

# التحري الجنائي في مسرح الجريمة الإلكترونية\*

أ. بن فريجة رشيد\*\*

د. ميهوب يوسف\*\*\*

---

\* تاريخ التسليم: 2015/2/9م، تاريخ القبول: 2015/12/21م.  
\*\* أستاذ باحث (مساعد أ) / جامعة عبد الحميد ابن باديس/ الجزائر.  
\*\*\* أستاذ مساعد/ جامعة عبد الحميد ابن باديس/ الجزائر.

يستخدمها المجرمون للاستفادة من التكنولوجيا لتحقيق المكاسب الشخصية غير المشروعة مستفيدين مما توصلت إليه التكنولوجيا من تقدم للوصول إلى أغراضهم، فعلى سبيل المثال تقدر تكلفة الخسائر التي تتلقاها الشركات الأمريكية بسبب الاستخدام غير القانوني للكمبيوتر بما مقداره من خمسمائة مليون إلى خمسة بلايين دولار سنوياً<sup>(1)</sup>.

التحقيق في الجرائم المعلوماتية أمر يتطلب نوع من الدهاء والخبرة التقنية والفنية فهي تختلف عن الجرائم التقليدية وإن كانت تتشابه معها في إجراءات البحث والتحري من معاينة والتفتيش في مسرح الجريمة وجمع الأدلة إلا أنها تتميز ببعض الخصوصية كونها تقع داخل الحاسب الآلي أو داخل نظامه.

كما تتميز الجرائم المعلوماتية بصعوبة اكتشافها وإثباتها وذلك يعود إلى أنها لا تخلف آثاراً ظاهرة تنصب على البيانات الموجودة في النظم المعلوماتية، فالتحقيق في هذه الجرائم يستوجب استحداث الأساليب العلمية والتقنية ومواكبة التقدم التكنولوجي.

### أهمية الدراسة:

إن دراسة موضوع التحري الجنائي في مسرح الجريمة الإلكترونية من الموضوعات الحديثة التي جذبت اهتمام الكثير من الباحثين في عصرنا الحالي نظراً لتطور الوسائل التكنولوجية ويتطور هذه الأخيرة أصبحت للجرائم أبعاد أخرى، إذ ظهرت جرائم تسمى بالجرائم الإلكترونية، تلك التي تعد من الجرائم التي يصعب التحقيق فيها ويجب أن تتوفر عدة وسائل بشرية أو مادية للتحقيق في مسرح الجريمة الرقمية، وبالتالي أردنا أن نسلط الضوء على طرق البحث والتحري في مثل هذا النوع من الجرائم الذي يتميز بخصوصيته بالمقارنة مع الجرائم التقليدية.

### مشكلة الدراسة وتساؤلاتها:

تسعى هذه الدراسة إلى تعرف كيفية التحقيق في الجرائم المستحدثة في عصرنا الحالي، ألا وهي الجرائم المعلوماتية أو الإلكترونية، وذلك نظراً للاستعمال الواسع للحاسب الآلي، إذ إن هناك عدة صعوبات تواجه التحريات والتحقيقات في مثل هذا النوع من الجرائم، وهذا ما سنحاول توضيحه في هذا الموضوع.

أما تساؤلاتها فيمكن تلخيصها على النحو الآتي :

- ◀ ما هي أهم طرق التحري في الجرائم المعلوماتية؟
- ◀ وكيف يتم استخلاص الأدلة في مثل هذا النوع من الجرائم؟ وهل الدليل الإلكتروني كاف للكشف عن الجاني؟

### منهجية وخطة الدراسة:

اعتمدنا لدراسة موضوع التحري الجنائي في مسرح الجريمة المعلوماتية على المنهج التحليلي من أجل تقديم دراسة تحليلية حول كيفية استخلاص الأدلة المعلوماتية من أجل تعقب الجناة، وللإجابة عن التساؤلات التي طرحت سابقاً ارتأينا تقسيم الموضوع إلى ثلاثة مباحث، تمثل المبحث الأول في مفهوم الأدلة الإلكترونية، أما المبحث الثاني فسنتناول فيه استخلاص الأدلة الإلكترونية، أما بالنسبة للمبحث الثالث فسنتناول فيه إلى كيفية تعقب مرتكبي الجرائم الإلكترونية.

### ملخص:

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة في عالمنا المعاصر، ويتطور الجريمة كان لزاماً على رجال البحث والتحري تطوير امكانياتهم لمكافحة هذا النوع من الجرائم، وبطبيعة الحال فإن التحقيق في أي جريمة سيكون وفق إجراءات محددة كاستخلاص الأدلة، وتعقب الجناة، وهذا ما سنحاول توضيحه في هذه الدراسة.

الكلمات المفتاحية: الجريمة الإلكترونية- التحري الجنائي-

مسرح الجريمة

### The criminal investigation in Cyber crime Scene

### Abstract:

*Electronic crime of modern crimes in the contemporary world, and with the evolution of the crime, there was the need for specialists in the research and investigation to develop their potential to combat this type of crime, and of course, the investigation of cyber crime will be in accordance with specific procedures for the conclusion of the evidence, track down cybercriminals.*

**Key words:** *electronic crimes, criminal investigation, crime scene*

### مقدمة:

التحقيق الجنائي لما يتضمنه من قواعد إجرائية وفنية في التعامل مع مسرح الجريمة كالانتقال والمعاينة والتفتيش، باعتباره مكان الحادث الذي شهد النشاط الإجرامي، تنبثق منه الأدلة بأنواعها المختلفة، إذ يتزود بها الباحث أو المحقق الجنائي من خلال تدوينه واستنباطه للمعلومات الضرورية، حتى يستلهم بذلك حقيقة النشاط المرتكب سواء أكان مسرحاً لجريمة تقليدية أم لجريمة مستحدثة كالمترتبة بالحاسب الآلي.

