جامعة عمان العربية
كلية القانون

مدى حجية الدليل الالكتروني
في الإثبات الجزائي

How far the electronic evidence would
Be adopted as a penal proof

إعداد

محمد حمزة احمد كميل

إشراف

الدكتور فهد يوسف الكساسبة

قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام
جامعة عمان العربية

عمان – ٢٠١١

تفويض

أنا محمد حمزة أحمد كميل

أفوض جامعة عمان العربية بتزويد نسخ عن أطروحتي للمكاتب

أو المؤسسات أو الهيئات أو الأشخاص عند طلبها.

الاسم: محمد حمزة أحمد كميل

التوقيع: 

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها مدى حجية الدليل الالكتروني في الاثبات الجزائي يوم الاربعاء في تاريخ 2011/7/27 .

أعضاء لجنة لجنة المناقشة:

الاسم	التوقيع
الدكتور احمد المومني	رئيساً
الدكتور فهد الكساسبة	عضواً ومشرفاً
الاستاذ الدكتور علي جبار	عضواً

الشكر والتقدير

الحمد لله رب العالمين، والصلاة والسلام على سيد المرسلين محمد (صلى الله عليه وسلم)، أما بعد.....

أتقدم بخالص الشكر الجزيل والعرفان إلى أستاذي الدكتور فهد يوسف الكساسبة المشرف على الرسالة والذي تجاوز بوقته وجهده واجبات الإشراف ليثري الرسالة بعلمه وملاحظاته، فكل الشكر لأستاذي الكريم، واشكر الأساتذة الأفاضل في كلية الحقوق في جامعتي جامعة عمان العربية، الذين لم يترددوا في تقديم العون والنصيحة للباحث خلال فترة العمل على انجاز هذه الدراسة.

الإهداء

إلى من آثرني على نفسه أبي.....

إلى من أودعتني لله اهديكي هذا البحث أمي.....

إلى من تذوقت معهم أجمل اللحظات إخوتي وأخواتي.....

إلى روح الشهيد (جهاد كميل).....

إلى شهداء فلسطين الحبيبة.....

قائمة المحتويات

مدى حجية الدليل الإلكتروني في الإثبات الجزائي

إعداد:

محمد حمزة كميل

إشراف:

الدكتور فهد يوسف الكساسبة

الملخص باللغة العربية

تناولت هذه الدراسة مدى حجية الدليل الإلكتروني في الإثبات الجزائي سواء أكانت جريمة معلوماتية أم جريمة تقليدية في ظل ازدياد الجرائم المعلوماتية في العصر الحالي، وبالرغم من ازدياد هذه الجرائم لا يزال التشريع قاصرا عن مجابهة هذه الجرائم، كما أن عدم ملاءمة أدلة الإثبات التقليدية للجرائم المعلوماتية ظهرت الحاجة إلى أدلة جديدة من ذات الطبيعة التي تتميز بها هذه الجرائم المستحدثة، وذلك من خلال الحاجة إلى نصوص قانونية خاصة تعالج هكذا جرائم.

وقد تناول الباحث موضوع هذه الدراسة من خلال خمسة فصول، وقد خصص الفصل الأول منها للمقدمة، كما خصص الفصل الثاني لدراسة ماهية الدليل الإلكتروني وتعريفه والطبيعة القانونية لهذا الدليل التي تنبع من مبدأين رئيسين، مبدأ المشروعية أي مشروعية الحصول على الدليل الإلكتروني، ومبدأ يقينية الدليل الإلكتروني الذي يحقق العدالة.

وقد تناول الفصل الثالث حجية الدليل الإلكتروني سواء بالنسبة للجرائم التقليدية التي يمكن إثباتها بكافة طرق الإثبات، لذلك يعد الدليل الإلكتروني من القرائن القضائية التي لم ينص عليها القانون والتي يعود أمر تقديرها إلى القاضي. أما الجرائم الإلكترونية فإن القاضي يأخذ بهذه الأدلة عند توافر شروط معينة:

١- صدور هذه الأدلة عن إرادة حرة.

٢-مناقشة الأدلة الإلكترونية تطبيقا لمبدأ شفوية المرافعة.

٣-أن لا يطرأ على الدليل الإلكتروني أي تغيير.

٤-أن يكون الدليل الإلكتروني على علاقة بالجريمة المعلوماتية.

وقد تناول الفصل الرابع إجراءات الحصول على الدليل الإلكتروني سواء أكانت في مرحلة الاستدلالات أم في مرحلة التحقيق، كما تناول مدى قناعة القاضي الجزائي بالدليل الإلكتروني، وقد توصل الباحث إلى أن اقتناع القاضي يرتبط بنظام الإثبات الجنائي المعمول به، لذلك فإن عدم توافر المعرفة والخبرة العالية لدى القاضي في الأدلة الإلكترونية ، يجعله صعب الاقتناع في هذه الأدلة، بسبب قلة التعامل مع هذه الجرائم وقلة الخبرة والدراية الفنية العالية بها.

أما الفصل الخامس فقد تناول الباحث الخاتمة وما توصل إليه من خلال الدراسة، ثم عرض ما تم التوصل إليه من الاستنتاجات وما خلص من توصيات يعتبرها الباحث ضرورية قد تعمل على إيجاد لبنة علمية متواضعة يمكن البناء عليها، خصاصةً مع التطور التكنولوجي الحاصل في العصر الحاضر.

كما أن عدم ملاءمة قواعد الإثبات التقليدية لهذه الجرائم المستحدثة كان لزاما على المشرع أن يتدخل لسن التشريعات الخاصة بهذه الجرائم وإيجاد كفاءات خاصة قادرة على التعامل مع الجرائم المعلوماتية.

How far the electronic evidence would

Be adopted as a penal proof

Prepared by:

Mohammad Hamzah Kmail

Supervised by:

Dr. Fahad Yousef Al Kasasbeh

Abstract

This study has addressed the extent of authenticity related to the electronic evidences as a proof in penal cases, either of a cyber or conventional crime in light of the increasing number of cyber crimes at the present time. Despite the growing number of these crimes, legislations have not so far been able to cope with these crimes. Besides, the fact that conventional proofs are not appropriate to substantiate cyber crimes which led to the need for new evidence of the same nature peculiar to modern crimes through drawing up special legal provisions to tackle such crimes.

The researcher discussed the subject matter of this study in five chapters.

Chapter one was allocated to the introduction, and chapter two was designed to study the electronic evidence in terms of essence, definition and legal nature which stems from two major principles: legitimacy principle, i.e. legitimacy of obtaining the electronic evidence and the certainty principle of the electronic evidence which will yield justice.

Chapter three discussed the authenticity of the electronic evidence with relation to the conventional crimes which can be proven through all methods of confirmation, therefore, the electronic evidence constitutes one of the judicial presumptions which were not stipulated by law and which were left for the judge to assess.

On the other hand, proofs related to electronic crimes shall be taken into consideration particularly when certain conditions are met:

- Legitimacy.
- These evidences are issued on the basis of free will.
- Electronic evidences are discussed as an implementation of the principle of verbal nature of pleadings.
- No change is made to the electronic evidence.
- Electronic evidence should be related to the cyber crime.

Chapter four explained the procedures for obtaining the electronic evidence, either in the inference phase or in the investigation phase. This chapter also discussed how far the penal judge is convinced of the electronic evidence, and the researcher came to the conclusion that such conviction depends on the criminal proof adopted. Our judges are not experienced enough in handling such crimes. To overcome this problem, it will be necessary to create judicial panels which have minimal knowledge of computer technology.

In the fifth chapter, the researcher deals with conclusion and the findings through his study and display those findings; conclusion and important concluded recommendations that might work to find a scientific widest brick can be built upon. That especially goes with the technological development occurring in today's world.

In view of the conventional rules of substantiation which are inappropriate for these modern crimes, it is necessary for the lawmaker to intervene for enacting legislations pertaining to these crimes, and to provide qualified cadres capable of dealing with cyber crimes.

الفصل الأول : المقدمة:

يعد موضوع الإثبات في جرائم الكمبيوتر من الموضوعات الشائكة لما تتصف به هذه الجرائم من سرعة وسهولة في ارتكابها وإخفاء معالمها، على خلاف الجرائم التقليدية التي نص المشرع صراحة على وسائل إثباتها، وبعد اعتماد المجتمعات الحديثة في تسيير شؤونها على أنظمة الحاسب الآلي، فإن على الأجهزة الأمنية والنيابة الجنائية ومع تقلص دور الأدلة التقليدية في الإثبات أن تتعامل في ممارستها لحماية الحقوق والمصالح العامة والخاصة للمجتمعات مع أشكال جديدة من الأدلة غير المادية، وذلك في مجال الإثبات الجنائي، والذي يفرض على السلطة المختصة (سلطة الضبط القضائي) في جمع هذه الأدلة أن تسعى دوما إلى تطوير أساليب كشف الجريمة المعلوماتية، والوسائل المستخدمة في عمليات البحث الجنائي وهو ما يتطلب تأهيل الكوادر التدريبية لاكتساب المهارات في استخدام أنظمة الحاسب الآلي، ومن ناحية أخرى تحديث هذه الأساليب المتبعة لجمع الأدلة في جرائم أنظمة الكمبيوتر بشكل دوري، دون أن تتعرض حقوق الأفراد وحرياتهم ومصالحهم الخاصة إلى الخطر عند إثبات أي من هذه الجرائم.

ولا تثور أية مشكلة بالنسبة لإثبات الجرائم التقليدية ولكن الأمر يختلف فيما إذا كان للأدلة الإلكترونية مكان في إثبات الجرائم التي ترتكب بوسائل حديثة، كجرائم الحاسوب.

فشبكة الإنترنت بوصفها أداة للربط والاتصال بين مختلف الشعوب يمكن أن تشكل أداة لارتكاب الجريمة أو قد تكون محلا لها، وذلك عن طريق استغلالها والكشف عن المعلومات على نحو غير مشروع ، مما يؤدي إلى ظهور مجموعة جديدة من الجرائم عرفت بالجرائم المعلوماتية.

ومع تزايد استخدام الحاسوب والإنترنت تزايدت نسبة الجريمة المعلوماتية، وعلى الرغم من أن التعامل في مسرح الجريمة يتطلب إجراءات معينة إلا أن استخلاص الدليل الالكتروني يتطلب إجراءات من نوع خاص، لأن البرامج والمعلومات الرقمية عنصران يحتمان على أجهزة إنفاذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها.

ولقد أفرزت الثورة التكنولوجية الجديدة الحاجة الماسة إلى تطوير نظم المعلومات في جميع قطاعات الحياة بما يساير التطورات التكنولوجية والاجتماعية والاقتصادية التي تتزايد يوما بعد يوم، وذلك من أجل الإفادة من هذه الثورة التكنولوجية وإخضاعها إلى خدمة المجتمع، فقد بدأ العالم يدخل عصرا جديدا وهو عصر الالكترونيات.

ونظرا لعدم كفاية وملاءمة هذه النظم التقليدية في إثبات مثل هذه الجرائم سواء من الناحيتين القانونية أو التقنية، فقد كان لزاما على المشرع أن يستحدث التشريعات التي تلائم مثل هذه الجرائم بما في ذلك ملاحقتها وطرق إثباتها، أما الجرائم التقليدية فهي جرائم يكون محلها شيئاً مادياً ملموساً مما يسهل التعامل معها وجمع أدلتها، وهي جرائم لا تحتاج إلى تقنيات عالية لارتكابها، لأن الجاني يقوم بفعل أو يمتنع عن فعل يعد مخالفا للقانون ويعاقب حسب فعله بما هو منصوص عليه في القانون.

ومع ذلك فإن الأدلة التقليدية قد تضاءل دورها في عملية إثبات هذه الجرائم التي ترتكب بوسائل حديثة، الأمر الذي أدى إلى ظهور ما يعرف بالدليل الإلكتروني، الذي يتم الحصول عليه من خلال عملية البحث والتحري في حاسوب الجاني أو المجني عليه، أو في غرف المحادثة، أو في المواقع الإلكترونية التي سبق وزار أي منهما، فالأدلة الإلكترونية التي تنتج عن هذا البحث والتحري التقني تبقى هي الأساس الأول والحدث المهم الذي يمكن به التوصل إلى دليل قاطع يثبت الجريمة.

ومما يزيد من خطورة هذه الجرائم أن النصوص العقابية المطبقة لا تكفي لحماية حرمة الحياة الخاصة من الاعتداء عليها باستخدام الوسائل الالكترونية المستحدثة ، ولا بد من الإشارة أنه وعن طريق استخدام الحاسب الآلي فقد أمكن بوساطة عملياته الدقيقة أن تكون الحياة الخاصة للإنسان مجردة من كل حصانة تحميها.

وفي ظل التطور المستمر في أساليب ارتكاب مثل هذه الجرائم الحديثة، فلا بد أن يقوم المشرع بتنظيم الأحكام المتعلقة بجرائم نظم المعلومات وسبل مواجهتها، وينبغي على الأجهزة المعنية ملاحقة هذه الجرائم، من خلال تدريب وتأهيل الكوادر اللازمة واكتساب المهارات التي تجعلهم قادرين على التعامل مع الحاسب الآلي، وبالتالي القدرة على التعامل مع مرتكبي هذا النوع من الجرائم، فجرائم أنظمة المعلومات جرائم تقنية يرتكبها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات وتطال المعلومات المخزنة في أجهزة الحاسب الآلي أو المنقولة عبرها، حيث إن التشريع لايزال غير مواكب للجرائم الحديثة، ولم يضع قواعد موضوعية أو شكلية، تبين كيفية إثبات هذه الجرائم.

ويعد موضوع البحث من الموضوعات الشائكة التي تحتاج إلى دراسة وتوضيح، فالدليل الإلكتروني بوصفه دليلا معنويا يحتاج إلى كوادر مؤهلة لاستخلاصه، وتشريعات قادرة على ملاحقة وإثبات هذه الجرائم.

مشكلة الدراسة :

تهدف هذه الدراسة إلى بيان مدى حجية الدليل الإلكتروني في إثبات الجرائم الإلكترونية في ظل تطور أساليب ارتكاب الجرائم بصورة عامة، والوقوف على إجراءات ضبط الدليل الإلكتروني وبيان مدى قوته في الإثبات أمام المحكمة الجزائية.

عناصر مشكلة الدراسة:

تتمثل عناصر مشكلة الدراسة فيما يلي:

١. ماهية الدليل الإلكتروني مقارنة بأدلة الإثبات الجزائية الأخرى وما هي طبيعته القانونية ؟

٢. ما هي النتيجة القانونية للدليل الإلكتروني في مجال الإثبات الجزائي وما مدى حجيته أمام المحاكم الجزائية ؟

٣. ما هو موقف التشريعات المقارنة من الدليل الإلكتروني؟

٤. هل يوجد في التشريعات العربية ما يدلل على حجية الدليل الإلكتروني في الإثبات الجزائي؟

أهمية الدراسة:

يعد موضوع الدراسة من الموضوعات الجديدة، فهو يتعلق ببيان أهمية الدليل الإلكتروني وحجيته في إثبات الجرائم غير التقليدية المرتكبة بوساطة الحاسب الآلي والإنترنت ، إن موضوع جرائم نظم المعلومات هو من الجرائم المستحدثة ، كما إن انتشار النظم المعلوماتية وازدياد ظاهرة الإجرام في ظل عصر النهضة الإلكترونية يتطلب القيام بالواجبات التي تكفل حماية المجتمع من القرصنة الإلكترونية ويقع على عاتق الدولة مسئولية مكافحة هذه الجرائم من خلال سن التشريعات أو تعديل القوانين والبحث عن وسائل جديدة لإثبات هذه الجرائم وملاحقتها والحد منها.

وترجع أهمية الموضوع بصفة خاصة إلى دخول أجهزة الحاسب الآلي في حياة الفرد وفي سير المجتمع فلم يعد مجال للاستغناء عن جهاز الحاسب الآلي، ومن هنا فقد ظهرت الحاجة إلى حماية الفرد من أنظمة هذا الجهاز الآلي وما يمثله ذلك من خطورة على القيم الاجتماعية الأساسية كحماية الخصوصية والمصالح العامة الأخرى.

وتبدو الأهمية العلمية في مجال الأدلة الإلكترونية في معرفة ما توصل إليه الآخرون في مجال مكافحة جرائم الحاسب الآلي، وذلك في سبيل الوصول إلى سن التشريعات الخاصة المناسبة لمثل هذه الجرائم للوقوف بها أمام مرتكبي هذا النوع من الجرائم في المحاكم الجزائية.

أهداف الدراسة:

١. تعريف ماهية الدليل الإلكتروني ومدى حجية الدليل الإلكتروني في الإثبات الجزائي.
٢. توضيح موضوع الإثبات بالدليل الإلكتروني، وكيفية استخلاص هذه الأدلة المخزنة داخل الحاسب الآلي.
٣. بيان ماهية الطبيعة القانونية للدليل الإلكتروني.
٤. بيان موقف التشريع الأردني من الدليل الإلكتروني والتشريعات المقارنة من حجية الأدلة الإلكترونية في الإثبات الجزائي.

محددات الدراسة:

يتناول موضوع هذه الدراسة مدى حجية الدليل الإلكتروني في الإثبات الجزائي، وبالتالي تخرج من نطاق هذه الدراسة الأدلة التقليدية إلا بما يتطلبه البحث من إيضاح، وبيان خصائص هذا الدليل وكيفية استخلاصه، ومدى قناعة القاضي بالأخذ بهذا الدليل في ظل التشريع الأردني ودوره في إثبات هذه الجرائم المرتكبة بوساطة الحاسب الآلي.

منهجية الدراسة :

سوف يتجه الباحث إلى بيان حجية الدليل الإلكتروني في مجال إثبات الجرائم المعلوماتية. لذلك سوف يكون منهج البحث على النحو التالي:

المنهج التحليلي: وهو المنهج القائم على التفسير والتحليل لجزئيات البحث للتعرف على أهداف البحث، وقد عملت على تحليل المادة التي جمعتها.

المنهج الوصفي: وهو المنهج القائم على وصف جزئيات البحث للتعرف على ماهية الدراسة.

الفصل الثاني ماهية الدليل الإلكتروني وطبيعته القانونية

إن الوصول إلى إثبات الجريمة الإلكترونية، يتطلب من القائمين بأعمال البحث والتحري ملاحقة الجرائم الإلكترونية التي تشكل ظاهرة جرميه متزايدة في المجتمع، والقيام بجمع الأدلة المتعلقة بها لتدعيم الإجراءات القانونية اللازمة التي تكفل عدم المساس بهذه المعلومات وحمايتها، وذلك في سبيل إظهار القيمة القانونية التي يعكسها الدليل الإلكتروني في إثبات الجرائم الإلكترونية، والحد من خطورتها، ومن خلال جمع الأدلة المتعلقة بهذه الجرائم وتطور أساليب مكافحتها، كان لابد من استخدام التقنيات الفنية الحديثة، التي تسهم بشكل كبير في استخلاص الأدلة العلمية و الفنية الحديثة لحماية هذه المعلومات من القرصنة الإلكترونية.

ومع تطور تكنولوجيا المعلومات وتزايد الظاهرة الجرمية المعلوماتية، تطورت معها أساليب وأشكال جمع المعلومات والأدلة اللازمة لمنع انتشار هذه الجرائم ، الأمر الذي يتطلب الوقوف على القيمة والطبيعة القانونية للدليل الإلكتروني، وبناءً على ذلك سنتناول دراسة هذا الموضوع في البندين التاليين:-

أولا : ماهية الدليل الإلكتروني.

ثانيا : الطبيعة القانونية للدليل الإلكتروني.

أولا: ماهية الدليل الإلكتروني

إن الإثبات في حقيقته هو البحث عن الدليل المتعلق بواقعة معينة، وتقديمها إلى السلطات المختصة، وهو ما يستتبع البحث في مفهوم وماهية الدليل الإلكتروني، ثم التعرف على خصائصه وميزاته، وعليه سنتناول أولا التعريف بالدليل الإلكتروني ثم نبين ثانيا خصائصه وثالثا مساوئ هذا الدليل:

١. تعريف الدليل الإلكتروني.

