الخبرة في الجريمة المعلوماتية.
تابري مختار، المجلد الحادي عشر، العدد 3، ديسمبر 2020،
ص ص 380-399

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

الخبرة في الجريمة المعلوماتية.

Cybercrime expertise

مختار تابري (*)
جامعة سيدي بلعباس، الجزائر
tabri.mokhtar@gmail.com

تاريخ الإيداع: 2020/11/21 تاريخ القبول: 2020/12/21 تاريخ النشر: 2020/12/31

الملخص:

التحقيق الجنائي هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فهو له قواعد ثابتة راسخة وبدونها ما كان ليتمتع التحقيق بتلك الصفة، وهذه القواعد قانونية وفنية، الأولى وأن كانت لها صفة الثبات التشريعي لا يملك المحقق إزائها شيء سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير.

إن التحقيق ليس أسئلة تلقى وإجابات تدون، لكن فن ودراسة، خبرة وفراسة، صراع بين الحقيقة والخيال، بين الصدق والضلال، وكم ضاعت الحقيقة في الصحف فقضى ببراءة مجرم آثم أو إدانة بريء نتيجة لتحقيق خاطئ أو لقصور فيه. لذلك تعتبر الخبرة القضائية في الجرائم المعلوماتية من أهم الوسائل التي يعتمد عليها المحقق للحصول على الدليل الالكتروني.

الكلمات الدالة:

الجريمة الالكترونية، الخبير، المحقق، اتباث، الكتروني.

Abstract:

The criminal investigation is a science that yields to what all other sciences undergo., it has established rules , without them this latter would not have that status, these rules are legal and technical, , although the first has the characteristic of legislative stability, the investigator hasn't a choice but compliance and subjection, while the second is characterized by flexibility in addition to experience, intelligence and skills supplied by the investigator. The investigation is not only asked questions and written answers, but it's an art and a scrutinise study of facts , an experience and an insight or discernment. Furthermore , investigation is a struggle between truth and fiction, between honesty and deceitfulness or mislead. Indeed, the innocence of a guilty criminal or an innocent accused as a result of a false investigation or

(*) المؤلف المرسل: مختار تابري tabri.mokhtar@gmail.com

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

inadequacy due to lost of facts. There fore, judicial expertise in Cyber-crimes is one of the most important means on which the investigator can obtain the Electronic evidence.

Keywords: Cybercrime , Expert , Investigator , Electronic-evidence.

****

من المسلم به أن العالم يعاصر اليوم عهدا جديدا من النهضة في المجالات الالكترونية وتكنولوجيا المعلومات والتي تعد بحق الثورة الصناعية الثانية في حياة البشرية، فإن لنا أن نتصور عمق التغير والتحول والمتوقعين في أنماط الحياة والبناء الاجتماعي والاقتصادي مقارنة بما أحدثته الثورة الصناعية من تأثيرات على المجتمع الإنساني ككل.

وجديرا بالذكر أن الثورة الالكترونية – بخلاف الثورة الصناعية الأولى – لا تعتمد على الثروات الطبيعية إلا بقدر يسير، بينما تمثل الثروات البشرية أساس هذه الثورة، فالفكر البشري والقدرة على الابتكار والتطوير هما لب هذه الثورة، بينما يمثل الجهد الإنساني يدها التي تقوم بتحويل الأفكار إلى منجزات ذات ابتكار وكفاءة.وبالتالي فإن هذا الفكر البشري يجب أن يقابله فكر بشري مقابل من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يتغير ويتطور أيضا وذلك نتيجة طبيعة لمواجهة فكر أسلوب المجرم المعلوماتي.

ومن ثم فإن الأمر يتطلب بحث عن الخبرة في التحقيق الجنائي للجرائم المعلوماتية، اذيقوم المحقق الجنائي في مجال الكشف عن غموض الجريمة وفاعلها باتخاذ الكثير من الإجراءات والوسائل المتنوعة اللازمة لتحقيق هدفه، ولما كان ذلك يحتاج إلى جهد لا يستطيع القيام به بمفرده، وتيسيرا عليه لأداء عمله، وتفرغه التام لأداء البحث، وتحقيقا لمبدأ هام وهو "مبدأ التخصص"، وتقسيم العمل، فإن الأمر يقتضي الاستفادة بأهل الخبرة والاستعانة بهم.وعليه سنتحدث عن الخبرة القضائية في الجرائم الالكترونية من خلال المحورين الآتيين :

المحور الأول: مفهوم الخبرة.

المحور الثاني: الخبرة في مجال الانترنت والعالم الافتراضي.

المحور الأول: مفهوم الخبرة.

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

يقصد بالخبرة، بصفة عامة، المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة أو نتيجة دراسات خاصة تلقاها أو نتيجة الاثنين معا أي العمل والدراسة، ومن هنا يطلق على ذوي هذه المهارات "بالخبراء".ومن هذا المنطلق سوف نتناول في هذا المبحث ماهية الخبرة، وتعريف الخبير، وأنواع الخبراء، والصفات الواجب توافرها في الخبير المعلوماتي، ومجالات الخبرة في الجرائم المعلوماتية وذلك على النحو التالي:

أولا: ماهية الخبرة.

الخبرة القضائية هي إجراء للتحقيق يعهد به القاضي إلى شخص مختص ينعت بالخبير، تتعلق بواقعة أو وقائع مادية 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.[1]والخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق والمحكمة تحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو المادي، وإنما هي تقييم فني لهذا الدليل، فهي في مجملها تقرير أو رأي فني صادر عن الخبرة في أمر من الأمور المتعلقة بالجريمة.

والعنصر المميز للخبرة عن غيرها من إجراءات[2] التحقيق كالمعاينة والشهادة والتفتيش هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها في الإثبات، والذي يتطلب معارف علمية أو فنية خاصة لا تتوافر سواء لدى المحقق أو القاضي.وإذا كان القانون قد أخذ في الاعتبار ضرورة توافر الأركان الشكلية والموضوعية في الخبرة[3]، فإن الأمر يستدعي أن يقوم القضاء بالاستعانة بخبراء مصنفين في هذا الشأن مم هو مندرج في قائمة المحكمة، وهو ما يطلق عليه نظام جدول الخبراء الذي يتميز به النظام القانوني الفرانكوفوني، دون نظيرة الأنجلوسكسوني، فحين يندب القاضي في هذا النظام خبيرا فإنه يقوم بذلك مستعينا بجدول الخبرة المعد في كل محكمة.