تعد الجرائم المترتبة بالحاسب الآلي نمطاً حديثاً من أنماط الجريمة لم تعرفها إلا المجتمعات المعاصرة، فقد أدى الاستخدام الواسع لأجهزة الحاسب في المعاملات الحكومية المدنية والعسكرية والمعاملات التجارية إلى دفع بعض الأشخاص إلى الاستفادة غير القانونية من هذه التكنولوجيا المتقدمة، ومن الأمثلة على استخدام الحاسب أداة للجريمة سرقة الخدمات وذلك بأن يقوم مجرم الحاسب بالاستخدامات غير المشروعة للحاسب أو استخدام الحاسب قانونياً ولكن لأغراض غير مسموح بها، بما في ذلك الدخول غير المشروع على نظام الحاسبات الخاصة ويمكن استخدام المعلومات الموجودة على الحاسب لأغراض شخصية، ومن أجل تحقيق الأرباح الشخصية كما يمكن استخدام الحاسب من أجل إجراء أنواع متعددة من العمليات غير المشروعة كالدخول إلى حسابات العملاء وتحويلها إلى حساب شخصي أو سرقتها بالإضافة إلى سرقة الممتلكات عن طريق الحاسب بطريقة غير شرعية، كل ذلك من الوسائل التي

## المبحث الأول: مفهوم الأدلة الإلكترونية

للأصل ولها ذات القيمة العلمية والحجية الثبوتية الشيء الذي لا يتوافر في أنواع الأدلة التقليدية، ما يشكل ضماناً شديداً للفعالية للحفاظ على الدليل ضد الفقد، والتلف، والتغيير، عن طريق عمل نسخ طبق الأصل من الدليل.

3. الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد اتلافها، وإظهارها بعد إخفائها، ما يؤدي إلى صعوبة التخلص منها، وتعد هذه الخاصية من أهم خصائص الدليل الرقمي، بالمقارنة مع الدليل التقليدي، فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي جرى حذفها أو إلغائها، سواء حصل ذلك بأمر الحذف (Delete) أو حصل بإعادة تهيئة أو تشكيل للقرص الصلب والبرامج التي تم إتلافها أو إخفائها، سواء كانت صوراً أو رسوماً أو كتابات أو غيرها، ما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها.

4. الأدلة الجنائية الرقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات اتصال متعددة لحدود الزمان والمكان<sup>(7)</sup>.

5. ويعتبر الأستاذ أمين البشري أن الدليل الرقمي لا يعتبر دليلاً مادياً بالدرجة الأولى بل يمكن في بعض الحالات تخيله في شكله وحجمه، وهذا ما يتميز عن الدليل التقليدي الذي يكون مادياً في معظم الأحيان<sup>(8)</sup>.

### المبحث الثاني: أنواع الأدلة الإلكترونية وكيفية استخلاصها

إن التعامل مع مسرح الجريمة سواء أكان مسرحاً مادياً أم مسرحاً معلوماتياً يحتم ضرورة إتباع إجراءات التحقيق الجنائي العادي والمتفق عليها لحماية الأدلة وإبراز قيمتها الاستدلالية غير أن تعدد أساليب وطرق حفظها واستخلاصها تختلف من مسرح الجريمة المادي إلى مسرح الجريمة الإلكتروني أو الرقمي، ذلك أن التطبيقات أو البرامج والبيانات المرقمة عنصران أساسيان يتطلب على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية، جمعهما واستخلاصهما.

#### المطلب الأول: أنواع الأدلة الإلكترونية

توجد الأدلة الإلكترونية على عدة أشكال مختلفة، بحيث يجب علينا معرفتها ما يسهل على رجال البحث والتحري الوصول إليها عند التفتيش فهي قد تكون في شكل<sup>(9)</sup>:

◆ الأقراص المرنة والأقراص الصلبة وهي من أهم الأدلة لأنها تحتوي على البيانات وعلى المعلومات وعلى كلمات المرور وعلى الصور وعلى التقارير وعلى خطط ارتكاب الجريمة مثلاً وغير ذلك.

◆ أشرطة تخزين المعلومات التي تستخدم عادة لحفظ النسخ الاحتياطية.

◆ أدلة ورقية مثل مخرجات الطباعة والتقارير والرسوم البيانية.

◆ أجهزة الحاسبات الآلية وتتضمن معها ملحقات الحاسب من شاشات وغير ذلك.

في أثناء عملية البحث والتحري في مسرح الجريمة الإلكترونية يجري كشف مجموعة من الأدلة تسمى بالأدلة الإلكترونية أو الرقمية، وهذا ما سنركز عليه في هذا المبحث، إذ سنقسمه إلى مطلبين؛ يتمثل المطلب الأول في تعريف الأدلة الإلكترونية، أما المطلب الثاني فتطرقنا فيه إلى خصائص الأدلة الإلكترونية وتمييزها عن الأدلة التقليدية.

#### المطلب الأول: تعريف الأدلة الإلكترونية

إن الدليل الإلكتروني عبارة عن معلومات يقبلها المنطق والعقل ويعتمدها العلم، ويتم الحصول عليه بإجراءات قانونية وعلمية بترجمة البيانات الحاسوبية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه<sup>(2)</sup>.

واعتبر الفقه الجنائي الأدلة الجنائية الرقمية بأنها التي تشمل على جميع البيانات الإلكترونية أو الرقمية التي يمكن أن تثبت وجود وقوع الجريمة، أو توجد علاقة بين الجريمة المرتكبة والجاني أو توجد علاقة بين الجريمة والضحية والبيانات الرقمية هي مجموعة الأرقام التي تمثل المعلومات الرقمية المختلفة الواردة سواء أكانت رسومات ونصوص مكتوبة أم الخرائط والصوت والصورة<sup>(3)</sup>.

ويعرف الدليل الرقمي أيضاً على أنه ذلك الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل مجالات أو نبضات مغناطيسية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويجري تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه، وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون<sup>(4)</sup>.

ويعرف آخرون الدليل الإلكتروني على أنه ذلك الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها<sup>(5)</sup>.

#### المطلب الثاني: خصائص الأدلة الإلكترونية وتمييزها عن الأدلة التقليدية

للأدلة الإلكترونية مجموعة من الخصائص تميزها عن الأدلة التقليدية وهذا ما أكده المختصين في مجال البحث الجنائي، وتتمثل هذه الخصائص فيما يأتي<sup>(6)</sup>:

1. الأدلة الرقمية تتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية، واستخدام نظم برمجية حاسوبية.

2. يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة

المحقق العادي<sup>(12)</sup>.

