مجلة روح القوانين – كلية الحقوق جامعة طنطا

عدد خاص – المؤتمر العلمى الدولى الثامن – التكنولوجيا والقانون

الدليل التقني المستمد من مسرح الجريمة الالكترونية

إعداد الدكتور/ محمود رجب فتح الله

دكتوراه القانون الجنائي

كلية الحقوق – جامعة الاسكندرية

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

ملخص الدراسة

من المقرر ان مسرح الجريمة الالكترونية طرح نفسه ضمن أهم الابحاث من التي شغلت الفقه القانوني الجنائي وكذلك المشرعين، واكد اهميته بجلاء في مجال الإثبات الجنائي على اختلاف نظمه، وذلك لكون الدليل الرقمي المستقي من مسرح الجريمة الالكترونية، دليلا مستحدثا ذو طبيعة معقدة وصعبة.

اذ ترتكز عملية الإثبات الجنائي لجرائم تقنية المعلومات على الدليل الجنائي التقني؛ باعتباره الوسيلة الرئيسية لإثبات هذا الصنف من الجرائم، لذا يعد الإثبات الجنائي بالأدلة الرقمية المستمدة من مسرح الجريمة الالكترونية، من أبرز تطورات العصر الحديث في كافة النظم القانونية، تلك التطورات التي جاءت لتلائم الثورة العلمية والتكنولوجية والتقنية في عصرنا الحالي، والتي تطور معها الفكر الإجرامي، فظهر نوع جديد من الجرائم تعرف بجرائم تقنية المعلومات.

وازاء التزايد المضطرد في جرائم تقنية المعلومات التي صاحبت تطور تقنية الحوسبة وشبكات الإتصال، ظهر ما سمي بأدلة مسرح الجريمة الالكترونية، كنوع جديد يضاف إلى قائمة الأدلة الجنائية المعروفة الأخرى، ليتميز عنها بعدة خصائص يستمدها من البيئة الرقمية التي يولد فيها.

الامر الذي حدا الي عدم كفاية الإجراءات التقليدية لجمعه واستخلاصه نظرا لخصوصيته، حيث يتطلب الدليل الرقمي خبرة تقنية ويفرض على سلطات التحري والتحقيق خبرات تقنية متطورة، لذلك ولضمان تتبع أدلة مسرح الجريمة الالكترونية، يجب استحداث إجراءات جديدة مثل مراقبة الإتصالات الإلكترونية، مع مراعاة ضرورة تحقيق توازن بين الحرية الشخصية للفرد وحق المجتمع في تتبع الجناة ومعاقبتهم.

ومن المقرر ان العقبات والصعوبات التي تواجه مسرح الجريمة الالكترونية، لا تقف عند حد كيفية الحصول عليه واجراءات حفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالاقتناع به لبناء الحكم على أساسه بالبراءة أو الادانة.

الكلمات المفتاحية :

جريمة – مسرح الجريمة – الجريمة الالكترونية – تنظيم الجريمة

Study summary

It is decided that the cybercrime scene has presented itself as one of the most important studies that have occupied criminal jurisprudence as well as legislators, and its importance has been clearly confirmed in the field of criminal proof, regardless of its various systems, because the digital evidence derived from the cybercrime scene is new evidence of a complex and difficult nature.

The process of criminal proof of information technology crimes is based on technical forensic evidence. As the main means of proving this type of crime, criminal proof using digital evidence derived from electronic crime scenes is considered one of the most prominent developments of the modern era in all legal systems, those developments that came to suit the scientific, technological and technical revolution in our current era, with which criminal thought developed, A new type of crime has emerged, known as information technology crimes.

In the face of the steady increase in information technology crimes that have accompanied the development of computing technology and communication networks, what is called electronic crime scene evidence has emerged as a new type added to the list of other known forensic evidence, distinguished from it by several characteristics derived from the digital environment in which it is born.

This has led to the inadequacy of traditional procedures for collecting and extracting it due to its privacy, as digital evidence requires technical expertise and imposes on the investigation and investigation authorities advanced technical expertise. Therefore, to ensure tracking electronic crime scene evidence, new procedures must be developed such as monitoring electronic communications, taking into account the need to achieve a balance. Between the personal freedom of the individual and the right of society to track down and punish offenders.

It is decided that the obstacles and difficulties facing the electronic crime scene do not stop at the limit of how to obtain it and the procedures for preserving it, but rather extend to the extent of the probative strength that this evidence has, and the extent of the trial judge's freedom to be convinced by it to base the ruling on its basis of acquittal or conviction.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

أولا : المقدمة :

من المقرر ان مسرح الجريمة الالكترونية طرح نفسه ضمن أهم الابحاث من التي شغلت الفقه القانوني الجنائي وكذلك المشرعين، واكد اهميته بجلاء في مجال الإثبات الجنائي على اختلاف نظمه، وذلك لكون الدليل الرقمي المستقي من مسرح الجريمة الالكترونية، دليلا مستحدثا ذو طبيعة معقدة وصعبة.

اذ ترتكز عملية الإثبات الجنائي لجرائم تقنية المعلومات على الدليل الجنائي التقني؛ باعتباره الوسيلة الرئيسية لإثبات هذا الصنف من الجرائم، لذا يعد الإثبات الجنائي بالأدلة الرقمية المستمدة من مسرح الجريمة الالكترونية، من أبرز تطورات العصر الحديث في كافة النظم القانونية، تلك التطورات التي جاءت لتلائم الثورة العلمية والتكنولوجية والتقنية في عصرنا الحالي، والتي تطور معها الفكر الإجرامي، فظهر نوع جديد من الجرائم تعرف بجرائم تقنية المعلومات.

وازاء التزايد المضطرد في جرائم تقنية المعلومات التي صاحبت تطور تقنية الحوسبة وشبكات الإتصال، ظهر ما سمي بأدلة مسرح الجريمة الالكترونية، كنوع جديد يضاف إلى قائمة الأدلة الجنائية المعروفة الأخرى، ليتميز عنها بعدة خصائص يستمدها من البيئة الرقمية التي يولد فيها.

الامر الذي حدا الي عدم كفاية الإجراءات التقليدية لجمعه واستخلاصه نظرا لخصوصيته، حيث يتطلب الدليل الرقمي خبرة تقنية ويفرض على سلطات التحري والتحقيق خبرات تقنية متطورة، لذلك ولضمان تتبع أدلة مسرح الجريمة الالكترونية، يجب استحداث إجراءات جديدة مثل مراقبة الإتصالات الإلكترونية، مع مراعاة ضرورة تحقيق توازن بين الحرية الشخصية للفرد وحق المجتمع في تتبع الجناة ومعاقبتهم.

ومن المقرر ان العقبات والصعوبات التي تواجه مسرح الجريمة الالكترونية، لا تقف عند حد كيفية الحصول عليه واجراءات حفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالاقتناع به لبناء الحكم على أساسه بالبراءة أو الادانة.

لذلك حاول المشرع والقضاء والفقه المقارن التصدي لهذه المسألة، وذلك بتحديد الشروط التي يجب توفرها في الادلة المستقاه من مسرح الجرائم الالكترونية حتى يمكن قبولها من قبل القضاء.

ثانيا : اشكالية الدراسة:

ذلك ان الوصول إلى أدلة مسرح الجريمة الالكترونية، تعترضه عقبة أخرى تكمن في أن الجناة المتمرسين يجتهدون في إخفاء هويّاتهم للحيلولة دون تعقبهم أو كشف أمرهم، بحيث تظل

أنشطتهم مجهولة بمنأى عن علم السلطات المعنية بمكافحة الجريمة، فقد يكون مسرح الجريمة الالكترونية ناتج عن استخدام الحواسب الموجودة بالأماكن العامة، أو اللجوء إلى مقاهي الانترنت، على اعتبار أن معظم هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم، مما يجعل المراقبة والتعقب للمشتبه فيه أمراً ينطوي على صعوبة وغير ميسور في كثير من الاحيان، وربّما تتعقد المسألة أكثر عند استخدام الانترنت اللاسلكي، الذي هو آخذ في الانتشار في أيامنا هذه على حساب الانترنت السلكي.

ثالثا : أهمية الدراسة.

ازاء تضاؤل خبرة أجهزة العدالة الجنائية من مأموري ضبط وسلطة تحقيق ومحاكمة، يفتقر هؤلاء جميعا إلى التأهيل الكافي في ميدان مسرح الجريمة الالكترونية والتقنية، وهو ما يزيد من صعوبة وصولهم إلى أدلته الرقمية وكيفية ضبطها والمحافظة عليها، فنقص الخبرة لدى هؤلاء قد يفضي إلى تدمير الدليل وإتلافه، على اعتبار أن جهلهم بأساليب ارتكاب جرائم تقنية المعلومات يجعلهم في كثير من الاحيان يقعون في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها من مسرح الجريمة الالكترونية، مثل إتلاف محتويات الاقراص الممغنطة وأوعية المعلومات التي تُخزَّن بها البيانات.

رابعا : أهداف الدراسة :

اذ ايجب أن تتوافر الوسائل لإثبات أن الأدلة الرقمية الناتجة عن مسرح الجريمة الالكترونية لم تتعرض لأية تعديات، سواء بالحذف، او الاضافة، او التعديل، او أية تغييرات أخرى، منذ لحظة التحصل عليها.

ومن المقرر ان الطبيعة غير المادية لمسرح الجريمة الالكترونية، والمعلومات المخزنة بشكل إلكتروني، من السهل التلاعب بها، وهي أكثر عرضة للتغيير من الاشكال التقليدية للأدلة، وقد شكل هذا تحدياً خاصاً لأجهزة العدالة حيث يتطلب التعامل مع هذه البيانات، أو المعلومات طريقة خاصة لضمان سلامة الأدلة التي يوفرها مسرح الجريمة الالكترونية.

خامسا : منهج الدراسة:

يعتمد البحث الأسلوب النظري الوصفي في تسليط الضوء علي مسرح الجريمة الالكترونية، والأدلة الرقمية المتولدة عنه، وتحليل الاتجاه التشريعى للمشرع المصرى في هذا الشأن

سادسا : خطة الدراسة :

تتضمن الدراسة تناول البحث من خلال فصلين، على النحو التالى:

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

الفصل الاول : ماهية الأدلة التقنية لمسرح الجريمة الالكترونية

المبحث الاول : تعريف مسرح الجريمة الالكترونية.

المبحث الثاني : التحليل الجنائى الرقمي لمسرح الجريمة الالكترونية.

المطلب الاول : التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية.

المطلب الثاني : أهداف التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية.

المبحث الثالث : مفهوم الدليل الرقمي في مسرح الجريمة الالكترونية.

المطلب الأول : مفهوم الدليل الرقمي وخصائصه.

المطلب الثاني : مدى قبول الأدلة الرقمية فى الاثبات.

المطلب الثالث : أهمية الدليل الرقمي في مسرح الجريمة الالكترونية.

المطلب الرابع : مبادئ الأدلة الرقمية لمسرح الجريمة الالكترونية.

المبحث الرابع : مصادر الأدلة الرقمية لمسرح الجريمة الالكترونية.

المطلب الأول : أجهزة الحاسب الآلى ووحدات التخزين لمسرح الجريمة الالكترونية.

المطلب الثاني : الشبكات بمسرح الجريمة الالكترونية Computer networks.

المطلب الثالث : شبكة الانترنت بمسرح الجريمة الالكترونية.

الفصل الثاني : المعالجة التشريعية لمسرح الجريمة الالكترونية فى القانون المصري.

المبحث الاول : مفهوم الدليل الرقمي فى القانون المصري.

المبحث الثاني : حجية الأدلة الرقمية فى القانون المصري.

خاتمة البحث : النتائج والتوصيات.

الفصل الأول

ماهية الأدلة التقنية لمسرح الجريمة الالكترونية

تمهيد وتقسيم:

من المقرر ان ثورة المعلومات والتكنولوجيا امتدت لتشمل طرق الاثبات بصفة عامة والأدلة الجنائية بصفة خاصة، ذلك ان التوافق المطلوب تحقيقه دائماً بين طبيعة الدليل وطبيعة الجريمة التي يتولد منها، أدى إلى استحداث نوعاً جديداً من الأدلة يتماشى مع طبيعة جرائم تقنية المعلومات، وهو ما عرف بمسرح الجريمة الالكترونية، والدليل الناتج عنها يجري اثباته من خلال فحص المكونات المعنوية أو البرمجية للحواسب وشبكة الانترنت(١).

فإذا كان السلاح الناري والذخيرة هو الدليل في جريمة القتل التقليدية، وان المحرر المزور هو احد الأدلة في جريمة التزوير التقليدية، فإن الأدلة المنبثق عن مسرح الجريمة الالكترونية لا تخرج عن هذا الاطار.

ذلك ان إثبات هذه الجرائم يحتاج إلى طرق تقنية تتناسب مع طبيعتها، بحيث يمكن ترجمة النبضات والذبذبات الالكترونية إلى أدلة إثبات أو نفي على ارتكاب هذه الجرائم من خلال مسرح الجريمة الالكترونية.

وقد ساهم القضاء المقارن في رسم معالم الدليل الرقمي، سواء من حيث فائدته أم من حيث قيمته القانونية، حيث اعتدَّ به القضاء بناء على نص تشريعي تارة، وعلى الاجتهاد القضائي تارة أخرى، وهو دليل له اهميته الجوهرية، خاصة فيما يتعلق بجمع الأدلة وحفظها، ويمكن للقضاة الاستفادة منها، والاجتهاد حسب طبيعة مسرح الجريمة الالكترونية.

وترتيبا علي ذلك، نتطرق في اطار هذا الفصل الي تناول تعريف مسرح الجريمة الالكترونية، من خلال مبحث اول، علي ان يخصص المبحث الثاني لعرض التحليل الجنائى الرقمي لمسرح الجريمة الالكترونية، ليتناول المبحث الثالث مفهوم الدليل الرقمي في مسرح الجريمة الالكترونية، علي ان يختتم ذلك الفصل ببيان مصادر الأدلة الرقمية لمسرح الجريمة الالكترونية، علي الترتيب التالي.

المبحث الاول : تعريف مسرح الجريمة الالكترونية.

---

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، دار الجامعة الجديدة، الطبعة الاولي، سنة ٢٠١٨، ص ٤٧٨ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون المصري ١٧٥ لسنة ٢٠١٨، الاسكندرية، دار الجامعة الجديدة، الطبعة الاولي، سنة ٢٠١٨، ص ٨٩٣ وما بعدها.

المبحث الثاني : التحليل الجنائى الرقمي لمسرح الجريمة الالكترونية .

المبحث الثالث : مفهوم الدليل الرقمي في مسرح الجريمة الالكترونية.

المبحث الرابع : مصادر الأدلة الرقمية لمسرح الجريمة الالكترونية.

المبحث الاول

تعريف مسرح الجريمة الالكترونية

يمكن تعريف مسرح الجريمة بأنه "هو كل محل أو وحدة من منشأة أو رقعة من الأرض تضم بؤرة الجريمة ومركزها بحيث تكون ميداناً لأنشطة الجاني أو الجناة من الفاعلين الأصليين عند أرتكاب الأفعال المؤثمة جنائياً و التي تدخل في عداد الأعمال التنفيذية المكونة للجريمة أو الشروع فيها.(١)

ويدخل في عداد ذلك الملحقات المتصلة التي تكون مع المكان وحدة واحدة وهذا النطاق المكاني يكتسب صفة مسرح إرتكاب الجريمة من واقع إحتوائهِ على مركز وقوعها بداخله ووجود آثار ومخلفات إرتكابها أو إحتمال وجود ذلك.

ويجب أن تكون هذه المواقع ميداناً لأنشطة الجاني الذي إرتكب الجريمة وحده أو الجناة من الفاعلين الأصليين عند تعددهم، ومارسوا أفعالاً تضفي عليهم هذه الصفة وذلك بإرتكاب كل أو بعض الأعمال التنفيذية للجريمة أو الشروع فيها.

ولعل أهمية تحديد المجال المكاني للمعاينة والتي تنصب أساساً على مسرح الجريمة تكمن في تعيين السلطة صاحبة الإختصاص المكاني بمباشرة إجراءات المعاينة، هذا بجانب إبراز معالم الحدود الميدانية التي تمارس فيه هذه السلطات أنشطتها عند إجراء المعاينة كقواعد إرشادية لإدراك أهمية المناطق المتصلة بمركز وقوع الجريمة وتقدير مدى أولويتها في تركيز البحث والتنقيب عن الآثار والمخلفات والمتغيرات الطارئة والناشئة عن إرتكابها بهدف توضيح الإسلوب الأمثل لكشف كامل أبعادها دون إغفال موقع أو جزء أو جانب منها (٢) .

اما الجريمة المعلوماتية او الالكترونية، فترتكب في مسرح خاص هو يتمثل في عالم افتراضي مفرغ cyberspace وهو ما يختلف كليا عن المسرح الذي ترتكب فيه الجرائم في صورتها التقليدية حيث تطبق القواعد العامة لانتداب الخبراء في اقتفاء آثار الجناة، الذين

---

(١) انظر في ذلك : د . خالد ممدوح إبراهيم ، امن الجريمة الالكترونية، الدار الجامعية، الاسكندرية، سنة ٢٠٠٨، ص ١٦٨.

(٢) انظر في ذلك : د . خالد ممدوح إبراهيم، المصدر السابق، ص (١٦٨،١٦٩) .

يرتكبون جرائم تتكون من سلوك مادي ملموس وله محل مادي ملموس ايضا، مما لا يتناسب ونوع الخبرة المطلوبة لمعاينة مسرح الجريمة المعلوماتية المرتكبة في الفضاء الالكتروني.

ولذلك يستعين المحقق بخبراء في هذا المجال بحسب كل قضية وملابساتها، كما يمكن الاستعانة ببعض خبراء مسرح الجريمة التقليدية، مثل خبير البصمات وخبير التصوير.

وعند الشروع في جمع الأدلة من مسرح جريمة من جرائم تقنية المعلومات، ينبغي التعامل معه على أنه مسرحين هما:

- **مسرح تقليدي:** ويقع خارج بيئة الحاسب الآلي والانترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، وقد يترك فيها الجاني آثار عدة، كالبصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.
- **مسرح افتراضي":** ويقع داخل بيئة الحاسب الآلي وشبكة الانترنت، ويتكون من البيانات الرقمية التي تتواجد وتنقل داخل بيئة الحاسب وشبكاته، في ذاكرته وفي الاقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن يتم على يد خبير متخصص في التعامل مع الأدلة الرقمية.