وتقتضي الخبرة شرط التخصص والتعمق من قبل المتصف بها فالخبير هو ذلك الشخص الضليع بعلم من العلوم عن طريق مهارة فنية عالية، سواء كان ذلك من خلال الدراسة الخاصة التي تلقاها أو الخبرة الطويلة التي حصدها من مرور العددي من السنين مكنته من الإلمام بالمهنة ودقائقها الجزئية التي تصعب على العامة.

والقاضي حين يقوم بالاستعانة بالخبرة في مسألة ما تخص القضية المعروضة أمامه، فإنه يسعى إلى الخبير بحسب تخصصه، ومجال التخصص محكوم بقاعدة طبيعية وهي

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

قاعدة العلم المؤسس التحصيل الدراسي، كما هو الشأن في دراسة الطب أو الهندسة أو علوم الكمبيوتر في مجال الجريمة كدراسة علم البصمات وعلوم الصيدلة والتحاليل والاختصاص في مجال الكهرباء والالكترونيات...الخ، وهذه كلها أمور تحتاج إلى دراسة وخبرة كافيين في هذا المجال.

ثانيا: تعريف الخبير.

الخبير قد يكون موظف عام مثل الطبيب الشرعي وخبير البصمات والمهندس الفني، وقد لا يكون كذلك مثل أصحاب الحرف المختلفة مثال الصائغ – النجار – الحداد، وقد يكون من الكوادر الخاصة مثل أستاذة الجامعات في مختلف التخصصات.والخبير هو شخص مختص فنيا في مجال المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ويستطيع بما له من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلى خبرة فنية خاصة.[4]

ويشترط في الخبير حقيقة الجمع بين العلم ذي الاختصاص والخبرة العملية، بل أن الخبرة العملية، بل أن الخبرة العملية في بعض المهن قد تغطي جانب اشتراط الاختصاص، إلا أن العلم وحده لا يكفي في نظرنا في إعطاء صفة الخبير في نطاق معين أو مهنة معينة التي لابد أن تدعم الخبرة الواقعة العملية، إذا لا نستطيع أن نقبل من حيث المنطق إعطاء صفة الخبير لمن هو خريج احدى الكليات أو المعاهد والذي لا يملك خبرة عملية تتجاوز عدة سنوات، فالعلم النظري مطلوب كقاعدة للانطلاق في فن هذه المهنة ومعرفة سبلها اللازمة إلا أن الاتقان دائما يأتي من الممارسة الفعلية..[5]هذا وقد صدر القانون رقم 96 لسنة 1952 بتنظيم الخبرة أمام جهات القضاء بتاريخ 1952/6/20[6]، وقد نص في المادة الأولى منه على "أن يقوم بأعمال الخبرة أمام جهات القضاء خبراء الجدول الحاليون وخبراء وزارة العدل ومصلحة الطب الشرعي والمصالح الأخروي التي يعهد إليها بأعمال الخبرة، وكل من تري جهات القضاء عند الضرورة الاستعانة برأيهم الفني من غير من ذكروا".

هذا وقد نصت المواد من 85 إلى 89 من قانون الإجراءات الجنائية على الأحكام الخاصة بعمل الخبراء، ونصت المادتين 292، 293 من ذات القانون على حق المحكمة في ندب الخبراء بناء على طلب الخصوم أو من تلقاء نفسها، وكما أشرنا فإن المواد الخاصة بالخبراء قد وردت في الفصل الثالث من الباب الثالث من قانون الإجراءات الجنائية وأوردت نصوص هذا الفصل أحكاما تفصيلية في شأن الاستعانة بالخبراء أمام المحاكم الجنائية (م 292، 293 أج)،

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

ولذلك استقر قضاء النقض على اعتبار نصوص الفصل الحالي واجبة الاتباع أمام المحاكم ومكملة لنص المادتين سالفتي الذكر.[7]

ثالثا: أنواع الخبراء.

يمكن تقسيم الخبراء إلى نوعين وذلك على النحو التالي:

- الطائفة الأولى: وهم الخبراء من ضباط الشرطة الذين يعملون في مجال المعمل الجنائي والأدلة الجنائية يقتضي تخصصهم تلقينهم وتدريبهم تدريبا خاصا ودراسة بعض العلوم كالكيمياء والطبيعة والهندسة والتصوير، وذلك لمعاونتهم في التحليل العلمي في مجال التخصص وهذه الطائفة تتخصص في مجال فحص الأسلحة النارية وللكشف عن التزوير والتزييف ومضاهاة الخطوط وفحص قضايا الحريق.الطائفة الثانية: وهم الخبراء من خريجي الكليات العملية كالطب والهندسة والعلوم ويتم تدريب هؤلاء وتلقيتهم بعض المواد القانونية والشرطية بما يتفق واحتياجتهم في مجال الفحص.[8]

رابعا: الصفات الواجب توافرها في الخبير المعلوماتي.

هناك صفات لابد من توافرها بالنسبة للخبراء ويمكن تلخيصها على النحو التالي:

1. الالتزام بأحكم ونصوص القوانين واللوائح وخاصة أحكام قانون الإجراءات الجنائية وقانون الإثبات في المسائل المدنية والتجارية وقانون مكافحة الجرائم المعلوماتية.
2. الإلمام بعلم التحقيق الفني الجنائي من وسائل ارتكاب الجرائم ومحاولة إخفاء الأدلة وطرق البحث للوصول إلى الفاعل.
3. الاستفادة من كافة الآثار الموجودة بمسرح الجريمة المعلوماتية مهما كان حجمها.
4. تقدير أهمية الدليل وأثره على محل الحادث.[9]
5. أن يكون صبورا أو مثابرا لا يتسرب إليه الضيق أو الملل في العناية بالأثر مهما صغر.
6. عليه التعرف على ظروف الحادث من وقت ارتكابه حتى اكتشافه وأطرافه والهدف من ارتكابه.
7. على الخبير إلا يستنتج استناجا يحتمل التأويل، بل عليه أن يفحص الآثار فحصا دقيقا، وأن يلتزم جانب الصدق والأمانة في عمله، وأن يكون هدفه دائما إظهار الحقيقة وتحقيق العدل.
8. عدم قيامه بفحص الآثار أو كتابة التقرير المتضمن النتائج إذا كانت بينه وبين أحد أطراف الواقعة أية صلة.