### الفرع الأول: الضوابط الفنية التي يجب مراعاتها أثناء جمع الأدلة الرقمية

يجب على فريق التفتيش مراعاة مجموعة من الضوابط أثناء التحري وضبط جريمة الحاسب الآلي حتى يسهل الحصول على الأدلة وتحريزها تلك التي هي كالتالي<sup>(13)</sup>:

◆ تحديد نوع نظام المعالجة الآلية للمعلومات - كمبيوتر معزول أو متصل بالشبكة - لأن عملية البحث والتحري والتفتيش تكون صعبة في حالة وجود محطات طرفية.

◆ حصر الطرفين وتحديد طبيعة الروابط الموجودة فيها وذلك لمعرفة الطريقة التي يتم بها نقل المعلومات من موقع لآخر - الأسطوانات، الأشرطة المغنطة، خطوط الاتصال أو أي وسيط معلوماتي - ومن المهم ما إن كانت للأجهزة حاسبات خارج نظام معالجة المعلومات وبها إمكانية الاتصال بالشبكة ثم يقوم المختصون بتعرف كل آلة وماركتها وموديلها وقدرتها على نقل المعطيات.

◆ اتخاذ الحيطة والحذر لأن الدليل في المعالجة الآلية للبيانات يمكن أن يختفي في وقت قصير.

◆ اتخاذ التدابير لمنع الجاني من التدخل من خلال وحدة طرفية لإتلاف المعلومات المخزنة في الوحدة الرئيسية للجهاز - الوحدة الأم-السيرفر.

◆ التعامل مع تيار الكهرباء بطريقة تؤدي إلى الحيلولة دون التلاعب في المعلومات أو محوها.

◆ فصل خطوط الهاتف أو نحو ذلك خشية استعمال مودم في جهاز المعالجة الآلية أو محوها.

◆ إبعاد أي شخص عن أجهزة الحاسب الآلي.

### الفرع الثاني: جمع الأدلة الإلكترونية

يتطلب جمع الأدلة مجموعة من الإجراءات والتمثلة في المعاينة والتي تلعب دورا مهما في كشف غموض مسرح الجريمة، إلا أن دورها في كشف خبايا مسرح الجريمة المعلوماتية وضبط مجموعة من المعلومات التي قد تفيد إثبات ارتكابها ووقوعها، قد لا ترق إلى نفس الدرجة من الأهمية ومرد ذلك إلى الاعتبارات الآتية<sup>(14)</sup>:

◆ مشكلة إخفاء الدليل الإلكتروني بتعديله أو محوه في ثوان قليلة.

◆ إمكانية تلاعب الجاني بالبيانات عن بعد أو محوها عن طريق التدخل من خلال وحدة طرفية، لذلك أي تغيير أو تعديل في المعلومات المسجلة في ذاكرة الحاسوب أو وسائط التخزين أو بنك المعلومات أو قاعدة بيانات، قبل قيام سلطة التحقيق بإجراء المعاينة وهذا ما انتهجه القوانين الوضعية المختلفة في تشريعاتها وما يهمنها هو التشريع الجزائري، إذ نص على هذا الأمر في قانون الإجراءات الجزائية وبالضبط ما جاء في نص المادة الثالثة والأربعون منه<sup>(15)</sup>.

◆ الجرائم الإلكترونية قلما يتخلف عند ارتكابها آثارا مادية تتمثل في بيانات غير مرئية.

◆ أجهزة المودم والتي تستخدم في نقل المعلومات ويمتاز بعضها بإمكانية العمل كجهاز الرد على رسائل الهاتف Answer Machine ما يجعله دليلا محتملا بالغ الأهمية، وعند العثور على مودم يجب الاهتمام بتسجيل الكابلات المتصلة به عند ضبطه، وكيف كانت متصلة بالحاسب أو الهاتف مع التقاط وتسجيل رقم الهاتف.

◆ القطع الإلكترونية التي يمكن أن تكون أدلة مهمة كأجهزة الإرسال التي تكون في صورة قطعة إلكترونية، ولذلك يجب الاهتمام بفحصها للتأكد من طبيعتها وبخاصة في قضايا التجسس، وقد يكون الدليل الحاسم في قضية ما قطعة إلكترونية ملقاة في صندوق مهمل في أحد زوايا الغرفة ربما تكون جهاز الإرسال الذي يمكن المجرم من إرسال معلوماته إلى شريكه.

◆ الطابعات وأجهزة التصوير للمستندات: وما قد تحتويه من أوراق مطبوعة أو مصورة أو ما هو مخزن في ذاكرتها من معلومات.

◆ البرامج وهي تمثل الأدوات الرئيسية التي يستغلها المجرم في ارتكاب جريمة نظم المعلومات.

إن للأدلة المعلوماتية أهمية كبيرة؛ إذ تعدّ من وسائل الإثبات الحديثة ولها خصائص فنية مختلفة ما يؤهلها لتكون إضافة جديدة لأنواع الأدلة الجنائية، وذلك نظرا لأن<sup>(10)</sup>:

1. الأدلة الرقمية لا تعتبر أقل من الأدلة المادية فحسب، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعين. وتتكون الأدلة الرقمية تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة ولا يدركها الرجل العادي بحواسه.

2. يعدّ من الصعوبة إتلاف الأدلة الجنائية الرقمية في جميع الأحوال التي يمكن استرجاعها من الحاسب الآلي بعد محوها أو القضاء عليها.

3. يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية للشيء الذي لا يتوفر في أنواع الأدلة الأخرى.

4. يمكن تعرّف الأدلة الرقمية المزورة بمقارنتها مع الأدلة الأصلية.

5. ليس شرطا أن تتواجد الأدلة الرقمية في مسرح الجريمة التقليدي بل يمكن تواجدها أيضا في مكان الجريمة الافتراضي أي داخل الشبكة العنكبوتية Virtual Scene of Crime.