ولا شك ان المعضلة الحقيقية بالنسبة لمسرح الجريمة الالكترونية، تتمثل في في طرق ضبط وإثبات الادلة المتولدة عنها، وهو ما يرجع الى افتقاد الاثار التقليدية التي قد يتركها مسرح أي جريمة الكترونية، فالبيانات يتم إدخالها مباشرة في الجهاز دون ان تتوقف على وجود وثائق او مستندات، لانه كثيرا ما يكون هناك برامج معدة ومخزنة سلفا على الجهاز ولا يكون عليه سوى ادخال البيانات في الاماكن المعدة لها كما هو الحال بالنسبة للمعاملات المصرفية والمؤسسات التجارية الكبرى ويمكن في هذه الفروض ارتكاب جرائم الاختلاس والتزوير، فيفتقد مسرح الالكترونية الي الجريمة اثارها التقليدية.

فالجريمة المعلوماتية ترتكب في مسرح خاص هو يتمثل في عالم اقتراضي مفرغ cyberspace وهو ما يختلف كليا عن المسرح الذي ترتكب فيه الجرائم في صورتها التقليدية حيث تطبق القواعد العامة لانتداب الخبراء في اقتفاء اثار الجناة، الذين يرتكبون جرائم تتكون من سلوك مادي ملموس وله محل مادي ملموس ايضا، مما لا يتناسب ونوع الخبرة المطلوبة لمعاينة المسرح السيبيري للجريمة المعلوماتية المرتكبة في الفضاء الالكتروني.

المبحث الثاني

التحليل الجنائى الرقمي لمسرح الجريمة الالكترونية

من المقرر ان التحليل الجنائى الرقمي، ويعرف كذلك بعلم الطب الشرعي الرقمي، هو عملية التحقيق في الجرائم المرتكبة باستخدام أي نوع من أجهزة الحوسبة.

والتحليل الجنائي الرقمي، يعرف بتطبيقه في مجالات مسرح الجريمة الالكترونية، بغية تحقيق أهداف محددة، لا يمكن الوصول اليها الا بسلوك هذا المجال الحرج.

وترتيبا علي ذلك، نتناول تعريف التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية، من خلال مطلب اول، علي ان يعرض المطلب الثاني، لأهداف التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية، علي الترتيب التالي :

المطلب الاول : التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية.

المطلب الثاني : أهداف التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية.

المطلب الاول

التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية

التحليل الجنائى الرقمي، او علم الطب الشرعي الرقمي، باعتباره عملية دقيقة للتحقيق في الجرائم المرتكبة باستخدام أي نوع من أجهزة الحوسبة، مثل:

- أجهزة الحاسب الآلي .
- الخوادم وأجهزة الحاسب المحمولة والهواتف المحمولة .
- الأجهزة اللوحية والكاميرا الرقمية وأجهزة الشبكات وأجهزة إنترنت الأشياء (IoT) أو أي نوع من أجهزة تخزين البيانات.

ذلك ان التحليل الجنائى الرقمي مسؤول أيضًا عن فحص الهجمات التي تنشأ من الفضاء الإلكتروني؛ مثل برامج الفدية والتصيد وهجمات أوامر SQL وهجمات رفض الخدمة الموزعة (DDoS) وخرق البيانات وأي نوع من الهجمات الإلكترونية التي تسبب خسائر مالية أو سمعة.

ولا شك ان الهدف النهائي للتحقيق الجنائي الرقمي هو الحفاظ على الأدلة الرقمية وتحديدها والحصول عليها وتوثيقها لاستخدامها في المحاكم.

المطلب الثاني

أهداف التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية

يتم استخدام التحليل الجنائي الرقم، للتحقيق في أي جريمة تنطوي على استخدام الأجهزة الإلكترونية، سواء تم استخدام هذه الأجهزة لارتكاب جريمة أو كهدف لها.

ولا شك ان القدرة على التحاليل الجنائية الرقمية أمرًا في غاية الأهمية، باالنسبة للمنظمات الحديثة للتحقيق في انتهاكات السياسة الداخلية والهجمات الخارجية ضد أنظمتها المحوسبة .

وعلى سبيل المثال ، تمتلك الشركات الكبرى بالفعل مثل هذه القدرة التي تتجاوز قدرة العديد من إدارات الشرطة الحكومية.

ذلك ان هناك العديد من المنهجيات أو العمليات المقترحة لإجراء تحقيقات الطب الشرعي الرقمي، ومع ذلك فإنها تشترك جميعًا في المراحل الرئيسية الأربعة التالية :

أولا : أغراض التحقيق الجنائي الرقمي :

- استعادة الكمبيوتر والمواد ذات الصلة وتحليلها وحفظها بطريقة تساعد جهات التحقيق على تقديمها كدليل في محكمة قانونية.
- معرفة الدافع الرئيسي وراء الجريمة وهوية الجاني الرئيسي.
- تصميم الإجراءات في مسرح الجريمة المشتبه به مما يساعد على ضمان عدم تلف الأدلة الرقمية التي تم الحصول عليها.
- الحصول على البيانات ونسخها: استعادة الملفات المحذوفة والأقسام المحذوفة من الوسائط الرقمية لاستخراج الأدلة والتحقق من صحتها.
- التعرف على الأدلة بسرعة، كما يسمح بتقدير التأثير المحتمل للنشاط الضار على الضحية.
- إنتاج تقرير جنائي حاسوبي وتقدم تقريرًا كاملاً عن عملية التحقيق.
- حفظ الأدلة.

ثانيا : الوظائف في مجال التحليل الجنائي الرقمي :

بعض الوظائف في مجال التحليل الجنائي الرقمي ما يلي:

- محقق الكمبيوتر الجنائي Computer Forensics Investigator
- فني الكمبيوتر الجنائي Computer Forensics Technician
- محلل أمن المعلومات Information Security Analyst
- محلل أمن نظم المعلومات Information Systems Security Analyst
- محلل كمبيوتر شرعي Forensic Computer Analyst
- مستشار أمني Security Consultant

ثالثا : مهارات التحليل الجنائي الرقمي :

من المقرر ان التحليل الجنائي الرقمي لمسرح الجريمة الالكترونية، يحتاج الي العديد من المهارات التقنية والمهنية والوظيفية، ومن هذه المهارات :

١ـ الكفاءة الفنية.

ذلك ان وظائف التحليل الجنائي الرقمي تركز على التكنولوجيا، تحتاج إلى العمل عبر مجموعة متنوعة من التقنيات، من أجهزة الحاسب الآلي إلى الأجهزة المحمولة وأنظمة التشغيل، لتحديد الاختراقات الأمنية واختراقات الشبكة والاستجابة لها.

٢ـ الاهتمام بالتفاصيل.

ذلك ان المحقق في مسرح الجريمة الالكترونية، يحتاج إلى التركيز على التفاصيل من أجل فرز كميات كبيرة من البيانات بعناية للكشف عن الأدلة الرقمية وفحصها، حيث ان الدقة والتركيز على التفاصيل هي مهارة أساسية في التحليل الجنائي الرقمي.

٣ـ فهم القانون والتحقيق الجنائي.

إن التحليل الجنائي الرقمي يتعلق بالتكنولوجيا، وهي تحتاج إلى فهم قوي لجرائم ذوي الياقات البيضاء، والقانون الجنائي، والتحقيق الجنائي، وهذه مهارات يمكن بناؤها جميعًا.

٤ـ مهارات الاتصال.

حيث ان المحقق، مطالب بشرح النتائج للآخرين داخل المؤسسة العدلية، أو حتى إلى قاعة المحكمة كجزء من قضية جنائية، ولذلك تعد مهارات الاتصال، جنبًا إلى جنب مع المهارات الأساسية الأخرى، في التحليل الجنائي الرقمي ضرورة تتطلب أن يكون قادرًا على نقل المعلومات التقنية بوضوح ودقة إلى الأفراد من مستويات مختلفة من الفهم التقني.

٥ـ فهم أساسيات الأمن السيبراني.

رغم أن الأمن السيبراني والتحليل الجنائي الرقمي هما مجالان منفصلان، إلا أنهما مرتبطان ارتباطًا وثيقًا ويمكن أن يساعد وجود أساس في الأمن السيبراني على التفوق في مجال

التحليل الجنائي الرقمي، ليكون المحقق قادرًا على حل الجرائم الرقمية بشكل فعال، يحتاج إلى فهم قوي للأساليب التي يستخدمها المجرمون لخرق الأنظمة، وكيف يعمل محترفو الأمن السيبراني لمنع مثل هذه الهجمات.

٦- المهارات التحليلية.

يعد امتلاك القدرة الطبيعية على التفكير التحليلي أمرًا ضروريًا لأي شخص يعمل في مجال التحليل الجنائي الرقمي، لان المحقق يحتاج إلى تحليل الأدلة، ومراقبة المواقف عن كثب، وأنماط الملاحظة والتناقضات، وتفسير البيانات، وفي النهاية، حل الجرائم، وكلها تتطلب مستوى عالٍ من القدرة التحليلية.

٧- الرغبة في التعلم.

كما هو الحال مع أي مجال تقني، فإن التحليل الجنائي الرقمي يتغير بسرعة، يحتاج إلى الالتزام بمواكبة أفضل الممارسات واتجاهات الصناعة الناشئة، ويحتاج دائمًا إلى التعلم والتعليم الذاتي على مدار الساعة.

٨- القدرة على العمل مع المواد الصعبة.

حيث يدخل في مهام المتخصصين في التحليل الجنائي الرقمي، خاصة أولئك الذين يعملون في مناصب إنفاذ القانون، إجراء تحقيقات تتضمن مواد مسيئة أو مزعجة تستلزم القدرة على العمل مع مثل هذا المحتوى الصعب على أساس منتظم مهم.

المبحث الثالث

مفهوم الدليل الرقمي في مسرح الجريمة الالكترونية

ازاء التطور السريع في التقينات، أصبح المجرمون يستخدمون الوسائل التقنية المتطورة لتنفيذ أعمالهم الاجرامية، وهذا يؤكد ضرورة التعرف على الأدلة المنبثقة عن هذه الوسائل.

ويلاحظ أن الدليل الرقمي لا يتعلق فقط بجرائم تقنية المعلومات، فقد تكون هناك جريمة عادية، مثل القتل أو التهريب أو غيرها، لكن الدليل الذي يدين المجرمين هو دليل رقمي.

وترتيبا علي ذلك، نعرض لماهية الدليل الرقمي وخصائصه، من خلال المطلب الاول، ثم نوضح من خلال المطلب الثاني لمدى قبول الأدلة الرقمية فى الاثبات، علي ان يتناول المطلب الثالث لأهمية الدليل الرقمي، وأخيرا يختتم هذا المطلب ببيان مبادئ الأدلة الرقمية، من خلال المطلب الرابع والاخير، علي الترتيب التالي.

المطلب الأول : مفهوم الدليل الرقمي وخصائصه.

المطلب الثاني : مدى قبول الأدلة الرقمية فى الاثبات.

المطلب الثالث : أهمية الدليل الرقمي في مسرح الجريمة الالكترونية.

المطلب الرابع : مبادئ الأدلة الرقمية لمسرح الجريمة الالكترونية.

المطلب الأول

تعريف الدليل الرقمي وخصائصه

من المقرر ان جميع الاجراءات الجنائية تعتمد على الأدلة لتحديد إدانة أو براءة المتهم أو للبت في موضوع دعوى في الدعاوى القضائية، اذ كانت الأدلة على شكل مادي، مثل المستندات والصور، أو الشهادة الشفوية للشهود.

وحيثُتشتق الأدلة الرقمية في مسرح الجريمة الالكترونية من الاجهزة الالكترونية، مثل أجهزة الحاسب وأجهزتها الطرفية، وشبكات الحاسب، والهواتف المحمولة والكاميرات الرقمية والاجهزة المحمولة الاخرى، بما في ذلك أجهزة تخزين البيانات، وليس لها أي شكل مادي مستقل.

ومع ذلك، فان الأدلة الرقمية في مسرح الجريمة الالكترونية لا تختلف عن الأدلة في الجرائم التقليدية، من ناحية أنه يتعين على أحد أطراف الدعوى إدخالها في الاجراءات القانونية، فهي تعكس مجموعة من ظروف ارتكاب الجريمة، وتقدم معلومات عن الجريمة كما وقعت بالفعل.

يضاف إلى ذلك، انه يجب أن تتوافر الوسائل لإثبات أن مسرح الجريمة الالكترونية لم يتعرض لأية تعديات، سواء بالحذف، او الاضافة، او التعديل، او أية تغييرات أخرى، منذ لحظة التحصل عليها.

ومن المقرر ان الطبيعة غير المادية للبيانات، والمعلومات المخزنة بشكل إلكتروني في مسرح الجريمة الالكترونية ، من السهل التلاعب بها، وهي أكثر عرضة للتغيير من الاشكال التقليدية للأدلة، وقد شكل هذا تحدياً خاصاً لأجهزة العدالة حيث يتطلب التعامل مع هذه البيانات، أو المعلومات طريقة خاصة لضمان سلامة الأدلة التي يوفرها(١).

وقد ذهب جانب من الفقه الى تعريف الأدلة الرقمية لمسرح الجريمة الالكترونية، على النحو التالي:

الدليل الرقمي digital evidence : هو البيانات الرقمية المستقاه من مسرح الجريمة الالكترونية والمخزّنة في الاجهزة الحاسبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية.

وحيث تشترك الأدلة الرقمية في مسرح الجريمة الالكترونية مع الاشكال التقليدية للأدلة في معظم الخصائص، ولكنها تمتلك أيضاً بعض الخصائص الفريدة. (٢)

ويلاحظ فى هذا الاطار، ان الدليل الرقمي في مسرح الجريمة الالكترونية، لا يتعلق فقط بجرائم تقنية المعلومات بالنظر الى الطبيعة غير المادية للبيانات، والمعلومات المخزنة بشكل إلكتروني، والتى من السهل التلاعب بها

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، دار الجامعة الجديدة، سنة ٢٠١٧، ص ٤٧٨ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، دار الجامعة الجديدة، سنة ٢٠١٨، ص ٧٨٧ وما بعدها.

(2) Nigel Jones (United Kingdom), Esther George (United Kingdom), Fredesvinda Insa Mérida Spain), Uwe Rasmussen (Denmark) , Victor Völzow (Germany): electronic evidence guide a basic guide for police officers, prosecutors and judges.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

١- **ذات طبيعة غير مرئية للعين**: حيث تتواجد الأدلة الرقمية في مسرح الجريمة الالكترونية، في الاماكن التي يمكن الوصول إليها عبر المتخصصين فقط، أو عن طريق استخدام أدوات خاصة.

٢- **ذات طبيعة متغيرة**: حيث يمكن الكتابة في بعض الاجهزة وتحت ظروف معينة في ذاكرة الحاسب، مما يعني تغيير الدليل الذي يحتويه مسرح الجريمة الالكترونية، كما يمكن أن تطرأ تغييرات عليه من خلال الاعمال المعتادة كتشغيل الجهاز، أو إعادة تشغيله، أو لفقدان جهاز الحاسب للطاقة، أو الحالة التي يحتاج فيها نظام التشغيل إلى كتابة معلومات جديدة فوق الجزء القديم بسبب عدم وجود مساحة في الذاكرة(١)

يضاف إلى ذلك، إمكانية تعرض ذاكرة الحاسب للتلف نتيجة للعوامل البيئية مثل الحرارة الشديدة، أو الرطوبة، أو وجود الحقول الكهرومغناطيسية، كما أن أجهزة الحاسب تتغير بسبب اية استخدامات اخرى، سواء كان ذلك بناء على طلب المستخدم، كالحفظ، او النسخ، أو تلقائياً بواسطة نظام تشغيل جهاز الحاسب.

٣- **القابلية للنسخ**: حيث يمكن نسخ المعلومات الرقمية من مسرح الجريمة الالكترونية بصورتها الاصلية، وهذه الصفة الفريدة تعني أنه يمكن إجراء فحص الأدلة الرقمية في مسرح الجريمة الالكترونية من قبل المختصين، وبالتوازي من مختلف الاختصاصات، ولأسباب مختلفة، مع الحفاظ على الاصل.

٤- **الحاجة إلى متخصصين للتعامل معها**: ذلك ان كل نوع من الاجهزة الحاسبية، والاجهزة الالكترونية، والشبكات المعلوماتية، وغيرها التي قد تتواجد في مسرح الجريمة الالكترونية، تتطلب إجراءات خاصة، والتعامل من قبل غير المتخصصين قد يتلف الأدلة، أو يمحوها.

٥- **القابلية للاسترجاع**: حيث يلجأ بعض المجرمين في مسرح الجريمة الالكترونية إلى حذف البيانات والملفات التي يمكن أن تحتوي أدلة رقمية قد تمثل ادانة لهم، وهذا لا يعني أن البيانات قد حذفت بالفعل، حتى لو جرى إتلاف التجهيزات فيزيائياً، إذ يمكن في معظم الاحيان، عبر استخدام أدوات وبرامج استرجاع البيانات المحذوفة، والطريقة الاكثر استخداماً لحذف الملفات بصورة نهائية هي الكتابة فوقها، حيث يعمد بعض المشتبه بهم إلى

(1) Cybercrime Division , Council of Europe, Strasbourg (France) 2014 P 11-12

كتابة أصفار فوق البيانات القديمة مما يجعل استرجاعها مستحيلاً، ونكون أمام حالة طمس الأدلة الرقمية من مسرح الجريمة الالكترونية.(١)

المطلب الثاني

مدى قبول الأدلة الرقمية فى الاثبات

من المقرر ان هناك عدد من المعايير والشروط التى يتعين توافرها للاخذ بالدليل الرقمى المستمد من مسرح الجريمة الالكترونية، والاحتجاج به امام المحكمة المختصة بنظر احدى جرائم تقنية المعلومات التى عرض هذا الدليل بشأنها: (٢)

من حيث الصحة: يجب أن يقدم الدليل الحقائق المستمدة من مسرح الجريمة الالكترونية بطريقة لا يمكن التنازع عليها.

من حيث الاكتمال: يجب أن يتضمن أي تحليل أو رأي في مسرح الجريمة الالكترونية، استناداً إلى الأدلة الرقمية، وان تكون الواقعة كاملة، دون أن يكون مصمماً ليتناسب مع وجهة نظر فردية أو خاصة.

ذلك انه، عندما يعرض الاستوديو Gallery view الصور، ينشئ صوراً مصغرة من الصور المعروضة thumbnail ، وإذا قام أحد بالنقر على الصورة المصغرة، يُمكن أن يرى الصورة الحقيقية الاكبر، لكن كل الصور الكبيرة قد جرى حذفها من مسرح الجريمة الالكترونية، ورغم حذف هذه الصور، يمكن للخبراء استعادة ما بقي من أثر من كل صورة ومعرفة البيانات الفائقة في قاعدة بيانات البرنامج.