٢. خصائص الدليل الإلكتروني.

٣. مساوئ الدليل الإلكتروني.

١. تعريف الدليل الإلكتروني

يعرف البعض الدليل الإلكتروني بأنه"الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجيا خاصة، (برامج خاصة تقوم بتحويل النبضات الكهربائية إلى بيانات ومعلومات ثم إرسالها عبر الحاسب الآلي)، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم ، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون".(عبد المطلب، ٢٠٠٦، ٨٨).

وقد عرفه الدكتور محمد طارق الخن بأنه"المعلومات أو البيانات الرقمية المخزنة في الحاسوب أو المنقولة بوساطته ، والتي يمكن استخدامها في إثبات أو نفي جريمة ما".(الخن، ٢٠١١، ٣٤٢).

وعرفه الدكتور خالد ممدوح إبراهيم بأنه"أية معلومات سواء أكانت من صنع الإنسان أم تم استخلاصها من الحاسوب، وبشكل يمكن قراءته أو تفسيره من أشخاص لديهم مهارات في إعادة تشكيل المعلومات، بمساعدة من برامج الكمبيوتر".(إبراهيم، ٢٠٠٩، ١٧٨).

ولم يأت القانون المؤقت لجرائم أنظمة المعلومات الأردني لسنة ٢٠١٠ بتعريف صريح للدليل الإلكتروني، بل أشار إليه، في المادة ١٣ من الفقرة ب من القانون ذاته والتي نصت على انه"مع مراعاة حقوق الآخرين ذوي النية الحسنة باستثناء المرخص لهم وفق أحكام قانون الاتصالات

ممن لم يشتركوا بأية جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها".

وبناءً على ما تقدم يمكن للباحث تعريف الدليل الإلكتروني بأنه "عبارة عن بيانات رقمية سواء أكانت مخزنة في جهاز الحاسوب أم منقولة عبره، تكون ذات قيمة دلالية على ثبوت أو نفي الجريمة، وقد تتخذ عدة أشكال متنوعة مثل النصوص أو الأصوات أو الصور أو الرسوم، ويمكن قبولها أمام المحكمة الجزائية".

ويظهر من ذلك أن الدليل الإلكتروني عبارة عن نبضات إلكترونية غير مرئية تنتقل من خلال أجهزة الحاسب الآلي دون أن تترك آثاراً مادية، ومثل هذه الأدلة تحتاج إلى قدرة عالية من التقنية والخبرة الفنية في التعامل معها واشتقاقها لتكون ذات قيمة ثبوتية قاطعة في الإثبات.

ومن خلال ما تقدم، فإن الدليل الإلكتروني هو عبارة عن مجموعة معلومات أو بيانات رقمية يمكن تقسيمها على النحو التالي:

-البيانات المخزنة في جهاز الحاسوب وهي عبارة عن بيانات رقمية محفوظة داخل الحاسب الآلي، ويمكن لهذه البيانات الانتقال من جهاز كمبيوتر إلى آخر حتى لو كان في دولة أخرى.

-البيانات المنقولة وهي عبارة عن مخرجات جهاز الحاسب الآلي مثل بطاقات شحن الهاتف الجوال.

ولابد من الإشارة إلى القيمة الثبوتية التي يتمتع بها الدليل الإلكتروني، لأن هذا الدليل يمكن استخدامه في إثبات أو نفي الجرائم التقليدية أيضا، كما لو كانت هناك رسالة الكترونية تحمل اعترافا للجاني بارتكابه جريمة القتل أو الاغتصاب أو الاحتيال العادي، في حين القواعد التقليدية للإثبات تقف عاجزة أمام الجرائم المعلوماتية ذات الطبيعة الخاصة، فهي بحاجة إلى وسائل إثبات من ذات الطبيعة حتى تكون قادرة على مواجهتها، لأنها جرائم لا تترك آثاراً مادية بل آثاراً معنوية غير محسوسة

٢. خصائص الدليل الإلكتروني:

لا يكفي لتتبع المجرمين وإحالتهم إلى العدالة البحث فقط في الوسائل التقليدية للإثبات الجزائي، إذ مع ظهور المجرم المعلوماتي تعذر ملاحقته عن طريق الوسائل التقليدية، إنما يتم تتبع هذا المجرم عن طريق الوسائل والأدلة الإلكترونية، التي تطورت مع تطور الأنظمة المعلوماتية.

ويتمتع الدليل الإلكتروني بعدة خصائص تميزه عن غيره من الأدلة التقليدية، وهي:

١. إمكانية النسخ إذ يمكن نسخ الدليل الإلكتروني نسخة مطابقة للأصل تماما، وهذه الميزة لا تتوافر في الأدلة التقليدية.

٢. يمكن للجاني أن يعمد إلى محو الدليل، وهذا الفعل يشكل دليل إدانة ضده، إذ يمكن استخلاص هذا النشاط الذي قام به الجاني من جهاز الحاسب الآلي الخاص به وإستخدامه ضده،(إبراهيم، ٢٠٠٩، ١٨٢).

٣. يعتبر الدليل الإلكتروني دليلا غير مرئي، أي ليس ماديا، ويتمثل في معلومات غير مرئية لا تفصح عن شخصية معينة عادة، بل إن هذه العملية لا تعدو كونها عملية نقل لتلك البيانات من طبيعتها الإلكترونية إلى الهيئة التي يمكن الإفادة منها كدليل إثبات، أما الوسائل التقليدية للإثبات فهي أدلة مادية يمكن تحريفها، (إبراهيم، ٢٠٠٩، ١٨٠).

٤-صعوبة محو الدليل الإلكتروني وهي من أهم خصائصه التي يتمتع بها، فلا يمكن التخلص من الأدلة الإلكترونية المتمثلة في البيانات الرقمية أو الملفات أو الأقراص التي تكون مخزنة في الحاسب الآلي بالأمر (Delete) وبالإمكان استرجاعها في أي وقت، وهو على خلاف مع الوسائل التقليدية التي يمكن محو الدليل فيها والتخلص منه بكل سهولة، إذ يمكن التخلص من بصمات الأصابع بمسحها مثلا من مسرح الجريمة.

والقاعدة العامة التي يوصي بها بعض الخبراء عند جمع الأدلة الرقمية هي جمع قدر المستطاع من الأدلة، حيث إنه بمجرد مغادرة مسرح الجريمة يصبح من الصعب العثور على أية أدلة في حالة عودة المحقق مرة أخرى لعمل ذلك، ولهذا يجب مراعاة طبيعة هذا الدليل غير المرئية، التي لا تخلف آثارا مادية، ولسهولة محوها من قبل الجاني مرتكب الجريمة، فإن جمع هذه الأدلة في أسرع وقت لا تعطي الجاني الفرصة للعودة وإزالة هذه الأدلة التي تدينه، (إبراهيم، ٢٠٠٩، ١٨٦).

مساوئ الدليل الإلكتروني عديدة وفيما يلي استعراض لأهمها:

١. إعاقة الوصول إلى الدليل الإلكتروني

عندما يرتكب الجاني جريمته فإنه يحتاج إلى ما يخفي به هذه الجريمة، وهنا يعمد إلى وضع العقبات أمام أجهزة التحقيق لعدم حصولها أو حتى وصولها إلى الدليل الذي يدينه في ارتكاب الجريمة، عن طريق حماية وسيلة ارتكاب الجريمة وهو جهاز الحاسب الآلي ، من خلال تزويده بكلمة سر معينة تمنع أي دخول إليه وإظهار الملفات المخزنة في داخله، والتي قد تساعد أجهزة التحقيق في استخراج الدليل الذي يدينه.(المناعسة وآخرون، ٢٠٠١، ٢٩٠).

٢-قلة الخبرة بتقنية المعلومات

مع تطور أساليب ارتكاب الجريمة في ظل تقنية المعلومات والتكنولوجيا كان لابد من تطوير الكوادر وتأهيلها لاكتساب مهارات تجعلها قادرة على التعامل مع هذه الجرائم المعلوماتية، إذ إن قلة الخبرة ببرامج الحاسب الآلي يحول دون القدرة على مكافحة مثل هذه الجرائم.

٣. كثرة البيانات التي يوجد فيها الدليل الإلكتروني

إن بطاقة الذاكرة للحاسب الآلي تحتوي على كمية هائلة من المعلومات وبالتالي صعوبة الوصول إلى الجزء الصغير الذي قد يشكل دليلا على هذه المعلومات.

ويمكن تشبيه حجم المعلومات هذه بموجات الراديو الموجودة في الهواء والتي تحتوي على بيانات متشابكة، الأمر الذي يجعل من الصعوبة معرفة مكان الإشارة المطلوبة وترجمتها إلى بيانات مفهومة.(الخن، ٢٠١١، ٣٤٥).

لذلك يجب أن تمتلك أجهزة التحقيق الخبرة والقدرة على التعامل مع أجهزة الحاسب الآلي والبرامج والملفات المخزنة في داخله، كونها برامج دقيقة تحتاج إلى خبرة كافية للتعامل معها، الأمر الذي يسهل على أجهزة التحقيق تفتيش هذه البرامج واستخراج المعلومات المخزنة وتحليلها، لأن الوصول إلى جمع الأدلة الإلكترونية من خلال أجهزة الحاسب الآلي باهظة التكاليف تحتاج إلى خبرة واسعة وقدرة عالية للدخول إلى الحاسب الآلي والشبكة العنكبوتية (الإنترنت) بأقل التكاليف وأسهل الطرق، (المناعسه وآخرون، ٢٠٠١، ٢٩١).

وتعقيبا على ما تقدم فقد جاء في توصيات المجلس الأوروبي الصادرة في سنتي (١٩٨٥)، (١٩٩٥)، وهي معاهدة بين دول الاتحاد الأوروبي على مكافحة الجرائم المعلوماتية ومركزه فرنسا، ودوره استشاري محض وآراؤه غير ملزمة، بما يفيد ضرورة استحداث دوائر جديدة تضطلع بمهمة مكافحة جرائم الحاسب الآلي وتزويدها بالموظفين الأكفاء ذوي الخبرة والدراية العلمية، بالإضافة إلى توافر الأجهزة والمعدات التقنية اللازمة، وأوصى بتجريم الاستخدام غير المشروع لنظام الحاسب الآلي الذي ينجم عنه ضرر يلحق هذا النظام ووظائفه، ومن توصياته أن توضح القوانين إجراءات تفتيش أجهزة الحاسب الآلي وضبط المعلومات التي تحويها، ومراقبة المعلومات أثناء انتقالها، والأردن من الدول التي استجابت حديثا لذلك، حيث أنشئت في عام ١٩٩٧ إدارة المختبرات والأدلة الجرمية، واستحدثت فيها قسم (الحاسب الآلي) للقيام بتلك المهمة،(المناعسة وآخرون، ٢٠٠١، ٢٩٢).

ونظرا لحداثة جرائم تقنية المعلومات فإن القوانين الحالية تفتقر إلى الكثير من النصوص الخاصة لمواجهة جرائم الحاسب الآلي، نظراً لخصوصيتها التي تحتاج إلى إجراءات تتفق وطبيعتها، وهذا يشكل قصورا تشريعيا، ومن أبرز هذا القصور عدم النص صراحة على الدليل الإلكتروني في الإثبات، علما بأن المادة (٧/أ) من قانون المعاملات الإلكترونية الأردني قد أشارت إلى أن السجل الإلكتروني والعقد الإلكتروني والتوقيع الإلكتروني والرسالة الإلكترونية منتجة للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لأطرافها أو صلاحيتها في الإثبات،(حجازي، ٢٠٠٢، ٨٣).

ثانيا: الطبيعة القانونية للدليل الإلكتروني

كرست معظم الدساتير في العالم مبدأ "المتهم بريء حتى تثبت إدانته بحكم قضائي مبرم"، وذلك حفاظا على كرامة الإنسان، فإذا لم يقم الدليل القاطع على ارتكابه الجريمة، فإن ذلك يعني براءته من الجرم المسند إليه،(الخن، ٢٠١١، ٢٩٥).

وعليه فإن مجرد وصول دليل يثبت وقوع الجريمة ونسبتها لشخص معين لا يكفي للتعويل عليه لإصدار الحكم بالإدانة، إذ يلزم أن يكون لهذا الدليل طبيعة قانونية، وهذه الطبيعة للدليل الإلكتروني تتوقف على مسألتين رئيستين:

١. مبدأ مشروعية الدليل الإلكتروني وهذا ما سنتناوله في البند الأول.

٢. مبدأ يقينية الدليل الإلكتروني وهذا ما نشير إليه في البند الثاني.

١. مبدأ مشروعية الدليل الإلكتروني

لا شك أن الجريمة المعلوماتية تطورت نتيجة للتطور التكنولوجي، الأمر الذي يتطلب إيجاد وسائل جديدة تتفق وطبيعة هذه الجرائم، نظراً لقصور وسائل الإثبات التقليدية في إثباتها، وعليه يجب أن تستند الأدلة على إجراءات مشروعة لقبولها أمام المحاكم الجزائية، وحتى يقتنع القاضي ويأخذ بها عند القبض على المتهم وتفتيشه سواء بالإدانة أو البراءة،(سليمان، لات، ٤٢٥).

ويمكن القول إن النظم القانونية تتبع في موقفها من الأدلة التي تقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه، موقفين رئيسين:

١. ١: نظام الأدلة القانونية المقيد

١. ٢: نظام حرية الإثبات

١: نظام الأدلة القانونية المقيد:

وفقا لهذا النظام فإن المشرع هو الذي يحدد حصرا الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القيمة الإقناعية لكل دليل، بحيث يقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون،(هلالي، ١٩٩٩، ٤٩).

فلا مجال لأن يكون الدليل ضمن أدلة الإثبات طالما لم ينص عليه القانون صراحة، ولا يستطيع القاضي أن يقوم بتقدير حجية هذا الدليل لأن يكون دليلا قاطعا أو نافيا للجريمة، لذلك سمي هذا النظام بنظام الأدلة المقيد، حيث إن القانون يقيد القاضي بعدد من الأدلة التي نص

عليها، وهذا النظام تتبناه الدول التي تتبع النظام الانجلوسكسوني، مثل بريطانيا والولايات المتحدة الأمريكية، وفي ظل هذا النظام لا يمكن الاعتراف للدليل الإلكتروني بأية قيمة قانونية في الإثبات ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، وبالتالي فإن خلو القانون من النص على الدليل الإلكتروني يفقده قيمته الإثباتية، مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لإثبات أو نفي الجريمة.

وتطبيقا لذلك فقد نص المشرع الأمريكي في قانون الإثبات في المواد الجنائية لسنة (١٩٨٣) على قبول الدليل الإلكتروني وحدد قيمته الإثباتية، وحدد أن النسخ المستخرجة من البيانات التي يحتويها الحاسب الآلي تكون مقبولة بوصفها أفضل الأدلة المتاحة في مجال الإثبات.(سليمان، لات، ٤٢٨).

ويمكن أن يعاب على قانون الإثبات القانوني هذا أن من شأنه تقييد حرية القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون،

ولهذا فقد بدأ هذا النظام ينحصر نطاقه حتى في الدول التي تعتبر الأكثر اعتناقا له، ففي بريطانيا مثلا فقد بدأت

تخفف من غلوه، حيث ظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك، والتي مفادها أن القاضي يستطيع أن يكون عقيدته من أي دليل وإن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعا في دلالته،(هلالي، ١٩٩٩، ٩١).

٢: نظام حرية الإثبات:

يسود الإثبات الحر في ظل الأنظمة اللاتينية، ووفقا لهذا النظام يتمتع القاضي الجزائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، ويقتضي هذا النظام عدم قيام القاضي سلفا بتحديد الأدلة التي يجب أن يستند إليها في إصداره لحكمه بل يتمتع "بسلطة تقديرية واسعة سواء من حيث قبول الأدلة ذاتها وعددها، أو من حيث تقديره الشخصي لقيمة كل منها، وكل ذلك تبعا لما يطمئن إليه"(هلالي، ١٩٩٩، ٢٩).

ويستند هذا النظام على مبررات عدة منها:

١. أعطى هذا النظام للقاضي سلطة تقديرية واسعة في قبول الدليل أو رفضه.

٢. اعتمد هذا النظام على كافة الطرق والوسائل المتاحة للإثبات.

وعلى ذلك فقد قيد المشرع المصري حرية القاضي خوفا من استبداده وتحكمه بما يتناسب من القواعد والضوابط، ما هو كفيل لعدم استبداده، بحيث إن إثبات جريمة الزنا مثلا، هي القبض عليه حال تلبسه بالفعل أو اعترافه أو وجود مكاتيب أو أوراق أخرى مكتوبة منه أو موجوده في مكان مخصص للجريمة،(عفيفي، ٢٠٠٣، ٣٩١).

ومما يلاحظ على هذا النظام أنه يعطي القاضي الحرية المطلقة في مسألة قبول الدليل او رفضه بعد البحث في مصدر هذا الدليل ومشروعيته، على اعتبار أن المشرع لا يتبع سياسة النص على قائمة الأدلة المقبولة للإثبات، لذلك فمسألة قبول الدليل الإلكتروني تعتمد على مدى اقتناع القاضي به، ووفقا لهذا النظام فإن الأصل في الأدلة مشروعية وجودها.

ولعل أكثر المسائل إثارة للجدل بخصوص الأدلة الإلكترونية ما إذا كان يعتبر الدليل المستخرج من الكمبيوتر ونظم التقنية أصليا أم أنه مجرد صورة عن الدليل، والحقيقة إن الجدل بهذا الخصوص امتد ليشمل مختلف النظم القضائية، لا في الدعاوي الجزائية فحسب، بل في الدعاوي الحقوقية، ومرد ذلك أن النظم القضائية تتطلب تقديم الدليل الأصلي للاحتجاج به في معرض بينات الإثبات، ويمكن القول إن اعتبار نسخة الدليل الإلكتروني أصلا لم يتحقق في الواقع إلا من خلال التدخل التشريعي، فلا تعتبر المصغرات الفيلمية أو الصور أو مستخرجات الكمبيوتر من سجلات ونحوها أصولا إلا بإقرار القانون

وبناءً على ذلك اتجه المشرع الأردني في الاتجاه الصحيح حين نص في قانون البينات المعدل رقم (٣٧) لسنة ٢٠٠١ على قوة مخرجات الحاسوب من حيث الإثبات، فقد جاء في المادة (١٣/ج) "وتكون لمخرجات الحاسوب المصدقة أو الموقعة قوة الإسناد العادية من حيث الإثبات ما لم ثبت من نسب إليه أنه يستخرجها أو لم يكلف أحد باستخراجها".

وبناءً على ذلك، فإن المادة (٢٠٠١) من قانون الإثبات الفدرالي الأمريكي لسنة (١٩٨٣) والتي تتطلب للاحتجاج بمحتوى الكتابة أو الصور أو السجل أن يقدم الأصل، إلا أنها اعتبرت المستخرجات المطبوعة أو أية مستخرجات بصورة مقروءة والخاصة بالمعطيات المخزنة في الكمبيوتر أو الأجهزة الشبيهة، إذا عكست دقة و صحة هذه المعطيات أصلا يعتمد عليها، ولكي تحقق هذه المستخرجات هذا الشرط فإن معايير تقنية وفنية تحكم وتنظم الملفات ذات الطبيعة التقنية ينبغي الرجوع إليها لإمكانية اعتمادها وذلك لضمان الثقة بعملية الاستخراج،(عرب، ٢٠٠٢، ٥١٢).