### المطلب الثاني: أساليب جمع الأدلة الرقمية وأماكن تواجدها

إن الأدلة الفنية المضبوطة في جرائم نظم المعلومات لها أهمية كبرى، وقد يكون الفصل فيها بين الإدانة والبراءة للمتهم، ويجب أن يعتني فريق التفتيش وفريق جمع الأدلة بتخزين هذه الأدلة في بيئة مناسبة حتى لا تفسد والقاعدة الذهبية هنا هي أن المكان المناسب لحفظ الأدلة هو المكان المناسب لك فإذا كان المكان مريحا لك فسيكون مناسباً للأدلة<sup>(11)</sup>. من أجل التعامل مع الأدلة الرقمية لابد من تقديمها في المحكمة عن طريق الشهود الخبراء والتقنيين باستخدام أساليب الكشف عن وجودها ومحتواها وهذا ما يضعه في فئة الأدلة الكامنة، ولا يمكن تقديمه من قبل

أقوى مظاهر التعامل القانوني أو القضائي مع ظاهرة تكنولوجيا المعلومات والانترنت، فهي تؤدي دورا لا يستهان به إزاء نقص المعرفة القضائية الشخصية لظاهرة الانترنت (17).

إن عمليات الضبط والحجز والتأمين وتحليل الأدلة الرقمية المخزنة في شبكات المعلوماتية هي التحدي الذي يواجه أجهزة العدالة الجنائية في هذه المرحلة التي تعاني تلك الأجهزة من الأمية المعلوماتية.

وفي الوقت الذي جرى فيه إعداد الخبرة والمختبرات الأكاديمية الجنائية المهمة بالبحث الإلكتروني كنتيجة لانتشار تقنية المعلومات في مجال الجريمة، الشيء الذي يتطلب معاملة ومختبرات خاصة، وإعداد الموارد البشرية كخبرة تجمع بين التكوين القانوني ومهارة التحقيق الإلكتروني، وعلاوة على ذلك يتطلب لمواجهة هذه الجرائم التنسيق والتعاون بين أجهزة تنفيذ القوانين والمؤسسات التي تقوم بتقديم خدمات المعلومات (18).

#### الفرع الثالث: أماكن تواجد الأدلة الإلكترونية

تتواجد الأدلة الإلكترونية في عدة أماكن ولكن هناك بعض المساحات التي يقوم المختصين بالبحث فيها أكثر من غيرها، فنجدها تتواجد في (19):

#### أولاً: جيوب المتهم

يحمل الكثير من مستخدمي الحاسب بعض الأقراص المرنة في جيب القميص، ويكون بها عادة الكثير من المعلومات، ومع تقدم العلم فهناك الآن أقراص مرنة رخيصة تتسع لأكثر من «مائة ميغا بايت» من المعلومات ويمكن أن توضع بسهولة في جيب القميص.

#### ثانياً: واجهة أو شاشة الحاسب الآلي

هي الموضع المفضل للصق بعض الأوراق اللاصقة الصفراء الصغيرة التي تحمل بعض المعلومات، مثل أرقام الهاتف أو اسم الفهرس الذي يحتوي على المعلومات داخل الحاسب أو كلمات المرور، فكثير من مستخدمي الحاسب يستخدمون كلمات مرور متعددة ويقومون بتغييرها باستمرار، ولذلك فالكثير منهم يلصق ورقة صغيرة على شاشة الحاسب لتذكيره ببعض هذه الكلمات.

#### ثالثاً: المفكرة الإلكترونية

المفكرات الإلكترونية أصبحت من أهم الأدلة التي يجب التحفظ عليها، فهي تحتوي على أسماء وأرقام وهواتف وعناوين بريد إلكتروني، وعلى مواعيد ومذكرات مختصرة وعلى تواريخ مهمة، وغير ذلك من معلومات تكون لها فائدة كبيرة عند القيام بالتحريات اللازمة.

#### رابعاً: قرب الهاتف

عادة ما توجد بجوار الهاتف بعض أرقام الهاتف أو الفاكس أو بعض الرسائل المختصرة أو ملخص لمحادثة مهمة أو أسماء بعض الشركاء.

#### خامساً: حافظة النقود

تحتوي حافظة النقود عادة على بطاقات الائتمان وبطاقات الهاتف ومذكرات صغيرة وأسماء الشركاء، وأرقام هواتفهم وكلمات المرور، وجدول المهام المطلوب إتمامها، وربما يوجد قرص مرن في الحافظة.

♦ تردد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنية الطويلة بين ارتكابها واكتشافها مما يفسح المجال لحدوث إتلاف أو تغيير أو عبث بالأثار المادية، ما يدخل الشك على الدليل المستمد من المعاينة.

أما من ناحية التفتيش عن الأدلة المعلوماتية في مكونات الحاسوب الذي يفيد الكشف عن حقيقتها وعن مرتكبيها وضبط الأدلة فإن الفقه الجنائي اختلف حول مدى قابلية البيانات المعلوماتية من عدمها لأن تكون موضوع التفتيش طبقاً للنصوص التقليدية. ويكون هذا وفقاً لما يمليه القانون من الإجراءات تحدد طبيعة التفتيش مراعاة لعدم المساس بحرية الأشخاص وهذا ما جاء في نص المادة 64 من قانون الإجراءات الجزائية الجزائري. (الأمر رقم 66 - 156 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو سنة 1966 الذي يتضمن قانون الإجراءات الجزائية) على أنه: «لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات. ويجب أن يكون الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبوسعه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه».

إلا أن المشرع قد أورد استثناءات بموجب قانون رقم (06 - 22) المعدل والمتمم لأمر رقم (66 - 155) والمتضمن قانون الإجراءات الجزائية، فجاء في تفتيش المنظومة المعلوماتية في المادة 06 من قانون رقم (09 - 04) مؤرخ في 14 شعبان عام 1430، 05 غشت 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه يمكن تفتيش المنظومة المعلوماتية عن المعطيات بما يفيد الكشف عن الجريمة ومرتكبيها، وفقاً لما يقتضيه القانون فنصت المادة 06 من قانون الإجراءات الجزائية الجزائري على أنه: «عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحران وفقاً للقواعد المقررة في قانون الإجراءات الجزائية».

يعد التفتيش من الإجراءات الخاصة بالتحقيق الابتدائي التي تمس بالحرية الشخصية وانتهاك حرمة الحياة الخاصة للأفراد، لذلك حرص المشرع الجنائي على إسنادها لجهة قضائية تكفل تلك الحريات والحقوق وتضمنها. إلا أن هذه التشريعات الجنائية لم تسر على وتيرة واحدة فيما يخص تحديد الجهة التي يعهد لها بالتحقيق الابتدائي لتكون صاحبة الاختصاص الأصلي بإجراء التفتيش (16).