ويجب ان يتم تقديم تقرير من قبل الخبراء يتضمن ما يلي:

١- **التوثيق**: حيث يجب أن لا تكون هناك أية ملاحظات على الطريقة التي جمعت بها الأدلة من مسرح الجريمة الالكترونية، أو أي شك بصحتها في أي وقت.

٢- **المصداقية**: حيث يجب أن يكون الدليل من مسرح الجريمة الالكترونية مقنعاً، ويمكن الاعتماد عليه في المحكمة سواء كدليل إثبات، أو كبينة.

(1) R v Ross Warwick Porter: England and Wales Court of Appeal (Criminal Division) Decisions, 2006.
"http://www.spannertrust.org/documents/R_v_Porter.pdf".

(2) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow: Pervious reference P 13

٣- **العدالة**: ذلك إن الطرق المستخدمة لجمع الأدلة من مسرح الجريمة الالكترونية، يجب أن تكون عادلة ومتناسبة مع مصلحة المحكمة والعدالة، ولا تتعرض لحقوق أي طرف، واستخدامها فقط في حدود القيمة الثبوتية للدليل، أي قيمته كدليل.

وعليه يجب أن تكون الأدلة الرقمية في المحاكمات الجنائية، والمستمدة من مسرح الجريمة الالكترونية، كما ذكرنا مقبولة، وصحيحة، ودقيقة، وكاملة، ويجب أن تتوافق مع القوانين والقواعد المعمول بها، كي تكون مقبولة كدليل له حجيته لدى المحكمة(١).

وتنظر النيابة في مراجعة القضية، إذا كان من الممكن ربط الملفات، او اذا ظهر أن هناك ترابطاً بين الأدلة من خلال مسرح الجريمة الالكترونية، وحال المحاكمات الجنائية، حيث يجب على المدعي استخدام الأدلة لإثبات القضية في المستوى الجنائي بما لا يدع مجالا للشك، وتقوم النيابة العامة بدراسة الأدلة الرقمية لتحديد ما إذا كانت الأدلة كافية، فّإذا كانت هناك نقاط ضعف، فإن ذلك يتطلب مزيداً من الأدلة من مسرح الجريمة الالكترونية محل الواقعة، او اذا تم ذلك في مرحلة مبكرة قد يكون لا يزال هناك فرصة للحصول على أدلة إضافية من مصادر متنوعة قبل أن تحال القضية للمحاكمة.

ويجب على النيابة العامة أن تقدم مذكرات شارحة، وواضحة، ومتماسكة مع المستندات الداعمة إذا لزم الامر، وينبغي أن يطلب الشاهد للحصول على معلومات وتفسيرات محددة بشأن النقاط التي من المرجح أن يثيرها الدفاع حول مسرح الجريمة الالكترونية.

وتظهر الاهمية خاصة فيما يتعلق بأي من التناقضات الواردة في البيانات، أو معارضتها من شهود عيان في مسرح الجريمة الالكترونية، فى توقيت وفترة ما قبل المحاكمة، او اذا لزم الامر أثناء المحاكمة الرئيسية، حيث قد تجد النيابة العامة أنه من المفيد مناقشة الدفاع في نطاق الأدلة الرقمية بمسرح الجريمة الالكترونية، من أجل توضيح حالتها الثبوتية، وعند تقديم أي من شهود مسرح الجريمة الالكترونية أدلة رقمية جديدة، يجب على القاضي التأكد من أنها موثوقة، ومحايدة، وواضحة.

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، مرجع سابق، ص ٤٧٨ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ٧٨٧ وما بعدها.

المطلب الثالث

أهمية الدليل الرقمي في مسرح الجريمة الالكترونية

من الثابت ان استخدام الوسائل الرقمية، والانترنت، ان خلق للمجرمين فرصاً جديدة ومستحدثة لارتكاب جرائمهم، وتطورت اسراتيجيات جديدة متطورة في مسرح الجريمة الالكترونية، مختلفة عن مسرح الجرائم التقليدية، اذ يجب أن تكون الأدلة الرقمية المستخرجة من مسرح الجريمة الالكترونية، والمقدمة في المحاكمات الجنائية، مقبولة، وصحيحة، ودقيقة، وكاملة.

ذلك ان استغلال قنوات الاتصال الجديدة، ونشأة فئات جديدة من جرائم تقنية المعلومات، اوجب على جميع المشاركين في النظام القانوني أن يكونوا على دراية جيدة لمسرح الجريمة الالكترونية، وعلي ادراك تام لأشكال الأدلة الرقمية المستخرجة عنه، وعلى معرفة تامة بكيفية وآليات التعامل معها.

يضاف الي ذلك، ان مسرح الجريمة الالكترونية، غالباً ما يرتبط بجهاز إلكتروني يحتوي على ذاكرة وأي شكل من أشكال البرمجيات، حتى عندما تكون الجريمة نفسها لم يُستخدم فيها مثل هذا الجهاز، ولكن يمكن أن يساعد في القبض على الجاني، أو في عمليات التحقيق، اذ ان ما تسجله كاميرات مراقبة، أو ما يقدمه نظام تحديد المواقع العالمي (GPS) للهاتف أو للسيارة، وغيرها من الادوات، تساعد المحكمة كثيراً في الوصول إلى المجرمين، وقد أصبح تأمين مسرح الجريمة الالكترونية ، والحرص علي ما ينتج عنه من الأدلة الرقمية، وفحصه عبر الشرعية الرقمية يشكل الاداة الرئيسية في تقديم المجرمين للعدالة.

كما أدى تطور شبكة الانترنت وتطبيقاتها إلى الحصول على الأدلة في مسرح الجريمة الالكترونية من مواقع الانترنت، والشبكات الاجتماعية، وفي رسائل البريد الالكتروني، وغرف الدردشة.

وقد تنوعت مصادر الحصول على الدليل الرقمي من مسرح الجريمة الالكترونية، ليس فقط من الحاسب الشخصي للجاني، وإنما من خلال المعلومات التي يوفرها مقدمو الخدمات على الشبكة، ومنها خدمات النفاذ إلى الشبكة، وخدمات التواصل على الشبكة، وخدمات الاستضافة على الشبكة.

كما أن تطوير الحوسبة السحابية من خلال مسرح الجريمة الالكترونية، حيث يتم تخزين التطبيقات والبيانات عن بعد، وخارج الحدود الوطنية، في مواقع متنوعة ومنتشرة في العالم، أضاف تحدياً آخرَ في ضرورة تطوير الحصول على الدليل الرقمي، تحقيقا للعدالة، وعدم إهمال أية معلومات تستقي من مسرح الجريمة الالكترونية، قد تقود المحكمة إلى معرفة المجرمين.

المطلب الرابع

مبادئ الأدلة الرقمية لمسرح الجريمة الالكترونية

من المقرر ان هناك عددا من المبادئ اللازمة لتوجيه المختصيين بمسرح الجريمة الالكترونية، وخاصة القضاة، والمحققين، والمحاميين، لدي التعامل مع الأدلة الرقمية، اذ ينبغي عليهم عند اتخاذ التدابير القانونية، أن يأخذوا في حسبانهم الوثائق، واللوائح القانونية الخاصة، ومراعاة المبادئ التالية(١):

ـ المبدأ الاول: سلامة البيانات:

حيث ينبغي للإجراءات المتخذة تجاه مسرح الجريمة الالكترونية، ضمان عدم حصول أي تغيير في البيانات التي يمكن استخدامها، كأدلة في المحكمة، لانه يجب أن لا يتم تغيير الاجهزة أو البيانات الرقمية، ذلك ان الشخص المسؤول عن معاينة موقع مسرح الجريمة الالكترونية أو جمع الأدلة منه، هو المسؤول الأول والاخير عن الحفاظ على سلامة المواد المستخلصة من مسرح الجريمة الالكترونية، ويجب أن يتم الوصول إلى البيانات على نظام الحاسب واستخلاصها، بالطريقة التي تسبب أقل تأثير على البيانات، ومن قبل شخص مؤهل للقيام بذلك.

ـ المبدأ الثانى: المراجعة والتتبع:

اذ يجب إنشاء سجل لجميع الاجراءات المتخذة عند التعامل مع مسرح الجريمة الالكترونية، والأدلة الرقمية عنه، والحفاظ عليها بحيث يمكن مراجعتها في وقت لاحق، ويجب أن يتم تحليل الأدلة، ويصل إلى النتائج نفسها، ومن الضروري أن يُسجَّل كافة البيانات المستخرجة من مسرح الجريمة الالكترونية.

وقد تنوعت مصادر الحصول على الدليل الرقمي بحسب دقة كل نشاط في مسرح الجريمة الالكترونية لتمكين طرف ثالث لإعادة الاجراءات إذا لزم الامر، حيث ان جميع النشاطات المتعلقة بالتفتيش والمصادرة والوصول، وتخزين أو نقل الأدلة الرقمية، يجب أن تكون موثقة بشكل كامل.

(1) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen , Victor Völzow Pervious reference P 14.

- **المبدأ الثالث: الدعم الخاص:**

إذا كان من المتوقع العثور على الأدلة الرقمية من مسرح الجريمة الالكترونية في سياق عملية مخطط لها، يجب على الشخص المسؤول إخطار المختصين والمستشارين الخارجيين في الوقت المحدد، وترتيب وجودهم أثناء جمع الأدلة من مسرح الجريمة الالكترونية، إذا أمكن ذلك.

- **المبدأ الرابع: التدريب المناسب:**

يجب تدريب الشخص الموكل بأول عملية تفتيش لمسرح الجريمة الالكترونية، تدريباً جيداً، لضمان عدم فقدان الأدلة أثناء عمليات التفتيش.

المبحث الرابع

مصادر الأدلة الرقمية لمسرح الجريمة الالكترونية

يجب على المحققين والقضاة، النظر في احتمال أن يسفر مسرح الجريمة الالكترونية، بما يشمله من الاجهزة الالكترونية والمعدات عن أدلة رقمية، ذلك إن وجود مثل هذه الاجهزة قد لا يكون واضحاً وبديهياً، حيث تتعدد الاجهزة في مسرح الجريمة الالكترونية التي تحتوي على الأدلة الرقمية بشكل شبه يومي.

حيث تتوافر ضمن مسرح الجريمة الالكترونية، مصادر الأدلة الرقمية، أجهزة الحاسب الآلى ووحدات التخزين، وايضا الشبكات Computer networks، لتأتي من بعد شبكة الانترنت، كاخطر تلك المصادر للأدلة الرقمية.

ونورد القائمة التالية من مسرح الجريمة الالكترونية، المصادر المحتملة للأدلة الرقمية، لكن هذا لا يعني أنها واردة علي سبيل الحصر وشاملة، ولكنها تحتوي على الأمثلة الاكثر شيوعاً(١)، لنعرض من خلال المطلب الأول لأجهزة الحاسب الآلى ووحدات التخزين بمشرح الجريمة الالكترونية، علي ان يخصص المطلب الثاني لبيان الشبكات بمسرح الجريمة الالكترونية Computer networks، ثم نعرض لشبكة الانترنت بمسرح الجريمة الالكترونية، من خلال المطلب الثالث والاخير، علي السياق التالي.

المطلب الأول : أجهزة الحاسب الآلى ووحدات التخزين لمسرح الجريمة الالكترونية.

المطلب الثاني : الشبكات بمسرح الجريمة الالكترونية Computer networks.

(1) Donald R. Mason: Digital Evidence & Computer Forensics, the national center for justice, University of Mississippi, 2011.

المطلب الثالث : شبكة الانترنت بمسرح الجريمة الالكترونية.

المطلب الأول

أجهزة الحاسب الآلى ووحدات التخزين لمسرح الجريمة الالكترونية

تأتي أجهزة التخزين أيضاً في العديد من الاشكال والاحجام، وتختلف في الطريقة التي تخزن فيها البيانات أو تحتفظ بها.

وعلى ذلك، فان جميع الاجراءات المتعلقة بالتفتيش والمصادرة بمسرح الجريمة الالكترونية، وتخزين أو نقل الأدلة الرقمية منه، يجب أن تكون موثقة بشكل كامل، من خلال محاضر رسمية.

ونذكر من هذه الوحدات على سبيل المثال:

- الاقراص الصلبة Hard disk drives (HDD)
- الوسائط المتنقلة Removable media (DVD,CD)
- بطاقات الذاكرة (Memory cards (Flush cards
- أجهزة تخزين البيانات data storage devices (USB)
- أجهزة الحاسب اللوحي Tabet devices
- الهواتف الخليوية Mobile telephones
- الاجهزة الطرفية Peripheral devices (Scanner, printers,webcam)
- أجهزة وكاميرات التصوير Photo and video recording (Digital cameras)

ويمكن اعتبار وحدات التخزين، بما فيها أجهزة الحاسب، بمسرح الجريمة الالكترونية، المصدر الاساسي للأدلة الرقمية، وعلى سبيل المثال لا الحصر فهي قد تقدم البيانات التالية، والتي قد تحتوي أدلة(١):

- الصور والفيديو Images & Video.

(1) Donald R. Mason: previous reference.

- المستندات والوثائق بأنواعها.
- جلسات المحادثة، وسجل البريد الالكتروني.
- ملفات تسجيل العمليات؛ Log files.
- المعلومات التاريخية للتصفح، والملفات المخبأة؛ Cash files.
- مفاتيح التشفير، وكلمات المرور passwords & encryption keys.

المطلب الثاني

الشبكات بمسرح الجريمة الالكترونية

ذلك انه عندما يتم ربط جهازي حاسب أو أكثر، يكون لدينا شبكة، فان أجهزة الحاسب في الشبكة تكون قادرة على تبادل البيانات والموارد الاخرى فيما بينها، وكثيراً ما تكون مرتبطة بمكونات وأجهزة إضافية، ويمكن أن تكون شبكات الحاسب محدودة مثل تلك التي توجد في المنزل.

وعلى سبيل المثال، قد ينشئ أفراد أسرة شبكة، موصولة إلى جهاز إنترنت أو واسعة النطاق مثل تلك المستخدمة من قبل الشركات الكبرى أو الحكومات التي تربط بين المئات أو حتى الالاف من أجهزة الحاسب معاً.

وهنا يجب على المحققيين معرفة أن الأدلة المعلوماتية بمسرح الجريمة الالكترونية، قد لا تكون موجودة في جهاز الحاسب الخاص بالمتهم، أو الوحدات الخاصة به، وانما يمكن أن تكون أيضاً موجودة في مخدمات، أو وحدات تخزين عبر الشبكة، قد يستخدمها المجرمون(١).

ولذا فإنه من الممكن معرفة المستخدمين الذين قاموا بأية عمليات على الشبكة، من خلال حسابات المستخدمين، ونتيجة لذلك، تكون الشرعية الرقمية للشبكة، إذا جاز التعبير، جزء لا يتجزء من الشرعية الرقمية للحاسب، وتشكل تحدياً للمحققين، ومع ذلك، وباستخدام منهجيات مناسبة لطبيعة الحادث والفاعل، يمكن الكشف عن جرائم تقنية المعلومات التي وقعت على الشبكة، أو باستخدامها في مسرح الجريمة الالكترونية.(٢)

---

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، مرجع سابق، ص ٤٧٨ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ٧٨٧ وما بعدها.

(2) Ioannis A. Apostolakis: Network Forensics: Problems and Solutions, Conference Paper· January 2006, P13.

المطلب الثالث

شبكة الانترنت ومسرح الجريمة الالكترونية

ذلك ان الشرعية الرقمية للشبكة المعلوماتية، تعد جزء لا يتجزء من الشرعية الرقمية للحاسب الرقمى على الانترنت، فإذا كانت الاجهزة الحاسبية، ووحدات التخزين المصدر الاساسي للأدلة الرقمية بمسرح الجريمة الالكترونية، فإن شبكة الانترنت هى المصدر الاوسع والاهم لها. (١)

ومن اهم التطبيقات العملية فى هذا المقام:

حيث تم الكشف من خلال مسرح جريمة الكترونية، عن جريمة الوصول غير المصرح به من خلال صلاحيات موظف في ١٨ مارس عام ١٩٩٧، حينما ألقي القبض على السيد "أليسون" في بريطانيا بناء على إذن مؤقت صادر بموجب قانون تسليم المجرمين الصادر سنة ١٩٨٩، وبناء على طلب من حكومة الولايات المتحدة، التي ادعت أنه تآمر مع سيدة تدعى جوان وغيرها ما بين ١ يناير عام ١٩٩٦ و ١٨ يونيو من عام ١٩٩٦ في نطاق الولاية القضائية للولايات المتحدة الامريكية، وقام بما يلي:

أ- تأمين الوصول غير المصرح به لنظام حاسب أمريكان إكسبريس American Ex press بقصد ارتكاب جريمة السرقة.

ب- الوصول غير المصرح به لنظام الحاسب الخاص بشركة أمريكان إكسبريس بقصد ارتكاب التزوير.

ج- التعديل غير المصرح به في محتويات نظام الحاسب الخاص بشركة أمريكان إكسبريس.

حيث كانت "جوان أوجومو" موظفة في شركة أمريكان إكسبريس(٢)، وانتدبت لقسم الائتمان في مكتب الشركة في فلوريدا كمحللة، وكان عملها اليومي يمكِّنها من الوصول إلى

---

(1)http://www.publications.parliament.uk/pa/ld199899/ldjudgmt/jd990805/bow.htm

R v Bow Street Magistrates Court and Allison (AP) Ex parte Government of the United States of America (Allison) [2002]2 AC 216.

(١) من المقرر ان شركة أمريكان اكسبريس American Express Company هي شركة عالمية للخدمات المالية متنوعة مقرها الرئيسي في مدينة نيويورك وقد تأسست في عام ١٨٥٠، وهي الان أحد ٣٠ شركة المكونة لمؤشر داو جونز الصناعي، وتشتهر الشركة بعملها في مجالي البطاقات الائتمانية

جميع حسابات العملاء، لكن لا يُرخص لها الا الوصول إلى الحسابات التي تم تعيينها لها، الا أنها وصلت إلى الحسابات والملفات التي لم يكن لها حق الوصول إليها، وبعد الوصول إلى تلك الحسابات والملفات من دون صلاحيات، قدمت معلومات سرية تم الحصول عليها من تلك الحسابات والملفات، إضافة إلى معلومات أخرى، إلى السيد أليسون، واستخدم الاخير المعلومات التي قدمت له لترميز بطاقات ائتمان، وتوفير أرقام PIN جرى استخدامها بعد ذلك عن طريق الاحتيال للحصول على مبالغ كبيرة من المال من المصارف الآلية(١).

وأظهرت معاينة الأدلة من مسرح الجريمة الالكترونية، فيما يخص صلاحية جوان، وصولَها إلى بيانات لم يكن لديها الصلاحية بالوصول إليها، واعترفت أنها قامت بالحصول على بيانات لم يكن لديها في أي وقت من الاوقات صلاحيات الوصول إلى أي منها، مما يعتبر خرقاً لسياسة الشركة والاخلاقيات المهنية.

