعمل الاتحاد الأوربي على وضع مشروع اتفاقية دولية لمواجهة هذه النوعية المستحدثة من الجرائم ، ويقضي مشروع هذه الاتفاقية بمعاقبة أي وصول غير مشروع الى معطيات المعلوماتية (٦١) .

وعلى المستوى الإقليمي فقد اهتمت منظمة التعاون والتنمية الاقتصادية الأوربية بموضوع الجريمة المعلوماتية ، فبعد أن عرفتها بأنها سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به ، يرتبط بالمعالجة الإلية للبيانات أو نقلها ، حاولت وضع الحلول والمقترحات في هذا المجال ، بعد رصد هذه الظاهرة وتحليلها بواسطة مجموعة من الخبراء المتخصصين (٦٢) .

ومن جهود الأمم المتحدة في ذلك ان مؤتمرها الثامن لمنع الجريمة والمجرمين والذي عقد في هافانا ١٩٩٠ ، قد حث في قراره المتعلق بالجرائم ذات العلاقة بالحاسب الآلي ، الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال الحاسب بفاعلية ، وذلك بتجريم هذه الأفعال جنائياً واتخاذ تدابير تضمن وحدة الإجراءات والقوانين الراهنة بشأن سلطات التحقيق والأدلة ، وادخل تغييرات مناسبة عليها آذ دعت الضرورة لذلك ، وحث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من اجل مكافحة الجرائم المتصلة بالحاسبات وتبادل المساعدة في المسائل الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب ، فضلاً عن توصيات أخرى هدفها مواجهة هذه النوعية من الجرائم بفعالية أكثر (٦٣) .

الخاتمة

(النتائج والتوصيات)

لقد تحددت إشكالية هذا البحث في وجود صعوبة في إثبات الجرائم التي تقع على العمليات الالكترونية بالوسائل الالكترونية ، بالنظر إلى الطبيعة الفنية المعقدة لهذه الجرائم واتصاف مرتكبيها بالذكاء والاحتراف ، مما يصعب معها تحديد الدليل الجنائي للجرائم المعلوماتية ، وقد توصل البحث من خلال هذه الدراسة إلى النتائج الآتية :

١- اظهر البحث ان الدليل في الجرائم المعلوماتية يكون عبارة عن بيانات ومعلومات على شكل نبضات الكترونية غير مرئية تنساب عبر النظام ألمعلوماتي مما يجعل أمر طمس الدليل ومحوه كلياً من قبل الفاعل أمراً في غاية السهولة ، خاصة وان انتحال الشخصية وكذلك التسلسل الالكتروني هما ابرز أمثله السلوك الإجرامي في الجريمة المعلوماتية .

٢- أظهر البحث أن ضحايا الجرائم المعلوماتية هم من الأسباب الأساسية في تصعيب اكتشاف هذه الجرائم بسبب نقص الخبرة الفنية التقنية لديهم بالمقابل أن معظم ممن يرتكبون الجرائم المعلوماتية هم من الخبراء في مجال الحاسب الآلي ، وان سلطات التحري والتحقيق تبحث أول ما تبحث عن خبراء الكومبيوتر عند ارتكاب هذا النوع من الجرائم ، كذلك عــدم اتخاذ المجني علية الحيطة والحذر يسهل ارتكاب مثل هــذه الجرائم ، بل إن بعضهم يحجم عن التبليغ عنها عند وقوعها مما يساعد على انتشارها وضياع معالمها نتيجة لعدم إدراكه لخطورة هذه الجرائم اظهر البحث أن الجرائم المعلوماتية لا تخلف أثاراً مادية كتلك التي تخلفها الجريمة العادية مثل التغير الذي يحصل في العالم الخارجي نتيجة الإتلاف أو الجرح أو الضرب أو الإيذاء أو تغيير الحقيقة في

مستند ،ويرجع السبب في فقدان الآثار التقليدية للجريمة المعلوماتية إلى أن هناك بعض العمليات التي يجري إدخال بياناتها مباشره في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها ،كما لو كان البرنامج معداً ومخزناً على جهاز الحاسب ، لذلك لا تؤدي المعاينة التي يجريها عضو الضبط للقضائي دوراً مهماً في كشف غموض الجريمة المعلوماتية وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبها .

٣- أظهر البحث أن جهات الضبط القضائي تعاني عموماً من ضعف الثقافة القانونية اللازمة للتعرف على الجرائم المعلوماتية وتقدير خطورتها ، ومثل هذه الإشكالية تتضاعف أضعافاً في الدول التي لا تملك قانوناً خاصاً بمكافحة الجرائم المعلوماتية، فهو ضرورة لا غنى عنها لتعريف المجتمع عموماً وجهات الضبط القضائي خصوصاً بخطورة هذه الجرائم ، ولتحديد الأفعال التي تشكل هذه الجرائم من عدمها.

٤- أظهر البحث أن الاستعانة بالخبراء في الحصول على الدليل الجنائي في الجرائم المعلوماتية أمر صعب أيضاً على ضوء نقص الخبراء والفنيين ، ذلك أن الخبرة في مجال تكنولوجيا المعلومات تتميز عن الخبرة في أي فرع أخر من الفروع التي يمكن أن تكون محلاً للخبرة أمام القضاء.

٥- أظهر البحث أن من الصعوبات التي تواجه جهات التحقيق في الحصول على الدليل الجنائي في الجرائم المعلوماتية هو ضعف التعاون الدولي في مكافحة الجرائم المعلوماتية لعدم وجود نموذج موحد للنشاط الإجرامي ، أي نسبية هذه الجرائم لاختلاف البيئات والعادات والديانات والثقافات ، كما أن اختلاف النظم القانونية الإجرائية وعدم وجود معاهدات ثنائية أو جماعية وعدم وجود قنوات اتصال بين الدول يساهم

في عدم اكتشافها وعدم الحد منها ، بل أن مشكلة تطبيق القانون من حيث المكان وما به من إشكالات فاقم من عملية عدم الاكتشاف .

- وعلى ضوء هذه النتائج فان البحث يضع بعض التوصيات وهي :

١- يجب أن تسرع التشريعات العربية وبخطى واقعية لتعديل تشريعاتها العقابية لكي تواكب ثورة الاتصالات عن بعد ، ولكي لا يحدث انفصال بين الواقع والقانون بما يضر المجتمع وإفراده ، وعلى النحو الذي سارت عليه الكثير من التشريعات الأجنبية وبعض التشريعات العربية .

٢- يجب الاهتمام بتدريب الخبراء المحققين والقضاة على التعامل مع الجرائم المعلوماتية ذات الطبيعة الفنية والعلمية المعقدة ،بحيث يمكن الوصول إلى الحقيقة وإماطة اللثام عن هذه الجرائم تحقيقاً لصالح المجتمع وإفراده ، ولصالح المتهمين أنفسهم لكي لا يدان ألا المسيء ويبرأ البريء.

٣- يجب على الدولة ممثلة بمؤسساتها التعليمية والقانونية والإعلامية أن تقوم بنشر الثقافة القانونية بين مواطنيها ومؤسسات المجتمع المختلفة ، وتحذيرهم بخصوص خطورة الجرائم عموماً والجرائم المعلوماتية خصوصاً وكذلك إرشادهم إلى ضرورة اتخاذ كافة الاحتياطات اللازمة والكفيلة بضمان عدم وقوع ضحايا لمثل هذه الجرائم .

٤- بالإضافة إلى ما تقدم وفي سبيل الحد من الجرائم المعلوماتية وضبط الأدلة التي تثبت تورط القائمين بها يجب تفعيل دور الضبط الإداري ومنحة الصلاحيات اللازمة للوقاية من كافة صور الإجرام ، حيث يقوم الضبط الإداري بدور فعال في مكافحة الجرائم المعلوماتية وذلك من خلال اتخاذ كافة الإجراءات والوسائل للحيلولة دون وقوع تلك الأخيرة ، عن طريق حفظ النظام بعناصره الثلاث (الأمن العام والسكينة العامة والصحة العامة) .