إلا أنه في التشريع الجزائري فقد أخذ بنظام الفصل بين سلطتي الاتهام للنيابة العامة والتحقيق عن طريق قاضي التحقيق. فالشخص الذي يكلف بجمع الأدلة الرقمية هو الخبير المتخصص والمدرّب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها وإثبات الجرائم المعلوماتية، كونها مرتبطة بمسائل فنية آية في التعقيد ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشفها إلا متخصص وعلى درجة كبيرة من التميز في مجال تخصصه، فإجراء الذكاء والفن لا يكشفه ولا يفله إلا ذكاء فن مماثلين وذلك من خلال الخبرة التقنية، التي تعد

## المبحث الثالث: آليات ملاحقة مرتكبي الجرائم الإلكترونية

المحترفين الذين يتسمون بالقدرة والذكاء والمهارة، ويرتكبون جرائمهم عن طريق التخطيط، حيث يقومون بأعمالهم بعد دراسة وتمعن. فنجد عندما يرتكب المجرمين الجرائم الإلكترونية يحيطون أنفسهم بتدابير أمنية واقية تزيد من صعوبة كشف سترها، وكمثال لذلك فإنهم قد يستخدمون التشفير وكلمات السر التي تمكنهم من إخفاء الأدلة التي قد تكون قائمة ضدهم، وقد يدسون تعليمات خفية بين الأدلة لتصبح كالمزج فلا يمكن لغيرهم أن يفهم مقصدها، وقد يقومون أيضا بتشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة. ما يجعل الوصول إليها في منتهى الصعوبة وليس بخاف كذلك أن هؤلاء الجناة قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم، فقد يستخدمون البريد الإلكتروني في إصدار تكليفاتهم بارتكاب جرائم القتل والاعتقالات والتخريب دون أن يتمكن أحد من تحديد أماكنهم أو تسجيل هذه التكليفات على النحو الذي كان يحدث في الاتصالات بشتى أنواعها. كذلك فإن مرتكبي جرائم الإنترنت يصعب ملاحقتهم لاستحالة تحديد هويتهم سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها، لأنهم في الغالب يستخدمون أسماء مستعارة أو يدخلون إلى الشبكة ليس عن طريق أبواب حساباتهم الآلية، وإنما عن طريق مراكز الإنترنت (22).

● خامسا: يلاحظ أن ملاحقة جرائم الإنترنت قد تتعلق ببيانات تكون مخزنة في داخل دولة أجنبية بواسطة شبكة الاتصال عن بعد، ولذلك فإنه قد يصعب ضبط مثل هذه الأدلة لأن هذا الإجراء يتعارض مع مبدأ السيادة الذي تحرص عليه كل دولة. ولعل هذا الأمر يكشف لنا عن أهمية التعاون القضائي الدولي في مجال الإنابة القضائية خاصة في مجال الجرائم العابرة للقارات والتي منها تلك الجرائم التي تقع بسبب ثورة الاتصالات عن بعد (23).

● سادسا: الدليل الإلكتروني يتميز بكونه دليل مرن يصعب التعامل معه على عكس الدليل التقليدي، فنجد أن من أهم الصعوبات التي تواجه المحققين في أثناء التحري عن الدليل الرقمي والعمل على ضبطه ما يستدعي ضرورة التمعن والدقة في البحث وهي أن: الدليل الرقمي غير مرئي لأنه عبارة كهرومغناطيسي مخزن في نظام آلي في شكل ثنائي، بالإضافة إلى أن الطابع الافتراضي للدليل الرقمي، إذ هناك إمكانية حدوث تغيير أو تلف أو تلفيق أو عبث بالآثار المادية الناجمة عن على الجريمة أو زوال بعضها (24)، وأخيرا مشكلة ارتفاع تكاليف الحصول على الدليل الرقمي (25).

سابعاً: إن للقاضي الجنائي الحرية في تقدير الأدلة المعروضة عليه وبناء اقتناعه الشخصي فيما يتعلق بالدليل الإلكتروني وتقدير قيمته الناتج عن الجرائم المستحدثة أي الجريمة المعلوماتية مما يتحتم على القاضي التعامل مع هذا النوع من الأدلة. ويعد مبدأ الاقتناع القضائي أحد المبادئ التي تقوم عليها نظرية الإثبات في المواد الجنائية، وعنه تتفرع معظم القواعد التي تحكم هذا الإثبات (26). فقد كرس المشرع الجزائري مبدأ اقتناع القاضي طبقاً للمادة (212) من قانون الإجراءات الجزائية الجزائي والتي تضمنت ما يلي: «يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص. ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت

إن خطورة الجرائم الإلكترونية وصعوبة إثباتها، جعلت نسبة كبيرة من رجال الأعمال يرفضون إجراء أي عمليات تجارية من خلال شبكة الانترنت، ما دفع القائمين عليها إلى محاولة إعادة الثقة عن طريق تامين المصادر لحماية الأجهزة الأم المعروفة بالخدمات، وعدم السماح بنقل المعلومات والاطلاع عليها أو تغييرها إلا باستخدام خطوات عديدة لفك الشفرات، كما قام منتجو الإسطوانات والبرامج بوضع فيروسات داخلها تنشط حالة تعرضها للسرقة لتدمر السارق أو لص المعلومات رغم عدم مشروعية ذلك، ولكي نتطرق إلى هذا المبحث المتعلق بآليات ملاحقة مرتكبي الجرائم الإلكترونية سنقسمه إلى مطلبين سنتطرق في المطلب الأول إلى ضرورة توثيق الأدلة الإلكترونية، أما المطلب الثاني سنتناول فيه تعقب مرتكبي الجرائم الإلكترونية.

### المطلب الأول: ضرورة توثيق الأدلة المعلوماتية

الأدلة الجنائية المعلوماتية أو الرقمية كغيرها من الأدلة المادية تتطلب الحفظ والتوثيق والحماية بالقدر الذي يكفل لها المصادقية، ويبعد العيوب عنها وذلك لأسباب عدة منها (20):

● أولا: التوثيق الذي يحفظ الأدلة الرقمية في شكلها الأصلي يستعمل لعرض وتأكيد مصداقية الدليل، وعدم تعرضه لتحريف أو تعديل الصورة المسجلة بالفيديو - مثلا - يمكن الاستعانة بها في تأكيد مدى صحة المناقشة الحية بين الطرفين عن طريق مطابقة النص الرقمي مع نص الصور على الشاشة.