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

9. أن يبتعد عن مواطن الشبهات من أماكن أو أشخاص.
10. ألا يختلط أثناء عمله بأحد من أطراف الواقعة سواء جاني أو مجني عليه أو شاهد، حتى لا يتأثر بما يدلي به أحدهم من أراء ويكون لها مآرب شخصية من وراءها.
11. الاستزادة من التكنولوجيا والعلوم القائمة والتبصير بالعلوم والاختراعات الحديثة التي تحت التجارب والإلمام بها.[10]

خامسا: مجالات الخبرة في الجرائم المعلوماتية.

تتنوع المجالات التي تقتضي الخبرة، بحيث أنها قد تشمل الموظفين التابعين للدولة أو غيرهم فهي تشمل مثلا الأطباء الشرعيين الذين يتلقون بالإضافة إلى علم الطب دراسات تخصصية في الإصابات الجنائية بأنواعها المختلفة ويقدم هؤلاء خبراتهم في مجال الفحص الطبي والتشريح لتوضيح أسباب الإصابة أو الوفاة وكيفية حدوثها ونوع الأداء المستخدمة في ارتكاب الجريمة، ووقت الحدوث والنتائج المترتبة عليها.كذلك يوجد ما يسمى بخراء البصمات والذين يقومون بالكشف عن آثار البصمات التي قد يكون الجاني تركها في مكان ارتكاب الجريمة ومقارنتها مع بصمات أخرى من المشتبه بهم ومعتادي الإجرام.

ويوجد أيضا ما يسمى بخبراء التصوير الجنائي الذي يقع على عاتقهم الاختصاص بتصوير مسرح الجريمة بالمحتويات التي قد يتضمنها وتوضيح بعض الآثار والمخلفات التي وجدت فكأنما يقوم بتسجيل المكان بأكمله عن طريق الصور الفوتوغرافية، حيث يتمكن المحققون والمحكمة من الاطلاع عليها وبيان مسرح الجريمة بكل محتوياته.[11]بالإضافة إلى هؤلاء يوجد أيضا من يسمون بالخبراء الجنائيين والذين ينقسمون إلى عدة طوائف كالخبراء بالفحوص البيولوجية، وهناك أيضا من يسمون بخبراء الفحوص الكيميائية والذين يتخصصون في تحليل المواد سواء كانت عضوية أو غيرها لتحديد نوعها والمواد التي تتركب منها وعناصرها أو أية مواد أخرى قد توجد في مسرح الجريمة ولا يعرف مكنونها.

ويوجد خبراء الأسلحة الذين يتولون فحص الأسلحة وتحديد نوعها ونوع الأظرف المستخدمة في إطلاق النار وفيما إذا كانت تعود للسلاح الذي تم ضبطه أم لا، وزاوية إطلاق النار أو الوضعية التي كان عليها كل من المتهم والمجني عليه.[12]ويوجد أيضا خبراء بالحرائق حيث يختصون في كشف المكان وبيان المواد المستخدمة في اشعال الحريق وهل كان متعمدا أم كان نتيجة لالتماس كهربائي ويقوم أيضا بتحدي منطقة بدء الحريق والأسباب التي أدت إليه والزمن الذي تطلبه اشتعال المواد المستخدمة أو الوقت الذي استغرقه الحريق.

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

كذلك يوجد الخبراء يكون اختصاصهم كشف التزييف والتزوير في المحررات التي قد يطعن أحد الخصوم بالدعوى أنها مزورة فيقوم هنا المحقق أو القاضي بإحالتها إلى خبير يختص بدراسة هذا المستند وبيانات التغيير أو العبث الذي تم في أو الفصل فيما إذا كان هذا المستند نسخة أصلية أو أنها نسخة مقلدة منها ولا شك أن هذا الأمر يحتاج إلى استخدام العديد من الطرق الفنية والحديثة للمضاهاة وتقرير ما إذا كان هناك تزييف أو تزوير.

وهناك أيضا طوائف قد لا تتبع الجهاز الحكومي أو ما يسمى بخبراء الجدول ولكن يعتبرون من أهل الخبرة الجائز اللجوء إليهم لأخذ رأيهم في الأمور التي قد تحتاج إلى مثل ذلك الرأي بحسب تقدير المحقق والتي يعجز عن تقويمها هو بنفسه، كما هو الحال في أصحاب الهوايات الذين أصبحوا أصحاب معرفة واضطلاع في تربية بعض الحيوانات كالأغنام والإبل والحمام خاصة فيما يتعلق بتقدير قيمتها عند إصابتها أو نفوقها من قبل فعل المتهم غير المشروع.[13]

سادسا: الاستعانة بالخبراء في الجرائم المعلوماتية

لا يلجأ إلى ندب خبراء من غير الجدول أو خبراء وزارة العدل أو الطب الشرعي أو المصالح الأخرى المعهود إليها بأعمال الخبرة إلا عند الضرورة ولظروف خاصة تقتضي الاستعانة بالرأي.أن الاستعانة بالخبراء وفق المنهج التقليدي في الإجراءات الجنائية يرتبط في الحقيقة بمنطق تقليدي يجب أن يتسع صدر المشرع الإجرائي بصددها بما يسمح بتجاوزها في إطار جرائم الانترنت، ذلك أنه فضلا عن قاعدة أنه ليس في القانون ما يمنع من محكمة الموضوع من ندب خبراء من غير المقيدين بجدول المحكمة، فإن هذا التوجه القضائي يجب أن يتم تطويره لكي يمكن الاستعانة بخبراء في العالم الافتراضي دون حاجة لإبداء أسباب في منطق الاستعانة بالخبراء من خارج الجدول، على أن يشمل التطوير إمكانية أن يكون الاستعانة المادية بين الدول، وبحيث يمكن أن يكون هؤلاء الخبراء في خارج الإقليم، وهو أمر تسمح به مقومات العالم الإفتراضي هنا كونه يعد بيئة اتصالية رقمية كاملة.

فيمكن مثلا الاستعانة بمراكز وهيئات ومؤسسات حكومية أو خاصة تعمل في بيئة تكنولوجيا المعلومات حيثما كانت قصد استجلاء الغموض الفني في نظم الانترنت ودون أن يكون ذلك مكلفا على النحو الذي يفترض حدوثه في العالم المادي، وإنما كل ما يحتاج إليه هو توافر بيئة اتصالية رقمية بتكنولوجيا المعلومات والانترنت، فإذا ما توافرت مثل هذه البيئة الرقمية أمكن استصدار تشريع يحقق المقصود القانوني من هذا النظام.

