دور الخبرة في إثبات المعاملات الإلكترونية والقواعد الفنية التي تحكمها في اكتشاف الدليل الرقمي

The role of experience in proving electronic transactions and the technical rules governing them in the discovery of digital evidence

تاريخ الاستلام : 2020/04/30 ؛ **تاريخ القبول :** 2022/02/13

[1] * طالب دكتوراه. تقي مباركية

[2] د. فاطمة الزهراء غريبي

1 كلية الحقوق والعلوم السياسية، مخبر بحث الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر.
2 كلية الحقوق والعلوم السياسية، مخبر بحث الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر.

ملخص

لقد ترتب عن التطور التقني في نظم المعالجة الآلية إلى تغيير كبير في المفاهيم السائدة حول الدليل، وقاد مثل هذا القول في الحقيقة إلى تعاظم دور الإثبات العلمي وإعلان انضمام الخبرة التقنية إلى عالم الخبرة القضائية، ذلك أن اشتقاق الأدلة الرقمية المطلوبة في إثبات الجرائم المعلوماتية وكشف أنماطها أمر يضطلع به الخبراء المتخصصون في هذا المجال، ولا يمكن التصور أن يرفض القاضي اللجوء إلى ندب خبير في قضايا تقنية المعلومات، إذ هي قضايا فنية تتطلب خبرة خاصة، ويكون حكمه مجانبا للمنطق العلمي ومعيبا إذا لم يستند إلى الخبرة التقنية في هذا المجال تحقيقا لمبدأ هام هو مبدأ التخصص.

الكلمات المفتاحية: دليل؛ خبرة تقنية؛ تخصص؛ جرائم معلوماتية.

Résumé

L'évolution technique des systèmes de traitement automatisés a entraîné un changement majeur dans les concepts de preuve en vigueur, ce qui a entraîné le rôle croissant des preuves scientifiques et la déclaration d'adhésion de l'expertise technique au monde de l'expertise judiciaire. Il est inconcevable que le juge refuse de recourir aux services d'un expert en informatique, questions techniques qui nécessitent une expertise particulière et dont le jugement est contraire à la logique scientifique et erroné si l'expertise technique dans ce domaine n'est pas fondée sur son principe. Il est le principe de spécialisation.

Mots clés: Preuve; expertise technique; spécialisation; crime informationnel.

Abstract

The technical development of the automated processing systems has resulted in a major change in the prevailing concepts of evidence, and in fact such a statement has led to a growing role of scientific proof and the announcement of the joining of technical expertise in the world of judicial experience. The fact that digital evidence required to prove and expose informational crimes is something of a concern for experts in this field, and it is inconceivable that a judge will refuse to resort to the sendacement of an expert in information technology cases, as they are technical cases requiring special expertise. His judgment is contrary to scientific logic and flawed if it is not based on technical expertise in this field in order to achieve an important principle of specialization.

Keywords: Evidence; technical expertise; specialization; informational crime.

* Corresponding author, e-mail: t.maebarkia@lagh-univ.dz

مقدمة

لاشك أن التطور الحاصل في مجال المعلوماتية قد رتب آثارا هامة انعكست على الجرائم من حيث الوسائل التي ترتكبها، والمحل الذي تقع عليه، ونوع الجناة الذين يرتكبوها، وهذه الجرائم أي الجرائم المعلوماتية تجمع بين ذكاء المجرم (الذكاء الإنساني) وذكاء الأجهزة الرقمية (الذكاء الإصطناعي)، لذلك فإن هذا التطور التكنولوجي يجب أن يواكبه تطوير لقوانين العقوبات و قوانين الإجراءات الجزائية من أجل استيعاب الجرائم المستحدثة التي ترتكب عبر الوسائط الإلكترونية، كما يجب العمل على تطوير وسائل الإثبات الجزائية بما يتوافق والحقائق العلمية، فالقانون يجب أن لا ينفصل عن الواقع الذي أنتجه.