ومع دخول الكمبيوتر إلى الحياة البشرية واعتمادها على هذه الأجهزة والشبكة العنكبوتية في مجالات الحياة المختلفة، لا بد من حمايتها بطبيعتها الإلكترونية المحضة من أي اعتداء عليها، سواء أكان بالإتلاف أم التعديل حتى تكون مقبولة أمام المحاكم الجزائية، في حين أن قانون جرائم أنظمة المعلومات المؤقت الأردني لسنة ٢٠١٠ لم ينص صراحة على الدليل الإلكتروني، بالرغم من ازدياد الاعتماد على نظم الحاسب الآلي في مختلف نواحي الحياة.

١-مبدأ يقينية الدليل الإلكتروني :

قبل أن يحكم القاضي الجزائي بالدعوى المقامة أمامه سواء بالبراءة أو الإدانة لابد أن تكون قناعته قد تشكلت عند النطق بالحكم، فلا يستطيع القاضي أن يصل إلى الحقيقة ما لم تكن قناعته بالدليل القائم في الدعوى يقينياً لا احتمالياً، فيقينه بحدوث الجريمة هو أساس العدالة.

ويمكن للقاضي أن يتوصل إلى يقينية الدليل الإلكتروني لإظهار العدالة في المحكمة عن طريق المعرفة الحسية، التي تدركها الحواس، من خلال فحص الدليل الإلكتروني ومعاينته، وعن طريق التحليل والاستنتاج العقلي، من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها، فإن القاضي لم ينته إلى الجزم بنسبة الفعل أو الجريمة المعلوماتية إلى المتهم ألمعلوماتي، وأخيرا يمكن أن يصل إلى اليقين عن طريق استنتاج الظروف المرتبطة بالواقعة، فإما أن يقضي بالبراءة، لأن القاضي لا يحقق العدالة بالشك إنما باليقين الذي يجب أن يتكون لدى القاضي عند الإدانة، أو أن الشك يمكن أن يستفيد منه المتهم المعلوماتي

ويتضح من ذلك أن الدليل الإلكتروني أيا كان شكله سواء اتخذ شكل النصوص أو الأشكال والرسوم أو الأصوات أو النبضات المغناطيسية والكهربائية أو الصور فهو يخضع إلى السلطة التقديرية للقاضي الجزائي، حيث إن القاضي عندما تتشكل لديه القناعة اليقينية بهذا الدليل دون الشك والاحتمال يكون قد حقق العدالة الاجتماعية وأظهر الحقيقة المؤكدة.

أما في الدول التي تأخذ بنظام الإثبات الحر ومنها مصر، فقد قيد القضاء المصري القاضي بضرورة أن يكون اقتناعه يقينيا من أي دليل أو قرينة يأخذ بها،(عفيفي، ٢٠٠٣، ٣٩٠-٣٩١).

أما في أمريكا فقد نصت قوانين بعض الولايات، كما هو الحال في (كاليفورنيا) (وأيوا)، على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تعد أفضل السبل المتاحة لإثبات هذه البيانات، وبالتالي يتحقق مبدأ يقينية المخرجات الكمبيوترية، بيد أن هذا لا يمنع القضاء الأمريكي من استبعاد هذه المخرجات، إذا كانت ناتجة عن حاسب لا يؤدي وظائفه بصورة سليمة، أو كان القائم عليه لا تتوافر فيه الثقة والطمأنينة،(هلالي، ١٩٩٩، ٩٥).

وأما المشرع الأردني فقد أخذ بنظام الإثبات الحر، ومنح بالتالي القاضي الحرية المطلقة في اقتناعه بأي دليل يثبت أو ينفي الجريمة، فلم يقيده بقائمة من الأدلة، إلا في بعض الحالات الخاصة، أما ما عدا ذلك فله حرية الإثبات بكافة الوسائل، وهذا ما نصت عليه المادة (١٤٧) من قانون أصول المحاكمات الجزائية الأردني: (٢- تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات ويحكم القاضي حسب قناعته الشخصية).

وبناءً على ذلك فإن المادة(٩٧) من الدستور الأردني لسنة (١٩٥٢) قد نصت على أن (القضاة مستقلون لا سلطان عليهم في قضائهم لغير القانون)، وعلة هذا المبدأ هو أن يتفق مع أسلوب التفكير العادي والمنطقي في الحياة العادية، وفي البحث العلمي، إذ يستقي الناس الحقيقة من أي دليل ولا يتقيد تفكير الناس بأدلة معينة، ناهيك عن أن إثبات الجريمة بكافة الأدلة، هو الأسلوب الأنجح في الكشف عن الجرائم ومرتكبيها،(السعيد، ٢٠٠٥، ٧١٨-٧١٩).

كما أن القانون الأردني، لم يحدد للقاضي قائمة من أدلة الإثبات، إلا في حالات معينة، كجريمة الزنا مثلا اشترط القانون أن يكون هنا تلبس أو اعتراف بالجريمة، لكنه وضع قاعدة عامة

هي قناعة القاضي دون أن يحدد نوع البينات المقبولة، إلا إذا نص القانون على طريقة إثبات معينة كما في جريمة الزنا، وتطبيقا لهذا نصت المادة(٢/١٤٧) أصول جزائية على (أن تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات ويحكم القاضي حسب قناعته الشخصية)، في حين نصت الفقرة الثالثة على أنه (إذا نص القانون على طريقة معينة للإثبات وجب التقييد بهذه الطريقة).

ويعتنق قانون الإجراءات المصري رقم (٩٥) لسنة ٢٠٠٣ نظام الأدلة الإقناعية، فقد نصت المادة (٣٠٢) منه على أن "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته"، ومع ذلك لا يجوز له أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة، وكل قول يثبت أنه صدر من أحد المتهمين أو الشهود تحت وطأة الإكراه أو التهديد يهدر ولا يعول عليه.

ومفاد ذلك أنه لا قيد على حرية القاضي في اختيار الدليل ، فله أن يأخذ بأي دليل يطمئن إليه، ويطرح مالا يطمئن إليه، فقد يرفض الأخذ باعتراف المتهم لشكه في صحته، وقد يأخذ بشهادة فردية ويطرح شهادة جماعة. وللقاضي أن يجزئ أقوال الشاهد ، ويأخذ ببعضها ويهدر سائرها، وله إذا تعدد المتهمون وإقرار احدهم على نفسه وعلى الآخرين أن يأخذ بأقواله كاملة أو يأخذ بها بالنسبة لبعض المتهمين دون البعض، أو يقصرها على من أقر وحده، ويهدرها بالنسبة للآخرين، والمرجع في ذلك كله وجدان القاضي ومدى اطمئنانه إلى صدق الدليل، ولما كان الأمر يتعلق بوجدان القاضي وهو اعتبار شخصي بحت فإن تقدير القاضي للدليل لا يخضع إلى رقابة محكمة النقض،(عوض، ١٩٩٩، ٦٦٥).

على أن حرية القاضي الجنائي في مجال الإثبات لا يقتصر على تقدير الدليل، بل يتجاوز ذلك إلى تحصيله أيضا، وهذا ما صرحت به المادة ٢٩١ من قانون الإجراءات الجنائية المصري حيث نصت على أن "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة".

وهذا ما نص عليه القانون الأردني من قانون الإجراءات الجنائية الأردني المعدل لسنة ٢٠٠١،

حيث جاء في المادة (١/٢٢٦)على أن "للمحكمة أثناء النظر في الدعوى أن تستدعي من تلقاء نفسها أي شخص للاستماع إلى أقواله كشاهد إذا رأت أن ذلك يساعد على إظهار الحقيقة، ولها إصدار مذكرة إحضار إذا دعت الضرورة لذلك، ولها أيضا أن تسمع شهادة أي إنسان يحضر من تلقاء نفسه لإبداء معلومات في الدعوى".

ويرى الباحث إن قبول الدليل الإلكتروني في الإثبات الجزائي يعد بمثابة تطور لقوانيننا العربية، خاصة أن هذه الدول تأخذ بنظام حرية الإثبات فلا توجد مشكلة من حيث مشروعية الدليل الإلكتروني طالما تم الحصول عليه بطريقة مشروعة على اعتبار أن المشرع لم يقيد القاضي بقائمة أدلة الإثبات، حيث ترك للقاضي حرية تقديرية واسعة.

وطالما هذا الدليل الإلكتروني يصلح لطرحه أمام القضاء فهو دليل له قيمة ثبوتية في إثبات الجرائم المعلوماتية، حيث إنه دليل مادي وملموس بعد استخراجه من على شاشة الحاسب الآلي على ورقة مادية ملموسة، في حين أن يقين هذا الدليل يمكن أن يتحقق عن طريق الخبراء الفنيين الذين لديهم مهارات في التعامل مع جهاز الحاسب الآلي، فلا يوجد ما يمنع الاعتماد على الدليل الإلكتروني في إثبات الجريمة أو نفيها .

الفصل الثالث حجية الدليل الإلكتروني

مع تطور أساليب ارتكاب جرائم نظم المعلومات، تطورت معها وسائل الإثبات، فقد جاءت هذه الأدلة مرتبطة مع هذه الجرائم المعلوماتية، ومع أن الجرائم التقليدية ماتزال تحتل مكان الصدارة وخاصة في الدول العربية، فسوف نبحث حجية هذه الوسائل والأدلة الجديدة في إثبات الجرائم التقليدية، ومدى حجيتها في الجرائم المعلوماتية.

وللوقوف على ذلك فلا بد من التمييز بين الجريمة التقليدية و الجريمة المعلوماتية وخصائص كل منهما ومن ثم البحث في مصادر الدليل الإلكتروني، قبل الوقوف على حجيته في الجرائم التقليدية.

وعليه فسوف نقسم هذا الفصل إلى خمسة بنود وعلى النحو التالي:

أولاً: تعريف الجريمة وخصائصها.

ثانياً: كيفية استخلاص الدليل الإلكتروني ووسائل اكتشافه.

ثالثاً: مدى ملاءمة قواعد الإثبات التقليدية في الجرائم المعلوماتية.

رابعا: دور الدليل الإلكتروني في إثبات الجرائم التقليدية

خامساً: دور الدليل الإلكتروني في إثبات الجرائم المعلوماتية.

أولاً: تعريف الجريمة وخصائصها

يظهر الواقع العلمي وجود نوعين من العمليات الإجرامية، العمليات الإجرامية المعلوماتية والتي ترتكب بوساطة الحاسب الآلي، والعمليات الإجرامية التقليدية وهي العمليات الإجرامية التي يقوم بها الإنسان بوسائل تقليدية، وهذا ما سنبحثه فيما يلي:

١. تعريف الجريمة التقليدية وخصائصها

٢. تعريف الجريمة المعلوماتية وخصائصها.

١.١: تعريف الجريمة التقليدية:

عرف البعض الجريمة التقليدية بأنها "هي الفعل أو الامتناع عن فعل لا اجتماعي بغرض تحقيق غرض إجرامي تقليدي محدد يتمثل في الاعتداء على النفس أو المال أو المصلحة العامة".(موسى، ٢٠٠٥، ١٣).

وعرفها البعض الآخر بأنها "ظاهرة اجتماعية يقصد بها كل فعل يتنافى مع القيم السائدة في المجتمع وهي خطيئة اجتماعية تعارض قيم وأخلاق المجتمع. والجريمة هي كل فعل أو امتناع يصدر عن إرادة مدركة تخرق أمن ومصالح وحقوق الأفراد والمجتمع ويعاقب مرتكبها بعقوبة أو تدبير احترازي"،(نجم، ٢٠٠٢، ١٠).

وتعرف أيضا بأنها"عبارة عن سلوك منحرف يمثل عدوانا على الحقوق أو المصالح التي تحظى بالحماية الجنائية، سواء أكانت حقوقاً أم مصالح خاصة بالأفراد أو متعلقة بالمصلحة العامة للدولة وصون نظمها، وهذا السلوك قد ينطوي على مواقف ايجابية، يتخذها الجاني فيما كان يجب الامتناع عنه، أو مواقف سلبية يتخذها الجاني فيما يجب القيام به"،(إبراهيم، ٢٠٠٩، ١٦٤).

يتضح من ذلك أن الجريمة التقليدية إما أن تكون القيام بفعل أو الامتناع عن الفعل الذي يشكل مخالفة للقانون، مما يؤدي إلى إيقاع العقوبة المناسبة لهذه المخالفة القانونية، وهي جريمة تقع مثلا على النفس أو المال أو المصلحة العامة.....الخ، وبالتالي فهي تقع على القيم والأخلاق السائدة في المجتمع، مما يؤثر سلباً على سير الصالح العام، وحقوق الأفراد، وعلى انتظام الأمن داخل حدود الدولة.

ولهذا السلوك انعكاس مادي ونفسي، تبدأ مظاهره منذ الإعداد للجريمة وتنفيذها وتحقيق نتائجها، ثم التخلص من آثارها، وأدوات ارتكابها، والإفادة من متحصلاتها أو التخلص منها،

وإذا كان الانعكاس المادي يتمثل في ارتكاب الوقائع، وتخلف الآثار المادية الملموسة، وكافة المتغيرات التي تطرأ على ساحة الأحداث، من جراء ارتكابها فإن الانعكاس المعنوي يتمثل في الآثار والانطباعات النفسية، التي انعكست على الخصوم والأطراف الذين واجهوا أحداث الجريمة في أي جانب من جوانبها كمتهمين أو مجني عليهم أو شهود،(إبراهيم، ٢٠٠٩، ١٦٥).

٢.١: خصائص الجريمة التقليدية:

بناءً على ما تقدم فإن الجريمة التقليدية تتميز ببعض الخصائص وتتمثل فيما يلي:

١. الجريمة سلوك إنساني اجتماعي

ولكي تقوم الجريمة لابد من ارتكاب السلوك الاجتماعي المخالف للقانون، حيث إن عدم القيام بهذا السلوك ينفي وقوع الجريمة وبالتالي لن تكون هناك جريمة أصلا، ذلك أن النوايا في العقل لا تكفي لقيام الجريمة التقليدية، إنما يجب على الجاني أن يقوم بفعل مادي ملموس لقيامها،(إبراهيم، ٢٠٠٩، ١٦٤).

٢. نطاق الجريمة

إذا قامت الجريمة وجد الجزاء، لذلك فإن مسرح هذه الجريمة محصور في نطاق جغرافي معين لا يتعداه، كما أن معاينة هذه الجريمة تنحصر في البحث عن الأدلة المادية الملموسة، بيد أنها تترك آثاراً معينة تسهل على رجال الضبط القضائي جمع الأدلة وإثبات الجريمة.(إبراهيم، لات، ٥١).

٣. الجريمة تهديد للمجتمع ولمصالح الأفراد الأساسية

ارتكاب هذا السلوك الإجرامي يؤدي إلى الإخلال بقواعد الأمن والسلامة في المجتمع ولهذه الأهمية تدخل المشرع وجرم المساس بهذه القواعد وفرض الجزاء على مخالفتها،(أبو عامر، ٢٠٠٢، ٧٨).

٤- الجريمة ما يعتبره المشرع مخالفاً لقيم المجتمع ومصالح أفراده الأساسية

وهذه الخصيصة هي ما يضفي على الجريمة في مفهومها القانوني حقيقتها الاجتماعية، ومفادها أن الجريمة تتمثل في انتهاك فعلي لقيم المجتمع، فقد يقف الأمر عند حد تهديد هذه القيم والمصالح، بل إن جرائم الشروع التي تقف عند حد ارتكاب كل أو بعض السلوك المكون للركن المادي دون حدوث النتيجة، تمثل تهديداً للقيمة أو المصلحة المحمية في القاعدة الجنائية،(أبو عامر، ٢٠٠٢، ٨١).

وتجدر الإشارة هنا، أن طائفة من الجرائم التقليدية يشترط فيها أن يكون محل الجريمة له كيان مادي ملموس، وتنبع أهمية هذه الجرائم من خلال معاينة مسرح الجريمة فهي تنحصر في البحث عن الأدلة المادية الملموسة وفي نطاق جغرافي معين، فضلا عن سهولة الإبلاغ عنها نظرا لطبيعتها المادية.

وفي الجريمة التقليدية، فإن دليل الإثبات فيها يكون مرئياً ومن أمثلة 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 وفي كل هذه الأمثلة يستطيع رجل الضبط أو التحقيق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه،(حجازي، ٢٠٠٢، ٣٦).

١.٢: تعريف الجريمة المعلوماتية وخصائصها

أظهرت ثورة المعلومات في العصر التكنولوجي الذي يشهده العالم في الفترة الراهنة أساليب جديدة لارتكاب جرائم تطورت من صورتها التقليدية إلى جرائم تكنولوجية تعتمد على التكنولوجيا الحديثة في إخراج الجريمة إلى حيز الوجود، سميت بالجرائم المعلوماتية، إلا أن هناك من يطلق عليها جرائم الإنترنت أو جرائم الحاسوب أو جرائم نظم المعلومات أو الجرائم الإلكترونية.

ويبدو أنه ونتيجة التطور التكنولوجي فقد ظهر خلاف فقهي حول التعريف الشامل للجريمة المعلوماتية، فمن الفقهاء من يضيق من مفهوم الجريمة المعلوماتية ومنهم من يوسع من مفهومها.

فمن التعريفات التي وضعها أنصار الاتجاه المضيق أن الجريمة المعلوماتية هي"كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى"، كما عرفت بأنها"هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط"، أو هي "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه"،(إبراهيم، ٢٠٠٩، ٧٤).

وعرفها أصحاب الاتجاه الموسع بأنها"كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات يهدف إلى الاعتداء على الأموال المادية أو المعنوية "، وتم تعريفها كذلك أنها"كل سلوك سلبي أم ايجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للإفادة منها بأية صورة كانت"،(المومني، ٢٠٠٨، ٤٩).

وعرفها البعض منهم بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"،(عرب، ٢٠٠٢، ٢١٧).

وتعرف الجريمة المعلوماتية أيضا بأنها "الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة"،(عبد المطلب، ٢٠٠٦، ٤٧).

ولا بد من الإشارة إلى أن ما يهمنا في هذا البحث هو الوصول إلى تعريف للدليل الإلكتروني يكون شاملاً وقادراً على إثبات الجرائم المعلوماتية عموماً، والوصول إلى حجيته في إثبات الجرائم المعلوماتية في ظل التطور المستمر في ثورة المعلومات والتكنولوجيا في المجتمع.

٢.٢: خصائص الجريمة المعلوماتية

ترتبط الجريمة المعلوماتية بجهاز الحاسب الآلي والشبكة العنكبوتية (شبكة الانترنت)، مما يميزها بميزات وخصائص خاصة عن الجرائم التقليدية، وهي:

١-جريمة عابرة للحدود الدولية:

الجريمة المعلوماتية عابرة للحدود الدولية، فهي لا تقف أمام الحدود إنما تعبر حدود أية دولة كانت، فهي ذات طابع دولي ترتكب من أية دولة كانت، وقد تحقق نتيجتها في دولة أخرى، وبذلك يمكن لهذه الجريمة أن تخضع إلى أكثر من قانون جنائي نظراً لطبيعتها الدولية،(هروال، ٢٠٠٦، ٣٨).

مثل هذه الجرائم لا تعترف بالحدود الجغرافية للدولة، بسبب تطور شبكات المعلومات وسهولة انتقال هذه المعلومات، سواء بين الأجهزة الكمبيوترية نفسها أو بين الدول، ومن ناحية أخرى خلقت هذه الجرائم عدة مشكلات أهمها تحديد القانون الواجب التطبيق، بالإضافة إلى دولة الاختصاص، وهذه من أهم المشاكل التي تفرزها هذه الجريمة بشكل عام،(هروال، ٢٠٠٦، ٣٩).

وتأخذ الجرائم المعلوماتية بعداً دولياً، لذلك يمكن أن ترتكب الجريمة في دولة ما عبر الإنترنت وتكون نتيجتها في دولة أخرى، ونظرا لهذه الطبيعة المتطورة التي تشكلها كان لا بد من التعاون الدولي لحماية المعلومات من مجرمي المعلوماتية الذين لا يعترفون بالحدود الدولية، وتوفير جو من التنسيق بين حكومات الدول المتعاونة في هذا المجال وضبط المجرمين الدوليين ومنعهم من استخدام المعلومات عبر الإنترنت، لإخراج جرائمهم إلى حيز الوجود،(المومني، ٢٠٠٨، ٥٢).