٥- يجب تشكيل فريق من الخبراء من قطاعات مختلفة بالدولة حكومية وغير حكومية والجهات المعنية بالجريمة المعلوماتية يعمل هذا الفريق على تقييم الخبرة المكتسبة في مجال هذه الجرائم في ضوء التشريعات القائمة وما يمكن عملة في المستقبل . فالدليل العلمي المستمد من أعمال الخبرة متفق على وجوب مشروعيته في كافة النظم القانونية.

٦- يجب اتخاذ خطوات جادة بصدد التعاون الدولي في مكافحة الجريمة المعلوماتية من خلال رسم سياسة جنائية متناسقة عن طريق التدخل بالتقويم للأنشطة الإجرامية المعلوماتية والقضاء على التناقضات الموجودة في سياسة التجريم ، على أن يؤخذ بنظر الاعتبار ضرورة الموازنة بين واجب حماية الحق في الأعلام والاتصال من ناحية وأهمية مقاومة الإجرام ألمعلوماتي والقضاء علية من ناحية أخرى .

مصادر البحث

١- د. احمد خليفة الملط ، الجريمة المعلوماتية ، بدون جهة نشر ، ٢٠٠٥.

٢- د. احمد عبد اللطيف الفقهي ، الدولة وحقوق ضحايا الجريمة ، دار الفجر، القاهرة ، ط١ ، ٢٠٠٣.

٣- د. أيمن عبد الحفيظ عبد الحميد ، إستراتيجية مكافحة جرائم الحاسب الآلي ، دراسة مقارنة ، رسالة دكتوراه ، اكاديمية الشرطة ، بدون سنة طبع .

٤- د. جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية ، القاهرة ٢٠٠٢ .

٥- د. حاتم عبد الرحمن منصور ، الأجرام ألمعلوماتي ، دار النهضة العربية ، ط١ ،٢٠٠٢.

٦- د. حسين بن سعيد الغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ،دار النهضة العربية ، القاهرة ، ٢٠٠٩.
٧- د. خالد ممدوح إبراهيم ، التقاضي الالكتروني ، دار الفكر الجامعي ، الإسكندرية ، ط١ ، ٢٠٠٧.
٨- د. سامي النصراوي ، دراسة في أصول المحاكمات الجزائية ، الجزء الأول ، مطبعة دار السلام ، بغداد ، ١٩٧٨.
٩- د. سليم إبراهيم حربة والأستاذ عبد الأمير العكيلي ، شرح قانون أصول المحاكمات الجزائية بغداد ،١٩٨٨.
١٠- د. طارق إبراهيم الدسوقي عطية ، الأمن ألمعلوماتي (النظم القانونية للحاسبة المعلوماتية) دار الجامعة الجديدة ، ٢٠٠٩.
١١- عائشة بن قاره مصطفى ، حجية الدليل الالكتروني في مجال الإثبات ، دار الجامعة الجديدة ، الإسكندرية ،٢٠١٠.
١٢- د. عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت ، دار الكتب القانونية ، المحلة الكبرى ، مصر ، ٢٠٠٢.
١٣- د. عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت ، دار الكتب القانونية ، مصر ٢٠٠٧.
١٤- د.عبد الفتاح بيومي مجازي ، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي ، دار الفكر الجامعي ، الإسكندرية ، ط١ ،٢٠٠٦.
١٥- د. عمر أبو الفتوح عبد العظيم ، الحماية الجنائية للمعلومات المسجلة الكترونياً ، دار النهضة العربية ، القاهرة ، ٢٠١٠.
١٦- د. عمر محمد بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٤.