والحاصل أنه مع ظهور الجرائم المعلوماتية التي تمثل ضربا من ضروب الذكاء الإجرامي، والتي باتت تتخذ أنماطا جديدة أصبح لا يجدي معها إتباع الطرق التقليدية في تحصيل الدليل لإثباتها لما تثيره طبيعتها غير المادية من إشكالات، وما تؤديه التقنية الحديثة من دور في ارتكابها، فإثبات الجرائم المادية التي تترك آثارا ملحوظة أمر سهل وميسور،بعكس إثبات الجرائم المعلوماتية ذات الطبيعة المعنوية بالنظر إلى أنها لا تترك آثار تدل عليها، على أساس أن أغلب البيانات والمعطيات التي تتداول عبر الحاسبات الآلية التي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحواسب التي تحفظها.

فالتطور التقني الذي لحق نظم المعالجة الآلية فضلا عن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما ودون أي شك إلى تغيير كثيرٍ من المفاهيم السائدة حول إجراءات وطرق الحصول عليها، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم لمنهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية، فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع طبيعة البيئة التقنية، فتطوير الإثبات ووسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الإجرام، وهو الأمر الذي سوف نعالجه وفقا للإشكالية التالية:

ماهو دور الخبرة في الإثبات للحصول على الدليل الرقمي في المعاملات الإلكترونية؟

وكانت الإجابة عن هذه الإشكالية وفقا للمحاور التالية:

أولا: القواعد القانونية التي تحكم الخبرة القضائية في مجال الجرائم المعلوماتية.

ثانيا: القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم المعلوماتية.

المبحث الأول: القواعد القانونية التي تحكم الخبرة القضائية في مجال الجرائم المعلوماتية.

لا يمكن التصور أن يرفض القاضي اللجوء إلى ندب خبير في قضايا تقنية المعلومات، إذ هي قضايا فنية تتطلب خبرة خاصة، ويكون حكمه مجانبا للمنطق العلمي ومعيبا إذا لم يستند إلى الخبرة التقنية في هذا المجال[1] تحقيقا لمبدأ هام هو مبدأ التخصص، وإذا كانت الخبرة التقنية في مجال التعاون القضائي تعد أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات والأنترنت خاصة[2] إزاء نقص المعرفة لدى القانونيين بظاهرة تقنية المعلومات، فهل يعني هذا تعرض مبدأ القاضي خبير الخبراء لهزات عنيفة إزاء التزايد المتواصل لمبدأ التفاعل القانوني مع ظاهرة البيئة الرقمية التي تقع في اختصاص آخر غير الجوانب النظرية القانونية التي لا تسمح ثقافة القاضي المبنية على معايير الدراسات القانونية من التفاعل معها.

والخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية والعلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة.

وقد عرفها البعض بأنها الإستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه[3].

والخبير هو كل شخص لديه دراية خاصة بمسألة من المسائل قد يستدعي التحقيق فحصها ويستلزم ذلك كفاء خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، فيمكنه أن يستعين بالخبير كما هو الحال مثلا في تقرير الصفة التشريحية في جرائم القتل أو تحليل المادة المطعومة في جرائم التسمم أو فحص خطوط الكتابة في جريمة التزوير[4].

المطلب الأول: أهمية الخبرة في البحث عن الدليل الرقمي.

تكمن أهمية الخبرة في أنها تنير الطريق لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية، لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة من المواد 143 إلى 156 من قانون الإجراءات الجزائية واعتبارها من إجراءات البحث عن الدليل حيث نصت المادة 143 أنه لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما من تلقاء نفسها أو بناء على طلب من النيابة العامة و إما بطلب من الخصوم.

وإذا كانت الإستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهات التحقيق، فهي أوجب في مجال استخلاص الدليل الرقمي لإثبات الجرائم المعلوماتية حيث تتعلق بمسائل فنية آية في التعقيد، يصعب على المحقق أن يشق طريقة فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات[5]، ومنذ ظهور الجرائم المعلوماتية فإن الضبطية القضائية وسلطات التحقيق عموما تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي والمنظومات المعلوماتية وذلك بغرض كشف غموض الجريمة وتجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق ويلاحظ أن نجاح الإستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء، فإجرام الذكاء والفن لا يكشفه ولا يفله إلا ذكاء وفن مماثلين[6]، وتبرز أهمية الإستعانة بالخبير في مجال الجرائم المعلوماتية عند غيابه فقد تعجز الضبطية في كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل أو الإهمال عند التعامل معه[7].