١. الحاسب الآلي هو وسيلة ارتكاب الجريمة المعلوماتية:

إن أكثر ما يميز هذه الجرائم عن غيرها من الجرائم التقليدية، استخدام الحاسب الآلي في إخراج هذه الجريمة إلى حيز الوجود، مما يسهل ارتكابها ويجعل من الصعب إثباتها.

ويقصد بالحاسب الآلي "مجموعة من الأجهزة التي تعمل متكاملة مع بعضها بعضا بهدف تشغيل(Process) مجموعة البيانات الداخلة (Input data) وذلك طبقا لبرنامج (Programme) تم وضعه مسبقا للحصول على نتائج(Resultants) معينة"،(قشقوش، ١٩٩٢، ٦).

ويتكون جهاز الحاسب الآلي من كيان مادي ملموس يتمثل في أجهزة الحاسب الآلي المختلفة، مثل وحدات التخزين أو الإخراج أو أدواته المادية مثل الشاشة والسماعات، وكيان آخر ذي طبيعة معنوية تتمثل في البرامج الخاصة بجهاز الحاسب الآلي والبيانات والمعلومات المنقولة بوساطته،(هروال، ٢٠٠٦، ٣٧).

٢. الجريمة المعلوماتية جريمة معنوية:

إن جرائم الكمبيوتر أو المعلوماتية تصنف على أنها من الجرائم التي تتميز عن غيرها من الجرائم التقليدية، بأنها جرائم تستهدف المعنويات والتي تتمثل في البيانات والمعلومات داخل الحاسب الآلي، فهي ليست ماديات ملموسة،(هروال، ٢٠٠٦، ٢٦٤).

٣. أسلوب ارتكاب الجريمة المعلوماتية:

ظهرت الجرائم المعلوماتية في بداياتها عام ١٩٦٠ كجرائم نوعية، بحيث كانت الفئة الوحيدة القادرة على الوصول إلى الحواسيب والشبكات يمكن أن يكون أساتذة الجامعات والطلاب والباحثين، ومع تطورها وازديادها كان لا بد من معالجتها بقوانين حازمة تضبط هذه الجرائم التي أصبحت تستهدف ليس فقط شرائح معينة بل امتدت لتصل إلى الإنسان نفسه بأسلوب هادئ ودقيق (Chuch Easttom, 2010, 33).

يعتبر الإنترنت الحقل الأهم في ارتكاب الجرائم المعلوماتية، ذلك لأنها جرائم هادئة بطبيعتها ترتكب بأسلوب هادئ وسهولة في استخدام الحاسب الآلي، وبالرغم من ذلك يمكن أن تقع هذه الجرائم على شبكة الإنترنت نفسها أو الحاسب الآلي، فقد تكون محلا للجريمة في يد المجرمين المعلوماتيين،

ويتطلب ذلك قدرة فنية ومعرفة شاملة بوظائف الحاسب الآلي وشبكة الإنترنت التي لا تحتاج إلى العنف لإخراج الجريمة إلى حيز الوجود، بل إن المعرفة البسيطة في استخدام هذه الشبكة تؤدي إلى ارتكاب الجريمة بكافة أشكالها،(المومني، ٢٠٠٨، ٥٨).

أما الجرائم التقليدية فهي على خلاف الجرائم المعلوماتية فبعضها يتطلب قدرا من العنف واستخدام المجهود العضلي كما في جريمة القتل أو السرقة أو الإيذاء.....الخ.

٤. صعوبة إثبات الجريمة المعلوماتية:

لا يمكن إثبات الجرائم المعلوماتية عبر الوسائل التقليدية التي تسهم إلى حد ما في عملية الإثبات، لأنها جرائم تستهدف المعنويات ولا تستهدف شيئاً مادياً ملموساً على عكس الجرائم التقليدية، التي تخلف آثاراً مادية تؤدي إلى الكشف عن الجريمة، أما الجرائم المعلوماتية فهي

جرائم قد ترتكب وتأخذ فترة كبيرة قبل أن يتم الإبلاغ عنها مما يؤدي إلى ضياع الآثار المادية إن وجدت، وتكمن صعوبة إثباتها في عدم المعرفة والخبرة العالية في مجال استخدام الحاسب الآلي وبرامجه وأنظمته، وكونها جرائم ترتكب بوساطة الحاسب الآلي والإنترنت، الأمر الذي يشكل حاجزاً بين السلطات وأدلة الإثبات، كذلك تعتمد هذه الجرائم على الذكاء والمهارة العالية في استخدام جهاز الحاسب الآلي، وقد يؤدي عدم الخبرة في استخدام برامجه وأنظمته من قبل السلطات المختصة إلى إتلاف الدليل عن طريق الخطأ أو عدم الدقة والخبرة،(إبراهيم، ٢٠٠٩، ٧٩).

تعتبر هذه الخاصية العقبة الأكبر في جرائم المعلوماتية لما يواجهه رجال الشرطة من صعوبة في إثباتها، وقلة خبرة رجال الشرطة تشكل عائقاً آخر أمام الإثبات، لا سيما أن هذه الجرائم تتطلب حرفية فنية عالية للكشف عنها، في حين أن الفارق الزمني والمكاني والقانوني له دورٌ مهم في تشتيت رجال الشرطة والمحققين، كون مجرمو المعلوماتية يعتمدون على التخفي عبر دروب الإنترنت الخفية،(هروال، ٢٠٠٧، ٤٠).

كما أن الجرائم المعلوماتية تتسم بالخطورة البالغة نظرا لأغراضها المتعددة، ونظرا لحجم الخسائر الناجمة عنها قياسا بالجرائم التقليدية، ونظرا لأنها بذاتها تنطوي على سلوكات غير مألوفة، وبما تتيحه من تسهيل ارتكاب الجرائم الأخرى فإنها تجعل ملاحقة الجرائم التقليدية أمرا صعبا متى ما ارتكبت باستخدام الكمبيوتر،(عرب، ٢٠٠٢، ٢٩٣).

ثانياً: كيفية استخلاص الدليل الإلكتروني ووسائل اكتشافه

يشترط في الدليل الإلكتروني عموما أن يتم الحصول عليه بطريقة مشروعة، ليكون دليل إثبات مقبولاً أمام المحكمة الجزائية، وهذا يقتضي أن تقوم بجمع الدليل الإلكتروني الجهة المخولة من قبل القانون، مع التزامها بالشروط التي يحددها القانون في جمع واستخلاص أدلة الإثبات الإلكترونية، وهنا تثور مسألة دور الدليل الإلكتروني في الإثبات الجزائي، سواء بالنسبة للجرائم التقليدية أو دوره في الجرائم المعلوماتية، كما تبرز مسألة أخرى في مدى انطباق قواعد الإثبات التقليدية على الجرائم المعلوماتية، (سليمان، لات، ٤٢٥).

إن التحقيق في الجرائم المعلوماتية ينطوي على عدة مشكلات وتحديات قانونية خاصة عند ملاحقة الجناة، إذ يجب أن تتوافر لدى خبراء الحاسب الآلي المنتدبين للتحقيق المقدرة الفنية والعلمية في استخدام الحاسب الآلي ويجب التحفظ على وسائل ارتكاب الجريمة المعلوماتية، لسهولة محو الدليل من قبل الجناة إذا ما طالت فترة الملاحقة، وتمكنهم من الوصول إلى قاعدة البيانات التي تحوي الدليل القاطع ضدهم، (حجازي، ٢٠٠٢، ٩٧).

وبناءً عليه سنبين كيفية استخلاص الدليل الإلكتروني من أنظمة الاتصال وأدوات جهاز الحاسب الآلي ووسائل اكتشافه، في بندين وعلى النحو التالي:

١. كيفية استخلاص الدليل الإلكتروني.

٢. وسائل اكتشاف الدليل الإلكتروني.

١. كيفية استخلاص الدليل الإلكتروني

يتم استخلاص الدليل الإلكتروني من خلال الوصول والبحث في أنظمة جهاز الحاسب الآلي وملحقاته، وكذلك البحث في أنظمة الاتصال بالإنترنت، عن طريق الوسائل التي يستخدمها الخبير الفني في اكتشاف الدليل ومعرفة كيفية وقوع الجريمة.

البحث في أنظمة جهاز الحاسب الآلي وملحقاته:

ترتكب الجرائم المعلوماتية عن طريق جهاز الحاسب الآلي، نظرا لطبيعته في نقل البيانات والمعلومات ومعالجتها بطريقة رقمية، فبدون هذا الجهاز لا تكون هناك جريمة معلوماتية أو إلكترونية، فهي جريمة مرتبطة باستخدام هذا الجهاز، والذي من خلاله أيضا يمكن الحصول على الأدلة القاطعة لمواجهة مثل هذا النوع من الجرائم،(عبد المطلب، ٢٠٠٦، ٨٥).

فقد تناولت المحاكم في الولايات المتحدة حالات يتم التوصل بها إلى الدليل الإلكتروني في الجرائم المعلوماتية التي ترتكب عبر الإنترنت، حيث إن رسائل البريد الإلكتروني وحتى الهاتف النقال يمكن فحصها واسترجاعها من مقدم الخدمة إذا ما كانت قد أرسلت مع حفظ الخصوصية التي يتمتع بها المشترك، وعلى ذلك يمكن ارتكاب الجريمة المعلوماتية عن طريق الهاتف النقال باعتباره أداة تنقل المعلومات والبيانات أيضا عبر الإنترنت والاتصالات اللاسلكية،(Orins S.kerr, 2006, 35).

وضبط الأدلة الإلكترونية أو ما يتعلق بجرائم الكمبيوتر والإنترنت يتصل بضبط المكونات المادية لأنظمة الكمبيوتر، وضبط المكونات المعنوية – البرمجيات – وضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الكمبيوترات معا وما يتصل بها،(عرب، ٢٠٠٢، ٥١٩).

وعملية البحث في أنظمة جهاز الحاسب الآلي قد تتم في الجهاز الخاص بالمشتبه به أو المجني عليه أو البريد الإلكتروني، وهذا ما سنوضحه لاحقا:-

١. جهاز الكمبيوتر الخاص بالمشتبه به

ترتكب الجرائم المعلوماتية بوساطة الحاسب الآلي، وبالرغم من عدم تركها آثاراً مادية يمكن أن يستفاد من الجهاز الخاص بالمتهم، إذ يمكن فحص ذاكرة هذا الجهاز واستخلاص المعلومات والبيانات الموجودة فيه والتي قد تساعد في كشف الجريمة، (إبراهيم، ٢٠٠٩، ٢٠٢).

وعندما يقوم الشخص بالوصول إلى صفحات الإنترنت على الجهاز الخاص به يقوم المتصفح بتحميل تلك الصفحة في وحدة التخزين المؤقتة، وهذه المعلومات تنتقل بسرعة اكبر مما يتوقع، الأمر الذي يجعل الكشف عن ارتكاب الجريمة ممكناً، كل هذا يمضي دون اتخاذ أي إجراء (أو حتى معرفة) من يستخدم هذا الجهاز، ويمكن الوصول إلى هذه الملفات بالخبرة العالية ببرامج وأنظمة الحاسب الآلي،(Orin S.kerr, 2006, 10).

٢. جهاز الكمبيوتر الخاص بالمجني عليه

لا بد عند ارتكاب الجريمة أن تنتقل البيانات عبر أجهزة الحاسب الآلي، وعند ارتكابها يجب فحص جهاز المجني عليه سواء أكان شخصاً طبيعياً أم مؤسسة ما، فقد يتم اكتشاف بيانات أو أدلة أخرى تساعد السلطات المختصة في الإثبات،(إبراهيم، ٢٠٠٩، ٢٠٢).

وفي هذه الحالة لا توجد صعوبة في فحص الجهاز محل الجريمة، إذ يجوز ضبط أدلة الجرائم بموجب القواعد التقليدية للتفتيش المنصوص عليها في القانون، وعليه يمكن تتبع المعلومات والبيانات المخفية داخل الجهاز واستخلاص الأدلة أو بداية ظهورها والتي تتيح المجال للمحققين السير نحو الكشف عن باقي الأدلة واكتشاف الجريمة،(حجازي، ٢٠٠٦، ٢١٠).

٣. البريد الإلكتروني

يقصد بالبريد الإلكتروني "جميع تقنيات الاتصال التي تقوم بتناقل المعلومات عبر الوسائل الإلكترونية، مثل: الإنترنت أو نقل النصوص عن بعد"، وفي هذه الحالة يمكن الاستعانة بالبريد الإلكتروني في استخلاص الدليل من حيث التعرف على المعلومات التي تم تناقلها بين الجاني والمجني عليه، وتحديد المشتبه فيه ومكان وجوده سواء أثناء ارتكاب الجريمة أو بعدها،(هروال، ٢٠٠٧، ٢٧٦).

وعندما تسعى الحكومة إلى طلب المعلومات والبيانات الخاصة بالقضية من مزود خدمة الإنترنت فإنه يتم الحصول على محتويات البريد الإلكتروني في الحالات التالية:

١. بناء على مذكرة إحضار مع الحق في تفتيش ومراقبة ومراجعة الحسابات أو المحتويات.

٢. إذا تم توفير إشعار مسبق لمشترك البريد الإلكتروني مما يسمح له فرصة للطعن قبل أن يتم الكشف عن رسائل البريد.

٣. بناء على مذكرة تفتيش فيما إذا كان يعتقد أن البريد الإلكتروني له صلة أو إذا لم يكن أي من السببين السابقين حاضراً(Orin S. kerr, 2006, 39).

إن الكشف عن الدليل الإلكتروني قد يتسم ببعض الصعوبة، نظرا لكثافة ملحقات جهاز الحاسب الآلي، وقلة الخبرة التقنية لدى المحققين الذين يتعاملون في أغلب الأحيان مع الجرائم التقليدية،

وقد يتم الحصول على الدليل الإلكتروني واستخلاصه من مخرجات الطابعات، ومن الأقراص الصلبة أو المرنة وأجهزة التصوير، كذلك يمكن الحصول عليه من برامج معالجة الملفات، وبرنامج معالجة الملفات وهو "برنامج يُمَكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضغوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها"(إبراهيم، ٢٠٠٩، ٢٠٤).

ويمكن فحص الأقراص الخاصة ببدء تشغيل الكمبيوتر التي تتيح للمحققين الدخول إلى جهاز الحاسب الآلي، والذي يكون محمياً بكلمات مرور لا يمكن تشغيلها إلا بإدخال كلمة المرور، حيث يعمل هذا القرص على تشغيل الكمبيوتر دون إدخال لكلمة المرور، وبالتالي فحص هذه الأقراص قد يؤدي إلى نتيجة في الوصول إلى الدليل الذي يمكن أن يدين الجاني،(إبراهيم، ٢٠٠٩، ٢٠٣).

٢.١: البحث في أنظمة الاتصال بشبكة المعلومات (الإنترنت)

يشمل فحص أنظمة الاتصال بشبكة المعلومات العمليات التي تتم في جهاز الكمبيوتر المتصل بشبكة المعلومات، والتي قد تؤدي إلى الحصول على دليل إلكتروني يكشف وقائع ارتكاب الجريمة، ومن هذه الأنظمة النظام الأمني للشبكات ونظام مسار الإنترنت.

١. النظام الأمني للشبكات

إن جهاز الحاسب الآلي المنفرد غير المتصل بأي نوع من الشبكات لا يكون عرضة للاختراق المعلوماتي إطلاقا، وكل ما يمكن أن يتوافر له هو اختراق مادي، بحيث يتصل مرتكب الجريمة هنا بالكمبيوتر المنفرد اتصالا مباشرا(إبراهيم، ٢٠٠٩، ٢١٠).

أما أجهزة الحاسب الآلي المرتبطة بنظام تواصلي عبر شبكات، فإنها تكون أكثر عرضة لاستخدامها في ارتكاب الجرائم واحتوائها على الأدلة الرقمية، خاصة الشبكات غير المحصنة بالتشفير حيث إنها تكون أكثر عرضة للاختراق، ويقصد بالتشفير، طريقة لحماية سرية البيانات، بحيث تستخدم مفاتيح خاصة لتشفير وفك شيفرة بعض البيانات المحصنة بالتشفير، ولا يمكن قراءة هذه المعلومات إلا بوساطة شخص يتوافر لديه مفتاح التشفير الصحيح، وبالتالي إن فحص هذه الأجهزة الأخيرة يتطلب وقتا أكثر للحصول على دليل رقمي، في حين تشكل الشبكات المحصنة بالتشفير ذات وقت أقصر في تحصيل الدليل، لكون الاختراق يبدو واضحا من خلال الكشف الدوري عليها، فيتبين مداه من خلال فحص حركة الدخول هنا(إبراهيم، ٢٠٠٩، ٢١٠).

٢. مسار الإنترنت

يعني مسار الإنترنت "الحركة التراسلية للنشاط الممارس من خلال الإنترنت، فالحاسوب بمجرد أن يتعرف على المسار، يقوم تلقائيا باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات، وهذه هي الحركة التي أشار إليها علماء الإنترنت بأنها تتشابه مع شبكة العنكبوت من حيث عدم انتظام شكل المسار الاتصالي والتواصلي عبرها"(الخن، ٢٠١١، ٣٤٧).

ومن الملاحظ أن ما يتم التوصل إليه بفضل تتبع الحركة العكسية لمسار الإنترنت هو عنوان رقمي فقط، وهذا الدليل الرقمي لا يكفي لنسبة الجريمة إلى مالك الحاسوب، إذ من الممكن إلا يكون هو مرتكب الجريمة، كما لو كان حاسوبه مسروقا، أو أن يكون هناك من يستخدم حاسوبه احتيالا أو أن المشتبه به لا يعرف أي شيء عن الإنترنت، الأمر الذي يتطلب من جهات التحقيق توفير الدليل المادي كالاعتراف أو الشهادة أو الخبرة إلى جانب الدليل الرقمي، حتى يمكن أن تنسب الجريمة إلى مرتكبها(الخن، ٢٠١١، ٣٤٨).

ففي حالة فحص الأنظمة المتصلة بالإنترنت يمكن تتبع البيانات والمعلومات التي قد يكون من شأنها كشف الحقيقة، ونظراً لخطورة الأنشطة الإجرامية المعقدة والتي تنفذ بطريقة دقيقة وذكية، وذلك عن طريق الإسراع في تطوير القدرات الفنية والعلمية لرجال التحقيق، والتي قد تقود إلى الكشف عن مرتكب الجريمة الحقيقي و إدانته أمام المحكمة الجزائية،(الخن، ٢٠١١، ٣٤٧).

٢ . وسائل اكتشاف الدليل الإلكتروني

هناك وسائل يمكن من خلالها الوصول إلى المجرم المعلوماتي والدليل الذي يدينه في ارتكاب الجريمة ومن أهمها:

١.٢ جمع الدليل المستخرج من بروتوكول الإنترنت (TCP/IP)

تنتقل البيانات والمعلومات عن طريق عنوان الانترنت عبر الشبكة المعلوماتية المرتبطة بأجهزة الحاسب الآلي، وبالتالي تنتقل هذه المعلومات وتذهب لأهدافها لنقل أية رسالة تحتوي على البيانات والمعلومات،(إبراهيم، ٢٠٠٩، ١٥٣).

هذا وتوجد أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر، منها على سبيل المثال، ما يستخدم في حالة العمل على نظام تشغيل (Windows) حيث يتم كتابة (Winpcfg) في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP) ، وهو عنوان الانترنت وهو المسؤول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها ، وهو يشبه إلى حد كبير عنوان البريد العادي، مع ملاحظة أن عنوان الانترنت قد يتغير مع كل اتصال بشبكة الانترنت،(إبراهيم، ٢٠٠٩، ٣٠٤).