وأظهرت السجلات المخزنة في مسرح الجريمة الالكترونية، والكشف من خلال الحاسب انه تم الوصول إلى ١٨٩ حساباً لا تقع ضمن نطاق واجباتها، باستخدام هذه الاساليب، واعترفت أنها وزملاءها المتآمرين احتالوا على أمريكان إكسبريس بحوالي مليون دولار، وقد ألقي القبض على السيد أليسون مع ضبط بطاقات أمريكان إكسبريس مزورة بحوزته، والتى استخدمها للحصول على المال من المصارف الآلية في لندن(٢).

وقد اعتبر القانون البريطاني أن الموظف قد يرتكب جريمة الوصول غير المصرح به للبيانات، مما يتعارض مع المادة الاولي من قانون إساءة استخدام الحاسب ١٩٩٠، كما تسبب

والشيكات السياحية، وتعتبر أكبر مصدر للبطاقات الائتمانية في الولايات المتحدة، بنسبة تقارب ٢٤% من عمليات البطاقات الائتمانية.

(1) see : chehire and fifoot , the law of contract, London , 1964 , p.457.

(٣) جدير بالذكر ان شركة أمريكان اكسبريس، قد قيمت بالمركز الـ ٢٢ كأغلى علامة تجارية في العالم بقيمة تساوي ١٤.٩٧ مليار دولار وهي من أفضل ٣٠ شركة مرغوبة في العالم حسب مجلة فوربس، وأما علامة الشركة، والتي اختيرت عام ١٩٥٨، فهي ترمز إلى مصارع روماني ويظهر على الشيكات السياحية والبطاقات الائتمانية الخاصة بالشركة.

٣٠. Top Management Compensation اطلع عليه بتاريخ Aug. 2014 American Express Company (AXP) annual SEC income statement filing via Wikinvest by $ value. Amex presentation to investors at the Keefe, Bruyette & Woods 2009 Diversified Financials Conference. June 3, 2014

American Express to slash 7000 jobs". Bloomberg. Sydney Morning Herald. October 31, 2008 - اطلع عليه بتاريخ ٩- August- 2014.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

تسريب الموظفة عمداً للبيانات، ووصولها إلى بيانات غير مخولة بالوصول إليها لخسائر جسيمة، مما يخالف أيضاً بنود العقد الموقع من قبلها مع الشركة.(١)

لذلك نجد أن القانون قد بين ضرورة توضيح صاحب العمل لحدودَ صلاحيات الموظف بالوصول إلى البرامج أو البيانات، ويمكن الحديث عن الأدلة الرقمية في شبكة الانترنت انطلاقاً من العناصر التالية، على سبيل المثال لا الحصر.

١ - مواقع الويب:

وهى المصدر الاشمل للمعلومات المتاحة على شبكة الانترنت، وأول جزء من الأدلة الرقمية المحتملة بمسرح الجريمة الالكترونية هو وضوح محتوى الموقع، والثاني هو الجزء غير المرئي من المعلومات المرتبطة بهذا الموقع، والمحتوى غير المرئي هنا هو في الاساس متعلق بلغة البرمجة المستخدمة لإنشاء صفحات الويب.

وهنا يمكن أن تتوفر مجموعة من المعلومات، غير تلك التي تظهر في الواقع على الشاشة، ويمكن أن يرى المحقق مزيداً من المعلومات هنا وهناك بمسرح الجريمة الالكترونية، وبعضها قد يكون مفيداً جداً، وهناك بعض الامثلة من البيانات التي يمكن الحصول عليها بهذه الطريقة هي:

- تعليقات المستخدمين / المطورين وكلمات السر.
- الحقول المخفية.
- المراجع إلى المواقع الخارجية التي قد تكون مصادر مستقلة للأدلة.

كما يمكن استعراض الرمز المصدري الذي يمكن أن يساعد المتخصص في الشرعية الرقمية على معرفة الجهاز الحاسبي الذي وصل للموقع حتى لو قام المشتبه به بمسح السجلات التاريخية للإنترنت له وقام بتفريغ البيانات.

كما يمكن التعرف من خلال مزودي الخدمات على الشبكة على بيانات الحركة للمتهم بمسرح الجريمة الالكترونية، أي استعراض المواقع التي تصفحها، وكافة المعلومات المتعلقة بها وخاصة معلومات التاريخ والوقت.

---

(2) مشار إلى هذه القضية لدي : د. جميل عبد الباقي الصغير ، الجوانب الاجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، سنة ١٩٩٨م.

وأخيراً، هناك البيانات الفائقة Meta data أو البيانات الوصفية، أي التي تشرح البيانات، والتي يمكن أن توفر معلومات فنية رفيعة المستوى عن صفحة الويب نفسها، ومثال بسيط عن هذه النقطة هو تاريخ آخر تعديل لمورد ويب معين، كصفحة على شبكة الانترنت أو صورة، وهناك أدوات مفتوحة المصدر مثل FireBug تستخرج بعض المعلومات، ولكن فقط لتذكير القاضي بوجوب الطلب من مختصين ولجان خبرة استخراج القدر الاكبر من البيانات غير الظاهرة على صفحة الويب.

- تطبيق عملى : الدليل الرقمي لجريمة قتل معلوماتية:

ومن الامثلة الواقعية على الدليل الرقمي في مسرح الجريمة الالكترونية، كجريمة قتل حدثت بالفعل في الولايات المتحدة الامريكية، أن رجلاً قتل زوجته كانت موضوعة تحت المراقبة في المستشفى، بأن دخل عبر الانترنت إلى شبكة المعلومات الخاصة بالمستشفى، ثم قام بتغيير المعلومات الطبية الخاصة بالمجني عليها المريضة. (١)

٢ - البريد الالكتروني:

حيث يعتبر البريد الالكتروني مصدراً هاماً أيضاً للأدلة الرقمية في مسرح الجريمة الالكترونية، حيث يمكن بسهولة معرفة مصدر البريد الالكتروني، وتحديد من أرسل الرسالة، ذلك إن برامج البريد الالكتروني تخفي عادة المعلومات التقنية عن القارئ، وتوجد هذه المعلومات في ما يسمى ترويسة البريد الالكتروني(٢).

ولكن يمكن أحياناً اختراق البريد الالكتروني، فيقوم المخترق بإرسال بريد من حساب شخص آخر، ويمكن للمرسل أيضاً إخفاء تحركاته من خلال الذهاب الى مكان عام مثل مقهى للإنترنت، حيث سيكون العنوان IP ينتمي إلى المقهى ولا يشير له بمسرح الجريمة الالكترونية.

وفي حالة اختراق البريد - والذي هو جريمة بحد ذاته - يستطيع الخبراء تحليل الاختراق وتحديد مصدره من مسرح الجريمة الالكترونية، واذا تم إرسال البريد الالكتروني من مكان عام مثل فندق أو مقهى إنترنت، يمكن استخدام بعض الملفات للمساعدة في التعرف على العملاء الذين استخدموا الحاسب في الوقت الذي تم إرسال البريد الالكتروني.

ومن الهام أيضاً أن نلاحظ أن معظم المعلومات في ترويسة البريد الالكتروني يمكن التلاعب بها لأنها تضاف من قبل مخدمات او ملقمات البريد الالكتروني المختلفة، والتي قد لا

(1) http://www.theregister.co.uk/23/08/2006/email_bomber_guilty .

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، مرجع سابق، ص ٣٤٨ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ٧٩٩ وما بعدها.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

تكون جديرة بالثقة، وينطبق هذا على جميع المعلومات الموجودة أسفل عنوان البريد الالكتروني، لأنها تأتي مباشرة من مخدم البريد المرسل الذي يمكن أن يكون تحت سيطرة المتهم، لذلك يجب على القاضي دائما مراعاة الدقة في كل المعلومات والأدلة من مسرح الجريمة الالكترونية التي يمكن أن تقدم من خلال البريد الالكتروني للعميل.

ومن التطبيقات العملية على ذلك فى مجال مسرح الجريمة الالكترونية في المملكة المتحدة، والمتعلقة بإعاقة الوصول إلى الخدمة Denial of service attack ، حيث جرت هذه الواقعة مع ديفيد لينون في الفترة الواقعة بين ٣٠ يناير، و ٥ فبراير عام ٢٠٠٤ ، حيث قام بهذا الهجوم، والدخول غير المصرح به إلى جهاز حاسب خاص بالرحلات الداخلية لشركة mestic and General Group Plc (D&G)

وكانت الوقائع أن السيد لينون كان يعمل من قبل في الشركة D&G لمدة ثلاثة أشهر حتى أقيل في شهر ديسمبر عام ٢٠٠٣ ، وكان عمره آنذاك ١٦ عاماً، في ٣٠ يناير ٢٠٠٤ ، بدأ السيد لينون بإرسال رسائل البريد الالكتروني إلى D&G باستخدام برنامج يسمى AvalancheV3.6 ، الذي كان قد قام بتحميله من الانترنت، ثم وضع البرنامج بصيغة إرسال البريد حتى التوقيف، وهذا يعني أنه سيستمر في إرسال رسائل البريد الالكتروني إلى أن يتم إيقافه يدوياً.

وتشير التقديرات إلى أن استخدام السيد لينون للبرنامج تسبب بإرسال ما يقارب خمسة ملايين رسالة للبريد الالكتروني، والتي تم استلامها من قبل مخدم البريد الالكتروني للشركة D&G ترتب على ذلك تحطم وتوقف خادم البريد الالكتروني للشركة نتيجة العدد الهائل والضخم للرسائل المستقبلة، واستُدعي السيد لينون بتهمة التعديل غير المصرح به في محتويات الحاسب، والذي يتعارض مع المادة الثالثة من قانون إساءة استخدام الحاسب لعام ١٩٩٠ الصادر حينها.(١)

وفي محكمة الاحداث، جادل لينون بنجاح أنه لم يكن هناك أي رد من مخدم البريد الالكتروني للشركة، أي لم يرسل له أي جواب على رسالته، وهي الحالة العامة لعمل الشركة، وبالتالي وافق على تلقي رسائل البريد الالكتروني، وهذا يعتبر إذناً للمرسلين المحتملين لرسائل البريد الالكتروني لتعديل محتويات المخدم.

وقد وجدت محكمة الاستئناف أن هناك خللاً في تفسير مفهوم إجابة الشركة أو المخدم على الرسائل وأمرت بإعادة المحاكمة، وذكرت محكمة الاستئناف أنه على الرغم من أن الشركة قادرة على تلقي رسائل البريد الالكتروني، فالموافقة عادة لاستلام رسائل البريد الالكتروني

(1) Jonathan clough: principles of cybercrime, Cambridge University Press ،٢٠١٠،p171

الضمنية ليست بحدود، والموافقة تشمل فقط رسائل البريد الالكتروني التي أرسلت لغرض التواصل مع الشركة، وليس لغرض تعطيل عمل النظام، مما جعل السيد لينون مذنباً.

وايضا من التطبيقات العملية على مسرح الجريمة الالكترونية عام ٢٠٠٢ ، محاولة لابتزاز ٢٠٠ الف دولار من مايكل بلومبرغ Bloomberg عن طريق القرصنة على نظام حاسب شركته، والمتخصصة بتقديم بيانات ومعلومات مالية.

حيث كان زيزيف Zezev يعمل في شركة كازكوميرتس Kazkommerets ، وهي شركة للأوراق المالية في كازاخستان، حيث اشتركت في الخدمات التي تقدمها شركة بلومبرغ.

واستطاع زيزيف النفاذ غير المشروع والوصول إلى حسابات البريد الالكتروني للسيد بلومبرغ، مؤسس ومدير عام الشركة، وللسيد رئيس مكتب أمن الشركة، حيث أرسل زيزيف سلسلة من رسائل البريد الالكتروني إلى السيد بلومبرغ يطلب منه المال أو أنه سيكشف أن النظام قد تعرض للاختراق.

وكان الدليل الرقمى من مسرح الجريمة الالكترونية، من خلال مراجعة عمليات البريد الالكتروني، وتقارير الخبراء، على أن زيزيف استخدم البريد الالكتروني لتسجيل وصول المعلومات التي لم تأت من المصدر المزعوم.

وبعبارة أخرى، تظهر المعلومات المستقاه من مسرح الجريمة الالكترونية، التي تأتي من شخص (س)، أنها تأتي من شخص (ع)، وقد قدم الدفاع حجته في أن هذا العمل لا يؤثر على أداء منظومة الشركة، ولا يؤثر على مصداقية البيانات.

وقد رفضت المحكمة هذا الدفاع، حيث تبين من أدلة مسرح الجريمة الالكترونية أن القصد كان إعاقة تشغيل البرامج والتأثير على مصداقية البيانات، ونتيجة لذلك، كانت عناصر الجريمة جميعها متوافرة، واعتبرت المحكمة ان إرسال رسائل وهمية عبر البريد دخولاً غير مصرح به إلى البيانات التي قصد المتهم بشكل واضح التأثير على مصداقيتها(١).

كذلك من التطبيقات العملية لجرائم تقنية المعلومات فى مسرح الجريمة الالكترونية، حينما تلقى قسم شرطة Old Tbilisi في جورجيا شكوى من إحدى المواطنات (SS) ، بالقرصنة، والتلاعب في حسابها على الفيسبوك من قبل شخص قام بتغيير كلمة المرور لحسابها ومن ثم نشر صور غير لائقة لها.

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، مرجع سابق، ص ١٢٨ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ٩٨٧ وما بعدها.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

كما جرى إنشاء حساب مزيف لها دون موافقتها أيضاً في الشبكة الاجتماعية Odnoklassniki.ru ، حيث تم نشر معلومات خاصة عنها، والهواتف الخاصة بها وبأفراد أسرتها وأرقام اتصال أيضاً لتقديم خدمات جنسية، وقد ورد عدد من هذه الاتصالات من أشخاص مختلفين تطلب منها، ومن أفراد أسرتها، خدمات جنسية.

وبدأ التحقيق في مسرح الجريمة الالكترونية بموجب المادة ٢٨٤ ، غصن ١ من القانون الجنائي الجورجي، للوصول إلى نظام الحاسب دون وجه حق، وكان المتهم الرئيسي في القضية، كما أشارت المجني عليها خلال مقابلتها وعائلتها، هو صديقها السابق GA الذي منذ انفصاله عن SS ، كان غيوراً جداً، ويصر على مكالمتها هاتفياً، وقد توقف عن الاتصال بها فقط لبضعة أشهر سابقة لحادثة القرصنة لحسابها، وأيضاً في الماضي خلال العلاقة بينهما، سبق له ان أنشأ صفحة فيسبوك مشتركة، وكانت هناك حجة أخرى من قبل الضحايا أيضاً أن الصور غير اللائقة التي نشرت على الفيسبوك و Odnoklassni ki.ru ، صورت من كل من SS و GA في أحوال وظروف مختلفة، بما في ذلك اللحظات الحميمة، كما طلبت رموز IMEI لتحديد جميع المكالمات الواردة إلى (SS) يطلبون خدمات جنسية من مشغلي الاتصالات الرئيسية، والجداول ذات الصلة التي تظهر المكالمات الواردة، وأرقام الهواتف، ووردت رموز IMEI وحددت هوية المتصلين دون تأخير، ولكن لا يتضمن أي منها أية بيانات تتعلق ب GA ، ومع ذلك ظل هو المشتبه به الرئيسي.

وتم تقديم طلب البحث والمصادرة في ظروف طارئة لمكان إقامة المشتبه به، وتمت مصادرة حاسبه الشخصي، وذكر بالتحقيق أن GA يعلم باحتمال التحقيق معه، لذلك قد يعمد لتدمير الأدلة ذات الصلة بمسرح الجريمة الالكترونية، فكان البحث بالتالي ملحاً وللمصادرة ما يبررها، وقد وافق القاضي على الاسباب التي قدمت وأعلن أمر التفتيش والضبط.

وحيث يجب على قضاة التحقيق أن ينتبهوا لتلك الادلة في مسرح الجريمة الالكترونية من خلال مواقع شبكات التواصل الاجتماعي، وإرسال أجهزة الحاسب المضبوطة بمسرح الجريمة الالكترونية إلى مختبر الشرعية الرقمية، وتوجيه الاسئلة للخبير ما إذا تم العثور على أدلة تدين GA مثل الوصول إلى صفحات الشبكات الاجتماعية، وكلمات السر التي استخدمت لهذا الوصول، وعما إذا كانت الصور التي نشرت، قد تم تحميلها من جهاز الحاسب الخاص به بمسرح الجريمة الالكترونية.

وقد قدم الخبير إجابات سلبية عن كل من الاسئلة المذكورة، باستثناء الصور التي تم العثور عليها على القرص الصلب وكذلك القرص المضغوط الذي تم ضبطه مع جهاز الحاسب بمسرح الجريمة الالكترونية، ومع ذلك، لم يتم العثور على ما يدل على التحميل على الانترنت، من خلال تواريخ التصفح، والاجراءات التي اجريت من الحاسب، لذلك طلب من مزود خدمة الانترنت، وكذلك مقدمي خدمات الهاتف المحمول، بيانات الحركة الخاصة بالمتهم GA ولم يكن أي من

مقدمي خدمات الانترنت قادراً على تقديم المعلومات في ذلك الحين، وفقاً للقانون الجورجي، ولا ان يُطلب بموجب أي قانون، من مقدمي خدمات الانترنت الحفاظ على بيانات الحركة مع القليل من الأدلة المتوفرة بمسرح الجريمة الالكترونية، وهي حيازته للصور المنشورة، وقررت النيابة توجيه الاتهام ل GA بتهمة واحدة هي الوصول غير المشروع إلى نظام الحاسب.

وخلال المقابلة الاولية لـ GA اعترف تماماً بالذنب، وقدم للتحقيق معلومات عن أفعاله، بما في ذلك كلمة السر المستخدمة للوصول إلى حسابات الفيسبوك وOdnoklassniki ، فضلاً عن الاسباب والدوافع لمثل هذه الاعمال ومنها الغيرة وما إلى ذلك، ونتيجة لاعترافه والمفاوضات بين محاميه والنيابة العامة، تم إبرام اتفاق بين الطرفين، حيث ناشدت النيابة العامة تجريمه، وحكمه بالسجن مع وقف التنفيذ، وتغريمه.

وقد عقد القاضي جلسة الاستماع في اليوم التالي لإبرام الاتفاق مع الادعاء، وقد استعرض القاضي المواد في هذه القضية، وشكك المدعى عليه باحتمال وقوع الاكراه أو أي ظرف من الظروف الاخرى التي قد تفسد اعترافه أو تبرّئه، ووجد المتهم مذنباً وحكمت المحكمة عليه بالسجن لمدة سنتين مع وقف التنفيذ وغرامة مالية قدرها ٣٠٠٠ جيل جورجي.