ولعل هذه الأهمية للخبرة في مجال التحقيق في الجريمة المعلوماتية جعل بعض التشريعات لا تكتف بالنصوص التقليدية التي تنظم الخبرة وعمدت على إدراج نصوص قانونية خاصة تنظم الخبرة في هذا المجال، ومنها المشرع البلجيكي بموجب القانون الصادر في 2000/11/23 حيث نصت المادة 88 منه أنه يجوز للقاضي والشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق."

والمشرع الجزائري لم يتخلف عن هذه التشريعات حينما أشار في المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها أنه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.[8]

المطلب الثاني: شروط صحة الخبرة ومدى حجيتها.

نظرا للأهمية البالغة للخبرة والدور الذي تلعبه في عملية الإثبات في المجال الجنائي، فقد حرصت معظم التشريعات على تنظيم الخبرة ووضع شروط وضوابط لها. وبشكل عام فإن الفقه الجنائي يقدر أن الخبرة تستدعي توافر ركنين أساسين هما : الركن الشكلي والركن الموضوعي، وإذا كان هذا الأخير مقدورا له قدرا من الحرية العلمية ويكون الخبير فيه مستخدما لأدواته العلمية والعملية التي بمقتضاها ينطلق إلى وضع الإجابة على المعضلة الفنية محل سؤال جهات التحقيق، فإن الركن الشكلي فيها يمثل التخصص والعلم الذي اكتسبه الخبير، إذ يشترط في الخبير حقيقة الجمع بين العلم ذي الإختصاص والخبرة العلمية، فلا يكفي فقط كفاءة علمية عالية في مجال التخصص بل يضاف إليها سنوات من أعمال الخبرة في المجال، حيث سار التقليد القضائي في هذا الإطار على ضرورة اللجوء إلى الخبرة المتوافر فيها هذان الركنان.[9]

ومن الشروط التي درجت أغلب التشريعات على تحديدها منها ما يتعلق بالخبير ومنها ما يتعلق بتقرير الخبرة. فأما ما يتعلق بالخبير فأنه يشترط:

* إختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول المعد مسبقا، وقد نصت المادة 144 من قانون الإجراءات الجزائية على ذلك بقولها:" يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة"، وإذا لم يتضمن الجدول من الخبراء المتخصصين في مجال الخبرة فإنه يجوز لجهات التحقيق بصفة إستثنائية إختيار خبراء ليسوا مقيدين في الجدول.

وفي الحقيقة فإن الإستعانة بالخبراء وفق المنهج التقليدي في الإجراءات الجزائية يرتبط بمنطق تقليدي، يجب أن يتسع صدر المشرع الإجرائي بصددها بما يسمح بتجاوزها في إطار الجرائم المعلوماتية، ذلك أنه فضلا عن قاعدة أنه ليس في القانون ما يمنع جهات التحقيق من ندب خبراء من غير المقيدين بالجدول فإن هذا التوجه يجب أن يتم تطويره لكي يمكن الإستعانة بخبراء في العالم الإفتراضي إلى أبعد من النطاق الإقليمي ممثلا في الحدود المادية للدول بحيث يمكن أن يكون هؤلاء الخبراء من خارج الدولة وهو أمر تسمح به مقومات العالم الإفتراضي باعتباره بيئة اتصالية رقمية عالمية[10].