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

على أن الأمر هنا على درجة كبيرة من الأهمية تتعلق بالدراية الفنية للقائم بالتحقيق، سيما حال عدم وجود مثل هذه الدراية الفنية لديه بهذه النوعية من الجرائم فهل يجوز له الاستعانة المتواصلة بالخبير الرقمي طوال فترة التحقيق هنا، وهذه المسألة على درجة من الخطورة حيث أن القائم بالتحقيق يتواصل عمله بعمل الخبير الذي يستعين به في كافة مراحل التحقيق، فيظهر الأمر كما لو كان القائم بالتحقيق يستعين بخبير استشاري هنا، في حين أن بعض التشريعات منحت المتهم فقط صلاحية الاستعانة بخبير استشاري.

لقد منح القانون جهات التحقيق سلطة ندب خبراء طالما قامت حالة جدية تستدعي وجودهم في الدعوى الجنائية وذلك للقيام باستجلاء غموض وقائع تحتاج إلى تفسير علمي.[14]

كما منح القانون صلاحية التحقيق لغرفة الاتهام باعتبارها درجة ثانية من درجات التحقيق إذ تملك سلطات قاضي التحقيق بالإضافة إلى سلطتها القانونية في مراجعة التحقيق الذي قام به قاضي التحقيق أو النيابة العامة.ومن ثم يكون لها الاستعانة بالخبراء، وفضلا عن ذلك كله فإنه لما كان الأصل في القانون هو لمرحلة التحقيق التي تتم في جلسة المحاكمة فإن محكمة الموضوع تعد السلطة الأصلية التي يمنحها القانون الحق في إجراء تحقيق في الجلسة.[15]كذلك لا يوجد في القانون ما يمنع المتهم ذاته من صلاحية القيام بإجراء تحقيق خاص حول اتهامه وبما يوفر فرص أكبر لدفاعه في هذا الشأن، ومثل هذا الحق يملكه دفاعه من باب أولى، وهذا يفي بإمكانية أن يقوم المتهم بهدف دعم العدالة بإجراء تحقيق حول الموضوع الذي يكون عرضه للاتهام بمقتضاه، خاصة وأن القانون يمنح المتهم في أغلب الأحوال إمكانية إخلاء سبيله لضمان حضوره جلسة التحقيق والمحاكمة، وكلما تطلب الأمر استدعائه من قبل الجهة التي تتولى التحقيق معه.

والخبرة الاستشارية هي نشاط خبرة يمارسه المتهم دفاعا عن حقوقه إلا أن ذلك يمثل أحد متطلبات الدفاع التي تخضع للتقدير المطلب للمتهم ما تقتضيه طبيعة الدعوى في هذا الإطار، ومن ثم فإن القول بأن وجود الخبير الاستشاري رهن بوجود خبير قضائي منتدب في الدعوى لهو قول مردود بأن هذا الرأي يقيد حق الابداع سيما وأن القانون لم يقيد هذا الحق بأية قيود وإنما أطلق سلطان المتهم في تعيين خبير الاستشاري أو مجموعة خبراء.

على أن الأمر لا يقف عند هذا الحد، وكما أسلفنا، ففي بعض الأحوال التي لا يكون هناك دراية فنية لعضو التحقيق بجرائم معينة جديدة، كما هو الشأن في جرائم الانترنت، بل

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

حتى وأن كان لهذا العضو دراية فنية إلا أنها بسيطة أو سطحية كمعلومات علمية مثلا، فهل يجوز لعضو التحقيق الاستعانة بخبير استشاري في هذا الشأن.[16]

أن الخبير الاستشاري هو الخبير الذي يقوم عمله على تحقيق هدفين، الأول القيام بدور توضيحي للواقعة ثم إزاحة الغموض وعن وقائع معينة فيها، فمثلا في جرائم الانترنت يكمن عمل الخبير الاستشاري في توضيح عمل الانترنت وموضوعها ثم يطرح رأيه حول النقاط الغامضة في جريمة من جرائم الأنترنت، لذلك فإن طبيعة عمل الخبير الاستشاري تحتاج إلى مهارات فائقة قد لا تكون متوافرة في الخبرة القضائية العادية.[17]وعليه فالسؤال المطروح موضوعه مدى إمكانية استعانة القائم بالتحقيق بخبير استشاري خلال مرحلة التحقيق ليس للسؤال عن نقطة غامضة وإنما لمتابعة التحقيق معه في كافة مراحله.

والواقع أن مسألة استخدام المحقق لخبير استشاري من النقاط التي تثأر بقوة في الدول التي لا تزال في مرحلة النمو الرقمي أو التقني، ومثل هذه المسألة سوف تثير العديد من المشاكل الإجرائية إذا أدركنا أن استعانة القائم بالتحقيق بخبراء استشاريين بشكل غير رسمي إنما يعد أمرا محققا.[18]وبالتالي يعد وجها من وجوه البطلان إذا كان مرد الدفاع في هذا الشأن قيام الدفاع بالاستفسار من المحقق عن النواحي الفنية التي انتهى إليها والتوصل إلى تقييم بأن المحقق أو جهة الاتهام إنما تعبر عن منطق بعيد عن مدارك الاتهام القضائي هنا.

ومثل هذا الأمر يحتاج من المشرع التدخل في منطق الخبرة الاستشارية لتكون سندا لجهات الاستدلال والتحقيق والاتهام وليس فقط للمتهم، بحيث يسمح لها بالاستعانة بالخبرة الاستشارية الرقمية كخبرة كاملة هنا دون التقييد خبراء للدول المعتمدين.

المبحث الثاني: الخبرة في مجال الانترنت والعالم الافتراضي.