٣ - مواقع التواصل الاجتماعي:

بدأت مواقع الشبكات الاجتماعية كبداية صفحات الويب العادية، وتطورت بشكل كبير في تعقيدها، لذا فانه يتعين على قضاة التحقيق أن ينتبهوا لعدة امور هامة في مواقع شبكات التواصل الاجتماعي: (١)

- **المعرفات الداخلية**: حيث تستخدم هذه المواقع في مسرح الجريمة الالكترونية، هذه المعرفات على نطاق واسع لتعقب كل شيء، كالمستخدمين، والصور، والاحاديث، والمجموعات، وهذه المعرفات ترتبط في معظم الاحيان بمعرفات متاحة لمزود الخدمة.
- **المحادثات Chat:** حيث تقدم هذه المواقع في مسرح الجريمة الالكترونية، خدمات للمستخدمين لإجراء المحادثات مع النص والفيديو والصوت، ويمكنها أن توفر معلومات نوعية كبيرة إذا جرت معالجتها بشكل كاف، والهدف الرئيسي للمحقق جمع أكبر قدر ممكن من البيانات من مسرح الجريمة الالكترونية، وليس فقط ما يظهر في الصفحة.

(1) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow:Pervious reference P 105

٤ ـ الويب العميق:(١)

يمكن القول بان الانترنت هو المكان الذي تُنتشر فيه الخدمات والمعلومات من المزودين لنشر وتبادل البيانات مع الجمهور، وهناك أيضاً الطلب على ضرورة توفر مناطق خاصة للوصول إلى مجموعة محدودة من الناس لأغراض خاصة.

وبعض هذه المناطق هي الاماكن التي لا يمكن العثور عليها الا من قبل الاشخاص الذين لديهم العنوان الصحيح.

فعلى سبيل المثال، إذا رغب الزوجان في مشاركة صور زفافهما مع أسرهم وأصدقائهم، ولا يريدون مشاهدة الصور من قبل كل مستخدمي الانترنت، ففي هذه الحالة يتمكنون من تحميل الصور إلى خدمة من خدمات الانترنت المخصصة لهذا الغرض، وتبادل الرابط فقط مع الاصدقاء والاسرة، وبالطبع هذه ليست طريقة آمنة جداً لتبادل البيانات الخاصة، ولكن هذا الحل قد يكون كافياً بالنسبة لمعظم الاشخاص.

وهناك أيضاً مناطق أخرى خفية من شبكة الانترنت، وهناك حاجة إلى وثائق التفويض للدخول، والبريد الالكتروني العادي هو مثال عن المناطق الخاصة التي لا يمكن العثور عليها عن طريق محرك بحث أو الوصول إليها، بسبب اشتراط تسجيل الدخول لقراءة المعلومات، بالاضافة الى وجود مواقع مخبأة عمداً عن محركات البحث العامة، أي لا تظهر بنتائج البحث، يحتاج المستخدم إلى كلمة مرور او تعريف ما.

وهناك أيضاً مناطق أخرى خفية من شبكة الانترنت بها صلاحيات خاصة للنفاذ إليها، وهناك أيضاً المواقع وقواعد البيانات التي لا يمكن فهرستها من قبل محركات البحث أو لا يمكن فهمها أو تحليلها من قبلها، ويطلق اسم عام لجميع تلك المناطق المخبأة عن محركات البحث "الويب العميق" أو "الويب الخفي".

ويلاحظ ان فكرة الويب العميق ليست بدعة، وليست مرتبطة بالاجرام، وقد وجدت منذ الايام الاولى للإنترنت بناء على رغبة المستخدمين والشركات ببعض الخصوصية.

وفي الواقع يمكن بسهولة اعتبار الخوادم الاولى على شبكة الانترنت، وأول المواقع المتاحة على الشبكة العالمية جزءاً من الويب العميق.

وبالاضافة الى المواقع وقواعد البيانات والوثائق التي لا يمكن فهرستها من قبل محركات البحث هناك طبقة أخرى من الويب العميق تسمى الشبكة الظلامية Darknet أو الويب

(1) Nigel Jones, Esther George , Fredesvinda Insa Mérida , Uwe Rasmussen , Victor Völzow: Pervious reference P 110

الظلامي Darkweb، والشبكة الظلامية مشابهة للويب العميق، ولا يمكن البحث عنها باستخدام محركات البحث التقليدية، ومع ذلك، في حين أن مواقع الويب العميقة يمكن الوصول إليها عن طريق متصفح الانترنت العادي إذا كان الزائر يعرف العنوان ومعلومات تسجيل الدخول، فإن هذا غير صحيح لمواقع الشبكة الظلامية.

وعلى الرغم من أن الشبكة الظلامية تستخدم شبكة الانترنت الفيزيائية نفسها، فإنها تستخدم من الناحية العملية مساحة من الشبكة وعناوين داخلية مختلفة.

وهنا يلاحظ ان المحققون والقضاة فى حاجة لمعرفة العنوان المشكوك فيه، في الشبكة الظلامية لرؤية المحتوى، والشبكات الظلامية هي شبكات ثنائية، وهذا يعني أن كل مستخدم يرتبط مباشرة مع مستخدم آخر، ويمكن لأي شخص يمتلك مجموعة من المهارات المتميزة إنشاء شبكة ظلامية، ويمكنه دعوة مجموعة من الناس والموثوق بهم للمشاركة في هذه الشبكة الصغيرة.

ومع ذلك، نجد أيضاً أن بعض الشبكات الظلامية تتكون من الاف المستخدمين، أبرزها الشبكة "Freenet"، والشبكة "TOR" والمؤلفة من العديد من العقد، وكل عقدة تتصل فقط بالعقد جاراتها المباشرة لذلك لا يمكن لأي عقدة واحدة، والتي عادة ما تعني مستخدماً في سلسلة، معرفة من أرسل أو من تلقى أي طلب، ويستطيع المحققون والقضاة الوصول إلى شبكة TOR ببساطة عن طريق تحميل TOR browser82 ويمكن للمحقق الوصول إلى الخدمات المخفية عبر عناوين لها طبيعة خاصة مختلفة عن العناوين التقليدية من خلال مسرح الجريمة الالكترونية.

وقد عرفنا الويب العميق، والويب الظلامي ليتسنى للقضاة معرفة وجود هذه الانواع من الشبكات، وذلك لأن المجرمين، وخاصة تجار المخدرات(١)، ومجندي الشباب في منظمات إرهابية غالباً ما يستخدمون هذه الشبكات، ويحتاج القضاة إلى الطلب من المختصين بالبحث عن

(1) انظر فى ذلك: محمد فتحى عيد، السنوات الحرجة فى تاريخ المخدرات، نذر الخطر وعلامات التفاؤل، مرجع سابق، ص ١٣١، وايضا: تقرير الهيئة الدولية لمراقبة المخدرات لسنة ٢٠٠٠، الفقرات (٥٠ – ٥٦)، ص ١٢ ، ١٣، مطبوعات الامم المتحدة، نيويورك، ٢٠٠١، الوثيقة رقم Elincb 200D المنشور بتاريخ ٢١ فبراير ٢٠٠١، وكذلك انظر : مجلة الحقوق الكويتية، مجلس النشر العلمى، الكويت، ١٩٩٨، العدد الثالث، ص ٣٨١، منشور دورة البحث الجنائى للضباط رقم (٥) دراسات حول الجريمة الاقتصادية فى دولة الامارات، معهد البحث الجنائى، شرطة دبى، دولة الامارات العربية المتحدة، ١٩٩٨، ص ٩٨.

DUNCAN. Alfod. Anti- mony laundering regulations: Aburden on financial institutions, volume 19 north Carolina jounal of international and commercial regulations, p.p 441 – 442 (summer 1994).

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

الأدلة الرقمية في مسرح الجريمة الالكترونية التي يمكن أن تدين بعض الاشخاص الذين يستخدمون هذه الشبكات.

٥ - **الحسابات السحابية**: (١)

حيث ان التخزين على الانترنت أصبح موضوعاً ذا أهمية كبيرة، ولكي يكون القاضي قادراً على التعرف وفهم هذه الخدمات، يحتاج إلى معرفة ما هي الحوسبة السحابية.

والحوسبة السحابية هي نموذج لتمكين كل مستخدم، عادة ما تكون شركات، من الوصول إلى شبكة الانترنت واستخدام مجموعة كبيرة من مواردها من الخوادم، ووحدات التخزين، والتطبيقات، والخدمات التي يمكن توافرها، عند الطلب.

والملاحظ حول الحوسبة السحابية، تيسيرا للمحقق والقاضي، أن البيانات لا يتم تخزينها على جهاز حاسبي فعلي واحد، ولكن على خوادم متعددة، حتى أنه لا يمكن معرفة كيف وأين يتم تخزين بعض البيانات.

كما أن الخدمات السحابية قادرة على الحلول محل البنية التحتية لتقنية المعلومات في الشركة، بدءاً من خدمات البرمجيات مثل معالجة النصوص أو برامج المحاسبة وصولاً إلى استبدال كامل لجميع محطات العمل.

ومن اهم التطبيقات العملية فى مجال مسرح الجريمة الالكترونية: وهى جريمة قرصنة الموسيقى عبر شبكات الانترنت، ذلك ان الحوسبة السحابية هي نموذج لتمكين كل مستخدم، عادة ما تكون شركات، من الوصول إلى شبكة الانترنت واستخدام مجموعة كبيرة من مواردها، وتعتبر الموسيقى أكثر أشكال المحتوى المعرّض للقرصنة في العالم، ومع تحقيق العديد من الاجهزة المخصّصة للاستماع إلى الموسيقى، مثل الـــ iPod ، مبيعات متزايدة عبر العالم، فإن بيع الاقراص الليزرية هو في انخفاض مستمر منذ سنوات، ويعود السبب الرئيسي إلى تطور البرمجيات التي تسمح للمستخدمين بنسخ ملفات الموسيقى بعضهم من بعض، دون المرور بالمخدمات.

ويعرف هذا النوع من الشبكات بشبكات الند للند peer-to-peer ، وهي تطورت بوجه خاص بهدف تبادل المحتوى بين المستخدمين،عن طريق وضع تلك الملفات على مخدمات، ومن أشهر تلك الشبكات شبكة torrent وشبكة Emule

(1) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow: Pervious reference P 85- 89.

وبعد تفاقم تلك الظاهرة، خرجت شركات الانتاج عن صمتها وقامت بحملة كبيرة ضد مستخدمي تلك التطبيقات، وقد يتصور المستخدمون أنهم محميون من التعقب من مسرح الجريمة الالكترونية، بسبب عدم اعتمادهم على مخدّم وقيامهم بتبادل الملفات مباشرة، ولكن هذا ليس صحيحاً، فقد كان يكتفى بأن يدخل أحد المستخدمين الوهميين إلى الشبكة ويطلب جمع الملفات ليحصل على قائمة من العناوين للمستخدمين الذين يقومون بنسخ الملفات، وكان مزودو خدمة الانترنت ملزمين بتقديم البيانات التي تسمح بالتعرف على أولئك المستخدمين نظراً لقيامهم بأعمال غير قانونية تستوجب الملاحقة.

وقد استمرت الحملة التي قادتها رابطة صناعة التسجيلات الامريكية (RIAA) لمدة خمس سنوات كاملة، من الفترة من سنة ٢٠٠٣ حتى سنة ٢٠٠٨ ، قامت خلالها برفع عدد هائل من الدعاوى القضائية ضد المستخدمين الذين قاموا بتحميل أو مشاركة الاغنيات، وقد بلغ عدد الذين تعرضوا لتلك الدعاوى قرابة ٢٨ ألف شخص، قام أغلبهم بتسوية الدعوى بعد دفع مبالغ لا يستهان بها؛ ولان أغلبهم من الجيل الشاب والطلاب، فقد وجدوا أنفسهم مضطرين لترك الدارسة والعمل حتى يتمكنوا من دفع مبلغ التسوية الذي كان يتراوح بين ٣- ١١ ألف دولار.

ومن المميزات هنا، من الناحية الفنية، أن الالة الافتراضية في مسرح الجريمة الالكترونية، وهو البرنامج، يمكن نسخها بسهولة، ولكن اعتماداً على التشريعات ذات الصلة، فإن منح الترخيص القانوني المناسب لاعتراض تلك البيانات قد يواجه بعض المشكلات، ولكنه أيضاً يشكل تحدياً لضمان الحصول على البيانات وفقاً للإجراءات القانونية في الدولة الطالبة، وثمة عيب آخر هو أنه من المحتمل أن تكون البيانات المستردة أقل بكثير من البيانات اللازمة لتشكيل الدليل المستخرج من مسرح الجريمة الالكترونية.

وعلى ذلك، إذا عمد أحد المشتبه بهم إلى إنشاء جهاز افتراضي مؤقت لارتكاب جريمته، ثم حذف هذا الجهاز، فانه يكون من الصعب استرداد الدليل، لذلك يجب على القاضي في هذه الحالات الاستعانة بالمتخصصين للقيام بالبحث عن الأدلة في السحابات من مسرح الجريمة الالكترونية، واذا واجهت الخبير مشكلة صلاحيات الوصول إلى الشبكة، ويشتبه في استخدام الحوسبة السحابية يجب عليه اتخاذ جملة من الاجراءات بيانها علي التوالي(١):

البحث في مسرح الجريمة الالكترونية عن أيقونات فيها شعارات لخدمات الحوسبة السحابية، وهي خدمات البرمجيات Software as a Service (SaaS)، والبنية التحتية Infrastructure as a Service (IaaS)، ومنصات العمل Platform as a Service (PaaS)

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، مرجع سابق، ص ٣٨٩ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ٨٧٦ وما بعدها.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

- التحقق من تثبيت برامج لخدمات الحوسبة السحابية في مسرح الجريمة الالكترونية.
- البحث في قائمة الاجراءات عن أسماء الخدمات السحابية في مسرح الجريمة الالكترونية.
- البحث عن مشاركة عناصر أو محركات أقراص شبكية.
- مراقبة حركة مرور الشبكة في مسرح الجريمة الالكترونية.
- مراقبة قائمة المقابس Sockets المفتوحة في مسرح الجريمة الالكترونية.

الفصل الثاني

المعالجة التشريعية لمسرح الجريمة الالكترونية

فى القانون المصري

استجاب المشرع المصري لهذا الاتجاه، بالنص فى المادة (١١) من الباب الثاني من قانون مكافحة جرائم تقنية المعلومات، بشأن الأدلة الرقمية فى جرائم تقنية المعلومات، تحت اطار الاحكام والقواعد الاجرائية.

حيث تضمنت هذه المادة على ان "يكون للأدلة المستمدة أو المستخرجة من الاجهزة أو المعدات أو الوسائط او الدعامات الالكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الاثبات الجنائي متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية."

وعلى ذلك، يتضح أن المشرع المصري قد أجاز الاثبات في المسائل الجنائية بكافة صور الأدلة، أياً كان نوعها أو طبيعتها، على وجه تكون فيه جميع الأدلة متساوية في قمتها.

وتجدر الملاحظة علي وجوب أن يكون الدليل مشروعاً حتى يكون للإثبات أمام قضاء الحكم، إنما يخص دليل الادانة فقط، أما دليل البراءة فيمكن للمحكمة أن تستند إليه ولو كان مستمداً من إجراء باطل.

وفي هذا الصدد استقرت محكمة النقض على أنه "يشترط في دليل الادانة أن يكون مشروعاً إذا لا يجوز أن تبنى إدانة صحيحة على دليل باطل في القانون"، الا أن المشروعية ليست بشرط واجب في دليل البراءة.

الا أن هذا القضاء محل نظر، وذلك لأن إباحة استخدام الأدلة الناتجة عن وسائل غير مشروعة، ولو بهدف التوصل إلى البراءة، يعد من قبيل إهدار الثقة التي أولاها الافراد للهيئات

القضائية، التي تشترك بطريق غير مباشر في إهدار حقوق وحريات الافراد، رغم أنها الحارس الطبيعي للحريات العامة، ولا بد أن يبنى القضاء اقتناعه على الجزم واليقين، لأن هذا هو أساس الاحكام الجنائية.

كما استقر قضاء النقض المصري، على استبعاد الأدلة غير المشروعة في مجال الاثبات، واشترط مشروعية الدليل في المواد الجنائية واعتبر الدليل غير المشروع إذا تم الحصول عليه بالمخالفة لأحكام الدستور، أو قانون الاجراءات الجنائية، باطلا، وجعل البطلان في هذه الاحوال متعلق بالنظام العام.

الا أن تطور البحث عن الدليل في الآونة الاخيرة وظهور الكثير من الوسائل العلمية المستخدمة في هذا المجال، قد أدى إلى تردد الفقه والقضاء تجاه مشروعية استخدامها في المجال الجنائي، وكذلك استخدام الدليل المتحصل منها في مجال التدليل، خاصة وأن نتائج معظم هذه الوسائل غير مؤكدة الثبوت، كما أن معظمها أيضاً يمس مساساً مباشراً بحقوق وحريات الافراد الاساسية وينتهك الضمانات التي أقرها الدستور للمتهم في مراحل الدعوى الجنائية المختلفة .

ذلك إن ظهور التقنيات العلمية الحديثة مثل الانترنت، والتي تتيح للفرد سيل هائل من المعلومات والافكار، فإنه لا يوجد ما يمنع من استخدامها في المجال الجنائي، وذلك إذا ما تم تتبع الجريمة محل البحث والكشف عنها من قبل مأمور الضبط القضائي عبر مسرح الجريمة الالكترونية، ونشر الاعلانات التي تتضمن دعوة صريحة إلى الفسق والفجور، ومعرفة المواقع الموجودة على شبكة الانترنت، وتحديدها ومعرفة مستخدمي تلك المواقع والتوصل إليهم وضبط تلك الانشطة المنافية للآداب العامة.

فليس هناك ما يمنع من استثمار التطورات العلمية في خدمة العدالة الجنائية، بل أن هذه التطورات تساعد العدالة على مكافحة الجريمة، وبالتالي يكون الدليل المستمد منها دليل مشروع طالما أنه يهدف إلى تحقيق العدالة.

ولا يعيب هذا الراى في مشروعية الدليل المستمد من مسرح الجريمة الالكترونية، القول بأن تدخل القانون الجنائي في هذا الصدد يعتبر تدخلاً في حرية الافراد، وذلك في مجال حيوي بالنسبة لهم، خاصة وأن السلوك الجنسي يكون برضاء المشتركين فيه، وذلك مردود بأن استخدام الوسائل العلمية الحديثة مثل الانترنت، واستخدامه كدليل على وقوع جريمة الاعلان عن البغاء ونشر المطبوعات الفاضحة يستهدف المصلحة العامة.