٢.٢ البروكسي Proxy

البروكسي "Proxy" كلمة انجليزية، تعني الوكيل"، وتقوم مزودات البروكسي بدور الوسيط بين المشتركين لدى إحدى شركات تقديم خدمة الإنترنت، وبين المواقع الموجودة على الشبكة العالمية، أو بدور الوكيل عن هؤلاء المشتركين في طلب المعلومات من تلك المواقع، ونستطيع أن نتخيل مزودات البروكسي كذاكرات كاش كبيرة الحجم، كالتي تستخدم في الحصول على عمليات حسابية كبيرة مثل (الحاسبات)، مهمتها تسريع الحصول على المعلومات،(عبد المطلب، ٢٠٠٦، ٨٣).

وتتميز مزودات البروكسي أن ذاكرة الكاش لديه يمكنها الاحتفاظ بالعمليات التي تمت عليها نقل المعلومات أو المخزنة من خلاله داخل جهاز الحاسب الآلي، مما يجعل منه وسيلة إثبات قوية من خلال إخراج المعلومات المحفوظة عند مزود الخدمة،(عبد المطلب، ٢٠٠٦، ٨٣).

وهناك من الوسائل الإجرائية التي تستخدم في معركة كيفية وقوع الجريمة، فاقتفاء الأثر وتقصي أثر المجرم المعلوماتي من خلال نشر وثائق في المواقع الخاصة بالمخترقين تحمل بين جنباتها معلومات عن الجريمة، كما يمكن الاطلاع على عمليات التنظيم المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم إلى العملاء، ومراقبة المستفيدين والموارد والبرامج التي تعالج البيانات، وتسجيل الوقائع وحالات فشل الدخول إلى النظام،(إبراهيم، ٢٠٠٩، ٣٠٧- ٣٠٨).

ثالثا : مدى ملاءمة قواعد الإثبات التقليدية في الجرائم المعلوماتية

يقصد بالإثبات في المسائل الجزائية، إقامة الدليل لدى المحكمة المختصة على حقيقة واقعة ذات أهمية قانونية، وذلك بالطرق المقبولة قانونا، فالإثبات يهدف إلى إعادة رواية ما حدث من وقائع جرمية أمام القضاء، والإثبات هو العمود الفقري للعدالة الجزائية، فلا يمكن تحقيقها بدون نظام إثبات يضمن تحقيقها،(حسني، ١٩٨٨، ٤٠٥- ٤٠٨).

ترتكب الجرائم المعلوماتية في بيئة خاصة لا علاقة لها بالأوراق والمستندات، إنما تتم عن طريق الحاسب الآلي سواء أكان محلا لها أم وسيلة رئيسة في ارتكابها، حيث كان أول ظهور حقيقي لجرائم الحاسب الآلي في أواخر الستينيات، ويمكن للجاني في هذه الجرائم العبث في بيانات الحاسب الآلي وبرامجه وأنظمته بطريقة فنية وذكية، ويمكن العبث في بيانات ومعلومات داخل الدولة ويكون تأثيرها في دولة أخرى، مما يدلل على صعوبة هذا النوع من الجرائم الحديثة وسرعة وخطورة انتشارها، الأمر الذي يدعو السلطات أن تطور وسائل مكافحتها وتأهيل الخبراء الفنيين للتعامل وبيئة الحاسب الآلي، إذ يمكن من خلالهم كشف الأدلة ومنع انتشار الجرائم،(المناعسة وآخرون، ٢٠٠١، ٢٨٩).

ونظراً لظهور الجرائم المعلوماتية الجديدة في الآونة الأخيرة فإن القوانين الحالية تقف عاجزة أمام الكثير من هذه الجرائم المستحدثة، بسبب عدم وجود النصوص القانونية اللازمة لمواجهة الطبيعة الخاصة التي ظهرت بها هذه الجرائم المستحدثة، وتمثل ذلك في القصور التشريعي لمواجهة كثير من الأفعال التي تهدد حقوق الأفراد والمرتبطة بجهاز الحاسب الآلي.

لقد تبين في بعض الأحوال أن ثمة أفعالاً جديدة ترتبط باستعمال الحاسب الآلي، لا تكفي النصوص القائمة لمكافحتها، ومن ذلك الاعتداء على حرمة الحياة الخاصة، هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص، كما أن التداخل في نظام الحاسب الآلي وتغيير البيانات، قد يشكل صورا جديدة لم يعرفها قانون العقوبات قبل ظهور الحاسب الآلي نفسه، كل ذلك يؤكد قصور القواعد التقليدية في قوانين العقوبات عن مكافحة هذا النوع الجديد من الجرائم،(غنام، ٢٠٠٠، ٦٢٥).

والواقع العلمي للدليل الإلكتروني أنه يتمتع بطبيعة غير مرئية لا تنتج عنه آثارٌ مادية، مما يزيد من الصعوبة التي يواجهها رجال الضبط القضائي والمتمثلة في قصور القواعد القانونية الخاصة بتفتيش الحاسب الآلي خاصةً عندما يكون متصلا بجهاز آخر خارج الدولة، لذلك لا يمكن للمحققين تتبع الدليل الإلكتروني للكشف عن هذه الجرائم الحديثة، وهو يشكل عقبة كبيرة أمام كشفها،(المناعسة وآخرون، ٢٠٠١، ٢٩٣).

إن معاينة مسرح الجريمة المعلوماتية ليس بالفائدة أو الأهمية التي تتمتع بها معاينة مسرح الجريمة التقليدية، فالمعاينة بصورتها التقليدية تنحصر في البحث عن الأدلة المادية الملموسة، في حين أن الأثر الذي يتركه المجرم المعلوماتي، غالبا ما يكون ذا طبيعة معنوية غير محسوسة يصعب التعامل معه عبر الوسائل التقليدية، فعمليات التزوير والاختلاس التي تقع على المحررات الإلكترونية، وبرامج الحاسبات الآلية، لا تترك أثرا ماديا في محتواها، وهناك صعوبة كبيرة في إثباتها، فأغلب البيانات والمعلومات التي يتم تداولها عبر الحاسبات الآلية ومن خلالها تجري العمليات الإلكترونية، هي بطبيعتها رموز إلكترونية مخزنة على وسائط ممغنطة

موجودة في ذاكرة الحاسب الآلي، ويصعب أن تخلف وراءها آثارا مرئية يستدل من خلالها على الجناة،(إبراهيم، لات، ٥٠- ٥١).

ويلاحظ أن عدم وجود النصوص التجريمية التي تجرم الجرائم المعلوماتية الحديثة، وقصور نصوص التجريم التقليدية، يحول دون إثبات هذه الجرائم وبالتالي إفلات الجناة من العقاب في هذه الجرائم، يضاف إلى ذلك عدم وجود كوادر فنية يكون بمقدورها التعامل مع التقنية الجديدة للمعلومات والتطور التكنولوجي في العصر الرقمي.

إن الدراسة التحليلية لمختلف الاتجاهات الفقهية والقضائية أظهرت قصور نصوص التجريم التقليدية السائدة عن الإحاطة بهذه الجرائم المعلوماتية، ومرد ذلك إلى خصائص ثلاث أساسية(عرب، ٢٠٠٢، ٣٨١-٣٨٢):

الأولى: إن جرائم الحاسب الآلي تستهدف المعطيات ذات الطبيعة المعنوية، فعندما يكون الحاسب الآلي هدفا للجريمة فإن السلوك يستهدف المعلومات المخزنة فيه، أو المنقولة منه أو إليه وعندما يكون وسيلة لارتكاب الفعل، فإن السلوك يستهدف بيانات تمثل قيما مالية أو عينية، ويجري الفعل أو السلوك بطرق تقنية في بيئة معنوية وليست في بيئة سلوكات مادية، وعندما يكون بيئة للجريمة فإن محتوى الفعل غير المشروع هو المعلومات غير المشروعة كما هو الحال في جرائم المحتوى المعلوماتي الضار.

الثانية: إن مبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوافر النص القانوني، فلا جريمة ولا عقوبة إلا بنص، ومتى ما انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية الجزائية وتحقق القصور في مكافحة هكذا جرائم.

الثالثة: إن القياس في النصوص الجنائية الموضوعية محظور وغير جائز، ويكاد ينحصر في الحقل الجنائي بنصوص الإجراءات الجنائية كلما كانت أصلح للمتهم، ومؤدى ذلك امتناع قياس

أنماط جرائم الحاسب الآلي على الجرائم التقليدية التي تستهدف الأموال والاعتبار المالي، ومن جهة أخرى لا يصلح القياس على نصوص التجريم والعقاب، كقياس سرقة المعلومات أو سرقة وقت الحاسب الآلي، على الاستيلاء على القوى المحرزة كالكهرباء لتخلف علة القياس، ولأن هكذا نصوص شرعت خصيصا لتطال الأنماط التي تنظمها وهي نصوص خاصة لا يتوسع في القياس عليها وإذا كان الأمر كذلك بالنسبة لبعض النصوص الخاصة فإنه يعد استثناء على أصل والاستثناء لا يتوسع فيه.

وبخصوص النصوص الجنائية التقليدية فقد تضاءل دورها في عملية الإثبات، مما يؤكد ضرورة تطوير النصوص القادرة على مواجهة الجرائم المعلوماتية، فالنصوص الجنائية التقليدية غير ملائمة للتطبيق على جرائم الحاسب الآلي أحيانا، أو أن عقوبتها غير مناسبة ويلاحظ وجود نقص تشريعي في هذا المجال،(قشقوش، ١٩٩٢، ٩٠).

لا تزال السلطات القائمة قادرة على تنظيم السلوك الإجرامي التقليدي في معظم الأماكن، والأهم هو التعاون بين هذه السلطات في العالم لمكافحة الجرائم المعلوماتية التي لا يمكن ايقافها بالوسائل التقليدية، لذلك على كثير من الدول تحديث نصوص قوانينها لتكون قابلة للتنفيذ على الجرائم المعلوماتية مع احترام حقوق الأفراد وحرياتهم،(Report by McConnell International , 2000, 9).

ومن هنا يرى الباحث أنه لا يمكن التسليم بالقواعد التقليدية في إثبات الجرائم المعلوماتية، بسبب طبيعتها الخاصة التي تتمتع بها، فهي جرائم غير مرئية لا يمكن تسليمها للنصوص الجنائية التقليدية التي لا يمكن القياس عليها، وهي تختلف عن الأخرى في الطبيعة أو المحل أو الأركان العامة والخاصة، لذلك يتوجب على المشرع الأردني خاصة والمشرعين العرب عامة، أن يستحدثوا من النصوص الصريحة التي تشمل هذه الجرائم وأن يحددوا العقوبات الخاصة بها، خوفا من قصور القانون من ناحية، ومن إفلات الجناة في هذه الجرائم من ناحية أخرى، واتخاذ الخطوات اللازمة لمكافحتها، من خلال إتاحة الوسائل وإيجاد القوانين وتدريب الكوادر الفنية للتعامل مع هذه الجرائم الخطيرة.

رابعا : دور الدليل الإلكتروني في إثبات الجرائم التقليدية :

ذكرنا أن الجرائم التقليدية هي طائفة من الجرائم التي تستهدف ماديات ملموسة ولا تعنى بالأفكار والمعنويات،

كما أن أدلتها تنحصر في قائمة من الأدلة نص عليها القانون وأوجب عقوبة لكل جريمة، وهي غالبا جرائم محصورة في نطاق جغرافي مما يسهل على المحقق معاينة مسرح الجريمة وجمع أدلتها المادية، أما الجريمة المعلوماتية فهي جريمة ذات طابع خاص، تستهدف المعنويات وليست الماديات وتتم بوساطة الحاسب الآلي، وبالتالي فإن أدلة هذه الجرائم مرتبطة بها، ويتم استخلاصها من خلال فحص جهاز الحاسب الآلي وأنظمته ومكوناته.

ولم تتلاشى طرق الإثبات التقليدية من خلال الشهادة والقرائن والاعتراف والدليل الكتابي والخبرة أمام الجريمة المستحدثة، والتي انضم إليها مؤخرا نتيجة للتطور التكنولوجي وثورة الاتصالات الأدلة الإلكترونية، والمتمثلة في البيانات المستخرجة من أجهزة الحاسب الآلي أو بوساطته

ويعد الدليل الإلكتروني من القرائن القضائية أو الموضوعية وهي "القرائن التي لم ينص عليها القانون، ويمكن للقاضي أن يستخلصها من ظروف الدعوى وأن يقتنع بأن لها دلالة معينة، ويعود أمر تقديرها إلى القاضي"،(الخن، ٢٠١١، ٣١٣).

والدليل الإلكتروني يصلح لإثبات أية جريمة بما يتضمنه من معلومات عنها بأية طريقة، وتتوقف مشروعيته على طبيعة نظام الإثبات، ما إذا كان مقيدا أم حرا، ووفقا للقواعد العامة في القانون الأردني لا يوجد نص صريح للأخذ بالدليل الإلكتروني كدليل لإثبات الجريمة،(الخن، ٢٠١١، ٣٤٢).

في المقابل يوجد نص لكن في القضايا المدنية أو الحقوقية وهو نص المادة (٧) من قانون المعاملات الإلكترونية الأردني، والذي ينص "يعتبر السجل الإلكتروني والعقد والرسالة والتوقيع الإلكتروني منتجاً للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لأطرافها أو صلاحيتها في الإثبات".

وبناءً عليه، فقد أخذ كل من المشرع الأردني و المصري بنظام الإثبات الحر حسب نص المادة (٣٠٢) من قانون الإجراءات الجنائية المصري، الذي يسمح للقاضي أن يختار ما يقتنع به لإثبات الجريمة، وكان مصدرها مشروعا، وبالتالي تترك حرية الإثبات إلى أطراف الخصومة أن يقدموا ما شاءوا من أدلة لإقناع القاضي، الذي يملك الحرية المطلقة في الأخذ بالدليل أو عدم الأخذ به، وأخيرا فإن للقاضي حرية تقدير القيمة الإقناعية للدليل المقدم أمامه فإما أن يقبل به و إما أن لا يأخذ به، كما هو الحال في قانون أصول المحاكمات الجزائية الأردني ، المادة (٢/١٤٧)"تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات ويحكم القاضي حسب قناعته الشخصية"(عفيفي، ٢٠٠٣، ٣٩٠).

خامسا: دور الدليل الإلكتروني في إثبات الجرائم المعلوماتية :

إن الحصول على الدليل الإلكتروني يتطلب قدراً من الذكاء، كما يتطلب قدرة ودراية فنية وتقنية عند استخلاصه لتقديمه إلى القضاء، وحتى يكون الدليل الإلكتروني مقبولا ويأخذ به القاضي بالإدانة أو البراءة يجب أن تتوافر فيه عدة شروط يمكن إيجازها بما يلي:-

١. المشروعية:-

يجب توافر المشروعية عند الحصول على الدليل الذي يثبت الجريمة ، لذلك يجب أن يتم استخلاص الدليل الإلكتروني وفق اجراءات قانونية سواء صدرت من القاضي أو من المتهم عند استجوابه أو من الغير بعد القبض عليه وتفتيشه، حتى يكون الدليل مقبولا أمام المحكمة (سليمان، لات، ٤٢٥).

لذلك لابد من صحة الإجراءات القانونية التي يقوم بها القائمون على جمع الأدلة لتقديمها إلى القضاء، ولابد أن تتمتع هذه الإجراءات بالمشروعية حتى تتفق طريقة جمع الأدلة مع القانون وبالتالي تقديم دليل واضح وصحيح وسليم لا يشوبه أي عيب يجعل منه دليلاً مرفوضاً أمام القضاء.

مناقشة الأدلة الإلكترونية تطبيقا لمبدأ شفوية المرافعة:-

فإذا كانت مخرجات الرسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم، ويترتب على ذلك أن هذه المخرجات سواء أكانت مطبوعة، أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، تكون محلا للمناقشة عند الاعتماد عليها كأدلة أمام المحكمة(إبراهيم، ٢٠٠٩، ١٨٨).

٢. صدور الدليل عن إرادة حرة:-

يجب في الدليل أن يكون خاليا من أي عيب يشوب الإرادة، والحصول عليه بطريقة قانونية دون إرغام أو إكراه سواء على إرادة المتهم أو إرادة الغير.

وعندما يقوم شخص بتهديد شخص آخر عن طريق إرسال الرسائل الإلكترونية إليه، يعتبر هذا التهديد دليلاً على المتهم، بحيث يمكن إرسال الرسائل عبر البريد الإلكتروني مثل التهديد الشفوي لأنه صادر عن إرادة حرة برسالة إلكترونية(Chuck Esttom, 2010, 15).

٣. أن لا يطرأ على الدليل الإلكتروني أي تغيير:-

يمكن للجاني أن يعبث بمحتويات البيانات و المعلومات التي شكلت جريمة خلال انتقالها عبر الشبكة العنكبوتية، لذلك لا بد من التحفظ على الدليل وعدم العبث به حتى لا يكون هناك تغيير فيه ممن قام بجمعه، وأن تتم مراعاة الشروط الواجبة لحفظ سلامة الدليل وعدم العبث به حتى تقديمه إلى المحكمة(الخن، ٢٠١١، ٣٥٧).

أن يكون الدليل الإلكتروني على علاقة بالجريمة المعلوماتية:-

يتعين أن يكون الدليل الإلكتروني المستخرج من الكمبيوتر هو نفس ما هو موجود داخل الكمبيوتر، حتى لا يكون هناك إدعاء بعدم دقة عمل الكمبيوتر، وعدم دقة البيانات المستخرجة منه.

وتجدر الإشارة إلى أن على القاضي أن يكون متيقنا من الدليل المقدم أمامه لاستنتاج الحقيقة بعيدا عن الشك والاحتمال(سليمان،لات، ٤٢٤).

وفي ظل النظم القانونية التي تعتمد على النظام اللاتيني في الإثبات، كالنظام القانوني الأردني، فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته الإثباتية، وهذا النظام يعتمد على الإثبات الحر، إذ يملك القاضي أن يأخذ بأي دليل يقدم في الدعوى المعروضة أمامه، أو أن يرفضه، ففي هذا النظام لا يقيد القاضي بقائمة من الأدلة المنصوص عليها صراحة في القانون، بل يملك السلطة في أخذ الدليل أو رفضه، وهو يعتمد في ذلك على مدى اقتناعه الشخصي بهذا الدليل.

كما أن تقييم الدليل الإلكتروني يلعب دورا هاما من حيث القيمة الإثباتية للدليل، فقد تظهر أخطاء قد تشكك في سلامة الدليل الإلكتروني، سواء من حيث سلامته من العبث، أو من حيث طرق الحصول عليه، إذ يجب الحصول على هذا الدليل بطريقة مشروعة، والتأكد من سلامته وعدم العبث فيه أو تغييره(عبد المطلب، ٢٠٠٦، ١٢٦).

وتجدر الإشارة إلى أن هناك نوعاً من الأدلة الإلكترونية يسمى بالدليل المحايد وهو "الدليل الذي لا علاقة له بالإدانة أو البراءة وإنما تتم الاستعانة به لإثبات أنه لم يتم تعديل أو تغيير في النظام (ألمعلوماتي) بهدف استخدامه أو استخدام محتوياته كدليل"، فمن خلال هذا الدليل المحايد يمكن التأكد من عدم العبث بالدليل الإلكتروني ومطابقته للأصل الذي لم يتم العبث به،

ولا شك أن ثورة التكنولوجيا والتطور العلمي في الكمبيوتر، لها دور في تقديم المعلومات التي تساعد على الفهم والحصول على الدليل الإلكتروني، حتى في حالة عدم الحصول على النسخة الأصلية للدليل الإلكتروني، أو في حالة العبث بها، ففي الإمكان استخدام الكثير من

أنظمة الرياضيات كالخوارزميات للتأكد من أن الدليل لم يتم العبث به أو تعديله(عبد المطلب، ٢٠٠٦، ٩١).