● ثانيا: الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهادتهم حول مطابقة الأدلة التي قاموا بجمعها، مع تلك المقدمة أمام المحكمة. والتوثيق هو الأسلوب الوحيد الذي يمكن المحققين من القيام بهذا الدور أمام القضاء. ويعد فشل المحقق في التمييز بين أصل الدليل وصورته أمام القضاء سببا في بطلان الدليل.

● ثالثا: من المهم توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة، إذ إن تشابه أجهزة الحاسب الآلي وملحقاتها يجعل من الصعب إعادة ترتيبها، دون وجود توثيق سليم ومفصل يحدد الأجزاء والملحقات وأوضاعها الأصلية بدقة. يعتبر التوثيق جزءا مهما من عمليات حفظ الأدلة الرقمية حتى انتهاء إجراءات التحقيق والمحاكمة، إذ إن التحقيق يشمل تحديدا دقيقا للجهات التي تحتفظ بالأدلة وقنوات تداولها والتي ينبغي حصرها في نطاق محدود قدر الإمكان، فعند توثيق الدليل الرقمي يجب التأكد من: أين، كيف، متى وبوساطة من تم ضبط الدليل وتأمينه؟ كما أنه من الضروري توثيق الأدلة بعدة طرق كالتصوير الفوتوغرافي، والتصوير بالفيديو وخصوصا طباعة ونسخ من الملفات المخزنة في جهاز الحاسب الآلي أو المحفوظة في الأقراص، وعند حفظ الأدلة الرقمية على الأقراص يجب تدوين البيانات التالية: توقيع الشخص الذي قام بإعداد النسخة، نوع نظام التشغيل، اسم البرنامج المستعمل، الأوامر المستعملة لإعداد النسخ، المعلومات المضمنة في الملف المحفوظ، التاريخ والوقت (21).

● رابعا: إن منغذي الجرائم المعلوماتية من المجرمين

مواكبة التطور السريع في مجال الحاسب الآلي وذلك لانتشار الحاسب الآلي وتنوع مجالاته وبرامجه ما يجعل من الصعب حصر أساليب الجريمة وأشكالها، وبالتالي يصعب تدريب المحققين على مواجهة حالات محددة، بالإضافة إلى أن لأجهزة التحقيق مجالات عدة ينبغي تغطيتها وغير متفرغة لجرائم الحاسب الآلي فقط، مما يؤثر على قدرة تلك الأجهزة على مواكبة التطور، وتعتبر الميزانيات المالية التي ترصد لتكوين الموارد البشرية في أجهزة التحقيق التابعة للدولة غير كافية لاستقطاب النخبة المتميزة في مجال الحاسب الآلي والذين تستقطبهم عادة مؤسسات خاصة تتميز باستقلالها المالي.

إن مهمة التحقيق في مجال جرائم الحاسب الآلي تودع لدى أصحاب الخبرة المتخصصين في المجال، كالشركات الكبرى العالمية التي حققت نجاحا في ميدان حماية الحاسب الآلي، إلا أن تخلي أجهزة العدالة عن دورها في هذا النوع من الجرائم أصبح في غاية الخطورة<sup>(31)</sup>. وخصوصا الجرائم المتعلقة بأمن الدولة.

ولا شك أن من متطلبات العدالة الجنائية تقتضي تحمل الأجهزة الحكومية مسؤولياتها كاملة تجاه اكتشاف كافة الجرائم وضبط الجناة فيها وتحقيق العدالة في حقهم، وعلى الأجهزة الأمنية المعنية توفير الإمكانيات التقنية اللازمة للتحقيق في جرائم الحاسب الآلي والتقنية العالية، كما عليها استقطاب أكثر الكفاءات المهنية المتخصصة في هذا المجال للاستعانة بها في التحقيق في جرائم الحاسب الآلي وغيرها من جرائم التقنية العالية<sup>(32)</sup>.

إن الاستعانة بخبراء الحاسب الآلي في معاينة مسرح الجريمة أو القيام بعمليات التفتيش والضبط وفحص آثار الجريمة لا تشكل خلافا فنيا أو قانونيا، كما هو الحال في التحقيق مع الشهود والمتهمين، إذ إن أخذ أقوال الشهود واستجواب المتهمين يعتمد على خبرات المحققين. ويعتبر الاستجواب مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق، ومطالبتة له بإبداء رأيه في الأدلة القائمة ضده إما تفنيدا أو تسليما، وذلك قصد محاولة الكشف عن الحقيقة واستظهارها بالطرق القانونية<sup>(33)</sup>.

استجواب المتهم من طرف جهة التحقيق يخضع للإجراءات المقررة في النصوص القائمة في الإجراءات الجزائية. لذلك فإن استجواب المتهم في الجرائم الإلكترونية أو الرقمية تحكمه نفس القواعد العامة للاستجواب في أي جريمة تقليدية، إلا أنه الفرق بين الجريمتين يتمثل في ضرورة تأهيل السلطة المختصة التي تتولى إجراء الاستجواب، إذ يجب على جهات التحقيق أن تكون مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن استيعاب واقعة التحقيق. إن طريقة توجيه الأسئلة وترتيب أولوياتها واستنتاج الحقائق من طريقة التي يتحدث بها المتهم، وقراءة لغة الجسد لديه أمور مهنية لا يوفيهها حقها إلا المحققون الذين اكتسبوا الخبرة والمعرفة العلمية. كما أنه من الممكن أن يكون بين المتهمين في جرائم الحاسب الآلي أشخاص لم يبلغوا درجة عالية من العلم والمعرفة بنظم المعلوماتية، وبالتالي يصعب عليهم إدراك مصطلحاته الفنية<sup>(34)</sup>. ما يستوجب البحث على منهج خاص يحقق الترابط والانسجام بين أصحاب الخبرة الفنية والكفاءة المهنية للقيام بإجراءات التحري مع الأشخاص الذين لهم علاقة بجرائم الأنترنت.