فلقد تركت ثورة تقنية المعلومات انعكاسات واضحة على إثبات جرائم تقنية المعلومات عبر الوطنية بخلاف الجرائم التقليدية، بالنظر إلى طبيعة مسرح الجريمة الالكترونية وما يرتكب به من الجرائم وما تتسم به من خصائص وسمات.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

الامر الذي بات يثير كثيراً من التحديات ازاء مسرح الجريمة الالكترونية، وأمام القائمين بمكافحة جرائمه والتصدي لها، وتكمن المشكلات المتعلقة بالإثبات في أن هذه الجرائم باعتبارها تقع في البيئة الافتراضية لا تترك أية آثار مادية محسوسة خلافاً للجرائم التقليدية، فهذه الاخيرة يمكن إدراكها بالحواس، كما هو الحال في المحررات المزورة، والنقود والطوابع المزيفة، والاسلحة النارية، وما يمكن أن يخلّفه الجناة من آثار مادية أخرى في مسرح الجريمة كالشعر والدماء وبصمات الاصابع وآثار الاقدام، وما إلى ذلك.

وعلى النقيض، يغلب على جرائم تقنية المعلومات، وخاصة عبر الوطنية، صفة الخفاء، لأنها مستترة، وتعمد الجناة في كثير من الاحيان إلى إخفاء سلوكهم الاجرامي عن طريق تلاعبهم بالبيانات، الذي يتم في الغالب في غفلة من المجني عليه .

كذلك من اليسر والسهولة، التخلص من مسرح الجريمة الالكترونية، وهذه الأدلة الرقمية التي تتواجد به ومحوها، إذ يتم ذلك عادةً، في لمح البصر وبمجرد لمسة خاطفة على لوحة المفاتيح بجهاز الحاسب، على اعتبار أنّ الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما إن يشعر الجاني بافتضاح أمره، حتى يبادر الى إلغاء هذه الاوامر، الامر الذي يجعل كشف الجريمة وتحديد مرتكبها أمراً في غاية الصعوبة .

ومع مرور الوقت اكتسب الجناة خبرة واسعة في التلاعب بالبيانات وإتلافها من مسرح الجريمة الالكترونية، في غضون ثوانٍ معدودة قبل أن تتمكن الاجهزة المختصة من كشفهم أو التعرف عليهم، ويتأتّى هذا عادةً بالتوسّل ببرامج معينة لها خاصية إتلاف أو تدمير البيانات بصورة تلقائية بعد مضي فترة من الزمن بحسب رغبة مصمم البرنامج وفي الوقت الذي يشاء .

ويجتهد المهندسون في مجال مسرح الجريمة الالكترونية لابتكار برامج معينة لهذا الغرض، وتكمن آلية عملها في أنه بمجرد محاولة شخص غير مصرح له ولوج النظام أو استخدام جهاز الحاسب المزود بهذا البرنامج، فإن هذا الاخير يصدر أمراً للجهاز بحيث يتم إتلاف البيانات المخزنة به ومحوها بصورة تلقائية .

ومما يزيد من الصعوبات في مجال كشف الدليل من مسرح الجريمة الالكترونية بصورة خاصة؛ متى ارتكبت هذه الجرائم في مجال العمل من قِبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا أية آثار تدل عليهم .

وثمة وسيلة أخرى يلجأ إليها الجناة لتدمير وإتلاف البيانات المخزنة بجهاز الحاسب في مسرح الجريمة الالكترونية، متمثلة في إغلاق الجهاز بصورة فجائية ودون التقيد بالطريقة الامنة، ذلك أن الاغلاق الفجائي وغير الآمن كثيراً ما يتسبب في تدمير بعض البرامج أو إحداث عطب أو تخريب لملحقات الحاسب، وربما يتأتى ذلك من خلال تزويد الجهاز ببعض الفيروسات المتمثلة في القنابل المنطقية.

ذلك ان معظم مستخدمي الحاسب والانترنت من ذوي الخبرة في ميدان مسرح الجريمة الالكترونية، وهو ما من شأنه أن يمكّنهم من إدخال تعديلات على أوامر التشغيل، بحيث لو تجرأ أي شخص لإدخال أمر ما أو حاول نسخ أو طبع أية بيانات، فإن هذه البيانات تكون عرضة للتدمير والاتلاف بغية عرقلة أجهزة الضبط والتحقيق وعدم تمكينها من الوصول إلى الأدلة وضبطها.

فالمجرم المعلوماتي يتصف في الغالب بالذكاء والخبرة الواسعة مقارنة بنظيره المجرم العادي، وهذا يمكّنه من التخطيط لجريمته قبل أن يقدم على ارتكابها محاولاً بذل الجهد في الا يُكتشف أمره متوسّلاً بأساليب وتدابير الحماية الفنية التي من شأنها إعاقة مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل او التحصل عليه من مسرح الجريمة الالكترونية، كما في استخدام كلمات المرور Password، وترميز البيانات وتشفيرها للحيلولة دون الاطلاع على محتواها أو ضبطها.

وبالنظر إلى ازدياد انتشار هذه البرمجيات في الدول المتقدمة وما ينجم عنها من مخاطر، فإن بعضها استحدث تشريعات تمّ بموجبها تجريم اللجوء إلى هذه التقنيات بدون ترخيص من الاجهزة المختصة.

ومن هذه الدول هولندا، حيث سنّت تشريعاً يقضي بوضع ضوابط لعمليات التشفير، ومنها ضرورة الحصول على ترخيص من الجهات المعنية، إلى جانب إيداع مفاتيح التشفير لدى هذه الجهات .

وكذلك تبنت فرنسا ذات الاتجاه، ومن شأن الاقدام على هذا التشفير بدون ترخيص أن يصبح الفعل جريمة يعاقب عليها القانون، وأيضاً معاقبة الشخص الذي أعد برنامج التشفير بدون ترخيص.

فضلاً عن ذلك، فإن الوصول إلى الدليل الرقمي من مسرح الجريمة الالكترونية، تعترضه عقبة أخرى تكمن في أن الجناة المتمرسين يجتهدون في إخفاء هويّاتهم للحيلولة دون تعقبهم أو كشف أمرهم، بحيث تظل أنشطتهم مجهولة بمنأى عن علم السلطات المعنية بمكافحة الجريمة.

ومن الامثلة العملية على ذلك؛ استخدام الجاني حاسباً آخر غير حاسبه الشخصي، كاستخدام الحواسب الموجودة بالأماكن العامة، أو اللجوء إلى مقاهي الانترنت كمسرح الجريمة الالكترونية ، على اعتبار أن معظم هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم، سيما إذا علمنا أن شبكة الانترنت تتيح لمستخدميها استعمال الخط الواحد من أكثر من شخص في آن معاً، مما يجعل المراقبة والتعقب للمشتبه فيه أمراً ينطوي على صعوبة وغير ميسور في كثير من الاحيان، وربّما تتعقد المسألة أكثر عند استخدام الانترنت اللاسلكي، الذي هو آخذ في الانتشار في الآونة الاخيرة على حساب الانترنت السلكي .

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

يضاف إلى ذلك، تضاؤل خبرة أجهزة العدالة الجنائية من مأموري ضبط وسلطة تحقيق ومحاكمة، إذ يفتقر هؤلاء جميعا إلى التأهيل الكافي في هذا الميدان التقني لمسرح الجريمة الالكترونية.

الأمر الذي يزيد من صعوبة وصول تلك الاجهزة إلى الدليل الرقمي في مسرح الجريمة الالكترونية وكيفية ضبطه والمحافظة عليه، فنقص الخبرة لدى هؤلاء قد يفضي إلى تدمير الدليل وإتلافه، على اعتبار أن جهلهم بأساليب ارتكاب جرائم تقنية المعلومات يجعلهم في كثير من الاحيان يقعون في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها من مسرح الجريمة الالكترونية، مثل إتلاف محتويات الاقراص الممغنطة وأوعية المعلومات التي تُخزَّن بها البيانات.

ذلك أن كشف هذه الجرائم يقتضي أن تكون الاجهزة المعنية على دراية كافية بأساسيات التعامل مع مسرح الجريمة الالكترونية والجرائم المرتكبة به، وكيفية تقصّيها وضبطها وصولاً إلى مرتكبيها، مما يعني ضرورة تلقّي هؤلاء دورات تدريبية بشأن استراتيجية التحقيق والاستدلال عن هذه الجرائم وآليات التعامل مع مسرح الجريمة الالكترونية، إذ بدون ذلك لا يمكنهم مواجهة أساليب الجناة المعقدة التي يتوسّلون بها عادة لارتكاب جرائمهم، فهذه المتطلبات تفتقر إليها الاجهزة المذكورة، لاسيما في الدول النامية، ما يجعل دورها في كشف هذه الجرائم ومكافحتها محدوداً للغاية، وغالباً يكون مآل الجهود التي تبذلها في هذا المجال الفشل والاخفاق .

كذلك من العقبات التي تعيق عمل الاجهزة المذكورة، حتى على فرض أنه تم إعدادها الاعداد المناسب لهذه المهمة، ضخامة حجم البيانات محل مسرح الجريمة الالكترونية، مما يتعذّر معه على المحققين الاكفاء الوصول إلى الدليل.

فمن الناحية العملية يواجه المحققون تحديات كبيرة في فحص جميع البيانات من مسرح الجريمة الالكترونية، فذلك أمر مكلف ويستغرق في العادة وقتاً طويلاً، وكثيراً ما يؤدي بالنهاية إلى جعل المحققين ورجال الامن يضجرون وقد يصرفون النظر عن مواصلة البحث لاقتناعهم بأنه لا جدوى من ذلك، وينظرون إليه على أنه جهد ضائع وغير مثمر.

فكما هو معلوم، تتميز الحواسب على اختلاف فيما بينها، بقدرتها الهائلة على تخزين البيانات بما يوازي ويستوعب مئات الالوف من الصفحات الورقية.

مما يعني أنه لو تيسر للأجهزة الضبطية مثلاً طباعة محتويات أحد الاقراص الصلبة المستقاه من مسرح الجريمة الالكترونية، فإن ذلك يتطلب كميات هائلة من الورق، وقد تكون النتيجة رغم هذا الجهد سلبية بحيث لا يمكنها كشف الدليل المراد ضبطه أو تحصيله، وهذا مردّه في المقام الاول عدم وجود آلية للفرز الذاتي للملفات المخزنة، حتى يمكن الوقوف على الملفات غير المشروعة وضبطها، ومن هنا فالأمر مرهق جدا، بل وغير مجدٍ في كثير من الاحيان، لما

يستغرقه من وقت لا طائل منه، مما يجعل القضاء لا يكترث بالدليل الرقمي، ولا يعوّل عليه كثيراً لافتقاره إلى المصداقية التي تجعله جديراً بالثقة، وإذا كان هذا حال الدول المتقدمة، فما بالنا بالدول النامية التي لاتزال تفتقر إلى الكفاءات اللازمة في هذا الحقل التقني.

وفي واقع الامر أن المسألة تزداد تعقيداً، حينما يكون محل البحث هو الشبكة المعلوماتية بشأن الجرائم عبر الوطنية، إذ يصبح ضبط الدليل والبحث عنه أمراً في غاية الصعوبة من مسرح الجريمة الالكترونية، إن لم يكن مستحيلاً أحياناً، على اعتبار أن التفتيش والضبط في هذه البيئة الافتراضية يتطلب أن يتم خارج حدود الدول وفي نطاق دولة أخرى، ما يتطلب الحصول على إذن مسبق بذلك من سلطاتها، لما ينطوي عليه من مساس بسيادة هذه الدولة، فضلا عما يسفر عنه البحث من انتهاك لخصوصية الاخرين ممن تتعلق بهم البيانات أو المعلومات موضوع الضبط أو التفتيش .

ومما يزيد من الصعوبات التي تواجه الاجهزة المعنية بالبحث والتحري في البيئة المعلوماتية، يتجلى في إحجام المجني عليهم عادةً عن الابلاغ عن الجرائم التي يكونون ضحيتها إلى السلطات المختصة، فقد سجلت الاحصاءات في بعض الدول الغربية، ومنها فرنسا، انخفاضاً ملحوظاً في نسبة الابلاغ عن هذه الجرائم حرصاً على إخفاء أساليب ارتكابها للحيلولة دون تقليد الاخرين للجناة ومحاكاتهم في جرائمهم .

كما قد يتوخّى بعض المجني عليهم من وراء العزوف عن الابلاغ عدم إتاحة الفرصة للأجهزة الأمنية من الاطلاع على معلومات لم يجرِ الابلاغ عنها، وربما يتجلّى ذلك بصورة أكبر في نطاق جرائم تقنية المعلومات التي تقع على شركات التأمين أو البنوك رغبة في توقّي الخسائر التي يتوقع تحققها نتيجة هذا الابلاغ بسبب اهتزاز ثقة المتعاملين معها .

ورجوعا الى نص المادة (١١) من الباب الثاني من قانون مكافحة جرائم تقنية المعلومات، بشأن الأدلة الرقمية فى جرائم تقنية المعلومات، والتى تضمنت النص على ان "يكون للأدلة المستمدة أو المستخرجة من الاجهزة أو المعدات أو الوسائط او الدعامات الالكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات نفس قيمة وحجية الأدلة الجنائية المادية في الاثبات الجنائي متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية."

ومع الاخذ فى الاعتبار ان المشرع المصرى، احال بشأن الشروط الفنية الواجب توافرها فى الأدلة الرقمية لجرائم تقنية المعلومات، الى اللائحة التنفيذية التى اوجب اصدارها من مجلس الوزراء خلال ثلاثة اشهر من تاريخ نفاذ هذا القانون، الا انه يمكن الرجوع الى القواعد العامة، وتلك المقررة فى القانون المقارن، وايضا اقتراحات خبراء العلم الرقمى، للوقوف على تلك الشروط، خاصة وانها ذات طبيعة فنية وتقنية، ليكون لها حجيتها امام القضاء الجنائي، بشأن تطبيق العقوبات المقررة فى قانون مكافحة جرائم تقنية المعلومات.

وبناء على ذلك، نقسم هذا الفصل إلى مبحث أول يتناول مفهوم الدليل الرقمي فى القانون المصري، ثم نعرض فى المبحث الثاني بالعرض لحجية الأدلة الرقمية فى القانون المصري، على الترتيب التالى.

المبحث الاول: مفهوم الدليل الرقمي فى القانون المصري.

المبحث الثاني: حجية الأدلة الرقمية فى القانون المصري.

المبحث الاول

مفهوم الدليل الرقمي فى القانون المصري

من المقرر انه اصبح لازما التعرف على الأدلة الرقمية المنبثقة عن الوسائل التكنولوجية التى تفتق عنها الفترة الزمنية المنقضية، حيث ان جميع الاجراءات الجنائية صارت على الأدلة لتحديد إدانة أو براءة المتهم أو للبت في موضوع الدعوى في الدعاوى القضائية، وكانت الأدلة فى صورتها الاولية تتخذ الشكل المادي، مثل المستندات والصور، أو الشهادة الشفوية للشهود.

وحيثُتشتق الأدلة الرقمية لمسرح الجريمة الالكترونية من الاجهزة الالكترونية، مثل أجهزة الحاسب وأجهزتها الطرفية، وشبكات الحاسب، والهواتف المحمولة والكاميرات الرقمية والاجهزة المحمولة الاخرى، بما في ذلك أجهزة تخزين البيانات، وليس لها أي شكل مادي مستقل، فهي تعكس مجموعة من ظروف ارتكاب الجريمة، وتقدم معلومات عن الجريمة كما وقعت بالفعل.

يضاف إلى ذلك، انه يجب أن تتوافر الوسائل لإثبات أن الأدلة الرقمية المأخوذة من مسرح الجريمة الالكترونية، لم تتعرض لأية تعديات، سواء بالحذف، او الاضافة، او التعديل، او أية تغييرات أخرى، منذ لحظة التحصل عليها.

ومن المقرر ان الطبيعة غير المادية لبيانات مسرح الجريمة الالكترونية، والمعلومات المخزنة بشكل إلكتروني، من السهل التلاعب بها، وهي أكثر عرضة للتغيير من الاشكال التقليدية للأدلة، وقد شكل هذا تحدياً خاصاً لأجهزة العدالة حيث يتطلب التعامل مع هذه البيانات، أو المعلومات طريقة خاصة لضمان سلامة الأدلة التي يوفرها.

وعلى ذلك، يمكن تعريف الدليل الرقمي digital evidence بانه البيانات الرقمية المخزّنة في الاجهزة الحاسبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية.

ويتفق هذا التعريف، مع ما تبناه المشرع المصرى، من تعريف للدليل الرقمى، بموجب المادة الاولى من قانون مكافحة جرائم تقنية المعلومات، حيث عرفه بانه "أية معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، والممكن تجميعه وتحليله باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة."

وعلى ذلك، يتضح ان الأدلة الرقمية لمسرح الجريمة الالكترونية، تشترك مع الاشكال التقليدية للأدلة في معظم الخصائص، ولكنها تتميز ببعض الخصائص الفريدة(١)، ذلك ان الدليل الرقمي لا يتعلق فقط بجرائم تقنية المعلومات بالنظر الى الطبيعة غير المادية للبيانات، والمعلومات المخزنة بشكل إلكتروني، والتى من السهل التلاعب بها، وتتجسد تلك الخصائص على النحو التالى.

١- **ذات طبيعة غير مرئية للعين**: حيث توجد الأدلة الرقمية في مسرح الجريمة الالكترونية التي يمكن الوصول إليها عبر المتخصصين فقط، أو عن طريق استخدام أدوات خاصة.

٢- **ذات طبيعة متغيرة**: حيث يمكن الكتابة في بعض الاجهزة وتحت ظروف معينة في ذاكرة الحاسب، مما يعني تغيير الدليل الذي تحتويه، كما يمكن أن تطرأ تغييرات عليه من خلال الاعمال المعتادة كتشغيل الجهاز، أو إعادة تشغيله، أو لفقدان جهاز الحاسب للطاقة، أو الحالة التي يحتاج فيها نظام التشغيل إلى كتابة معلومات جديدة فوق الجزء القديم بسبب عدم وجود مساحة في الذاكرة. (٢)

يضاف إلى ذلك، إمكانية تعرض ذاكرة الحاسب للتلف نتيجة للعوامل البيئية مثل الحرارة الشديدة، أو الرطوبة، أو وجود الحقول الكهرومغناطيسية، كما أن أجهزة الحاسب تتغير بسبب اية استخدامات اخرى، سواء كان ذلك بناء على طلب المستخدم، كالحفظ، او النسخ، أو تلقائياً بواسطة نظام تشغيل جهاز الحاسب.