* حلف اليمين القانونية، إذ يجب لصحة عمل الخبير أداء اليمين القانونية وذلك لحمله على الصدق والأمانة في عمله وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، ولا يغني عن هذا الإجراء أي ضمانة أخرى من الضمانات، وقد أوجب المشرع الجزائري بنص المادة 145 من قانون الإجراءات الجزائية أن يحلف الخبير اليمين القانونية قبل أداء مهمته غير أنه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى.[11]

وأما الشروط المتعلقة بتقرير الخبرة فإن الخبير بعد انتهائه من أبحاثه وفحوصاته

يعد تقريرا يضمنه خلاصة ما توصل إليه من نتائج، بعد تطبيق الأسس والقواعد العلمية الفنية على المسألة محل البحث، وإن كان المشرع لم يوجب إتباع شكل معين في تقرير الخبرة فقد يكون شفويا وقد يكون كتابيا وفقا لما تحدده طبيعة المأمورية[12]، لكن الواقع العملي أثبت أن ما يتم في الغالب الأعم هو أن يطلب من الخبير إيداع تقريره كتابة، سيما إذا ما كانت المسألة موضوع الخبرة تتطلب إجراء أبحاث وتجارب وفحوصات علمية وعملية ومعملية، وغالبا ما يرفق الخبير بالتقرير ملحقا إيضاحيا بالصور حتى يسهل على جهة التحقيق فهم الخبرة وعلى جهة الحكم تكوين عقيدتها واقتناعها الذاتي بالدليل.

وإذا كان الحال كذلك بالنسبة لموضوعات الخبرة التقليدية فإن أهمية إعداد تقارير فنية مكتوبة وملاحق توضيحية مصورة تصبح حتمية في حالة الجرائم المعلوماتية، حيث يقتضي الأمر عرض وتوضيح وتحليل الدليل الجنائي الرقمي وكيفية اشتقاقه واستخلاصه.

ويشترط أيضا فيما يتعلق بتقرير الخبرة أن يقوم الخبير بإيداع تقرير خبرته خلال المدة المحددة له في أمر أو حكم الندب، فإن لم يودع تقريره خلال هذه المدة جاز للقاضي استبداله بغيره ما لم يقدم الخبير طلبا بتمديد هذه المهلة وذلك نظرا لما تتسم به الإجراءات الجزائية من طابع السرعة سيما إذا تعلق الأمر بالجريمة المعلوماتية.

المبحث الثاني: القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم المعلوماتية.

تنوع الوسائل الإلكترونية والأجهزة التي تستخدم نظام الحاسبات الآلية، كما تتنوع شبكات الإتصال بينها وتتمايز خصائصها الفنية فتندرج تحت تخصصات فنية وعلمية دقيقة مما يستوجب والحال كذلك أن يتوافر لدى الخبير الإمكانيات والقدرات العلمية والفنية في مجال التخصص، وعلى جهات التحقيق أن تدقق عند اختيارها للخبير وتتيقن من هذه المسألة.[13]

كما أن عملية تجميع الدليل الرقمي تعد من أصعب الأمور التي تواجه الخبير التقني، لذلك كان لزاما عليه إتباع خطوات وأساليب علمية تتناسب مع البيئة التي يتواجد بها هذا النوع من الدليل.

المطلب الأول: متطلبات أعمال الخبرة في مجال الجريمة المعلوماتية.

إنه بالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجريمة المعلوماتية فإنه ينبغي للخبير الإلمام بالموضوعات الآتية:[14]

- الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر ورموز التشفير.
- طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.
- القدرة على أداء المهام دون أن يترتب على ذلك إعطاب أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.
- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.
- بالإضافة إلى ضرورة إلمام الخبير أيضا[15] بنظم الحاسب الآلي بمكوناته المادية والبرامجية.
- معرفته لوسائل وطرق فحص نظام الحاسب الآلي كبرامج كشف وإزالة للفيروسات

وبرامج استرجاع البيانات والمعلومات وإصلاح التالف وإظهار المخفي منها.

- معرفته لوسائل نسخ البرامج والملفات وعمل نسخ من القرص الصلب طبق الأصل.

- معرفته لكيفية الربط بين الدليل المادي والدليل الرقمي في الوقائع محل البحث.

ولا ينجح الخبير المعلوماتي في أدائه لمهامه المنوطة به وإتمامه للمأمورية المكلف بها إن لم يكن لديه هذا القدر من المتطلبات الفنية.[16]

فالخبرة في الجرائم المعلوماتية تساعد في النهاية على:

- الكشف عن الدليل الرقمي.