المناقشة فيها حضوريا أمامه». يمكن القول أن الدليل الإلكتروني لا يحظى بأهمية كافية أمام القاضي الجنائي في الإثبات طبقا لما يمليه عليه ضميره واطمئنانه في تقديره للدليل فهو ليس ملزما بأن يؤسس اقتناعه على الدليل كما له أن يهدره، فالدليل الإلكتروني دليل علمي يساعد القاضي الجنائي على يقين من أجل الحد من الأخطاء التي قد ترد عن القضاء بهدف الوصول إلى الحقيقة وتحقيق العدالة.

### المطلب الثاني: تعقب مرتكبي الجرائم الإلكترونية

كما تكمن صعوبة التحقيق الجنائي في جرائم المعلوماتية، وهذا يتطلب منا أن نعهد إلى بيوت خبرة متخصصة في هذا المجال، ولا سيما وأن هناك شركات عالمية حققت نجاحا في بعض الحالات لكن هذا الأمر له خطورته إذ أنه يضحى بمصلحة الأفراد والمجتمع، ويضعها تحت رحمة هذه الشركات التي ليس لها هدف سوى الكسب المادي، فضلا عن الإخلال بمبدأ سرية التحقيق، سيما لو تعلق التحقيق بجرائم تمس خصوصية الأشخاص أو أسرارهم الشخصية أو حياتهم العائلية أو تعلق الأمر كذلك بأمن الدولة<sup>(27)</sup>.

يختلف مجرم المعلوماتية تماما عن المجرم العادي فيتمتع بمستوى عال من الفكر والتدريب وكذا الخبرة في مجال تكنولوجيا المعلومات. قراصنة الأنترنت لديهم القدرة على إنشاء برامج الفيروسات ونشرها عبر الأنترنت لتدمر قواعد البيانات للمؤسسات والأفراد على حد سواء، وهو شيء خطير فالجريمة المرتكبة قد تضر بلدا بأكمله<sup>(28)</sup>.

إن إجراءات التحقيق مع الأشخاص الذين لهم علاقة بالجريمة المعلوماتية هي نفسها الإجراءات المقررة للتحقيق في الجريمة التقليدية، إلا أنها تختلف من حيث الجهة المختصة التي يجب أن تكون مؤهلة لهذا نوع من الإجراءات بهدف تحصيل أدلة ضد المتهمين من إثبات أو نفي.

إن من أكثر الصعوبات التي تواجه المحققين في جرائم الحاسب الآلي من رجال الشرطة والنيابة العامة والقضاة مسألة فهم الجوانب التقنية التي تحيط بجرائم المعلوماتية وتقنياتها العالية، إذ إن الغالبية العظمى من الشرطة والنيابة والقضاء لا يدركون شيئا عن الحاسب الآلي وتقنياته المتطورة ولغاته المتنوعة<sup>(29)</sup>.

للعاملين في مجال الحاسب الآلي مصطلحات علمية خاصة أصبحت الطابع المميز لمحدثتهم وأساليب التفاهم معهم. ولم تقف تلك الأساليب في المصطلحات العلمية المستحدثة فحسب، بل اختصر العاملون في مجال الحاسب الآلي تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات Acronyms، ولغة المختصرات قائمة طويلة آخذة في التطور لتصبح لغة العاملين في المجال الحاسب الآلي Hackers يطلقون على أنفسهم صفة النخبة Elites بحجة أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاتها المتميزة. بينما تطلق تلك الفئة على رجال تنفيذ القانون من شرطة، النيابة، القضاء صفة الضعفاء أو القاصرين (30 Lamers).

لقد بدأت بعض الأجهزة التابعة للدولة سواء الأمنية منها أو القضائية في استقطاب المختصين في مجال الحاسب الآلي، كما يجري تدريب المحققين والمنخرطين في الشرطة على استخدام الحاسب الآلي، إلا أن كل ذلك لن يجعل من الأجهزة قادرة على

## الخاتمة:

لمواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص 56.

2. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص 234.

3. Eoghan Casey Digital Evidence and Computer Crime London Academic Press 2000 P.260

4. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول للعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 02-04/11/1468 هجري الموافق لـ 12-14/11/2007 ميلادي، ص 13.

5. المرجع السابق، ص 13.

6. المرجع السابق، ص 14-15.

7. المرجع السابق، ص 15.

8. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، المرجع السابق، ص 238.

9. حسن طاهر داود، المرجع السابق، ص 226.

10. محمد الأمين البشري، التحقيق الجنائي المتكامل، المركز العربي للدراسات الأمنية والتدريب، الرياض، 1997، ص 235.

11. حسن طاهر داود، جرائم نظم المعلومات، المركز العربي للدراسات الأمنية والتدريب، الرياض، الطبعة الأولى، 2000، ص 225.

12. Forensic computer crime investigation by Thomas A. Johansson 2005p 151

13. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، العراق، 2011، ص 74.

14. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، السنة الرابعة، العدد الثاني، يوليو 1999، ص 59.

15. تنص المادة 43 من قانون الإجراءات الجزائية الجزائري. (الأمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو سنة 1966 الذي يتضمن قانون الإجراءات الجزائية، المعدل والمتمم). على: «يحظر في مكان ارتكاب جنابة على كل شخص لا صفة له، أن يقوم بإجراء أو تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، وإلا عوقب بغرامة 200 إلى 1000 دج. غير أنه يستثنى من هذا الحظر حالة ما إذا كانت التغييرات أو نزع الأشياء للسلامة والصحة العمومية أو تستلزمها معالجة المجني عليه. وإذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من 1000 إلى 10000 دج».

16. قدرى عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005، ص 88.

17. عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت، المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية، بدون دار نشر، 2006، ص 1031، أشارت إليه

الجريمة المعلوماتية جريمة فنية هادئة لا عنف فيها فهي تقع من شخص يتمتع بالذكاء والخبرة الهائلة في مجال الحاسب الآلي ويعتبر أداة الجريمة، أما محل الجريمة فهو عبارة عن بيانات أو معلومات موجودة داخل النظام المستهدف، وبالتالي فالحاسب الآلي ركن أساسي في الجرائم المعلوماتية لا تقوم جريمة معلوماتية بدون هذه الميزة تميز الجرائم المعلوماتية عن الجرائم التقليدية الأخرى.