١٧- د. عمر السيد رمضان ، مبادئ قانون الإجراءات الجنائية ، الجزء الأول ، دار النهضة العربية ، القاهرة .
١٨- د. قدري عبد الفتاح الشهاوي، ضوابط الاستدلالات والإيضاحات والتحريات في التشريع المصري المقارن، منشأة المعارف الإسكندرية ،٢٠٠٢.
١٩- د. ماجد راغب الحلو ، القانون الإداري ، دار المطبوعات الجامعية ، الإسكندرية ، ١٩٩٤.
٢٠- د. مأمون محمد سلامة ، قانون الإجراءات الجنائية معلقاً علية بالفقه وأحكام القضاء ، دار الفكر العربي . ط١ ،١٩٨٠.
٢١- د. محمد الشناوي ، جرائم النصب المستحدثة ، دار الكتب القانونية ، مصر المحلة الكبرى ،٢٠٠٨.
٢٢- محمد أمين الرومي ، جرائم الكومبيوتر والانترنت ، دار المطبوعات الجامعية، الإسكندرية ، ٢٠٠٤.
٢٣- محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ط١ ، الرياض ، ٢٠٠٤.
٢٤- د. محمد زكي أبو عامر ، الإثبات في المواد الجنائية ، الفنية للطباعة والنشر ، الإسكندرية .
٢٥- د. محمد عبيد ألكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ،ط٢ ، دار النهضة العربية ، القاهرة ،٢٠٠٩.
٢٦- د. محمود صالح العادلي ، الجريمة الدولية ، دراسة مقارنة ، دار الفكر الجامعي ، الإسكندرية ،٢٠٠٣.
٢٧- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت ، دار النهضة العربية ،٢٠٠٠.

٢٨- د.نائلــة عــادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي القومية، ٢٠٠٥.
٢٩- نبيلــه هبــه هــروال ، الجــوانب الاجرائية لجــرائــم الانترنت ، دار الفكر الجامعي ، الإسكندرية ، ط١ ، ٢٠٠٧.
٣٠- نسرين عبد الحميد نبيه ، الجريمة المعلوماتية و المجرم ألمعلوماتي ، منشأة المعارف ،الإسكندرية ، ٢٠٠٨.
٣١- نهلا عبد القادر المؤمني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، ط١ ، ٢٠٠٨.
٣٢- د. هشــام محمد فــريد رستــم ، الجــوانب الإجرائية للجرائم المعلوماتية ، دراسة مقارنة ، مكتبة الآلات الحديثة ، أسيوط ، ١٩٩٤.
٣٣- د. هلالي عبد اللاة احمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست -٢٠٠١، دار النهضة العربية ، ط١ ، ٢٠٠٣.

هــــوامش البحث

١- د. عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت ، دار الكتب القانونية ، مصر ، ٢٠٠٧ ، ص ٥٨
٢- د. عمر السعيد رمضان ، مبادئ قانون الإجراءات الجنائية ، الجزء الأول ، دار النهضة العربية ، القاهرة . ص ٣٦٩ .
٣- د. خالد ممدوح إبراهيم ، التقاضي الالكتروني ، دار الفكر الجامعي ، الإسكندرية ، ط١ ، ٢٠٠٧ ص ٣٢٣ وما بعدها.
٤- د. عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت ، دار الكتب القانونية ، المحلة الكبرى ، مصر ، ٢٠٠٢ ، ص٢٤ .

٥- عائشة بن قاره مصطفى ، حجية الدليل الالكتروني في مجال الإثبات ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠١٠ ص ٦٢.
٦- د. جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنلوجيا الحديثة ، دار النهضة العربية ، القاهرة ، ٢٠٠٢ ، ص١٥ .
٧- د. جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنلوجيا الحديثة ، مصدر سابق ، ص ١١٥ .
٨- تجدر الإشارة إلى أن الأدلة المتحصلة من الوسائل الالكترونية قد تنتمي إلى أدله الإثبات التقليدية وذلك إذا كانت نتاج شهادة أو اعتراف أو خبره ، فقد يمكن أثبات جرائم الاحتيال والسرقة والاختلاس في الجرائم الالكترونية عن طريق الوثائق الأصلية المحفوظة في الميكروفلم أو بالشريط الممغنط او بحافظات الاكواد أو بمخرجات الحاسب وسجلات التشغيل.
٩- د. هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، دراسة مقارنه ، مكتبة الآلات الحديثة ، أسيوط ، ١٩٩٤ ، ص ٢٣ .
١٠- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، ط ١ ، ٢٠٠٨ ، ص ٥٦ .
١١- د. محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي ، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنت ، كلية الشريعة والقانون ، جامعة الامارات ،٢٠٠٠ ، ص ٥٢ .
١٢- نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الانترنت – دار الفكر الجامعي – الإسكندرية ، ط ١ ، ٢٠٠٧ ،
ص (٣٧-٣٨) .