وعادة ما تتبع جملة من الإجراءات الفنية للحصول على الدليل الإلكتروني، والتأكد من سلامة الإجراءات المتبعة في الحصول عليه وتقديمه إلى القضاء، وهي ما تسمى بإجراء اختبار السلبيات الزائفة أو الإيجابيات الزائفة.(عبد المطلب، ٢٠٠٦، ١٣٢).

ويهدف إجراء اختبار السلبيات الزائفة، إلى التأكد من أن الأدوات المستخدمة في الحصول على الدليل، تقدم كافة البيانات المتاحة وتعرض النتيجة النهائية التي تم التوصل إليها، وبنفس القدر يجب أن تكون قادرة على عرض أسماء الملفات المحذوفة، ونسخ كافة البيانات إلى الجهة المرغوب في نسخ البيانات فيها، أما إجراء اختبار الإيجابيات الزائفة، فهي تهدف إلى التأكد من عدم إضافة بيانات جديدة نتيجة لاستخدام الأدوات المعنية، ويعتبر هذا الاختبار من أصعب أنواع الاختبارات، وأكثر الطرق الفنية استخداما للتحقق من أن الأداة المستخدمة لا تؤدي إلى إضافة أو إدخال بيانات جديدة أو استخدام طريقة أخرى للتحقق من النتائج.(عبد المطلب، ٢٠٠٦، ١٣٢-١٣٣).

من خلال ما تقدم يمكن الوقوف على سلامة الدليل الإلكتروني من العبث فيه سواء في تغييره أو حذفه أو التعديل فيه، وإذا توافرت الشروط الواجبة في هذا الدليل المقدم من قبل المتهم أو الغير يمكن للقاضي أن يأخذ بهذا الدليل ليكون قناعته الشخصية في الدعوى المعروضة أمامه،

ولمزيد من التوضيح فسوف نستعرض مدى حجية الدليل الإلكتروني في الإثبات الجزائي في مصر والولايات المتحدة الأمريكية وانكلترا، وعلى النحو التالي:-

حجية الدليل الإلكتروني في القانون المصري:

سار التشريع المصري على نهج التشريعات اللاتينية المتمثلة في القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الايطالي والاسباني وقوانين أمريكا اللاتينية(سليمان، لات، ٤٢٦).

ويعتمد القانون المصري على نظام الإثبات الحر، الذي لا يقيد القاضي بدليل من أدلة الإثبات، بل يترك للقاضي سلطة تقديرية واسعة في تكوين عقيدته، وعليه يمكن للقاضي في مصر أن يأخذ أي دليل يقدم أمامه في المحكمة أو أن يرفضه، ولإطراف الخصومة أن يقدموا للقاضي الأدلة التي تثبت الدعوى أو تنفيها، وللقاضي أن يأخذ في أي دليل وأن يستعين بكافة طرق الإثبات لإثبات الحقيقة وكشف الجاني الحقيقي مرتكب الجريمة،(سليمان، لات، ٤٢٦).

ويقوم القاضي بتقدير كل دليل طرح أمامه، لأن مبدأ الحرية والاقتناع لدى القاضي في تقدير الأدلة قائم، وله أن يستمدها من أي مصدر يطمئن إليه، دون أن يملي عليه المشرع حجية معينة أو يلزمه بإتباع وسائل محددة للكشف عن الحقيقة كقاعدة عامة، ويبين القاضي الأدلة التي اعتمد عليها وكانت مصدرا لاقتناعه، وإذا كان تقديره لا يخضع إلى رقابة النقض، فليس لها أن تراقبه في تقديره، إلا أن لها أن تراقب صحة الأسباب التي استند عليها في تكوين قناعته(إبراهيم، ٢٠٠٩، ١٩٨).

ويرى جانب من الفقه العربي أيضا أن تقدير القاضي، لا يتناول القيمة العلمية القاطعة للدليل، ذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، أما ما يتعلق بالظروف والملابسات التي وجد بها هذا الدليل فإنها تدخل في نطاق تقديره الشخصي،(الخن، ٢٠١١، ٣٦٢).

ويعتبر الدليل المستمد من أجهزة الحاسب الآلي، تطبيقاً من تطبيقات الدليل العلمي، بما يتميز به من موضوعية وحياد وكفاءة في إقناع القاضي الجزائي، فالدليل العلمي ثابت له قيمة قاطعة مثل (البصمة الوراثية وآلات التصوير)، تساعد القاضي في تشكيل قناعته بالدليل المقدم أمامه،(الخن، ٢٠١١، ٣٦٢).

١. حجية الدليل الإلكتروني في القانون الأمريكي:

اعتبر القانون الأمريكي أنه متى ما تحققت مشروعية الدليل الإلكتروني، فإن سجلات الكمبيوتر تخضع إلى أحكام الشهادة السمعية، وقبلت المحاكم سجلات الكمبيوتر في معرض أدلة الإثبات، متى ما أظهرت الشهادة (البينة الشخصية) أن هذه السجلات تقع ضمن مفهوم (الاستثناء المقرر في نظام سجلات العمل الاعتيادي الذي يأخذ حكم السجلات التجارية) فاتجهت هذه المحاكم في ضوء ذلك، إلى قبول سجلات الحاسب الآلي باعتبارها من قبيل سجلات الأعمال المنظمة في معرض العمل الاعتيادي، والتي تأخذ حكم السجلات التجارية بموجب الاستثناء المنصوص عليه في المادة (٦/٨٠٣) من قانون البينات الفدرالي.(عرب، ٢٠٠٢، ٥٠٣).

وقد حسم المشرع الأمريكي حجية الدليل الإلكتروني بالنص عليه صراحة في القوانين الخاصة بالولايات المتحدة الأمريكية، حيث نص قانون الحاسب الآلي لسنة ١٩٨٤ م الصادر في ولاية (أيوا)، على أن مخرجات الحاسب الآلي تكون مقبولة، بوصفها أدلة إثبات بالنسبة لبرامج وبيانات الحاسب الآلي المخزنة في داخله،(إبراهيم، ٢٠٠٩، ١٩٩).

ونص كذلك قانون الإثبات الصادر سنة ١٩٨٣ في ولاية كاليفورنيا، على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب الآلي تكون مقبولة، بوصفها أفضل الأدلة المتاحة في مجال الإثبات، وهذا ما أكده القضاء الأمريكي في أحكامه المختلفة، طالما كان الحاسب المتولد عنه الدليل الإلكتروني يؤدي وظائفه بصورة سليمة، وكان القائم عليه تتوافر فيه الثقة والطمأنينة.(سليمان، لات، ٤٢٨).

ونلاحظ هنا أن المشرع الأمريكي في بعض الولايات أدرك أن الأدلة الإلكترونية، مرتبطة بالجريمة المعلوماتية، التي لا يمكن مكافحتها عبر الوسائل التقليدية، وبالتالي حسم المشرع الأمريكي في بعض الولايات أمر هذا الدليل الحديث المرتبط ظهوره بظهور الجرائم المتطورة نتيجة للثورة المعلوماتية، ونص عليه صراحة في القانون وجعله ضمن أدلة الإثبات المقبولة، وهذا يتفق مع الأساليب والإجراءات اللازمة لمواجهة هذا النوع من الجرائم، إذ يتعين على النظام القانوني ابتداءً أن يقبل بالدليل المستمد من الحاسب الآلي لإثبات الجرائم المرتبطة به.(سليمان، لات، ٤٢٧).

٢. حجية الدليل الإلكتروني في القانون الانجليزي:

في عام ١٩٨٤ صدر في انكلترا قانون الشرطة والإثبات الجنائي، وقد حدد هذا القانون الصلاحيات لشرطة "انكلترا"، كما ركز هذا القانون بصفة أساسية على قبول مخرجات الحاسوب كدليل في الإثبات، حيث حدد المشرع الإنكليزي في المادة (٦٩) من هذا القانون الشروط الواجب توافرها في المستند الناتج عن الحاسوب، حتى يقبل كدليل في الإثبات، وهذه الشروط هي:-

١. عدم وجود أسس معقولة للاعتقاد بأن البيان يفقد الدقة بسبب الاستخدام غير المناسب أو الخطأ للحاسوب.

٢. إن الحاسوب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فإن أي جزء لم يكن يعمل فيه بصورة سليمة، أو كان معطلا عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته.(الخن،٢٠١١، ٣٥٩).

وقد علق مجلس اللوردات على المادة (٦٩) المشار إليها بأنه: "يمكن للشهادة الشخصية الصادرة عن شخص على علم بطريقة تشغيل الحاسوب، أن تعطي الثقة بالدليل، وليس بالضروري أن يكون هذا الشخص خبيرا بالحاسوب"، وبناءً على ذلك قبلت المحاكم الإنكليزية – فيما يتعلق بسلامة نظام الحاسوب – بشهادات أشخاص لديهم علم بطريقة عمل نظام الحاسوب.(الخن، ٢٠١١، ٣٥٩).

ويرى الباحث أنه ومع التطور الحاصل في تكنولوجيا المعلومات وخاصة التطور في أجهزة الحاسب الآلي وقدراته التقنية والفنية، فقد بات من الضروري تدخل المشرع الأردني والعربي بنصوص صريحة تتضمن الإجراءات المتعلقة بقبول وسائل الإثبات الإلكترونية وذلك بهدف حماية المعلومات، كذلك تعديل هذه القوانين بما يمكنها من مواكبة التطور التكنولوجي وسهولة التدخل عند الحاجة.

ويرى الباحث كذلك أن قواعد الإثبات الحالية، غير قادرة على مواجهة هذا النوع الجديد من الجرائم المعلوماتية، الأمر الذي يحتم ضرورة استحداث القوانين الخاصة، والقادرة على مكافحة هذه الجرائم، وعلى المشرع الإسراع بالنص على الأدلة المستخرجة من أجهزة الحاسب الآلي وإعطائها قدرا مميزا في إثبات الجرائم المعلوماتية طالما أمكن الحصول عليها بطريقة مشروعة دون الإخلال بمصالح الأفراد أو المصالح العامة، على غرار ما فعل المشرع الأمريكي حينما نص على الدليل الإلكتروني ووضعه على رأس قائمة أدلة الإثبات.

وعلى ذلك يذكر للمشرع الأردني ما فعل في قانون البنوك الأردني حين نص على الأدلة الإلكترونية وجعلها من الأدلة المقبولة في القضايا المصرفية، وذلك في نص المادة (٢/٩٢) من قانون البنوك الأردني "على الرغم مما ورد في أي تشريع آخر يجوز الإثبات في القضايا المصرفية بجميع طرق الإثبات بما في ذلك البيانات الإلكترونية أو البيانات الصادرة عن أجهزة الحاسوب أو مراسلات أجهزة التلكس".

الفصل الرابع إجراءات الحصول على الدليل الإلكتروني

إن التطور العلمي في عصرنا الحالي خلق كثيرا من المشاكل القانونية تمخض عنها صعوبة مواجهتها بالقواعد والنصوص التقليدية، فقد ظهر القصور في العديد من النصوص والقواعد التقليدية، ومنها القواعد الخاصة بجريمة السرقة العادية التي لا يمكن تطبيقها على جريمة السرقة المعلوماتية، فهي قواعد تحتاج إلى تعديل وتطوير، ولا شك أن تطويرها يجعلها قادرة على مواكبة التطور العلمي الحاصل، وخاصة مكافحة ما ظهر من جرائم جديدة، أفرزها مجرمو المعلوماتية في استخدامهم للثورة المعلوماتية، وأجهزة الحاسب الآلي في ارتكاب جرائمهم بكل سهولة.(منصور، ٢٠٠٦، ٢٦٩).

تعتبر جرائم الحاسب الآلي جرائم مستحدثة، تحتاج إلى قواعد خاصة حديثة للتعامل معها، خاصة مع استحداث وسائل جديدة متطورة في ارتكاب تلك الجرائم، الأمر الذي خلق الكثير من المشاكل العملية وخاصة في مرحلتي جمع الاستدلالات والتحقيق.(عفيفي، ٢٠٠٣، ٣٤٧).

وهذا ما سنعرضه في هذا الفصل بالإضافة إلى بيان مدى قناعة القاضي بالدليل الإلكتروني وعلى النحو التالي:

أولا: إجراءات الحصول على الدليل الإلكتروني في مرحلة جمع الاستدلالات والتحقيق

ثانيا: مدى قناعة القاضي بالدليل الإلكتروني

أولا : إجراءات الحصول على الدليل الإلكتروني في مرحلتي جمع الاستدلالات والتحقيق

يجد محققو الشرطة والأجهزة المعنية بجمع الأدلة أنفسهم في مواجهة مع تحديات تقنية المعلومات، ويضطرون إلى التعامل مع أجهزة الكمبيوتر والاتصالات ومع البرامج وقواعد البيانات متى ما اتصلت بجريمة أو تعلقت بدليل يتصل بهذه الجريمة،

وبالتالي فإن ما يتعين على المحقق عمله في بيئة الحاسب الآلي والإنترنت يتطلب ابتداءً المعرفة الكافية والتدريب العلمي فيما يتعلق بالحصول على

الأدلة، وحفظها لتقديمها إلى المحكمة، لأن الأدلة وإجراءات التحري والتحقيق في بيئة جرائم الكمبيوتر لا يكفيها المعرفة العامة، بل تحتاج تدريبا متواصلا، يتوازن مع التحديات الجديدة في عالم التقنية، وهو تدريب يمتد إلى برمجيات البحث المتقدمة وأجهزة التواصل المعقدة مع النظم ووسائل وآليات كشف الأدلة.(عرب، ٢٠٠٢، ٤٩٩).

١. مرحلة جمع الاستدلالات:

الجرائم المعلوماتية جرائم ذات طبيعة إلكترونية تحتاج إلى أدلة وبيانات ذات طبيعة معلوماتية وفنية، وهذا لا يعني أن إثباتها بوسائل تقنية تقليدية أمر مستحيل، لكن هذه الدراسة تتركز هنا على الأدلة ذات الطبيعة الإلكترونية، لذلك يقوم رجال الضبط القضائي بمرحلة جمع الاستدلالات بمحاولات العثور على الأدلة لإحالتها إلى النيابة العامة والتي بدورها تحيلها إلى المحكمة.

ويلاحظ أن قانون الإجراءات الجنائية الإماراتي ومثله المصري وكذلك الأردني في المواد(٣٠\٢١\٨\٢/)، قد أناط بمأموري الضبط القضائي مهمة تقصي الجرائم، والبحث عن مرتكبيها، وجمع المعلومات والأدلة اللازمة للتحقيق والاتهام، هذه الإجراءات يخولها القانون لمأموري الضبط القضائي، وذلك بعد وقوع الجريمة، وهي بطبيعتها تختلف عن الإجراءات الإدارية المتمثلة في التدابير الوقائية والاحتياطات الأمنية التي ينفذها رجال الشرطة قبل وقوع الجريمة، فجرائم تقنية المعلومات تتطلب من رجال الضبط القضائي، أن يكونوا على قدر ودراية جيدة في الإلمام بطبيعة عمل الحاسب الآلي ونظم تقنية المعلومات ليتمكنوا من مباشرة إجراءات جمع الاستدلالات.(إبراهيم، لات، ٤٧).

والأصل أن تقوم السلطات العامة بمباشرة أعمالها بجمع المعلومات حول الجريمة بمجرد الإبلاغ عنها، نظرا لطبيعتها الخاصة غير المادية والمستترة وصعوبة الدور الوقائي من السلطات لمنعها، فهي جرائم ترتكب بوساطة الحاسب الآلي لا تستطيع السلطات أن تؤدي دوراً ايجابياً في هذا المجال، فهي تتطلب مهارات فنية لا تتوافر في الأشخاص العاديين، وتتمتع بهذه المهارات فئة مهنية متخصصة في مجال الحاسب الآلي والبرامج المعلوماتية وهي تعتبر العقل المفكر، لذلك هي بحاجة إلى حماية كافية وشاملة من القوانين ذات العلاقة لحماية المعلومات من السرقة، فليس بمقدور الوسائل التقليدية إثبات هكذا جرائم،(عفيفي، ٢٠٠٣، ٣٥١).

وفي جميع الأحوال، فإن الإبلاغ عن الجريمة المعلوماتية، سواء أكان فاعلها مجهولا أم معلوما ينبغي أن يتضمن تحديد مكان وقوعها بما يسمح بالدلالة عليها، كوصف موقع أو عنوان الشركة أو البنك الذي تعرض إلى الإعتداء، وتحديد نوع الجريمة المرتكبة، وما إذا كانت اعتداء على مال أو تزوير أو مساسا بالقيم الدينية، وينبغي في الإبلاغ تحديد محل الجريمة لرجال الضبط القضائي المختصين والجهاز الذي وقعت عليه الجريمة وكذلك تحديد الموقع الذي استهدفه الاعتداء.(إبراهيم، لات، ٤٩).

والإبلاغ عن الجريمة حق لكل فرد في المجتمع،من أجل المحافظة على تطبيق القانون واللجوء إلى السلطات العامة عند العلم بوقوع الجريمة أو حتى قبلها، فلا يشترط توافر صفة معينة في الشخص المبلغ، طالما أن الإبلاغ عن الجريمة هو إجراء يهدف إلى المحافظة على النظام ومصالح الأفراد الخاصة والمصلحة العامة، الأمر الذي يستدعي أن يتم الإبلاغ عن أية جريمة للتعامل معها بأسرع وقت ممكن.

وعند الإبلاغ عن وقوع جريمة ما على السلطات العامة ابتداءً التأكد من وقوعها ثم معاينة مسرح الجريمة المعلوماتية للبحث عن أية آثار أو أدلة مرتبطة بها ، مع أن الجريمة المعلوماتية لا تخلف أية آثار مادية ملموسة، على خلاف الجرائم التقليدية التي تترك آثاراً مادية

تسهل على السلطات جمع الأدلة والوصول إلى مرتكب الجريمة بسهولة، أما جرائم تقنية المعلومات فهي تحتاج إلى مهارات فنية خاصة وإلى كوادر مدربة حتى تكون قادرة على معاينة مسرح الجريمة المعلوماتية الذي لا حدود له، فهو منتشر على شبكة الإنترنت العالمية في جميع دول العالم.(إبراهيم، لات، ٥٠).

ولم يحدد المشرع المقصود بالمعاينة، وترك ذلك للفقه حيث عرفها البعض بأنها "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة".(عفيفي، ٢٠٠٣، ٣٥٣).

وتكمن أهمية المعاينة وفعاليتها في تسهيل عمل سلطة التحقيق فيما إذا تمت المبادرة إلى إجرائها كلما سنحت الفرصة لذلك وعلى وجه السرعة، ذلك لأن من شأن المبادرة الانتقال إلى مكان وقوع الجريمة لمعاينته وما قد يوجد به من أشخاص أو أشياء تساعد على جمع الأدلة المترتبة على ارتكاب الجاني لجريمته قبل أن تمتد إليها يد العبث أو قبل زوال معالمها، كما أن السرعة في المعاينة قد يمنح مأمور الضبط الفرصة لمشاهدة المسرح الذي وقعت فيه الجريمة بنفسه وبالتالي يتمكن من تقييم أقوال الشهود وغيرهم حول الجريمة وكيفية ارتكابها وغيرها من الأمور الفنية المتطلبة في التحقيق.(عفيفي، ٢٠٠٣، ٣٥٣).