٣- **القابلية للنسخ**: حيث يمكن نسخ المعلومات الرقمية بصورتها الاصلية من مسرح الجريمة الالكترونية ، وهذه الصفة الفريدة تعني أنه يمكن إجراء فحص الأدلة الرقمية من قبل

(1) Nigel Jones (United Kingdom), Esther George (United Kingdom), Fredesvinda Insa Mérida Spain), Uwe Rasmussen (Denmark) , Victor Völzow (Germany): electronic evidence guide a basic guide for police officers, prosecutors and judges.

(2) Cybercrime Division , Council of Europe, Strasbourg (France) 2014 P 11-12

المختصيين، وبالتوازي من مختلف الاختصاصات، ولأسباب مختلفة، مع الحفاظ على الاصل.

٤- **الحاجة إلى متخصصين للتعامل معها**: ذلك ان كل نوع من الاجهزة الحاسبية، والاجهزة الالكترونية، والشبكات المعلوماتية، وغيرها، تتطلب إجراءات خاصة، والتعامل من قبل غير المتخصصين في التعامل مع مسرح الجريمة الالكترونية، مما قد ؤدي الي تلف الأدلة، أو يمحوها.

٥- **القابلية للاسترجاع**: حيث يلجأ بعض المجرمين إلى حذف البيانات والملفات من مسرح الجريمة الالكترونية التي يمكن أن تحتوي أدلة رقمية قد تمثل ادانة لهم، وهذا لا يعني أن البيانات قد حذفت بالفعل، حتى لو جرى إتلاف التجهيزات فيزيائياً، إذ يمكن في معظم الاحيان، عبر استخدام أدوات وبرامج استرجاع البيانات المحذوفة، والطريقة الاكثر استخداماً لحذف الملفات بصورة نهائية هي الكتابة فوقها.

حيث يعمد بعض المشتبه بهم إلى كتابة أصفار فوق البيانات القديمة مما يجعل استرجاعها مستحيلاً، ونكون أمام حالة طمس الأدلة الرقمية.(١)

ويلاحظ ان هناك عدد من المعايير والشروط التى يتعين توافرها للاخذ بالدليل الرقمى من مسرح الجريمة الالكترونية، والاحتجاج به امام المحكمة المختصة بنظر احدى جرائم تقنية المعلومات التى عرض هذا الدليل بشأنها: (٢)

- **من حيث الصحة**: يجب أن يقدم الدليل الحقائق بطريقة لا يمكن التنازع عليها.
- **من حيث الاكتمال**: يجب أن يتضمن أي تحليل أو رأي، استناداً إلى الأدلة الرقمية، وان تكون الواقعة كاملة، دون أن يكون مصمماً ليتناسب مع وجهة نظر فردية أو خاصة.

ذلك انه، عندما يعرض الاستوديو Gallery view الصور، ينشئ صوراً مصغرة من الصور المعروضة thumbnail ، وإذا قام أحد بالنقر على الصورة المصغرة، يُمكن أن يرى الصورة الحقيقية الاكبر، لكن كل الصور الكبيرة قد جرى حذفها، ورغم حذف هذه الصور،

(1) R v Ross Warwick Porter: England and Wales Court of Appeal (Criminal Division) Decisions, 2006.
"http://www.spannertrust.org/documents/R_v_Porter.pdf".

(2) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow: Pervious reference P 13

يمكن للخبراء استعادة ما بقي من أثر من كل صورة ومعرفة البيانات الفائقة في قاعدة بيانات البرنامج.

ويجب ان يتم تقديم تقرير من قبل الخبراء يتضمن ما يلي:

١- **الموثوقية**: حيث يجب أن لا تكون هناك أية ملاحظات على الطريقة التي جمعت بها الأدلة، من مسرح الجريمة الالكترونية، أو أي شك بصحتها في أي وقت.

٢- **المصداقية**: حيث يجب أن يكون الدليل المستمد من مسرح الجريمة الالكترونية، مقنعاً، ويمكن الاعتماد عليه في المحكمة سواء كدليل إثبات، أو كبينة.

٣- **العدالة**: ذلك إن الطرق المستخدمة لجمع الأدلة من مسرح الجريمة الالكترونية، يجب أن تكون عادلة ومتناسبة مع مصلحة المحكمة والعدالة، ولا تتعرض لحقوق أي طرف، واستخدامها فقط في حدود القيمة الثبوتية للدليل، أي قيمته كدليل.

وعليه يجب أن تكون الأدلة الرقمية المستمدة من مسرح الجريمة الالكترونية في المحاكمات الجنائية، مقبولة، وصحيحة، ودقيقة، وكاملة، ويجب أن تتوافق مع القوانين والقواعد المعمول بها، كي تكون مقبولة كدليل له حجيته لدى المحكمة.

وتنظر النيابة في مراجعة القضية، إذا كان من الممكن ربط الملفات، او اذا ظهر أن هناك ترابطاً بين الأدلة، وحال المحاكمات الجنائية، حيث يجب على المدعي استخدام الأدلة لإثبات القضية في المستوى الجنائي بما لا يدع مجالا للشك، وتقوم النيابة العامة بدراسة الأدلة الرقمية المأخوذة من مسرح الجريمة الالكترونية، لتحديد ما إذا كانت الأدلة كافية، فّإذا كانت هناك نقاط ضعف، فإن ذلك يتطلب مزيداً من الأدلة، او اذا تم ذلك في مرحلة مبكرة قد يكون لا يزال هناك فرصة للحصول على أدلة إضافية من مصادر متنوعة قبل أن تحال القضية للمحاكمة.

ويجب على النيابة العامة أن تقدم مذكرات شارحة، وواضحة، ومتماسكة مع المستندات الداعمة إذا لزم الامر، وينبغي أن يطلب شاهد مسرح الجريمة الالكترونية، للحصول على معلومات وتفسيرات محددة بشأن النقاط التي من المرجح أن يثيرها الدفاع.

وتظهر الاهمية لذلك خاصة فيما يتعلق بأي من التناقضات الواردة في البيانات، أو معارضتها من شهود عيان في مسرح الجريمة الالكترونية، فى توقيت وفترة ما قبل المحاكمة، او اذا لزم الامر أثناء المحاكمة الرئيسية، حيث قد تجد النيابة العامة أنه من المفيد مناقشة الدفاع في نطاق الأدلة الرقمية من أجل توضيح حالتها الاثباتية، وعند تقديم أي من الشهود أدلة رقمية، يجب على القاضي التأكد من أنها موثوقة، ومحايدة، وواضحة.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

وحيث وفر استخدام وسائل الاعلام الرقمية، والانترنت، للمجرمين فرصاً جديدة لارتكاب جرائمهم، وتطورت اسراتيجيات جديدة متطورة عن الجرائم التقليدية، حيث يجب أن تكون الأدلة الرقمية في المحاكمات الجنائية مقبولة، وصحيحة، ودقيقة، وكاملة.

ذلك ان استغلال قنوات الاتصال الجديدة، ونشأة فئات جديدة من جرائم تقنية المعلومات، اوجب على جميع المشاركين في النظام القانوني أن يكونوا على دراية جيدة لأشكال الأدلة الرقمية المستقاه من مسرح الجريمة الالكترونية، وعلى معرفة في كيفية التعامل معها.

كما إن أية جريمة حديثة، غالباً ما يرتبط مسرح الجريمة الالكترونية فيها، بجهاز إلكتروني يحتوي على ذاكرة وأي شكل من أشكال البرمجيات، حتى عندما تكون الجريمة نفسها لم يُستخدم فيها مثل هذا الجهاز، ولكن يمكن أن يساعد في القبض على الجاني، أو في عمليات التحقيق، فما تسجله كاميرات مراقبة، أو ما يقدمه نظام تحديد المواقع العالمي (GPS) للهاتف أو للسيارة، وغيرها من الادوات، تساعد المحكمة كثيراً في الوصول إلى المجرمين، وقد أصبح تأمين الأدلة الرقمية، وفحصه عبر الشرعية الرقمية يشكل الاداة الرئيسية في تقديم المجرمين للعدالة.

كما أدى تطور شبكة الانترنت وتطبيقاتها إلى الحصول على الأدلة في مواقع الانترنت، والشبكات الاجتماعية، وفي رسائل البريد الالكتروني، وغرف الدردشة.

وقد تنوعت مصادر الحصول على الدليل الرقمي، ليس فقط من الحاسب الشخصي للجاني، وإنما من خلال المعلومات التي يوفرها مقدمو الخدمات على الشبكة، ومنها خدمات النفاذ إلى الشبكة، وخدمات التواصل على الشبكة، وخدمات الاستضافة على الشبكة.

كما أن تطوير الحوسبة السحابية، في مسرح الجريمة الالكترونية، حيث يتم تخزين التطبيقات والبيانات عن بعد، وخارج الحدود الوطنية، في مواقع متنوعة ومنتشرة في العالم، أضاف تحدياً آخرَ في ضرورة تطوير الحصول على الدليل الرقمي، تحقيقا للعدالة، وعدم إهمال أية معلومات قد تقود المحكمة إلى معرفة المجرمين (١)

كما ان هناك عددا من المبادئ اللازمة لتوجيه المختصيين في التعامل مع مسرح الجريمة الالكترونية، وخاصة القضاة، والمحققين، والمحاميين، عند التعامل مع الأدلة الرقمية، وينبغي عليهم عند اتخاذ التدابير القانونية، أن يأخذوا في حسبانهم الوثائق، واللوائح القانونية الخاصة، ومراعاة المبادئ التالية:

(1) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen , Victor Völzow Pervious reference P 14.

- المبدأ الاول: سلامة البيانات:

حيث ينبغي للإجراءات المتخذة في مسرح الجريمة الالكترونية، ضمان عدم حصول أي تغيير في البيانات التي يمكن استخدامها، كأدلة في المحكمة، لانه يجب أن لا يتم تغيير الاجهزة أو البيانات الرقمية.

ذلك ان الشخص المسؤول عن معاينة موقع الجريمة أو جمع الأدلة هو المسؤول عن الحفاظ على سلامة المواد المستخلصة، ويجب أن يتم الوصول إلى البيانات على نظام الحاسب واستخلاصها، بالطريقة التي تسبب أقل تأثير على البيانات، ومن قبل شخص مؤهل للقيام بذلك.

- المبدأ الثانى: المراجعة والتتبع:

يجب إنشاء سجل لجمي الاجراءات المتخذة عند التعامل مع الأدلة الرقمية لمسرح الجريمة الالكترونية ، والحفاظ عليها بحيث يمكن مراجعتها في وقت لاحق، ويجب أن يتم تحليل الأدلة، ويصل إلى النتائج نفسها، ومن الضروري أن يُسجَّل كافة البيانات.

وقد تنوعت مصادر الحصول على الدليل الرقمي من مسرح الجريمة الالكترونية، بدقة كل نشاط في مكان الحادث لتمكين طرف ثالث لإعادة الاجراءات إذا لزم الامر، حيث ان جميع النشاطات المتعلقة بالتفتيش والمصادرة والوصول، وتخزين أو نقل الأدلة الرقمية، يجب أن تكون موثقة بشكل كامل.

- المبدأ الثالث: الدعم الخاص:

إذا كان من المتوقع العثور على الأدلة الرقمية في مسرح الجريمة الالكترونية، في سياق عملية مخطط لها، يجب على الشخص المسؤول إخطار المختصين والمستشارين الخارجيين في الوقت المحدد، وترتيب وجودهم أثناء جمع الأدلة إذا أمكن ذلك.

- المبدأ الرابع: التدريب المناسب:

يجب تدريب الشخص الموكل بأول عملية تفتيش لمسرح الجريمة الالكترونية، تدريباً جيداً، لضمان عدم فقدان الأدلة أثناء عمليات التفتيش.(١)

ويجب على المحققين والقضاة، النظر في احتمال أن تسفر أي من الاجهزة الالكترونية والمعدات الموجودة في مسرح الجريمة الالكترونية عن أدلة رقمية، ذلك إن وجود مثل هذه

(1) Donald R. Mason: Digital Evidence & Computer Forensics, the national center for justice, University of Mississippi, 2011.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

الاجهزة قد لا يكون واضحاً وبديهياً، حيث تتعدد الاجهزة التي تحتوي على الأدلة الرقمية بشكل شبه يومي.

ونورد القائمة التالية من المصادر المحتملة للأدلة الرقمية من مسرح الجريمة الالكترونية، لكن هذا لا يعني أنها شاملة، ولكنها تحتوي على الامثلة الاكثر شيوعاً.

أ- أجهزة الحاسب الآلى ووحدات التخزين:

تأتي أجهزة التخزين المتواجدة في مسرح الجريمة الالكترونية، أيضاً في العديد من الاشكال والاحجام وتختلف في الطريقة التي تخزن فيها البيانات أو تحتفظ بها، وعلى ذلك، فان جميع الاجراءات المتعلقة بالتفتيش والمصادرة، وتخزين أو نقل الأدلة الرقمية، يجب أن تكون موثقة بشكل كامل، من خلال محاضر رسمية.

ونذكر من هذه الوحدات على سبيل المثال:

- الاقراص الصلبة Hard disk drives (HDD)
- الوسائط المتنقلة Removable media (DVD,CD)
- بطاقات الذاكرة (Memory cards (Flush cards
- أجهزة تخزين البيانات data storage devices (USB)
- أجهزة الحاسب اللوحي Tabet devices
- الهواتف الخلوية Mobile telephones
- الاجهزة الطرفية Peripheral devices (Scanner, printers,webcam)
- أجهزة وكاميرات التصوير Photo and video recording (Digital cameras)

ويمكن اعتبار وحدات التخزين، بما فيها أجهزة الحاسب المصدر الاساسي للأدلة الرقمية من مسرح الجريمة الالكترونية، وعلى سبيل المثال لا الحصر فهي قد تقدم البيانات التالية، والتي قد تحتوي أدلة(١):

- الصور والفيديو Images & Video.
- المستندات والوثائق بأنواعها.

(1) Donald R. Mason: previous reference.

- جلسات المحادثة، وسجل البريد الالكتروني.
- ملفات تسجيل العمليات Log files.
- المعلومات التاريخية للتصفح، والملفات المخبأة Cash files.
- مفاتيح التشفير، وكلمات المرور passwords & encryption keys.

ب - الشبكات Computer networks:

ذلك انه عندما يتم ربط جهازي حاسب أو أكثر، يكون لدينا شبكة، فان أجهزة الحاسب في الشبكة تكون قادرة على تبادل البيانات والموارد الاخرى فيما بينها، وكثيراً ما تكون مرتبطة بمكونات وأجهزة إضافية.

ويمكن أن تكون شبكات الحاسب محدودة مثل تلك التي توجد في المنزل، وعلى سبيل المثال ينشئ أفراد أسرة شبكة، موصولة إلى جهاز إنترنت أو واسعة النطاق مثل تلك المستخدمة من قبل الشركات الكبرى أو الحكومات التي تربط بين المئات أو حتى الالاف من أجهزة الحاسب معاً.

وهنا يجب على المحققيين معرفة أن الأدلة المعلوماتية التي يتضمنها مسرح الجريمة الالكترونية، قد لا تكون موجودة في جهاز الحاسب الخاص بالمتهم، أو الوحدات الخاصة به، وانما يمكن أن تكون أيضاً موجودة في مخدمات، أو وحدات تخزين عبر الشبكة، يستخدمها المجرمون.

ولذا فإنه من الممكن معرفة المستخدمين الذين قاموا بأية عمليات على الشبكة، من خلال حسابات المستخدمين، ونتيجة لذلك، تكون الشرعية الرقمية للشبكة، إذا جاز التعبير، جزء لا يتجزء من الشرعية الرقمية للحاسب، وتشكل تحدياً للمحققين، ومع ذلك، وباستخدام منهجيات مناسبة لطبيعة الحادث والفاعل، يمكن الكشف عن جرائم تقنية المعلومات، التي وقعت على الشبكة، أو باستخدامها.(١)

ت- شبكة الانترنت:

وهنا نخوض في الاجراءات الفنية والمنهجية للحصول على الأدلة من مسرح الجريمة الالكترونية، ذلك ان الشرعية الرقمية للشبكة المعلوماتية، تعد جزء لا يتجزء من الشرعية الرقمية للحوسبة الرقمية على الانترنت، فإذا كانت الاجهزة الحاسبية، ووحدات التخزين المصدر

(1) Ioannis A. Apostolakis: Network Forensics: Problems and Solutions, Conference Paper· January 2006, P13.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

الاساسي للأدلة الرقمية، فإن شبكة الانترنت هى المصدر الاوسع والاهم لها (١) (٢) والتى يجرى استخدمها فى ارتكاب جرائم تقنية المعلومات(٣).

لذلك نجد أن القانون قد بين ضرورة توضيح صاحب العمل لحدودَ صلاحيات الموظف بالوصول إلى البرامج أو البيانات، ويمكن الحديث عن الأدلة الرقمية في شبكة الانترنت انطلاقاً من العناصر التالية، على سبيل المثال لا الحصر.

١ - مواقع الويب:

وهذه المواقع هي المصدر الاشمل للمعلومات المتاحة على شبكة الانترنت، وأول جزء من الأدلة الرقمية المحتملة هو وضوح محتوى الموقع، والثاني هو الجزء غير المرئي من المعلومات المرتبطة بهذا الموقع، والمحتوى غير المرئي هنا هو في الاساس متعلق بلغة البرمجة المستخدمة لإنشاء صفحات الويب.

وهنا يمكن أن تتوفر مجموعة من المعلومات، غير تلك التي تظهر في الواقع على الشاشة، ويمكن أن يرى المحقق مزيداً من المعلومات هنا وهناك، وبعضها قد يكون مفيداً جداً، وهناك بعض الامثلة من البيانات التي يمكن الحصول عليها بهذه الطريقة من مسرح الجريمة الالكترونية، هي:

- تعليقات المستخدمين / المطورين وكلمات السر.
- الحقول المخفية.
- المراجع إلى المواقع الخارجية التي قد تكون مصادر مستقلة للأدلة.

كما يمكن استعراض الرمز المصدري الذي يمكن أن يساعد المتخصص في الشرعية الرقمية على معرفة الجهاز الحاسبي الذي وصل للموقع حتى لو قام المشتبه به بمسح السجلات التاريخية للإنترنت له وقام بتفريغ البيانات.

---

(1)http://www.publications.parliament.uk/pa/ld199899/ldjudgmt/jd990805/bow.htm
R v Bow Street Magistrates Court and Allison (AP) Ex parte Government of the United States of America (Allison) [2002]2 AC 216.

(2) see : chehire and fifoot , the law of contract, London , 1964 , p.457.