وتأسيساً على ما تقدم، يجب العمل على تحديث الوسائل العلمية والتقنية من أجل مواكبة هذا النوع من التطور التكنولوجي الذي أصبح يطبق في الجرائم الحالية، التي كان من الصعب التحري فيها والكشف عنها. ولا شك أن التحقيق في الجرائم المعلوماتية يشكل تحدي بالنسبة لرجال التحقيق نظراً لصعوبة إثباتها وهذا يعود لاستمرارية تطورها.

ومن خلال ما تطرقنا إليه في هذا الموضوع الذي تمثل في التحري الجنائي في مسرح الجريمة الإلكترونية توصلنا إلى النتائج الآتية:

1. تعدد المصطلحات حول تحديد ماهية الجريمة المعلوماتية بحيث نشهد فراغ قانوني من خلال التشريعات الدولية وكذا في التشريع الجزائري خشية حصرها في مجال ضيق نظراً لارتباطها ارتباطاً وثيقاً بالتكنولوجيا الحديثة ولمرونتها وتطورها المستمر.

2. التعامل مع الدليل الإلكتروني من حيث إجراءات المعاينة والتفتيش والعمل على تقصي الآثار المستخلصة من مسرح الجريمة المعلوماتية والمحافظة عليه وكذا الصعوبات التي تواجه الدليل من حيث أنه غير مرئي ذو طابع افتراضي ومدى حجية اقتناع القاضي بهذا الدليل.

3. صعوبة تحديد الجريمة المرتكبة عن طريق الحاسب الآلي عقب حدوثها والعمل على التبليغ عنها إلى الجهات المختصة تختلف عن الجريمة التقليدية ما يصعب إدراك عناصرها وطرق ارتكابها.

4. ومن خلال ما توصلنا إليه في خلاصة دراستنا الحالية نقدم مجموعة من التوصيات نحصرها فيما يلي:

5. ضرورة استخدام الوسائل العلمية الحديثة في التحقيق الجنائي الإلكتروني وذلك عن طريق تطوير واستحداث الأنظمة القانونية تماشياً مع تطور الجرائم وتقديم الأساليب الكشف عنها.

6. التأكيد والأخذ بمبدأ افتراض الدليل الرقمي كدليل أصلي نظراً لنقص وسائل المستخدمة في التحقيق الجنائي الإلكتروني.

7. إعداد الخبرة الفنية في مجال التحقيق الجنائي الإلكتروني وذلك بإنشاء أكاديميات فنية قضائية متخصصة من أجل تأهيل وتخريج الخبراء القضائيين في المجال الإلكتروني.

8. العمل على تبادل الخبرات بين الدول في مجال التحري عن الجرائم المعلوماتية.

## الهوامش:

1. عبد الله عبد العزيز اليوسف، أساليب تطوير البرامج والمناهج التدريبية

- مواجهة الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004.
7. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 02-04/11/1468 هجري الموافق لـ 12-14/11/2007 ميلادي.
8. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار الثقافة العربية للنشر، مصر، 2004.
9. محمد الأمين البشري، التحقيق الجنائي المتكامل، المركز العربي للدراسات الأمنية والتدريب، الرياض، 1997. الرياض، 1997.
10. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004.
11. محمد صلاح سالم، العصر الرقمي وثورة المعلومات، عين للدراسات والبحوث الإنسانية والاجتماعية، مصر، الطبعة الأولى، 2002.
12. محمد محدة، ضمانات المتهم أثناء التحقيق، الجزء الثالث، دار الهدى للطباعة والنشر، الجزائر، الطبعة الأولى، 1991.
13. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988.
14. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، السنة الرابعة، العدد الثاني، يوليو 1999.
15. قانون الإجراءات الجزائية الجزائري. (الأمر رقم -66 156 المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو سنة 1966 الذي يتضمن قانون الإجراءات الجزائية، المعدل والمتمم).
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المصري، رسالة ماجستير، دار الجامعة الجديدة، الإسكندرية، 2010، ص 139.
18. Rosenblatt K S High Technology Crime Investigation Cases Involving Computer, San Jose, K.S.K Publication 1999, p 21.
19. حسن طاهر داود، المرجع السابق، ص 227.
20. محمد الأمين البشري، المرجع السابق، ص 244.
21. المرجع السابق، ص 245.
22. المرجع السابق، ص 245-246.
23. المرجع السابق، ص 245-246.
24. عائشة بن قارة مصطفى، المرجع السابق، ص 252.
25. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار الثقافة العربية للنشر، مصر، 2004، ص 984.
26. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988، ص 412.
27. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، الطبعة الأولى، 2009، ص 295.
28. محمد صلاح سالم، العصر الرقمي وثورة المعلومات، عين للدراسات والبحوث الإنسانية والاجتماعية، مصر، الطبعة الأولى، 2002، ص 181.
29. محمد الأمين البشري، المرجع السابق، ص 120.
30. المرجع السابق، ص 121.
31. محمد الأمين البشري، المرجع السابق، ص 122.
32. محمد محدة، ضمانات المتهم أثناء التحقيق، الجزء الثالث، دار الهدى للطباعة والنشر، الجزائر، الطبعة الأولى، 1991، ص 306.
33. محمد الأمين البشري، المرجع السابق، ص 122.

### ثانياً المراجع الأجنبية:

1. Eoghan Casey, *Digital Evidence and Computer Crime*, London Academic Press, 2000.
2. *Forensic computer crime investigation by Thomas A. Johanson* 2005.
3. Peter Stephenson, *Investigation Computer Crimes*, London: C.R.C. 1999.
4. Rosenblatt. K.S, *High Technology Crime Investigation Cases Involving Computer*, San Jose, k. s. k Publications 1999.

### المصادر والمراجع:

#### أولاً المراجع العربية:

1. حسن طاهر داود، المرجع السابق، جرائم نظم المعلومات، المركز العربي للدراسات الأمنية والتدريب، الرياض، الطبعة الأولى، 2000.
2. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، العراق، 2011.
3. قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005.
4. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المصري، رسالة ماجستير، دار الجامعة الجديدة، الإسكندرية، 2010.
5. عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، الطبعة الأولى، 2009.
6. عبد الله عبد العزيز اليوسف، أساليب تطوير البرامج والمناهج التدريبية