- إجراء الإختبارات التكنولوجية على الدليل الرقمي للتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ القانون.

- تحديد الخصائص الفريدة للدليل الرقمي.

- إصلاح الدليل الرقمي وإعادة تجميعه من المكونات المادية للكومبيوتر.

- عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.

- جمع الآثار المعلوماتية الرقمية التي تكون قد تبدلت خلال الشبكة المعلوماتية.

المطلب الثاني: الأساليب الفنية في عمل الخبير المعلوماتي في اكتشاف الدليل الرقمي:

للخبير المعلوماتي في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله له أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي.[17]

ويعتمد عمل الخبير المعلوماتي في سبيل تحري الحقيقة في مجال الجرائم المعلوماتية على جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع **(Les serveurs)** ومن جهاز المعتدي بعد التوصل إلى تحديده، ثم يقوم بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، ومن ثم التوصل في النهاية إلى معرفة بروتكول الأنترنات **(IP)** للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية.

ويرى بعض المتخصصين أن عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر ثلاث مراحل:

1- المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل منها المجرم المعلوماتي ومحاولة إيجاد أثر له.

2- المرحلة الثانية: مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

3- المرحلة الثالثة: فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف جهات التحقيق بمكوناته المادية والمعنوية لاشتقاق الدليل وتقديمه لجهات التحقيق وتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه.

وقد وضعت وزراة العدل الأمريكية إطارا عمليا يحدد خطوات أساسية لجمع الأدلة الرقمية ثم فحصها ومن ثم تحليلها وأخيرا كتابة النتائج المتوصل إليها في تقرير، ويمكن إيجاز هذه الخطوات في المراحل التالية:

1- خطوات ما قبل التشغيل والفحص.

- التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها.
- التأكد من صلاحية وحدات نظام التشغيل.
- تسجيل معطيات وحدات المكونات المضبوطة.

2- خطوات التشغيل و الفحص.

- إستكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز.
- عمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب لإجراء عملية *الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير سواء عن سوء الإستخدام أو لوجود فيروسات أو قنابل برمجية.
- تحديد أنواع وأسماء المجموعات البرامجية كبرامج النظام (برامج التشغيل)، برامج التطبيقات وبرامج الإتصالات، وما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة
- إظهار الملفات المخبأة والنصوص المخفية داخل الصور.
- إسترجاع الملفات التي تم محوها من الأصل وذلك باستخدام أحد برامج استعادة المعلومات وكذلك بالنسبة للملفات المعطلة أو التالفة.
- تخزين هذه الملفات أو المعطيات وعمل نسخ أخرى طبق الأصل من الأسطوانة أو القرص المحتوي لها ولفحصها عن طريق تطبيق الخطوات سالفة الذكر.
- إعداد قائمة يجرد فيها الخبير كل الأدلة الرقمية التي تم الحصول عليها، مع إجراء مراجعة لكل صورة محتفظ بها في القرص الصلب لحاسوب آخر للتأكد من سلامة القائمة.
- تحويل الدليل الرقمي إلى هيأة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها أو وضعها في أي وعاء آخر حسب نوع المعطيات والمعلومات المكونة للدليل[18].

وفضلا عما سبق فإن الخبير المعلوماتي وهو في إطار القيام بعمله له أن يستخدم العديد من الوسائل العلمية والبرمجيات التي تمكنه من استخلاص الدليل الرقمي و تساعده في الوصول إلى المجرم المعلوماتي، وغالبا ما تكون هذه الوسائل أدوات فنية تستخدم في بنية نظام المعلومات.