تتعدد الأجهزة التي تخضع لفحص الخبير المعلوماتي، وللخبرة في المجال المعلوماتي أنواع، كما أن للخبير المعلوماتي أساليب معينة وفي النقاط التالية سوف نبحث ذلك بشيء من التفصيل.[19]

أولا: الأجهزة التي تخضع لفحص الخبير المعلوماتي:

هناك العديد من الأجهزة التي تخضع لفحص الطب الشرعي ومعرفة الدليل الخاص بارتكاب مثل تلك الجرائم، ومن هذه الأجهزة جهاز الرد الآلي، والهواتف، وجهاز النداء الآلي (Pager) والكاميرات الرقمية، والطابعة، والفاكس، ونظام تحديد المواقع عالميا (gps)، وأجهزة الحاسب المحمولة، والماسح الضوئي، وغيرها من الأجهزة التي يمكن أن يستخدمها

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

المشتبه فيه، وبفحص تلك الأجهزة يمكن أن نتعرف على كيفية الطريقة التي استخدمها المشتبه فيه في ارتكاب جريمته، ومن ثم نتعرض لجهاز الكمبيوتر كأهم تلك الوحدات في تخزين المعلومات.ويثور التساؤل حول مدى إمكانية قيام القضاء باللجوء إلى الخبرة حين اعتراض قضائه موضوعا من موضوعات الجرائم المعلوماتية، لا سيما وهو يواجه قاعدة خطرة تتمثل في حداثة موضوع العالم الافتراضي والرقمي ككل، مما يعني أن ما يمكن أن يردد كنتيجة للخبرة يمكن أن يكون غير الذي سوف يتقرر مستقبلا، ناهيك عن كونه يمكن أن يكون مثار جدل في الفترة المعاصرة.[20]

إن الخبرة التقنية في مجال الانترنت والعالم الافتراضي لا تشمل بالضرورة تلك النوعية من الخبرة الدراسية، فدراسات الكمبيوتر والانترنت لا ترتبط بمنهج دراسي أو بحثي معين أو حتى مدة زمنية يقضيها المرء دارسا في الجامعات والمعاهد المتخصصة، وإنما ترتبط بمهارات خاصة وبموهبة استعمال الكمبيوتر والانترنت والتعامل مع تقنية المعلومات، إذ أن أمهر مبرمجي نظم التشغيل حتى الأن مثل Bill Gates لم يكن تحصله العلمي يتجاوز المرحلة الثانوية، وذات الأمر ينطبق على عتاة الهكرة ومخترقي الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعلم الثانوي والسنوات الجامعية الأولى في أحسن الأحوال.ومن هذا المنطلق تتميز الخبرة في مجال تكنولوجيا المعلومات عن الخبرة في أي فرع آخر من الفروع التي يمكن أن تكون محلا للخبرة أمام القضاء.[21]

ثانيا: أنواع الخبرة في المجال المعلوماتي.[22]

الخبرة في المجال التقني قد تكون خاصة، وقد تكون عن طريق الجهات والمؤسسات التعليمية، وقد تتم عن طريق جهات الضبط القضائي وفيما يلي بيان لما أجمل:

أ- الخبرة الشخصية: وهذه تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة.[23]

وهي تضم في جنباتها الخبرة الفردية التي تعد أقوى وأهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والانترنت، ويكفي هنا أن نذكر أن المؤسسات الكبرى المتخصصة في الكمبيوتر والانترنت تسعى بكل جهودها إلى الاستعانة بأشخاص ثبتوا كفاءاتهم في مجال الكمبيوتر والانترنت، حتى عصاه القانون منهم، فهناك اتجاه اقتصادي يحاول جاهدا إثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون، وإنما يلزم اللجوء إلى الحلول الاقتصادية لكي يمكن أن يظلوا عاملين في إطار الأهداف الاقتصادية، بل إن من الدول ما

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

تسعى جاهدة إلى محاولة التعرف على قراصنة تحولوا مع مرور الوقت إلى رموز وطنية جراء تحركاتهم عبر الانترنت.

وإلى جوار الأفراد توجد المنظمات الخاصة في كافة المجالات والتي سوف يكون لها السبق في مجال الخبرة، وتختلف المنظمات الخاصة ما بين منظمات أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الالكترونية، وبين نوعية من المنظمات تسعى إلى فك طلاسم العالم الافتراضي على أسس تجارية.

ب- الجهات التعليمية :[24]ما كانت شبكة الانترنت تعد أحد منتجات العلم في حركته التقنية فإنه يمكن القول وبحق إن أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة في العالم الافتراضي يمكن أن تكون من خلال المؤسسات والجهات التعليمية، فهذه الأخيرة تعد مصدر دعم متكامل لمؤسسات الدولة ككل.وهذه المؤسسات تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضي على المشكلات التي تواجه البشرية، كما إن التفكير العلمي لا يمكن تجنبه في رصده للظاهرة الإنسانية، والاتجاه العالمي في رصد تطورات الجريمة عبر الانترنت يتجه إلى المؤسسات العلمية بحيث يتم دعمها ماديا ومعنويا، لتكون أفضل سبل المواجهة، سيما وإن المعتقد السائد في مواجهة الجريمة المالية والنقدية...الخ، فإنه ليس هناك أفضل من التقنيين في المعلوماتية لفك سر الجريمة عبر الانترنت.ولقد قامت عدة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها لتكون على أهمية الاستعداد لمواجهة الجريمة عبر الانترنت، ومن ذلك دراسات الكمبيوتر بشكل فائق في جامعة ستانفورد، كذلك معهد التكنولوجيا في ماساشوستس الذي قدم للبشرية خبراء على درجة عالية من التفوق.

ج- جهات الضبط القضائي: شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجراء على الأنترنت، وعلى رأس تلك الدول الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الانتربول.

وكان آخر نشاط مؤسسي في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية FBI أطلق عليه المعمل الإقليمي الشرعي للحاسوب[25]، ومقره سان دييجو San Diego، الذي تم افتتاحه في نوفمبر 2000 لكي يكون بيت خبرة عام متعدد الحواجي القضائية غرضه مكافحة التصعيد الخطير في الجريمة عبر الأنترنت، وذلك بتحليل وتصنيف الدليل الرقمي بحيث يتم إعداد محللين شرعيين للحاسب الآلي Computer

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

ForensicsExamuners الذين سوف يكون لهم أهمية كبرى في نطاق العمل على تكثيف مواجهة الجريمة عبر الانترنت.