ويتطلب معاينة مسرح الجريمة المعلوماتية نوعاً من القدرة الفنية والمهارات العالية للتعامل مع الحاسب الآلي، نظرا للصعوبات التي تواجهها أجهزة الأمن في استخلاص الأدلة المستخرجة من الحاسب الآلي، أيضا عجز القدرات الفنية والتقنية لدى أجهزة الأمن، فعلى السلطات المختصة بالمعاينة أن تكون قادرة ومؤهلة للتعامل مع أجهزة ونظم وبرامج الحاسب الآلي حتى تتمكن من جمع الأدلة الخاصة بالجريمة،

خاصة أن هذه الجرائم تزداد بسرعة هائلة وتطور مستمر، على عكس التشريعات التي لا توازيها في السرعة، مما يتطلب ضرورة تأهيل السلطات المختصة وتدريب رجال الأمن على استخدام الحاسب الآلي وإكسابهم الدورات المؤهلة إلى المعرفة والتقنية ببرامجه وأنظمته،(حجازي، ٢٠٠٢، ٨١).

ويجب على سلطات الاستدلال أثناء قيامها بالمعاينة التحفظ على جميع أدوات ارتكاب الجريمة أو ما ينتج عنها، لذلك ينبغي على القائمين على معاينة مسرح الجريمة مراعاة ما يلي.

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

٢. إثبات الطريقة التي تم بوساطتها إعداد النظام والعمليات الإلكترونية، وخاصة ما تحتويه السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام.

٣. إثبات حالة التوصيلات والكيبلات المتصلة بمكونات النظام كله، وذلك لإجراء المقارنة اللازمة عند عرض الأمر على القضاء.

٤. عدم نقل أية مادة متحفظ عليها من مسرح الجريمة قبل التأكد من خلو المحيط الخارجي بموقع الحاسب الآلي من أية مجالات لقوة مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة عليها.

٥. وضع الحراسة على المكان وعدم السماح لأي شخص من الاقتراب من الأجهزة ومكوناتها إلى حين الانتهاء من فحصها أو نقلها إلى الجهة المختصة إذا تطلب الأمر ذلك.(إبراهيم، لات، ٥١).

مما تقدم يتضح أن معاينة مسرح الجريمة المعلوماتية تكتنفها بعض الصعوبات الناتجة عن عدم تخلف الآثار المادية الملموسة، فهي جريمة لا تترك آثاراً مادية بل آثاراً ذات طبيعة معنوية تتمثل في البيانات والمعلومات وهذه تحتاج إلى خبرة فنية لاستخلاصها، على عكس الجريمة التقليدية التي تخلف الآثار المادية سهلة المعاينة وبالتالي جمع الأدلة وإدانة مرتكب الجريمة.

وتجدر الإشارة إلى وجوب تدريب الكوادر والأجهزة الخاصة بسلطات الاستدلال، وتوفير الوسائل والبرامج الخاصة في معاينة الجريمة المعلوماتية، حتى يستطيعوا مواجهة هذا النوع من الجرائم، ومكافحتها بطرق فنية وقدرة عالية على التعامل مع أجهزة الحاسب الآلي، وأنظمته، وبرامجه.

ونظرا للطبيعة الخاصة لجرائم تقنية المعلومات من حيث قدرة الجاني الفائقة على إخفاء أدلة الإثبات، وما يتميز به من احتراف في التعامل مع التقنيات الحديثة في هذا المجال، وعدم تنبه المجني عليهم إلى وقوع الجريمة إلا بعد مرور وقت على ارتكابها، فغالبا ما يكون الفاعل مجهولا أو معلوما ولم يقبض عليه، وفي هذه الحالة، فإن الخطوة التالية هي وضع خطة، للبحث والتحري عن الفاعل أو الفاعلين، وتحديد هويتهم وأماكن وجودهم وضبطهم وتقديمهم إلى جهة التحقيق، على أن يؤخذ في الاعتبار أن طبيعة الأدلة المستمدة من المعالجة الإلكترونية للبيانات يسهل تدميرها وبسرعة كبيرة، وإن كانت الجريمة التي يجري التحري بشأنها مستمرة من حيث نتائجها وتنفيذها، فإن ذلك يتطلب أن يكون المدى الزمني لتنفيذ الخطة قصيرا قدر الإمكان،(إبراهيم، لات، ٥٣).

وكذلك ينبغي على فريق البحث والتحري معرفة ما إذا كان وقوع الجريمة حقيقيا أم لا، فقد ترد بلاغات كاذبة لإثارة البلبلة والإرباك، ثم يجب بعد ذلك معرفة أسلوب ارتكاب الجريمة ليتسنى لفريق البحث كشف غموض الجريمة، وحصرها في فئة معينة، قادرة على ارتكاب الجريمة المعلوماتية بأسلوب معين، فهذا يساعد الفريق على سرعة وسهولة كشف الجاني مرتكب الجريمة وتقديمه إلى الجهات المختصة.

٢. مرحلة التحقيق:

ما يميز إجراءات التحقيق عن إجراءات مرحلة جمع الاستدلالات، أن الأولى يترتب على إجرائها، مساس بحرية الأشخاص وحرمة مساكنهم، لذلك أحاطها المشرع الأردني بضمانات، قيدت حرية رجال الضبط القضائي في إجرائها، واشترط عليهم الحصول على إذن سلطة التحقيق ممثلة في النيابة العامة، وإلا عد الإجراء باطلا، باستثناء بعض الحالات كحالة التلبس، فقد جاء في نص المادة (٨١) من قانون الإجراءات الجزائية الأردني"لا يجوز دخول المنازل وتفتيشها إلا إذا كان الشخص الذي يراد دخول منزله وتفتيشه مشتبها به بأنه فاعل جرم أو شريك أو متدخل أو حائز أشياء تتعلق بالجرم أو مخف شخص مشتكى عليه".

كما جاء في نص المادة (٢/٨٦)"وإذا كان المفتش انثى يجب أن يكون التفتيش بمعرفة أنثى تنتدب لذلك"، وجاء في المادة (١٠٣)من القانون ذاته،"لا يجوز القبض على أي إنسان أو حبسه إلا بأمر من السلطات المختصة بذلك قانوناً".

ومع ثورة تكنولوجيا المعلومات، ودخول الحاسب الآلي إلى حياة الفرد في كافة المجالات، ظهرت الجرائم المعلوماتية التي يكون فيها الحاسب الآلي إما محلا للجريمة المعلوماتية، أو وسيلة لارتكابها، وهذا يستدعي تفتيش هذه الأجهزة الإلكترونية، وضبط الأدلة المستخرجة منها لمواجهة الجاني بها وإدانته.

ويعرف غالبية فقهاء القانون الجنائي التفتيش بأنه إجراء من إجراءات التحقيق يقوم به موظف مختص بهدف البحث عن الأدلة المادية لجريمة وقعت بالفعل (جناية أو جنحة) سواء أكان ذلك في مكان له حرمة خاصة أو لشخص ما، من شأنه أن يفيد في كشف الحقيقة عن الجريمة ومرتكبها.(إبراهيم، لات، ٥٥).

ومع ذلك فإن الحاسب الآلي لا يترك آثاراً مادية بل يخلف آثاراً غير مرئية على عكس الجرائم التقليدية التي يُعنى بها التفتيش وفقا للمفهوم السابق، لأنها تملك آثاراً مادية يمكن اجراء التفتيش عليها، فالبيانات داخل جهاز الحاسب الآلي أو المنقولة عبره لا تتوافر فيها صفة المادة وبالتالي لا يمكن تطبيق إجراءات التفتيش التي تسري على الجرائم في تفتيش البيانات المعنوية داخل الحاسب الآلي

ويرى الباحث أن الحل إنما يتمثل في تعديل النصوص القانونية الخاصة بجمع الأدلة المادية، بحيث يشمل التعديل جمع الأدلة المعالجة إلكترونيا، وتفتيش مخرجات الحاسوب التي تعتبر من الأدلة المعنوية لجرائم الحاسب الآلي.

إن وسائل التفتيش بوجه عام تتصل بالمشروعية الإجرائية، وقانونية الإجراء مدار البحث، وتتعلق بحقوق الأفراد وضمانات الدفاع، وتقف في مقدمة تحدياتها قواعد الخصوصية وحق الأفراد في حماية حرياتهم الخاصة، وعدم التجاوز على حرياتهم من قبل سلطات التحقيق والتحري مما تقدم يتضح انه لا بد من مراعاة شروط محددة في التفتيش، نص عليها قانون أصول المحاكمات الجزائية الأردني في أكثر من موقع، ومنها ما جاء في نص المادة (٨١) أصول جزائية "لا يجوز دخول المنازل وتفتيشها إلا إذا كان الشخص الذي يراد دخول منزله وتفتيشه مشتبها به بأنه فاعل جرم أو شريك أو متدخل أو حائز أشياء تتعلق بالمجرم أو مُخف شخصا مشتكى عليه" وهذه الشروط هي:

١. وقوع الجريمة:

لا يكون هناك أي نوع من التفتيش إلا بوقوع الجريمة بصورة محققة، سواء أكانت هذه الجريمة جناية أم جنحة، فطالما وقعت الجريمة، وجب التفتيش لمعرفة مرتكبها وكشف هويته الحقيقية، لذلك لا يقوم التفتيش لمجرد الاعتقاد بوقوع الجريمة، أو احتمال وقوعها في المستقبل، كما لو جاء اتصال للسلطات المختصة عن جريمة يمكن أن تقع في مكان ما.

وبالنسبة لتفتيش الأشخاص، فالقاعدة العامة في هذا الشأن تقتضي بجواز تفتيش الشخص في الحالات التي يجوز فيها القبض قانونا، وذلك وفقا لنص الفقرة الأولى من المادة (٤٦) من قانون الإجراءات الجنائية المصري، وتتمثل هذه الحالات في حالتين رئيستين هما:

ضبط الشخص متلبسا بارتكاب جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر، فإذا كان المتهم أنثى فلا يجوز تفتيشها إلا بمعرفة أنثى على أن يقتصر ذلك على المواضع التي تعد من قبيل العورات.

١. حالة استصدار إذن من سلطة التحقيق المختصة بالقبض على شخص ما، حيث يجوز لمأموري الضبط القبض عليه وتفتيشه حتى ولو لم يتضمن أمر القبض ما يخوله التفتيش، وفي ذلك يجوز لمأموري الضبط القضائي عند القبض عليه تفتيش مسكن المتهم، ولا يقصد المسكن الدائم إنما يمتد ليشمل أيضا ما يتخذه الشخص لنفسه سواء أكان مسكناً دائماً أم مؤقتاً، طالما ان هذا المكان هو خاص به لا يدخله غيره حتى لو كان عقد إيجار،(عفيفي، ٢٠٠٣، ٣٥٩).

وفي القانون الأردني يمكن أن يتم تفتيش الأشخاص لجمع الأدلة أو المخرجات الدالة على وقوع الجريمة، وهذا التفتيش يشمل ملابس المشتكى عليه، وما يحمله من متاع وأدوات وحقائب، لكن يؤخذ على المشرع الأردني في قانون أصول المحاكمات الجزائية، أنه لم يرتب ضمانات لتفتيش الأشخاص غير ما ورد في المادة (٢/٨٦) من ضرورة تفتيش الأنثى بمعرفة أنثى أخرى تنتدب لذلك، حين نصت "إذا كان المفتش أنثى يجب أن يكون التفتيش بمعرفة أنثى تنتدب لذلك"(المناعسة وآخرون، ٢٠٠١، ٢٧٤).

أما تفتيش مسكن المشتكى عليه فوفقا للقانون الأردني، فقد وردت ضمانات تفتيش مسكن المشتكى عليه في المادتين (٣٦،٨٣) من قانون أصول المحاكمات الجزائية وهذه الضمانات هي:

تجري معاملة التفتيش بحضور المشتكى عليه إن كان موقوفا.

١. إذا تعذر حضوره أو رفض الحضور عندما لا يكون موقوفا، تتم معاملة التفتيش كما يلي:

- بحضور وكيله، أو اثنين من أقاربه (بلا تحديد)

- بحضور شاهدين يستدعيهما المدعي العام لهذه الغاية(المناعسة وآخرون، ٢٠٠١، ٢٧٣).

٢. نسبة الجريمة إلى فاعل معين:

عند وقوع جريمة ما تقوم السلطات العامة بالبحث والتحقيق لمعرفة مرتكبها، وكشف حقيقته لتقديمه إلى العدالة، فهناك ضوابط تتعلق بالتفتيش على هذا الجاني، سواء أكان التفتيش واقعاً عليه شخصيا أم واقعاً على مسكنه، باعتباره فاعلا أو شريكا في الجريمة، أو مساهما بها بأية طريقة كانت، فالتفتيش لهذا الشخص أو لمسكنه لا يتم إلا بمذكرة تفتيش تصدر عن السلطة المختصة بذلك وهي النيابة العامة، وتكون المذكرة متضمنة لاسم الشخص المراد تفتيشه ومكان مسكنه ونوع الجريمة وطبيعتها، أما إذا كان متلبسا بالجريمة فلا يلزم الإذن للتفتيش إنما يكون تفتيشه تلقائيا.

لكن القانون أعطى المدعي العام بصفته ممثلا للنيابة العامة في المادة (٨٢) من قانون أصول المحاكمات الجزائية الأردني صلاحيات إجراء التفتيش، في كافة الأمكنة التي يحتمل وجود أشياء و أشخاص يساعد اكتشافها أو اكتشافهم في ظهور الحقيقة، فقد نصت على "مع مراعاة الأحكام السابقة يحق للمدعي العام أن يقوم بالتحريات في جميع الأمكنة التي يُحتمل وجود أشياء أو أشخاص فيها يساعد اكتشافها أو اكتشافهم على ظهور الحقيقة".

٣. وجود إمارات قوية لوقوع الجريمة:

عند وقوع الجريمة تقوم السلطات المختصة بالإجراءات اللازمة بالكشف عن الجريمة وجمع الأدلة الخاصة بها، وبمجرد خروج الجريمة إلى حيز الوجود يحق للنيابة العامة تحريك دعوى الحق العام، حيث يقوم موظفو الضابطة العدلية باستقصاء الجرائم حتى لو لزم الأمر تفتيش غير المشتكى عليه، لكن وجب أن تكون هناك إمارات قوية دالة على أن شخص معين يخفي أشياء أو يخفي شخصاً ما ممكن أن يساعد في كشف الحقيقة،(المناعسة وآخرون، ٢٠٠١، ٢٧٢).

٣. ضبط أدلة الحاسب الآلي:

الضبط القضائي هو الأثر المباشر للتفتيش، وهو من بين إجراءات التحقيق التي تهدف إلى وضع اليد على الأدلة المتحصلة من التفتيش، وتحريزها وحفظها لمصلحة التحقيق، وضبط الأدلة الإلكترونية أو ما يتعلق بجرائم الكمبيوتر والإنترنت، ويتصل بضبط المكونات المادية لأنظمة الكمبيوتر، وضبط المكونات المعنوية – البرمجيات وضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط أجهزة الكمبيوتر مع بعضها بعضا وما يتصل بها(عرب، ٢٠٠٢، ٥١٩).

إن ضبط الأدلة المتعلقة بجرائم نظم المعلومات، لا يثير أية صعوبة في صلاحية جمع هذه الأدلة إذا كانت الجرائم المعلوماتية واقعة على المكونات المادية لجهاز الحاسب الآلي، إذ يمكن ضبط أدلتها بموجب قواعد التفتيش التقليدية.

أما الأدلة في الجرائم الواقعة على المكونات المعنوية بجهاز الحاسب الآلي، فإن الأمر يثير كثيراً من الصعوبات في جمع أدلتها، التي تتمثل في أدلة غير مرئية ليس لها آثار مادية، فهي عبارة عن بيانات ومعلومات إلكترونية تكون داخل جهاز الحاسب الآلي، فجمع أدلتها يحتاج إلى وسائل فنية وخبرة تقنية عالية لبرامج وأنظمة الحاسب الآلي وملحقاته.

وتكمن صعوبة ضبط الأدلة المعنوية في الجرائم الواقعة على الحاسب الآلي، في قلة الخبرة التقنية والمهارة الفنية في التعامل مع أجهزة الحاسب الآلي، فالشرطة أصلا تتعامل بقواعد التفتيش التقليدية، لذلك لا بد من تدريب السلطات المختصة على تكنولوجيا الحاسبات، كما إن عدم وجود الدليل المرئي يعد من المعوقات التي تقف أمام المحقق الجنائي في ضبط الأدلة التي تعتبر دليلا على ارتكاب الجريمة، وبذلك فهي تمثل عائقا أمام الأجهزة الأمنية في ملاحقة الجريمة وكشف مرتكبها الحقيقي، ولهذا السبب يجب تأهيل السلطات المختصة حتى يستطيعوا الحفاظ على سلامة الأدلة المتحصلة من الجرائم المعلوماتية من تلف أو محو،(حجازي، ٢٢٦،٢٠٠٦).

وبالإضافة إلى هذه الصعوبات فإن هناك صعوبات خاصة لمواجهة الجريمة المعلوماتية عبر الإنترنت، فهذه الجرائم تنبع أساسا من كونها تنتج عن طريقة التعامل أو تداول المعلومات على هذه الشبكة، الأمر الذي يزيد من إرهاق سلطات الضبط ورجال القضاء وهذه الصعوبات تتمثل في الآتي:

١. يشهد قطاع تكنولوجيا المعلومات طفرات وسرعة في الإنتاج الكمي والنوعي، وفضلا عن ذلك فإن الشبكة يمكن لكافة المستويات الاجتماعية والاقتصادية الاشتراك فيها، رغم تباين أسعار الاشتراك عالميا، فإن الخدمة متوافرة للجميع بصرف النظر عن أية اعتبارات أخرى.

٢. عدم وجود قوانين أو نصوص دستورية تجرم هذا النوع من الجرائم كونها لا تزال من الأفعال ذات الطابع الحديث في الشكل والمضمون.

٣. عدم وجود قضاء متخصص في الجرائم المعلوماتية.

٤. وجود بعض المواقع على شبكة الإنترنت تسهل إرسال الرسائل دون تحديد اسم المرسل، مما يؤدي إلى صعوبة الكشف عن المرسل الحقيقي لهذه الرسائل.(حجازي، ٢٠٠٢، ٨٧).

٥. صعوبة السيطرة على المشتركين، فلا توجد ضوابط دولية أو محلية تحدد فئة أو هدف المستخدم، لذلك توجد نسبة كبيرة من محترفي الجريمة المعلوماتية هدفهم اللهو.

لذلك يجب عقد الدورات التدريبية للأجهزة المختصة بمرحلة الاستدلال والتحقيق لاكتسابهم المهارات والقدرة الفنية والتقنية في التعامل مع هذه الأجهزة وبالتالي معاملة الجرائم المعلوماتية بنفس الصفة، ونفس الطبيعة الخاصة التي تتميز بها، في حين أن التدريب واكتساب المهارات يسهل في اكتشاف الأدلة الإلكترونية، وكشف الجناة وتقديمهم للمحاكمة، وذلك مع توفير الوقت والجهد للكشف عن الأدلة وإدانة مرتكبي هذا النوع من الجرائم.

وقد نص المشرع الأردني في قانون جرائم أنظمة المعلومات المؤقت لسنة ٢٠١٠ على تجريم الجريمة المعلوماتية، فقد جاء في المادة (١٣) من (الفقرة أ) على أنه "مع مراعاة الشروط والأحكام المقررة في التشريعات ذات العلاقة، يجوز لموظفي الضابطة العدلية الدخول إلى أي مكان يشتبه باستخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل المشتبه في استخدامها لارتكاب أي من تلك الجرائم، باستثناء بيوت السكن إلا بإذن من المدعي العام المختص قبل الدخول إليها وذلك لحماية خصوصية بيت السكن وحماية خصوصية ساكنيه، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك، ويقدمه إلى المدعي العام المختص".

لذلك لا بد من إعادة النظر في النصوص والقوانين الحالية، كذلك استحداث النصوص اللازمة لكشف مثل هذه الأدلة، والنص عليها صراحة وضمها إلى قائمة أدلة الإثبات، فجرائم نظم المعلومات لها طبيعة خاصة تحتاج إلى أدلة ذات طبيعة قابلة للتعامل معها، والجرائم المعلوماتية توجب لكشفها وإدانتها أدلة نابعة من نفس الطبيعة، حتى تكون دليلاً مباشراً وقاطعاً تستطيع المحكمة الأخذ به لإدانة الجناة وتحقيق العدالة.