ونذكر منها على سبيل المثال لا الحصر:

1- بروتوكول الأنترنت(IP): وهو المسؤول عن تراسل حزم البيانات عبر شبكة الأنترنت وتوجيهها إلى أهدافها، وهو يوجد بكل جهاز مرتبط بالأنترنت ويتكون من أربعة أجزاء كل جزء يتكون من أربع خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات المرتبطة، والرابع يحدد الكومبيوتر الذي تم الإتصال منه[19]، مع ملاحظة أن عنوان **(IP)** قد يتغير في كل اتصال بشبكة الأنترنت.[20]

2- نظام البروكسي(PROXY): يعمل هذا النظام كوسيط بين الشبكة ومستخدميها بحيث يضمن مقدم الخدمة توفير خدمات الذاكرة الجاهزة، وتقوم فكره البروكسي على تلقي مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد تم تتريلها من قبل فيقوم بإرسالها إلى المستخدم دون حاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يتم تتريلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية وهنا يستخدم البروكسي أحد عناوين **(IP)** ومن أهم مزايا هذا النظام أن الذاكرة المتوفرة لديه يمكن أن تتحفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة.

3- برنامج الدمج وفك الدمج (pkzip): ويستخدم هذا البرنامج لفك دمج البرامج، فقد يكون المجرم المعلوماتي قد قام بدمج برامجه فلا يمكن الإطلاع عليها إلا بعد فك الدمج.

4- برنامج (Visual route5.2a): وهو عبارة عن برنامج يلتقط أي عملية فحص ضد الشبكة *فيقوم بتقديم أجوبة تبين المعلومان التي حدث فيها المسح والمناطق التي تم فيها الهجوم، وبعد معرفة عنوان**(IP)** إسم الجهة يرسم البرنامج خطا يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

5- برنامج معالجة الملفات(Xtree Progold) : وهو برنامج يمكن من العثور على الملفات في *أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم والأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية.

6- برنامج (Hark Tracerv 1.2): وهو أحد برامج التتبع يتكون من شاشة رئيسية تقدم *للمستخدم بيان شامل بعمليات الإختراق التي تعرض لها جهازه، يحتوي على تاريخ الواقعة وعنوان **(IP)** الذي تم من خلاله عملية الإختراق واسم الدولة التي منها الإختراق واسم الشركة المزودة لخدمة الأنترنت المستضيفة للمخترق ورقم المنفذ والبوابة الخاصة وبيانات الشبكة التي تتبعها الشركة المستضيفة للمخترق بما فيها أرقام هواتفها.

خاتمة:

لا يوجد شك في أن إثبات الأمور المادية التي تترك آثارا ملحوظة يكون سهلا ميسورا، بعكس إثبات الأمور المعنوية فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه، بحسبان أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية فالجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإلكتروني يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها أو يستدل من خلالها على الجناة.

وكمثال لذلك نجد أن التجسس المعلوماتي بنسخ الملفات وسرقة وقت الآلة يصعب على الشركات التي تكون الضحية لمثل هذه الأفعال اكتشاف أمرها وملاحقة الجناة

عنها.

ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الإشتباه خاصة في حالات التلاعب في برامج الحاسبات.

ومن ثم فقد يستحيل عليهم الوصول إلى الجناة، فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع أي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية

فإن الجناة الذين يستخدمون الوسائل الإلكترونية في ارتكاب جرائمهم يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعة الفنية، ولذلك فإنهم يتمكنون من إخفاء الأفعال غير المشروعة التي يقومون بها أثناء تشغيلهم لهذه الوسائل الإلكترونية ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها، كما وأن هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الوسائل الإلكترونية ويكون أمرها حكرا عليهم كالتجسس على ملفات البيانات المختزنة والوقوف على ما بها من أسرار، كما أنهم قد ينسخون هذه الملفات ويتحصلون على نسخ منها بقصد استعمالها تحقيقا لمصالحهم الخاصة، كذلك فإنه قد يقومون باختراق قواعد البيانات والتغيير في محتوياتها تحقيقا لمآرب خاصة، وقد يخربون الأنظمة تخريبا منطقيا بحيث يمكن تمويهه.

كما لو كان مصدره خطأ في البرنامج أو في الأجهزة أو في أنظمة التشغيل أو التصميم الكلي للنظام المعالج آليا للمعلومات، وقد يدخلون كذلك بيانات غير معتمدة في نظام الحاسب أو يعدلون برامجه أو يحرفون البيانات المخزنة بداخله دون أن يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل.