ويبرز تعدد النواحي التي يتعامل معها المعمل الشرعي الجديد كونه يتكون من التقاء العديد من منظمات الضبط القضائي تتعاون فيما بينها لكي تتحقق الفائدة المرجوة منه، مثل إدارة مكافحة المخدرات Drug Enforcement Administration، ووحدة التحقيقات لمكافحة المجرمين Defense Criminal Investigative Services، ووحدة تحقيقات الجريمة في البحرية Naval Criminal Investigative Services، ووحدة الجمارك US Customs Services، ومكتب النائب العام للمقاطعة ومكتب حاكم المقاطعة وإدارة شركة كاليفورنيا.[26]

ثالثا: أساليب عمل الخبير المعلوماتي.للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله عليه أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه، وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي وإلا تعرض حكمها للطعن عليه بالنقض.

وهناك أسلوبان لعمل الخبير التقني.[27]

الأول: القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها – كما هو الشأن في التهديد Intimidation، أو النصب Fraud أو السب Defamation أو جرائم النسخ Infringement of copyrightsوبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق الأبيض ودعارة الأطفال وغيرها – ثم القيام بعملية تحليل رقمي لها لمعرف كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت IP الذي ينسب إلى جهاز الكمبيوتر الذي صدر عنه هذه المواقع.

الثاني: القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم، كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية ذلك حسب وزن الإنسان بإدعاء أنه إذا تم تتبع التعليمات الواردة فيها فلن يطالب الشخص بحالة إدمان، وأيضا كيفية زراعة المخدرات بعيدا عن أعين الغير، وأيضا كيفية أعداد القنابل وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها[28]، وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بتحديد مسار الدخول من

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

مكان ثابت، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشتركا لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها ويقوم بالولوج إلى الانترنت من محل إقامته، وهذا الأخير من الدفوع التي تلتزم محكمة الموضوع بالرد عليها.[29]

والخبرة في الجرائم المعلوماتية تساعد في المسائل الآتية:

1. الكشف عن الدليل الرقمي.
2. إجراء الاختبارات التكنولوجية والعلمية عليه لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديره لأجهزة إنفاذ وتطبيق القانون.
3. تحديد الخصائص الفريدة للدليل الرقمي.
4. إصلاح الدليل وإعادة تجميعه من المكونات المادية للكمبيوتر .Hard Drive
5. عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.
6. جمع الآثار المعلوماتية الرقمية Cyber trail digitalالتي قد تكون تبدلت خلال الشبكة المعلوماتية.
7. استخدام الخوارزميات Algorithm للتأكد من أن الدليل لم يتم العبث به أو تعديله.[30]
8. تحريز الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى.
9. تحديد الخصائص المميزة لكل جزء من الأدلة الرقمية مثل المستند الرقمي، البرامج، التطبيقات، الاتصالات، الصور، الأصوات... وغيرها.[31]

رابعا: وسائل الخبير في اكتشاف الدليل الالكتروني.

ثمة وسائل قد تساعد الخبير في الوصول إلى المجرم المعلوماتي ومعرفة كيفية وقوع الجريمة، ومنها الوسائل المادية ومنها الإجرائية، ونتناولها على النحو التالي:[32]

أولا: الوسائل المادية: هي الأدوات الفنية التي غالبا ما تستخدم في بنية نظام المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة، ومن أهمها:

1- عنوان بروتوكول الأنترنت **IP** والبريد الالكتروني وبرامج المحادثة:

عنوان الانترنت هو المسؤول عن تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجهات والشبكات

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

المعنية نقل الرسالة، وهو يوجد بكل جهاز مرتبط بالأنترنت.ويتكون من أربعة أجزاء وكل جزء يتكون من أربع خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الكمبيوتر الذي تم الاتصال منه.[33] وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة الانترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك.

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 بين فيه عنوان IP، مع ملاحظة أن عنوان الانترنت قد يتغير مع كل اتصال بشبكة الانترنت.أما في حالة استخدام أحد البرامج التحادثية كأداة للجريمة فإنه يتطلب تحديد هوية المتصل، كما تحدد رسالة البريد الالكتروني عنوان شخصية مرسلها حتى ولو لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الالكتروني معلومات صحيحة.[34]

2- البروكسي:**PROXY** يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمر وتوفير خدمات الذاكرة الجاهزة .Cache Memory

وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أم إنه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين [35] ومن أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دورة قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

3- برامج التتبع: تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم وتقديم بيان بها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان التي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الانترنت المستضيفة للمحترف، وأرقام مداخلها ومخارجها على شبكة الانترنت ومعلومات أخرى.[36]

4- نظام كشف الاختراق **Instrusion Detection:** ويرمز له اختصارا بالأحرف IDS وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد من الكمبيوتر أو الشبكة.[37]

ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومن بعض ملفات التشغيل الخاصة بتسجيل الأحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، والتي يطلق عليها أهل الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات كمبيوترية خاصة.[38]

ثانيا: الوسائل الجرائية: ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:[39]

1- اقتفاء الأثر: من أخطر ما يخشاه مجرم نظام المعلومات تقصى أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولادها نصيحة هي قم بمسح آثارك CoverYoursTracks، فلو لم يقم المخترق بمسح آثاره فمؤكد أنه سوف يتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم، ويمكن تقصي الأثر بطرق عدة سوء عن طريق بريد الالكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

2- الاطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته:

ينبغي على المحقق وهو بصدد التحقيق في احدى الجرائم المعلوماتية كالجرائم المتعلقة بشبكة الانترنت أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما ينبغي عليه الاطلاع على عمليات النظام المعلوماتي كقاعدة

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

البيانات وإداراتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، ومدى توزيع الصلاحيات للمستفيدين، وإجراءات أمن العاملين، وأسلوب النسخ الاحتياطي والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد والبرامج التي تعالج بيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام.

3- الاستعانة بالذكاء الاصطناعي: أثبتت تقنيات الكمبيوتر نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، كما يمكن الاستعانة بالذكاء الاصطناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات، ومن ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالكمبيوتر وفق برامج صممت خصيصا لهذا الغرض.[40]

خامسا: دور الخبير التقني في حفظ الأدلة الالكترونية.