ويرى الباحث أن الحاجة باتت ملحة إلى إعادة صياغة التشريعات الخاصة بالضبط والتفتيش في جرائم تقنية المعلومات بما يشمل الحفاظ على البيانات والمعلومات الإلكترونية والشخصية أيضا، يوجب حماية حقوق وحريات ومصالح الأفراد من ناحية، ومكافحة هذا النوع من الجرائم التي أوجدت تحديات خاصة لسلطات الاستدلال والتحقيق، وبذلك فهي تحتاج إلى قواعد تنظم هذه الإجراءات التي فرضتها هذه الجرائم في ظل قصور القواعد التقليدية، ويقترح الباحث أن يتم إنشاء مراكز لتدريب

وتأهيل سلطات الاستدلال والتحقيق على ضبط هكذا أدلة، خاصة أن هذه السلطات لا تتعامل معها بتقنية بل عن طريق الوسائل التقليدية، كما يجب تدريب القضاة وتأهيلهم بقدرات عالية خاصة في تقدير الأدلة الناتجة عن هذه الجرائم الحديثة.

ثانيا: مدى قناعة القاضي الجزائي بالدليل الإلكتروني

إن هدف عملية الإثبات هي الوصول إلى اقتناع القاضي الجزائي بالدليل المقدم أمامه وإظهار الحقيقة، والقاضي يسعى هو أيضا إلى إظهار الحقيقة بما يستطيع الحصول عليه من أدلة قاطعة سواء بالإدانة أو البراءة، حتى يتسنى له أن يحكم بما تقتضيه العدالة، فحكم القاضي في الواقعة محل الدعوى يجب أن يكون مبنيا على الجزم واليقين، وأن لا يكون مبنيا على مجرد الشك أو الاحتمال.

وتتميز الأدلة في المواد الجنائية بأنها متساندة، واعتمادها على الجزم واليقين، بمعنى ضرورة أن تؤدي إلى التسليم بموضوع الجريمة وصحة إسنادها إلى المتهم استنادا لا يقبل الشك، وبالتالي يكون الدليل ثابتاً وقاطعاً أمام القاضي الجزائي، وفي سبيل ذلك قد يتخذ الدليل شكل الدليل النفسي المنطبع في النفس مثل انطباعات الوعي والإدراك لدى الشاهد الذي شاهد الجريمة، وقد يتخذ شكل الأثر المنطبع في شيء مثل الإصبع للجاني أو الرائحة التي تفوح من مسدسه لتدل على أنه أطلق منها طلقات في ذات الوقت الذي وقعت فيه الجريمة، وأخيرا قد يتخذ شكل الأثر المتجسد في شيء ما مثل المخدر أو النقد المزيف.(سليمان، لات، ٤٢٤).

لذلك فإن اقتناع القاضي يرتبط بنظام الإثبات الجنائي المعمول به، والذي يكتسب أهمية كبيرة في مجال الإجراءات الجنائية، والإثبات هو إقامة الدليل والوقوف على حقيقة الوقائع التي نتجت عن الجريمة، وبناءً على نظام الإثبات المتبع يكون القاضي اقتناعه من الدليل المطروح أمامه، إما بناءً على نظام الإثبات المقيد والذي يقيد القاضي بقائمة من الأدلة التي لا يجوز له تجاوزها، أو نظام الإثبات الحر والذي يملك فيه القاضي الحرية في الأخذ بأي دليل يراه مناسبا.

ويمكن للقاضي أن يأخذ بهذا الدليل سواء بالإدانة أو البراءة، لذلك يجب أن يتصف هذا الدليل بالمشروعية، أي مشروعية الحصول عليه، وأن يكون صادراً عن إرادة حرة دون أي اعتداء على إرادة المتهم أو الغير ودون إكراه في الحصول عليه، كذلك لا بد أن يكون هذا الدليل متعلقا بالواقعة محل الدعوى التي ينظر بها القاضي.(الخن، ٢٠١١، ٣٦٣).

مما تقدم نخلص إلى القول بأن الجرائم المعلوماتية جرائم ذات طبيعة خاصة، تحتاج إلى أدلة من ذات الطبيعة حتى تكون قادرة على إثبات جرائم الحاسب الآلي، فلا بد من وجود مثل هذه الأدلة حتى يستطيع القاضي التعامل مع مثل هذا النوع من الجرائم، فلا يمكن إثباتها بقواعد الإثبات التقليدية، لكون هذه الجرائم لا تخلف أي دليل مرئي وراءها، وبالتالي تحتاج إلى نوع من الأدلة قادرة على التعامل معها، والقاضي يحكم بناء على الدليل الذي يستمد منه قناعته الشخصية، فلا يمكن إثبات جريمة السرقة المعلوماتية المرتكبة عن طريق أجهزة الحاسب الآلي بالاعتماد على القواعد التقليدية للإثبات.

وتجدر الإشارة إلى أن القضاة خاصة في الدول العربية لا يتعاملون مع هذا النوع من الجرائم بنفس الطريقة المتبعة في الإثبات، فهو ليس متمرسا على التعامل مع مثل هذه الجرائم لأنها جرائم حديثة ليست منتشرة انتشارا واسعا كما هي في دول أخرى،

الأمر الذي يجعل من الضرورة تدريب القضاة وتأهيلهم لاكتساب المهارات والخبرات العالية في التعامل مع الجرائم المعلوماتية، خاصة في تقديرهم لدليل الإثبات فلا يمكن إقناع القضاة بهذا الدليل دون أن تتوافر لديه المعرفة والتقنية في مجال الحاسب الآلي والأدلة المتحصلة منه، (حجازي، ٢٠٠٦، ٢٢٦).

لقد اكتسبت وسائل الإثبات الإلكتروني مكانة هامة في إثبات الجرائم المعلوماتية، لأن المعلومات والبيانات التي يتم تداولها وحفظها عبر الحاسب الآلي وشبكة الانترنت يمكن التمسك بها في ساحات المحاكم، ويجوز للقاضي الارتكان إليها والثقة بها في النزاع المعروض عليه، شريطة أن يتم تسجيلها بأسلوب منظم وبطريقة جديدة ومأمونة، وإن كان ذلك لا يغلق الباب أمام احتمال وجود خطأ أو عيب في عملية نقل المعلومات والبيانات سواء من جانب المصدر أو أثناء عملية النقل والاتصال،(منصور، ٢٠٠٦، ٢٧١).

ونظرا للطبيعة الخاصة التي تتمتع بها جرائم تقنية المعلومات، فيجب على القاضي أن يكون مدركا لهذه الطبيعة، فلا يقرر أحكاما لا تتفق وطبيعة هذه الجرائم، ولكون هذه الأدلة المتحصلة من أجهزة الحاسب الآلي أقوى وأفضل الأدلة في إثبات الجرائم المعلوماتية، فلا بد للقاضي من الأخذ بها في مجال الإثبات لقصور غيرها من الأدلة التقليدية في إثبات مثل هذه الجرائم، والقاضي يقتنع بأي دليل يقدم أمامه في الدعوى طالما أنه مشروعٌ، لا يخالف القانون، ولا يشوبه عيب من عيوب الإرادة،(سليمان، لات، ٤٢٥).

الفصل الخامس الخاتمة

من المسلم به عدم إمكانية التعامل مع جرائم تقنية المعلومات من خلال القواعد التقليدية وحدها، فهي غير قادرة على التعامل مع جرائم ذات طبيعة خاصة، أي الطبيعة الإلكترونية التي تتميز بها، فهذه الجرائم تحتاج إلى قواعد خاصة ذات طابع تقني إلكتروني حتى تستطيع التعامل مع أدلتها، لأن الدليل الإلكتروني هو من ذات الطبيعة وهو أفضل الأدلة القادرة على إثبات الجرائم المعلوماتية، ومخرجات الحاسوب هي أفضل أدلة الإثبات في الجرائم المرتكبة بوساطة هذا الحاسوب.

إن ظهور التقنية المعلوماتية والتقدم التكنولوجي أظهر هذا النوع الجديد من الجرائم، وهي الجرائم المعلوماتية والتي أصبحت تمثل تهديدا مباشرا للأمن والاستقرار في العالم بأسره، فقد أصبح مجرمو المعلوماتية يستخدمون التقنيات الحديثة والوسائل الإلكترونية لارتكاب جرائمهم، الأمر الذي يوجب ضرورة التصدي إلى هذه الجريمة وبنفس الوسائل الإلكترونية المستخدمة في ارتكاب الجريمة، ومن خلال الدراسة السابقة فقد توصل الباحث إلى عدد من النتائج والتوصيات تتمثل فيما يلي:

أولا: النتائج:

من خلال دراستنا فقد توصلنا إلى عدد من الاستنتاجات أهمها:

- إن الدليل الإلكتروني هو عبارة عن بيانات رقمية داخل الحاسب الآلي أو منقولة عبره، الأمر الذي يتيح جمع هذه البيانات والمعلومات وتحليلها عن طريق البرامج الخاصة وذلك:

-باستخراج هذه المعلومات لتصدر على شكل رسوم ونصوص أو أصوات وصور، وبالتالي يمكن استخدامها كدليل ضد الجاني أمام المحكمة.

-يمكن تقسيم الدليل الإلكتروني إلى بيانات ومعلومات مخزنة داخل الحاسب الآلي نفسه بحيث يمكنها الانتقال من كمبيوتر إلى آخر، وبيانات منقولة عبر جهاز الحاسب الآلي وهي بيانات تتمتع بقوة ثبوتية ضد مرتكب الجريمة.

-إن سهولة محو الدليل الإلكتروني يفسح المجال للمحققين الفنيين في سرعة ضبط الدليل، كما أن محاولة الجاني محو الدليل يعد محاولة منه لإتلاف الدليل أو تعطيله، أي أن كشف محاولة الجاني محو الدليل تتخذ بذاتها دليلا ضده في المحكمة.

-إن الأخذ بالدليل الإلكتروني يتوقف على نظام الإثبات المعمول به. فهناك نظام الإثبات المقيد الذي يقيد القاضي بقائمة من الأدلة، ونظام الإثبات الحر الذي يعطي القاضي سلطة واسعة في تقدير الدليل المقدم أمامه. والقانون الأردني أخذ بنظام الإثبات الحر الذي يعطي القاضي سلطة مطلقة في تقدير دليل الإثبات.

-إن القانون الأردني لم ينص صراحة على الدليل الإلكتروني كدليل إثبات إنما أعطى القاضي حرية تقدير هذا الدليل حسب ما يراه في الدعوى المنظورة أمامه فله أن يرفضه أو أن يأخذ به كدليل إثبات يدين الجاني.

-عدم ملاءمة قواعد الإثبات التقليدية في إثبات هذا النوع من الجرائم، لأن الجرائم المعلوماتية تختلف عن نظيرتها التقليدية في أركانها وطبيعتها الأمر الذي يحول دون تطبيق القواعد التقليدية على الجرائم المعلوماتية التي تتمتع بطبيعة خاصة، فهي جرائم لا تخلف وراءها آثارا مادية بل غير مرئية يصعب التعامل معها، ولذلك فإن هذا النوع من الجرائم تحتاج إلى الخبرة الفنية والتقنية لاستخلاص الدليل الإلكتروني واعتباره دليل إثبات.

-يمكن في بعض الحالات إثبات الجريمة التقليدية بغير القواعد التقليدية، لأن الدليل الإلكتروني يصلح لإثبات أية جريمة سواء أكانت من الجرائم التقليدية أم من الجرائم المعلوماتية.

-ينبغي أن يكون الدليل الإلكتروني مشروعا وصادرا عن إرادة حرة، كما يجب عدم التغيير أو العبث فيه حتى يكون دليلاً مقبولاً تأخذ به المحكمة في إدانة مرتكب الجريمة.

-يقوم رجال الضابطة العدلية بعملية جمع الاستدلالات والتحقيق، فيجوز لهم الدخول إلى أي مكان يشتبه باستخدامه لارتكاب الجريمة، ويجوز لهم تفتيش الأدوات والبرامج والوسائل المشتبه في استخدامها لارتكاب الجريمة المعلوماتية، كما يمكنهم تفتيش بيوت السكن بإذن من المدعي العام المختص، حماية لحرمة السكن وحرياتهم الشخصية.

ثانيا: التوصيات:

أما أهم التوصيات التي توصل إليها الباحث فهي:

١. ضرورة النص صراحة على الدليل الإلكتروني كدليل إثبات وإضافته إلى قائمة الأدلة، لأن قلة الخبرة والدراية العالية ببرامج وأنظمة الحاسب الآلي تؤدي إلى عدم اليقين بالأدلة الإلكترونية المستخرجة من الحاسب الآلي، وحتى تكون إجراءات رجال الضابطة العدلية في استخلاص الأدلة تتسم بالمشروعية.

٢. ضرورة النص على الوسائل والأدوات المستخدمة للتأكد من سلامة الدليل الإلكتروني، لأن الدليل الإلكتروني يشترط فيه أن يكون مشروعا وأن لا يطرأ عليه أي تغيير أو عبث.

٣. ضرورة إنشاء المؤسسات التدريبية والتأهيلية للأجهزة المختصة التي يقع على عاتقها التعامل مع هذه الجرائم الجديدة، مع إمكانية اكتسابهم الخبرات الفنية والتقنية عبر هذه المؤسسات التدريبية للتعامل مع أجهزة الحاسب الآلي ومع هذا النمط المستحدث من الجرائم.

٤. إنشاء جهاز متخصص بملاحقة الجرائم المعلوماتية يتبع للأجهزة الأمنية أو للنيابة العامة، بحيث يتم تدريب أفراد هذا الجهاز وتأهيلهم على التعامل مع الأنظمة والبرامج المعلوماتية وإمكانية تفتيش أجهزة وأنظمة الحاسب الآلي وضبط محتوياته.

٥. ضرورة تدريب الأجهزة المختصة بضبط الدليل، وتدريب القضاة على هذه الجرائم المعلوماتية لقلة التعامل معها وإكسابهم الخبرة والمهارات العالية ببرامج وأنظمة الحاسب الآلي، فهم غير قادرين على التعامل مع الجريمة المعلوماتية بقدر درايتهم بالجرائم التقليدية الأكثر انتشاراً خاصة في البلاد العربية.

٦. إيجاد قواعد بيانات لدى المراكز المتخصصة تعنى بالجرائم المعلوماتية، تتضمن دليلا إحصائيا يظهرها في السجلات الرسمية وإظهار السبل الكفيلة بملاحقة هذه الجرائم وإثباتها وبيان حجمها، فمن المسلم به أن هذه الجرائم لا تظهر ضمن السجلات والإحصاءات الجرمية الصادرة عن السلطات المختصة.

٧. ضرورة نص القوانين على إجراءات لتفتيش الحاسب الآلي وبرامجه حتى يتسنى لرجال الضابطة العدلية استخلاص الأدلة بطريقة مشروعة، أيضا لضبط المعلومات داخل الجهاز مع أخذ الحيطة والحذر عند التفتيش داخل الجهاز للحفاظ على الأسرار الخاصة داخله.

وبهذه النتائج والتوصيات يختتم الباحث دراسته، والتي تعتبر لبنة أساسية متواضعة، يمكن البناء عليها مستقبلا بدراسات أكثر تفصيلا وتعمقا، لا سيما مع تطور وسائل التكنولوجيا المستخدمة في ارتكاب الجريمة المعلوماتية، كما وأنها تفتح آفاقا واسعة للجادين والمهتمين للكتابة في الموضوعات ذات الصلة بهذا الجانب.

المصادر والمراجع

١. المؤلفات القانونية:

إبراهيم، خالد ممدوح. الجرائم المعلوماتية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩.

إبراهيم، خالد ممدوح. فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩.

أبو عامر، محمد. القسم العام في قانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٢.

أحمد، هلالي عبد الإله. الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٣.

أحمد، هلالي عبد الإله. حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، ١٩٩٩.

الخن، محمد عبد الرؤوف. جريمة الاحتيال عبر الانترنت، ط١، منشورات الحلبي الحقوقية، ٢٠١١.

الكسواني، عامر. التجارة عبر الحاسوب، ط١، دار الثقافة، عمان، ٢٠٠٨.

المومني، نهلا. الجرائم المعلوماتية، ط١، دار الثقافة، عمان، ٢٠٠٨.

المناعسة، أسامة، وجلال الزعبي وصايل الهواوشة. جرائم الحاسب الآلي والانترنت، ط١، دار وائل للنشر، عمان، ٢٠٠١.

حجازي، عبد الفتاح بيومي. الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ط١، منشأة المعارف، الإسكندرية، ٢٠٠٩.

حجازي، عبد الفتاح بيومي. الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، ٢٠٠٥.

حجازي، عبد الفتاح بيومي. التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٨.

حجازي، عبد الفتاح بيومي. الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، ط١، منشأة المعارف، الإسكندرية، ٢٠٠٩.

حسني، محمود نجيب. شرح قانون الإجراءات الجنائية، ط٢، دار النهضة العربية، ١٩٨٨.

سعيد، كامل. قانون أصول المحاكمات الجزائية، دار الثقافة للنشر، عمان، ٢٠٠٥.

سلامة، محمد أبو بكر. جرائم الكمبيوتر والانترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦.

سليمان، أيمن عبد الحفيظ. إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، لاط ، لات.

سليمان، أيمن عبد الحفيظ. الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، لاط ، ٢٠٠٥.

عبد المطلب، ممدوح عبد الحميد. البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦.

عرب، يونس. دليل أمن المعلومات والخصوصية الجزء الأول جرائم الكمبيوتر والانترنت، ط١، منشورات اتحاد المصارف العربية، ٢٠٠٢.

عفيفي، كامل عفيفي. جرائم الكمبيوتر، منشورات الحلبي الحقوقية، الإسكندرية، ٢٠٠٣.

عوض، محمد عوض. المبادئ العامة في قانون الإجراءات الجنائية، ١٩٩٩.

كحلون، علي. المسؤولية المعلوماتية، مركز النشر الجامعي، تونس، ٢٠٠٥.

مصري، عبد الصبور عبد القوي علي. الجريمة الالكترونية، دار العلوم للنشر والتوزيع، القاهرة، ٢٠٠٨.

منصور، محمد حسين. الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.

موسى، مصطفى محمد. أساليب إجرامية بالتقنية الرقمية ماهيتها...مكافحتها، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٥.

نجم، محمد صبحي. أصول علم الإجرام والعقاب، ط١، دار الثقافة والدار العلمية والدولية للنشر والتوزيع، عمان، ٢٠٠٢.

هروال، نبيلة هبة. الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.

٢. الرسائل الجامعية:

قشقوش، هدى. جرائم الحاسب الآلي في التشريع المقارن، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، دار النهضة العربية، القاهرة.

٣. الأبحاث والندوات:

إبراهيم، راشد بشير. التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية في إمارة أبو ظبي، ط١، مركز الإمارات للدراسات والبحوث الإستراتيجية أبو ظبي ، ٢٠٠٠.

غنام، محمد غنام. عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم لمؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات، مايو، ٢٠٠٠.

٤. القوانين:

قانون البينات الأردني المعدل رقم ٣٧ لسنة ٢٠٠١.

قانون أصول المحاكمات الجزائية الأردني المعدل رقم ١٦ لسنة ٢٠٠١.

قانون الإجراءات الجنائية المصري المعدل رقم ٩٥ لسنة ٢٠٠٣.

قانون البنوك الأردني رقم ٢٨ لسنة ٢٠٠٠.

المراجع باللغة الأجنبية :

1. Orin S. Kerr Page , Computer Crime Law, 0314144005, West Group, 2006

2. Chuck East tom, Computer Crime, Investigation, and the Law, 1st Edition, B003MAJU7Y,Delmar Learning,2010

3. Cyber crime and punishment? Archaic laws threaten global.