١٣- د . طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية) دار الجامعة

الجديدة ، الإسكندرية ، ٢٠٠٩ ، ص ٥٨٦ .

١٤- د . محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ، ط٢ ، دار النهضة العربية ، القاهرة ، ٢٠٠٩ ، ص ٤٢ .

١٥- د . محمد الشناوي ، جرائم النصب المستحدثة ، دار الكتب القانونية ، مصر ، المحله الكبرى ، ٢٠٠٨ ، ص ١٠٨ .

١٦- د . عبد الفتاح بيومي حجازي ، مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي ، دار الفكر الجامعي ، الاسكندرية ، ط١ ، ٢٠٠٦ ، ص ٩٦ .

١٧- د . حسين بن سعيد الغافري ، السياسية الجنائية في مواجهة جرائم الانترنت ، دار النهضة العربية ، القاهرة

، ٢٠٠٩ ، ص ٥٢٣ .

١٨- نظم قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ ، المعدل احكام الاخبار عن الجرائم في

الباب الثاني منه في المواد (٤٧- ٤٨) .

١٩- محمد أمين الرومي ، جرائم الكومبيوتر والانترنت ، دار المطبوعات الجامعية الاسكندرية ، ٢٠٠٤ ، ص ٣١ .

٢٠- د . عبد الفتاح بيومي حجازي ، المبادئ الاجرائية الجنائية ، في جرائم الكومبيوتر والانترنت ، المصدر السابق ، ص١١٠ .

٢١- للتوضيح الجرائم المعلوماتية هي الجرائم المتعلقة بالحاسوب والانترنيت ، فاصطلاح الجرائم المعلوماتية عام ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الانترنت مع ملاحظة ان جريمة الحاسب الالي هي الجريمة التي تقع بواسطة الحاسب الالي أو على مكوناته المادية والمعنوية ، اما جرائم الانترنت فهي الجرائم العابرة للحدود والتي ترتكب بواسطة الانترنيت أو عليه من شخص ذا دراية فائقة بها ، لمزيد من التفصيل للفرق بين جريمة الحاسب الالي وجريمة الانترنت انظر نبيله هبه هروال ، الجوانب الإجرائية لجرائم الانترنت ، المصدر السابق ، ص (٥٤-٥٥) .

٢٢- د . احمد عبد اللطيف الفقي الدوله وحقوق ضحايا الجريمة ، دار الفجر ، القاهرة ، ط١ ٢٠٠٣ ، ص (٢١-٢٨)

٢٣- د . عبد الفتاح بيومي حجازي ، المبادئ الاجرائية الجنائية ، في جرائم الكومبيوتر والانترنت ، المصدر السابق ص٨٤.

٢٤- فمثلا في جريمة التزوير نفترض وجود محرر مزور تم تزويره بغرض الاستعمال ، هذا المحرر من الاثار التقليدية لجريمة التزوير ، لوجود مضاهاة بأصل المحرر مع المحرر المزور ، وكذلك الحال في جريمة الاختلاس في صورتها العادية نجد مستندات تشير الى ارقام وخصائص قد تكون مبالغ مالية في الحسابات او بضاعة في المخزن اختلسها صاحب العهدة لنفسه ، لكن عند ارتكاب هذه الجريمة بطريقة الحاسب الالي لا يظهر للمشاهد سوى ارقام وبيانات لا يعلمها سوى صاحب الشأن نفسه ولا تعطى دلالة سوى لشخص تخصص .

٢٥- د . هشام محمد فريد رستم ، بحث مقدم الى مؤتمر القانون والكومبيوتر والانترنيت والذي عقد بدولة الامارات

العربية المتحدة سنة ٢٠٠٠ .

٢٦- د. خالد ممدوح ابراهيم ، التقاضي الالكتروني ، مصدر سابق ، ص ٣٢٤ .

٢٧- د . محمد زكي ابو عامر ، الاثبات في المواد الجنائية ، الفنية للطباعة والنشر ، الاسكندرية ص ١١٦ .

٢٨- د . خالد ممدوح ابراهيم ، التقاضي الالكتروني ، المصدر اعلاه ، ص ٣٢٥ .