وفي إطار جرائم الانترنت فإنه يميز بين الأدلة التي يلزم التحفظ عليها داخل جهاز الحاسب الآلي وبين تلك التي يلزم بقاؤها في العالم الافتراضي وبين أيضا تلك النوعية من الأدلة التي تنتمي إلى العالم الرقمي، ومع ذلك يمكن اللجوء إلى إخراجها من إطار الحاسوب والعالم الرقمي إلى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة في الجريمة تساعد في الإدانة وكذلك في البراءة.[41]إن التحفظ على الأدلة داخل جهاز الكمبيوتر Locating Computer evidenceمن العمليات المعقدة التي تحتاج بداية إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر، وهذا الأمر يستلزم بالضرورة قيام الخبير التقني بالكشف بداية على المدى الذي عليه صحة حركة الكمبيوتر سيما من حيث الخلل والعطب ويعطي العدوان الفيروسي مثالا حيويا هنا، إذا يكفي أن يكون هناك فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستفادة هذا الكمبيوتر، ومثل هذا الاتجاه نجده في التشريع الإنجليزي.

وتتم عملية حفظ الأدلة داخل جهاز الكمبيوتر بأساليب متعددة تتمثل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي وأقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه ذلك، إن الدليل الرقمي هو في العادة ملف يحتوي على بيانات رقمية تعطي مظهرا معلوماتيا محددا غير قابل للتحويل إلى مظهر آخر إلا بإجراء تعديلات رقمية في البيانات المذكورة.[42]

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

أما بالنسبة لعملية حفظ الأدلة في العالم الرقمي فإنه يتطلب من الخبير التقني القيام برصد موقع الإنترنت أو المعلومات التي تشير إلى الجريمة والتي تكون في مظاهر مختلفة الأشكال، كما لو كانت الجريمة من جرائم القذف والسب في غرفة المناقشة، ففي مثل هذه الحالة الأخيرة يتم اللجوء إذا ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي لكي يمكن للتوصل إلى تحديد موضوع السب والقذف وتاريخه وإذا كانت الجريمة من جرائم النشر عبر الانترنت فقد يكتفي بمجرد اللجوء إلى ذاكرة الحاسب الآلي المستخدم هنا دون وحاجة إلى تحديد الخادم ... الخ.ففي مثل هذه الحالات يقوم الخبير باستخدام برمجيات مساعدة للتوصل إلى القيم بالحفظ في العالم الرقمي، كما هو الشأن في حجز وتشفير مثل هذه المواقع بعد تعديد جدليتها ودقتها ومسارها، وهذا أمر ذلك يعد قرينة على أنه هو من ارتكب الجريمة.

وتستدعي عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير بعرض الأدلة في المحكمة أو على جهات التحقيق، ومثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة، كما هو الشأن حال عرض الدليل المقدم إلى محكمة الموضوع أمام جهة قضائية أعلى كالاستئناف أو النقض (في حالة اختصاصها بالموضوع – الطعن مرتين).[43]

الخاتمة

فعلى الرغم من أن ارهاصات الثورة التكنولوجية في مجال الاتصال عن بعد قد أفرزت العديد من الجرائم ذات الطبيعة الخاصة، فما زالت إجراءات البحث عن هذه الجرائم وضبطها تتم في إطار النصوص الإجرائية التقليدية التي وضعت لكي تطبق على الجرائم التقليدية التي تنص على القوانين العقابية[44]، الأمر الذي سيترتب عليه الكثير من المشكلات بالنسبة لضبط هذه الجرائم المعلوماتية ذات الكيان المعنوي والتي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الانترنت، كما هو الحال في شأن جريمة غسل الأموال عبر الانترنت، فيتعذر تبعا لذلك اتخاذ إجراءات جميع الدليل بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات.ولذلك نجد أن بعض الفقه في ألمانيا يشكك في إمكانية الدخول إلى أنظمة تقنية المعلومات لدى الحاسبات الأخرى التي توجد بالخارج بغرض ضبط البيانات المخزنة بها لأنه بدون وجود اتفاق بين الدول المعينة بتنظيم ذلك، فإن اتخاذ مثل هذا الإجراء يعد خرقا لسيادة كل دولة على إقليمها ويخالف الاتفاقيات الثنائية الخاصة بإمكانية التعاون في مجال العدالة القضائية.[45]

E-ISSN : 2571-9742
P- ISSN: 1112-945X
DM

ويلاحظ في هذا المجال تصادم التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية، وذلك لأن هذا التفتيش يتم – غالبا – على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، الأمر الذي قد يتجاوز النظام المعلوماتي المشتبه به إلى أنظمة أخرى مرتبطة، نظرا لشيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول ولا شك في أن امتداد التفتيش إلى نظم غير النظام محل الاشتباه قد يمس – في الصميم – حقوق الخصوصية المعلوماتية لأصحاب النظم المعلوماتية التي يمتد إليها التفتيش.

الإحالات :

[1] د. محمود جمال الدين زكي، الخبرة في المواد المدنية والتجارية، مطبعة جامعة القاهرة، 1990، ص 11.

[2] الخبرة أجراء من إجراءات التحقيق، وقد نصت على ذلك المادة (491) تعليمات من أن "انتداب الخبراء من إجراءات التحقيق الابتدائي وإذا افتتحت به النيابة الدعوى فإنه يعتبر تحريكا لها"، كذلك نصت المادة (492) تعليمات "على أعضاء النيابة الرجوع إلى أحكام المرسوم بقانون رقم 96 لسنة 1952 بشأن تنظيم الخبرة أمام جهات القضاء.

[3] الخبرة في المجال القضائي تستدعي توافر ركنين لها، ركن شكلي ويراد به التخصص في مستوى الدراسة والعلم الذي اكتسبه بمعنى أن يكونه مقتنا من قبل مؤسسة علمية معترف بها كجامعة أو معهد أو غير ذلك، والركن الثاني موضوعي ويقصد به أن يكون الخبير فيها مستخدما لأدواته العلمية والعملية.

- عمر بن يونس، الإثبات الجنائي عبر الأنترنت، ط 1، دار الفكر الجامعي، الاسكندرية، 2012 ، ص 30.

[4] J. Arquilla, & D. Ronfeldt, « Cyberwariscoming ! », Comparative Strategy, vol. XII, n° 2, printemps 1993, p120.

[5] محمد أنور عاشور، التحقيق الجنائي، بدون ناشر، 198دار الجامعة الجديدة، الاسكندرية ، مصر ، 2014 ، ص 222.

[6] نشر هذا القانون بالوقائع المصرية في العدد رقم 96 في 1952/5/26.

[7] المستشارة حسن علام، وسائل الاتباث في الجريمة الالكترونية، مؤسسة نوفل ، بيروت، لبنان ،2013، ص 192.