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الإلكترونية أنه يمكن محو الدليل في زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها، فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده، ويلاحظ أن المجني عليهم قد يساهمون بدورهم في عدم إماطة اللثام عن هذه الجرائم، فقد يحجمون عن تقديم الدليل الذي قد يكون بحوزتهم عن هذه الجرائم، وقد يكون مقصدهم من ذلك استقرار حركة التعامل الاقتصادي بالنسبة لهم، أو رغبتهم في إخفاء الأسلوب الذي ارتكبت به الجريمة لكي لا يتم تقليدها من الآخرين.

و لا شك أن قانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تعديل قانون العقوبات بموجب قانون 15/04 كانت لهما أهمية في تدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري و ذلك من خلال حسم المشرع الجدل الفقهي القائم حول طبيعة المعلوماتية باعتبارها مالا من نوع خاص باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في الفصل الثالث من الباب الثاني من الكتاب الثالث من المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات لكون أن القسم السابع ورد تحت الكتاب الثالث المتعلق بالجنايات و الجنح ضد الأموال.

وفي الأخير ما توصلنا إليه في هذا البحث من المقترحات سيكون طرحها في

التالي:

- ✓ فهم الأدلة الفنية التي تتحصل من الوسائل الإلكترونية يتطلب أيضا تدريب جهات الضبط القضائي والتحقيق والقضاء على فهم طبيعة المعطيات التي تقع عليها الجرائم الإلكترونية، والعمل على إلمامهم بمكونات الحاسب الآلية وكيفية عملها ومعرفة اللغة التي تتعامل بها، والتي تعتمد على المختصرات خاصة وان الجرائم التي تقع باستخدام الوسائل الإلكترونية في الغالب ما تعتمد على رموز تكون معروفة عند أهل العلم والخبرة.
- ✓ الأهمية المتزايدة لتدريب الخبراء القضائيين على تقنيات الحاسبات الآلية لتمكينهم من القيام بمهامهم في المسائل الإلكترونية الدقيقة وإعداد تقاريرهم الفنية فيها والتي تكون ذات أهمية بالنسبة لقضاء الحكم الذي غالبا ما يتخذ منها سندا يرتكن إليه في المسائل الفنية البحتة
- ✓ إن الجزائر وهي تخطوا الخطوات الأولى في تطبيق مشروع الحكومة الإلكترونية والذي من خلاله يتم السعي إلى استخدام تقنية المعلومات والاتصالات الإلكترونية في توفير وتقديم معلومات وخدمات الحكومة للمواطنين وجعلها متاحة للجمهور، فهذا المشروع لابد أن يستتبعه خطوة تشريعية هامة يكون الهدف منها توفير الحماية القانونية الشاملة لهذا المفهوم بصورة منسجمة ومتزامنة مع هذا التحول من أجل تخطي الثغرات القانونية التي قد يستفيد منها العابثون بأمن المعلومات، سيما وأن الأمر يتعلق بأنظمة معلوماتية تخص إدارات الدولة.
- ✓ أن من بين الصعوبات في تحديد هوية المجرم المعلوماتي هو استعمال هذا الأخير لحواسيب غير شخصية في تنفيذ جريمته وغالبا ما تكون في مقاهي الإنترنت، هذه الأخيرة التي يرتادها عدد كبير من الزبائن لا يمكن معرفة هوياتهم، لذلك أقترح على المشرع إعادة النظر في تسير هذه المقاهي وعدم اعتبارها مجرد نشاط تجاري كغيره من الأنشطة التجارية الأخرى، بل لابد من فرض أعباء والتزامات على مقدمي هذه الخدمة ومسيري مقاهي الإنترنت، كأن يطلب من أي زبون قبل شروعه في استعمال الإنترنت ملء استمارة تحدد فيها كامل هويته والتوقيت الذي استعمل فيه شبكة الإنترنت ورقم جهاز الحاسوب الذي استعمله،كما يلتزم مسير المقهى بالاحتفاظ بعناوين المواقع التي تم زيارتها في ذاكرة كل حاسوب لمدة معينة، ونفس الشيء بالنسبة لاستعمال شبكات الإنترنت الموجودة في المؤسسات العامة كالجامعات وغيرها.
- ✓ ضرورة تخصيص شرطة جنائية خاصة بجرائم الانترنيت في كل ولاية، مع تكوين لجان خبراء لهذا الشأن.
- ✓ تكوين هيئة وطنية لمراقبة ومتابعة جرائم الانترنيت، وتزويد البرلمان بكل التطورات الحاصلة، أي هيئة استشارية في المجال القانوني والإجرائي في مجال مكافحة الجرائم الالكترونية.