٢٩- د . سليم ابراهيم حربة وعبد الامير العكيلي شرح قانون اصول المحاكات الجزائية ، بغداد ، ١٩٨٨ ، ص ١٠٥ انظر المادة (٤٣) من قانون اصول المحاكمات الجزائية العراقي النافذ وتعليقنا على هذه المادة اننا نرى من الضروري شمول الجرائم المعلوماتية بالانتقال والمعاينة التي حددته هذه المادة دون اشتراط ان تكون الجريمة المعلوماتية مشهودة ذلك لان من خصائص هذه الجرائم انها تقع غالباً في الخفاء وبعيداً عن الانظار والاسماع كما نرى ضرورة منح صفة اعضاء الضبط القضائي بمقتضى القانون للموظفين او العاملين في مجال نظم المعلوماتية بالنسبة للجرائم المعلوماتية التي تقع في دوائرهم التي يعملون فيها وتتعلق باعمال وظيفتهم .

٣٠- د . عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية ، في جرائم الكومبيوتر والانترنت ، المصدر السابق ص ١٠٣ وما بعدها .

٣١- د. قدري عبد الفتاح الشهاوي ، ضوابط الاستدلالات والإيضاحات والتحريات في التشريع المصري والمقارن ، منشأة المعارف ، الإسكندرية ، ٢٠٠٢ ، ص١٦٢ .

٣٢- انظر المادة (٤١) من قانون أصول المحاكمات الجزائية العراقي ، وانظر د. رزطار محمد قادر ، شرح قانون أصول المحاكمات الجزائية ، ط١، اربيل ، ٢٠٠٣ ، ص ١٣٢ .

٣٣- محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، ط١، الرياض ، ٢٠٠٤ ، ص١٠٧

٣٤- ونؤكد ضرورة إصدار المشرع العراقي لمثل هذا القانون ، مع ضرورة النص فيه على منح بعض الموظفين العاملين في مجال المعلوماتية والاتصالات صفة الضبط القضائي بالنسبة للجرائم المعلوماتية التي ترتكب في دوائرهم والمتعلقة بأعمال وظيفتهم ، مثلما فعل المشرع الإماراتي من خلال قانون مكافحة جرائم تقنية المعلومات الاتحادية رقم (٢) لسنة ٢٠٠٦ ، وقانون الإجراءات الجزائية الإماراتي رقم ٣٥ لسنة ١٩٩٢ ، كونه بلا شك سيساعد في الإسراع من مهمة اكتشاف هذه الجرائم .

٣٥- د. عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت ، مصدر سابق ، ص ١٢٤.

٣٦- د. أجد راغب الحلو ، القانون الإداري ، دار المطبوعات الجامعية ، الإسكندرية ، ١٩٩٤ ، ص ٤٧١ .

٣٧- نبيله هبه هروال ، الجوانب الإجرائية لجرائم الانترنت ، المصدر السابق ، ص ٨٦ .

٣٨- د. عمر محمد بن يونس ، الجرائم الناشئة عن استخدام الانترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ ،ص ٨٠٩.

٣٩- د. ايمن عبد الحفيظ عبد الحميد ، إستراتيجية مكافحة جرائم الحاسب الآلي ، دراسة مقارنه ، رسالة دكتوراه ، أكاديمية الشرطة ، بدون سنة طبع ، ص ٣٧٤ وما بعدها .

٤٠- د. محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، مصدر سابق ، ص٥٢.

٤١- د. عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت ، مصدر سابق ، ص ١٣٠ .

٤٢- د . سليم ابراهيم حربة وعبد الامير العكيلي ، شرح قانون أصول المحاكمات الجزائية مصدر سابق،ص ١٢٥ .

٤٣- نصت المادة (٦٩) من قانون اصول المحاكمات الجزائية العراقي على انه

أ – يجوز للقاضي او المحقق من تلقاء نفسه او بناءً على طلب الخصوم ان يندب خبيراً او اكثر بأبداء الراي في
ماله صلة بالجريمة التي يجري التحقيق فيها .

ب – لقاضي التحقيق او المحقق ان يحضر عند مباشرة الخبير عمله .