[8] Y. Barthe & C. Lemieux, « Les risques collectifs sous le regard des sciences du politique. Nouveaux chantiers, vieilles questions », Politix, n° 44, 1999,p 200.

[9] Y. Barthe, M. Callon& P. Lascoumes, « Réponse à Franck Aggeri », Gérer et comprendre, n° 68, juin 2002, p80.

[10] U. Beck, Pouvoir et contre-pouvoir à l'heure de la mondialisation, Flammarion Champs Essais, 2009, p200.

[11] D. Bigo, « La mondialisation de l'(in)sécurité ? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation », Cultures & Conflits, n° 58, été 2005, p205.

E-ISSN : 2571-9742
P- ISSN: 1112-945X

[12] S. Brint, In an Age of Experts. The ChangingRole of Professionals in Politics and Public Life, Princeton, Princeton UniversityPress, 1994,p 70.
[13] P. Collier, « Spécial Internet : Fin de l'immunité pour les opérateurs techniques ? », Contrefaçon Riposte, n° 18/19, oct. nov. 2006, p 150.
[14] عمر محمد أبو بكر يونس، المرجع السابق، ص 890.
[15] B. Dupont & V. Gautrais, « Crime 2.0. le web dans tous ses états », Nouvelle revue internationale de criminologie, vol. VII, 2010, p 300.
[16] ENISA, Annual Incident Reports 2011, octobre 2012.p123
[17] عمر محمد أبو بكر يونس، المرجع السابق، ص 891.
[18] D. Garland, « On the concept of moral panic », Crime, Media, Culture, vol. IV, n° 1, avril 2008, p 305.
[19] C. Gilbert, Conférence Mines ParisTech : De la gestion des risques à l'organisation de la résilience. Implications d'un changement de perspectives, 7 juin 2011. F. Guarnieri& E. Przyswa, « Cybercriminalité - contrefaçon : les interactions entre 'réel et virtuel' », Cahiers de la sécurité n° 15, 2011, p 50.
[20] F. Guarnieri& E. Przyswa, « Cybercriminalité et contrefaçon : pour une nouvelle analyse des risques et des frontières », Murs et frontières, Hermès, n° 63, 2012,p 90.
[21] https://doi.org/10.3917/sestr.011.0049.
[22] عمر أبو بكر بن يونس، الإثبات الجنائي عبر الأنترنت، مرجع سابق، ص 36.
[23] حسين بن سعيد بن سيف الغافري،السياسة الجنائية في مواجهة جرائم الانترنت، العبيكان للنشر ، الرياض، 2015، ص 442.
[24] حسين بن سعيد بن سيف الغافري، مرجع سابق، ص 443 وما بعدها.
[25]The regional computer forensies.laboratoryTE.USA. cyber criminalite.p234
[26]Jerry seper – FBI steps up efforts to fights crimes related to computers, the Washington times, available on line nov. 2000 at : http://www.infowar.com
[27] عمر أبو بكر بن يونس، المرجع السابق، ص 42.
[28]Patrick S, Chen – An Automaic System for Collection Crime information on the internet – 31 October 2000 – Journal of information Law and Technology – Available online in jan 2001.p164. at : http://elj.warwick.ac.uk/jilt/00-3/chenhtml
[29] F. Guarnieri& E. Przyswa, « Cybercriminalité et contrefaçon : pour une nouvelle analyse des risques et des frontières », Murs et frontières, Hermès, n° 63, 2012.p.312
[30] الخوارزميات Algorithm، هي مجموعة من التعليمات التي يمكن أن تتبع لإنجاز عمل ما بعدد محدد من الخطوات وذلك عبر تجزئة المسألة البرمجية المراد حلها إلى أجزاء صغيرة بسيطة وبتجميع هذه الأجهزة يمكن التوصل إلى حل صحيح.
[31] MarkMonitor, Brandjacking Index, été 2009.p153.
[32] حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، المرجع السابق، ص 398.
[33]Arabiat 2000 On Line available at www.arabia.com

E-ISSN : 2571-9742
P- ISSN: 1112-945X

[34] سليمان بن مهجع العنزي،سليمان بن مهجع العنزي، المرجع السابق، ص 104 – 105. محمد أمين البشري: التحقيق في جرائم الحاسب الآلي والانترنت، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، العدد 30، جامعة نايف العربية للعلوم الأمنية، الرياض، 1420هـ، ص 186..

NOR2000 (2002), ON Line available at : www.non2000.com/network/html

[35] د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، 2002، ص 82.

[36] من الأمثلة على هذا البرامج برامج Hack Tracer v 1.2، وهو يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الاختراق التي تعرض لها جهازه، يحتوي على اسم وتاريخ الواقعة وعنوان IP التي تمت من خلاله عملية الاختراق، واسم الدولة التي تمت منها محاولة الاختراق واسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق بما فيها أرقام هواتفها والفاكسات الخاصة بها وآخر تحديث قامت به في أجهزة الخدمة بها، وغيرها من المعلومات.

- سليمان بن مهجع العنزي، المرجع السابق، ص 100.

[37]Bace, Rebecca (2000) Interusion Detection, Indianapolis, Indiaina MecmillabTechniccat Publishing.p.116.

[38] محمد بن نصير محمد، الاتباث في الجرائم الالكترونية، دار الحامد للنشر والتوزيع ، عمان ، الاردن ، ص 84.

[39] حول هذا الموضوع أنظر: سليمان بن مهجع العنزي، المرجع السابق، ص 104 – 105.

د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، 2002، ص 82.

[40] S. Leman-Langlois, « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial », Criminologie, vol. XXXIX, n° 1, printemps 2006, p99.

[41] OCDE, OECD Conference on empowering e-consumers : strenghtening consumer protection in the Internet economy, Summary of key points and conclusions, 23 avril 2010.p217.

[42] E. Przyswa, Cybercriminalité-Contrefaçon, FYP, 2010p.98.

[43] P. Sommer & I. Brown, « ReducingSystemicCybersecurityRisk », Organisation for EconomicCooperation and Development. Working Paper n° IFP/WKP/FGS 3, 2011.

[44] حسين بن سعيد بن سيف الغافري، المرجع السابق، ص 414.

[45]- Mohrenschlager « Manfred » : Computer crimes and other crimes against information technology in Germany, Rev. Inter. De. Dr. Pen. 1993. P. 351.