الهوامش:

[1] - عادل عزام سقف الحيط (2011)، جرائم الذم و القدح و التحقير المرتكبة عبر الوسائط الالكترونية دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، ص273.

[2]

[3] - ومن أهم التعريفات التي وردت بخصوص الخبرة القضائية أنها عبارة عن إجراءات من إجراءات التحقيق يعهد به القاضي إلى شخص مختص ينعت بالخبير وتتعلق بواقعة يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علما أو فنا لا يتوافر في الشخص العادي ليقدم له بيانا أو رأيا فنيا لا يستطيع المحقق الوصول إليه وحده.

[4] - وضاح محمود الحمود ونشأت مفضي المجالي(2005)، جرائم الإنترنت،دار المنار للنشر والتوزيع، ص124.

[5] - علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، حول الجوانب القانونية و الأمنية للعمليات الالكترونية دبي 2003 منشور على موقع **com.arablawinfo.www** :بدون ترقيم.

[6] - محمد حسام محمود لطفي(1987)، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، ص85.

[7] - فقد حدث أن طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعة تحت المراقبة بهدف كشف مرتكب الجريمة فحدث نتيجة لذلك أن تسببت دوائر الشرطة بدون قصد في إتلاف ما كان قد تم من الملفات والبرامج، أنظر للتفصيل أكثر د.هشام رستم(1994)، الجوانب الإجرائية للجرائم المعلوماتية، ص29.

[8] - عبد الفتاح بيومي حجازي(2002)، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول نظام التجارة الإلكترونية وحمايتها مدنيا، دار الفكر الجامعي، ص 85.

[9] - محمد أمين الرومي(2004)، التعاقد الإلكتروني عبر الأنترنيت، دار المطبوعات الجامعية، الإسكندرية، الطبعة1، ص 25.

[10] - عكاشة محي الدين(2001)، محاضرات في الملكية الأدبية والفنية، ديوان المطبوعات الجامعية، الجزائر، ص 123.

[11] - عبد الفتاح بيومي حجازي، المرجع السابق، ص 89.

[12] - علي عبد القادر القهوجي(1999)، الحماية الجنائية لبرامج الحاسب الآلي، المكتبة القانونية، القاهرة، ص 109.

[13] - يونس عرب، العقود الإلكترونية، أنظمة الدفع والسداد الإلكتروني، مقال منشور على **www.arab-law.org**

[14] - هشام محمد فريد رستم(1994)، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، الطبعة الأولى 1994.ص142-143.

[15] - أمال قارة(2007)، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة، الطبعة الثانية، ص 78.

[16]- القاضي كمال العياري(2003)، التطور العلمي وقانون الإثبات، ورقة عمل مقدمة في الندوة العالمية حول الإثبات باستعمال وسائل المعلوماتية والتكنولوجية الحديثة، بالمركز العربي للبحوث القانونية والقضائية، بيروت، لبنان.

[17] - نبيل صقر(2005)، موسوعة الفكر القانوني،جرائم الكمبيوتر و الأنترنت في التشريع الجزائري، دار الهلال للخدمات الإعلامية، طبعة1، ص 127.

[18] - طارق إبراهيم الدسوقي عطية(2009)، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للشرق، ص 75.

[19] - وتوجد أكثر من طريقة يمكن من خلالها معرفة عنوان **(IP)** الخاص بجهاز الحاسوب منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل **Windows** حيث يتم كتابة **WINPCFG** في أمر التشغيل ليظهر مرجع حوار بين فيه**(IP)** .

[20] - Michel Vivant(1999), les contrats du commerce électronique, Litec librairie de le cour de cassation, Paris; p 59.