٤٤- نصت المادة (٢٩) من قانون الاجراءات الجنائية المصري على انه « لمأموري الضبط القضائي اثناء جمع الاستدلالات ايسمعوا اقوال من تكون لديهم معلومات عن الوقائع الجنائية وان يسألوا المتهم عن ذلك ، ولهم ان يستعينوا بالاطباء وغيرهم من اهل الخبرة ويطلبوا رايهم شفهياً او بالكتابة » .

٤٥- انظر المادة (٤٤) من قانون اصول المحاكمات الجزائية العراقي .

٤٦- د . سليم ابراهيم حربة وعبد الأمير العكيلي ، شرح قانون أصول المحاكمات الجزائية مصدر سابق ، ص١٢٧ ، وانظر دكتور سامي النصراوي ، دراسة في اصول المحاكمات الجزائية ، الجزء الاول ، مطبعة دار السلام ، بغداد ، ١٩٧٨ ، ص ٣٦٥ .

٤٧- د . مأمون محمد سلامة ، قانون الإجراءات الجنائية معلق عليـــه بالفقه وأحكام القضاء دار الفكر العربي ، ١٩٨٠ ، ط١ ، ص٣٣٧ ، وانظر كذلك د . محمد زكي ابو عامر الاثبات في المواد الجنائية ، مصدر سابق ، ص ١٨٦ .

٤٨- د . حسين بن سعيد الغافري ، الخبرة ودورها في كشف الجرائم المتعلقة في الانترنت ، تقرير منشور في الانترنت ، بالموقع hssnrg66@hotmail.com

٤٩- د . هشام محمد فريد رستم ، المصدر السابق ، ص٣٨ .

٥٠- د . حسين بن سعيد الغافري، المصدر السابق .

٥١- د . محمد الامين البشري ، المصدر السابق ، ص ٥٩ .

٥٢- د. عمر ابو الفتوح عبد العظيم ، الحماية الجنائية للمعلومات المسجلة الكترونياً ، دار النهضة العربية ، القاهرة ، ٢٠١٠ ، ص ٤٣٨ .

٥٣- د. حاتم عبد الرحمن منصور ، الإجرام ألمعلوماتي ، دار النهضة العربية ، ط١، ٢٠٠٢ ، ص ١٥٣ .

٥٤- د. جميل عبد الباقي الصغير ، الجوانب الإجرائية ، المصدر السابق ، ص ٧٢ .

٥٥- د. حسين بن سعيد ألغافري ، السياسة الجنائية في مواجهة جرائم الانترنت ، المصدر السابق ، ص ٦٩٢ .

٥٦- د. نائله عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي القومية ، ٢٠٠٥ ، ص ٥٥ .

٥٧- هذا القواعد هي مكان القبض على المتهم ، مكان وقوع الجريمة ، أو محل إقامة المتهم .

٥٨- د. محمود صالح العادلي ، الجريمة الدولية ، دراسة مقارنه ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٣ ، ص ٦١ وما بعدها وانظر : نسرين

عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم ألمعلوماتي ، منشأة المعارف ، الإسكندرية ، ٢٠٠٨ ، ص ١٣٣ .

٥٩- د. حسين بن سعيد ألغافري ، السياسة الجنائية ، مصدر سابق ، ص ٦٩٢ .

٦٠- عقد المؤتمر الدولي لمكافحة استغلال الاطفال في الجنس في فيينا في شهر ايلول ١٩٩٩ ، بالنمسا ، انظر : د. مدحت رمضان ، جرائم الاعتداء على الاشخاص والانترنت ، دار النهضة العربية ، ٢٠٠٠ ، ص ١٢٨ .

٦١- د. هلالي عبد اللاه احمد ، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست ٢٠٠١ ، دار النهضة العربية ، ط١ ، ٢٠٠٣ ، ص ٣٣ .

٦٢- د. احمد خليفة الملط ، الجريمة المعلوماتية ، ٢٠٠٥ ، ص ٦٧٦ . بدون جهة نشر .

٦٣- د. عبد الفتاح بيومي حجازي ، مبادئ الاجراءات الجنائية في جرائم الكومبيوتر والانترنت ، مصدر سابق ، هامش ص ١٤٥ .