(٢) مشار إلى هذه القضية عند: د. جميل عبد الباقي الصغير ، الجوانب الاجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، سنة ١٩٩٨م.

كما يمكن التعرف من خلال مزودي الخدمات على الشبكة على بيانات الحركة للمتهم، أي استعراض المواقع التي تصفحها، وكافة المعلومات المتعلقة بها وخاصة معلومات التاريخ والوقت.

وأخيراً، هناك البيانات الفائقة Meta data أو البيانات الوصفية، أي البيانات التي تشرح البيانات، والتي يمكن أن توفر معلومات فنية رفيعة المستوى عن صفحة الويب نفسها.

ومثال بسيط عن هذه النقطة هو تاريخ آخر تعديل لمورد ويب معين، كصفحة على شبكة الانترنت أو صورة، وهناك أدوات مفتوحة المصدر مثل FireBug تستخرج بعض المعلومات، ولكن فقط لتذكير القاضي بوجوب الطلب من مختصين ولجان خبرة استخراج القدر الاكبر من البيانات غير الظاهرة على صفحة الويب.

ومن الامثلة الواقعية على الدليل الرقمي في مسرح الجريمة الالكترونية، جريمة قتل حدثت بالفعل في الولايات المتحدة الامريكية، أن رجلاً قتل زوجته التي كانت موضوعة تحت المراقبة في المستشفى، بأن دخل عبر الانترنت إلى شبكة المعلومات الخاصة بالمستشفى، ثم قام بتغيير المعلومات الطبية الخاصة بالمجني عليها المريضة. (١)

٢ - البريد الالكتروني:

حيث يعتبر البريد الالكتروني مصدراً هاماً أيضاً للأدلة الرقمية في مسرح الجريمة الالكترونية، حيث يمكن بسهولة معرفة مصدر البريد الالكتروني، وتحديد من أرسل الرسالة، ذلك إن برامج البريد الالكتروني تخفي عادة المعلومات التقنية عن القارئ، وتوجد هذه المعلومات في ما يسمى ترويسة البريد الالكتروني.

ولكن يمكن أحياناً اختراق البريد الالكتروني، فيقوم المخترق بإرسال بريد من حساب شخص آخر، ويمكن للمرسل أيضاً إخفاء تحركاته من خلال الذهاب الى مكان عام مثل مقهى للإنترنت، حيث سيكون العنوان IP ينتمي إلى المقهى ولا يشير له.

وفي حالة اختراق البريد - والذي هو جريمة بحد ذاته - يستطيع الخبراء تحليل الاختراق وتحديد مصدره، واذا تم إرسال البريد الالكتروني من مكان عام مثل فندق أو مقهى إنترنت، يمكن استخدام بعض الملفات للمساعدة في التعرف على العملاء الذين استخدموا الحاسب في الوقت الذي تم إرسال البريد الالكتروني.

ومن الهام أيضاً أن نلاحظ أن معظم المعلومات في ترويسة البريد الالكتروني يمكن التلاعب بها لأنها تضاف من قبل مخدمات او ملقمات البريد الالكتروني المختلفة، والتي قد لا

(1) http://www.theregister.co.uk/23/08/2006/email_bomber_guilty .

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

تكون جديرة بالثقة، وينطبق هذا على جميع المعلومات الموجودة أسفل عنوان البريد الالكتروني، لأنها تأتي مباشرة من مخدم البريد المرسل الذي يمكن أن يكون تحت سيطرة المتهم، لذلك يجب على القاضي دائما التدقيق في كل المعلومات والأدلة التي يمكن أن تقدم من خلال البريد الالكتروني للعميل.

ومن التطبيقات العملية على ذلك فى مجال مسرح الجريمة الالكترونية، وكانت في المملكة المتحدة البريطانية، والمتعلقة بإعاقة الوصول إلى الخدمة Denial of service attack ، حيث جرت هذه الواقعة مع ديفيد لينون في الفترة الواقعة بين ٣٠ يناير، و ٥ فبراير عام ٢٠٠٤ ، حيث قام بهذا الهجوم، والدخول غير المصرح به إلى جهاز حاسب خاص بالرحلات الداخلية لشركة D&G (mestic and General Group Plc)

وكانت الوقائع أن السيد لينون كان يعمل من قبل في الشركة D&G لمدة ثلاثة أشهر حتى أقيل في شهر ديسمبر عام ٢٠٠٣ ، وكان عمره آنذاك ١٦ عاماً، في ٣٠ يناير ٢٠٠٤ ، بدأ السيد لينون بإرسال رسائل البريد الالكتروني إلى D&G باستخدام برنامج يسمى AvalancheV3.6 ، الذي كان قد قام بتحميله من الانترنت، ثم وضع البرنامج بصيغة إرسال البريد حتى التوقيف، وهذا يعني أنه سيستمر في إرسال رسائل البريد الالكتروني إلى أن يتم إيقافه يدوياً(١)

٣ - مواقع التواصل الاجتماعي:

بدأت مواقع الشبكات الاجتماعية كبداية صفحات الويب العادية، وتطورت بشكل كبير في تعقيدها، لذا فانه يتعين على قضاة التحقيق أن ينتبهوا لعدة امور هامة في مواقع شبكات التواصل الاجتماعي: (٢)

- **المعرفات الداخلية**: حيث تستخدم هذه المواقع هذه المعرفات على نطاق واسع لتعقب كل شيء، كالمستخدمين، والصور، والاحاديث، والمجموعات، وهذه المعرفات ترتبط في معظم الاحيان بمعرفات متاحة لمزود الخدمة.

- **المحادثات Chat:** حيث تقدم هذه المواقع خدمات للمستخدمين لإجراء المحادثات مع النص والفيديو والصوت، ويمكنها أن توفر معلومات نوعية كبيرة إذا جرت معالجتها

(1) Jonathan clough: principles of cybercrime, Cambridge University Press ،٢٠١٠، p171

(2) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow:Pervious reference P 105

بشكل كاف، والهدف الرئيسي للمحقق جمع أكبر قدر ممكن من البيانات، وليس فقط ما يظهر في الصفحة.

٤ - **الويب العميق**:(١)

يمكن القول بان الانترنت هو المكان الذي تُنشر فيه الخدمات والمعلومات من المزودين لنشر وتبادل البيانات مع الجمهور، وهناك أيضاً الطلب على ضرورة توفر مناطق خاصة للوصول إلى مجموعة محدودة من الناس لأغراض خاصة.

وبعض هذه المناطق هي الاماكن التي لا يمكن العثور عليها الا من قبل الاشخاص الذين لديهم العنوان الصحيح، وعلى سبيل المثال، إذا رغب الزوجان في مشاركة صور زفافهما مع أسرهم وأصدقائهم، ولا يريدون مشاهدة الصور من قبل كل مستخدمي الانترنت، ففي هذه الحالة يتمكنون من تحميل الصور إلى خدمة من خدمات الانترنت المخصصة لهذا الغرض، وتبادل الرابط فقط مع الاصدقاء والاسرة، وبالطبع هذه ليست طريقة آمنة جداً لتبادل البيانات الخاصة، ولكن هذا الحل قد يكون كافياً بالنسبة لمعظم الناس.

وهناك أيضاً مناطق أخرى خفية من شبكة الانترنت وهناك حاجة إلى وثائق التفويض للدخول، والبريد الالكتروني العادي هو مثال عن المناطق الخاصة التي لا يمكن العثور عليها عن طريق محرك بحث أو الوصول إليها، بسبب اشتراط تسجيل الدخول لقراءة المعلومات، بالاضافة الى وجود مواقع مخبأة عمداً عن محركات البحث العامة، أي لا تظهر بنتائج البحث، يحتاج المستخدم إلى كلمة مرور او تعريف ما.

وهناك أيضاً مناطق أخرى خفية من شبكة الانترنت بها صلاحيات خاصة للنفاذ إليها، وهناك أيضاً المواقع وقواعد البيانات التي لا يمكن فهرستها من قبل محركات البحث أو لا يمكن فهمها أو تحليلها من قبلها، ويطلق اسم عام لجميع تلك المناطق المخبأة عن محركات البحث "الويب العميق" أو "الويب الخفي".

ويلاحظ ان فكرة الويب العميق ليست بدعة، وليست مرتبطة بالاجرام، وقد وجدت منذ الايام الاولى للإنترنت بناء على رغبة المستخدمين والشركات ببعض الخصوصية.

وفي الواقع، يمكن بسهولة اعتبار الخوادم الاولى على شبكة الانترنت، وأول المواقع المتاحـة على الشبكة العالمية جـزءاً من الويب العميق.

(1) –(2) Nigel Jones, Esther George , Fredesvinda Insa Mérida , Uwe Rasmussen , Victor Völzow: Pervious reference P 110

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

وبالاضافة الى المواقع وقواعد البيانات والوثائق التي لا يمكن فهرستها من قبل محركات البحث، هناك طبقة أخرى من الويب العميق تسمى الشبكة الظلامية Darknet أو الويب الظلامي Darkweb، والشبكة الظلامية مشابهة للويب العميق، ولا يمكن البحث عنها باستخدام محركات البحث التقليدية، ومع ذلك، في حين أن مواقع الويب العميقة يمكن الوصول إليها عن طريق متصفح الانترنت العادي إذا كان الزائر يعرف العنوان ومعلومات تسجيل الدخول، فإن هذا غير صحيح لمواقع الشبكة الظلامية.

وعلى الرغم من أن الشبكة الظلامية تستخدم شبكة الانترنت الفيزيائية نفسها، فإنها تستخدم من الناحية العملية مساحة من الشبكة وعناوين داخلية مختلفة.

وهنا يلاحظ ان المحققون والقضاة فى حاجة لمعرفة العنوان المشكوك فيه، في الشبكة الظلامية لرؤية المحتوى، والشبكات الظلامية هي شبكات ثنائية، وهذا يعني أن كل مستخدم يرتبط مباشرة مع مستخدم آخر، ويمكن لأي شخص يمتلك مجموعة من المهارات المتميزة إنشاء شبكة ظلامية، ويمكنه دعوة مجموعة من الناس والموثوق بهم للمشاركة في هذه الشبكة الصغيرة.

ومع ذلك، نجد أيضاً أن بعض الشبكات الظلامية تتكون من آلاف المستخدمين، أبرزها الشبكة "Freenet"، والشبكة "TOR" شبكة TOR والمؤلفة من العديد من العقد، وكل عقدة تتصل فقط بالعقد جاراتها المباشرة، لذلك لا يمكن لأي عقدة واحدة، والتي عادة ما تعني مستخدماً في سلسلة، معرفة من أرسل أو من تلقى أي طلب، ويستطيع المحققون والقضاة الوصول إلى شبكة TOR ببساطة عن طريق تحميل TOR browser82. ويمكن للمحقق الوصول إلى الخدمات المخفية عبر عناوين لها طبيعة خاصة مختلفة عن العناوين التقليدية.

ومن الاهمية تعريف الويب العميق، والويب الظلامي ليتسنى للقضاة معرفة وجود هذه الانواع من الشبكات، وذلك لأن المجرمين، وخاصة تجار المخدرات(١)، ومجندي الشباب في

---

(١) انظر فى ذلك: محمد فتحى عيد، السنوات الحرجة فى تاريخ المخدرات، نذر الخطر وعلامات التفاؤل، مرجع سابق، ص ١٣١، وايضا: تقرير الهيئة الدولية لمراقبة المخدرات لسنة ٢٠٠٠، الفقرات (٥٠ – ٥٦)، ص ١٢ ، ١٣، مطبوعات الامم المتحدة، نيويورك، ٢٠٠١، الوثيقة رقم Elincb 200D المنشور بتاريخ ٢١ فبراير ٢٠٠١، وكذلك انظر : مجلة الحقوق الكويتية، مجلس النشر العلمى، الكويت، ١٩٩٨، العدد الثالث، ص ٣٨١، منشور دورة البحث الجنائى للضباط رقم (٥) دراسات حول الجريمة الاقتصادية فى دولة الامارات، معهد البحث الجنائى، شرطة دبى، دولة الامارات العربية المتحدة، ١٩٩٨، ص ٩٨.

DUNCAN. Alfod. Anti- mony laundering regulations: Aburden on financial institutions, volume 19 north Carolina jounal of international and commercial regulations, p.p 441 – 442 (summer 1994).

منظمات إرهابية غالباً ما يستخدمون هذه الشبكات، ويحتاج القضاة إلى الطلب من المختصين بالبحث عن الأدلة الرقمية التي يمكن أن تدين بعض الاشخاص الذين يستخدمون هذه الشبكات.

٥ - **الحسابات السحابية**: (١)

حيث ان التخزين على الانترنت أصبح موضوعاً ذا أهمية كبيرة، ولكي يكون القاضي قادراً على التعرف وفهم هذه الخدمات، يحتاج إلى معرفة ما هي الحوسبة السحابية.

والحوسبة السحابية هي نموذج لتمكين كل مستخدم، وعادة ما تكون شركات، من الوصول إلى شبكة الانترنت واستخدام مجموعة كبيرة من مواردها من الخوادم، ووحدات التخزين، والتطبيقات، والخدمات التي يمكن توافرها، عند الطلب.

ويلاحظ بشأن الحوسبة السحابية، والذي يهم المحقق والقاضي، أن البيانات لا يتم تخزينها على جهاز حاسبي فعلي واحد، ولكن على خوادم متعددة، حتى أنه لا يمكن معرفة كيف وأين يتم تخزين بعض البيانات.

والجانب الاخر المثير للاهتمام ايضا، هو أن الخدمات السحابية قادرة على الحلول محل البنية التحتية لتقنية المعلومات في الشركة، بدءاً من خدمات البرمجيات مثل معالجة النصوص أو برامج المحاسبة وصولاً إلى استبدال كامل لجميع محطات العمل.

ويعرف هذا النوع من الشبكات، بشبكات الند للند peer-to-peer ، وهي تطورت بوجه خاص بهدف تبادل المحتوى بين المستخدمين،عن طريق وضع تلك الملفات على مخدمات، ومن أشهر تلك الشبكات شبكة torrent وشبكة Emule

ومن المميزات هنا، من الناحية الفنية، أن الالة الافتراضية، وهو البرنامج، يمكن نسخها بسهولة، ولكن واعتماداً على التشريعات ذات الصلة، فإن منح الترخيص القانوني المناسب لاعتراض تلك البيانات قد يواجه بعض المشكلات، ولكنه أيضاً يشكل تحدياً لضمان الحصول على البيانات وفقاً للإجراءات القانونية في الدولة الطالبة، وثمة عيب آخر هو أنه من المحتمل أن تكون البيانات المستردة أقل بكثير من البيانات اللازمة لتشكيل الدليل.

وعلى ذلك، إذا عمد أحد المشتبه بهم إلى إنشاء جهاز افتراضي مؤقت لارتكاب جريمته، ثم حذف هذا الجهاز، يكون من الصعب استرداد الدليل، لذلك يجب على القاضي في هذه الحالات

(1) Nigel Jones, Esther George, Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow: Pervious reference P 85- 89.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

الاستعانة بالمتخصصين للقيام بالبحث عن الأدلة في السحابات، واذا واجهت الخبير مشكلة صلاحيات الوصول إلى الشبكة، ويشتبه في استخدام الحوسبة السحابية يجب عليه(١):

- البحث عن أيقونات فيها شعارات لخدمات الحوسبة السحابية، وهي خدمات البرمجيات Software as a Service (SaaS، والبنى التحتية Infrastructure as a Service (IaaS)، ومنصات العمل Platform as a Service (PaaS
- التحقق من تثبيت برامج لخدمات الحوسبة السحابية.
- البحث في قائمة الاجراءات عن أسماء الخدمات السحابية.
- البحث عن مشاركة عناصر أو محركات أقراص شبكية.
- مراقبة حركة مرور الشبكة.
- مراقبة قائمة المقابس Sockets المفتوحة.

المبحث الثاني

حجية الأدلة الرقمية فى القانون المصري

من المقرر ان العقبات والصعوبات التي تواجه الدليل الرقمي في مسرح الجريمة الالكترونية، لا تقف عند حد كيفية الحصول عليه واجراءات حفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالاقتناع به لبناء الحكم على أساسه بالبراءة أو الادانة.

لذلك حاول المشرع والقضاء والفقه المقارن التصدي لهذه المسألة، وذلك بتحديد الشروط التي يجب توفرها في الدليل الرقمي أو في مخرجات الحاسب حتى يمكن قبوله من قبل القاضي.

ويقصد بهذه القاعدة أنه عند إثبات مضمون كتابات أو سجلات أو صور من مسرح الجريمة الالكترونية، فإن أصل هذه الكتابات أو السجلات أو الصور يجب أن يكون متوفراً، أي يجب تقديمه إلى المحكمة.

---

(١) راجع فى ذلك: د. محمود رجب فتح الله، الوسيط فى الجرائم المعلوماتية، الاسكندرية، مرجع سابق، ص ٢٣٩ وما بعدها، وراجع ايضا في هذا الصدد: د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ١١١١ وما بعدها.

وحتى يكون الدليل الرقمي مقبولاً أمام المحكمة، يجب أن تتوفر فيه الشروط التالية:

١- أن لا يطرأ على محتويات السجل الالكتروني أي تغيير، أي أن يكون الدليل المقدم إلى المحكمة هو نفس الدليل الذي تمّ جمعه من مسرح الجريمة الالكترونية، ويمكن للشخص الذي قامThe Federal Rules of Evidence بجمع الدليل أن يشهد بذلك أمام المحكمة، وهذا ما يطلق عليه مفهوم «سلسلة الرعاية Chain of Custody »، ويقصد بذلك أن الدليل الرقمي منذ لحظة جمعه وحتى لحظة تقديمه إلى المحكمة لم يطرأ عليه أي تغيير، ولا يوجد أي احتمال للعبث به، وأنه تمّت مراعاة سلامته حتى يبقى بنفس الحالة التي وجد عليها بمسرح الجريمة الالكترونية.

٢- أن تكون المعلومات الموجودة في السجل، قد صدرت فعلاً عن المصدر المزعوم من مسرح الجريمة الالكترونية، سواء كان هذا المصدر الانسان أم الالة. (١)

٣- أن تكون المعلومات الموجودة في السجل من مسرح الجريمة الالكترونية، والمتعلقة بالوقت والتاريخ، معلومات دقيقة.

أما القضاء الامريكي فقد تعرض في العديد من القضايا إلى مسألتي الاصالة والصحة، ففي إحدى القضايا، قررت المحكمة إن عضو مكتب التحقيقات الفيدرالي FBI الذي كان حاضراً عندما تمّ ضبط الحاسب الخاص بالمتهم، يمكن أن يقرر صحة الملفات المضبوطة، وفي قضية أخرى قبلت المحكمة سجلات الهاتف بعد أن أكّدت موظفة الفواتير في الشركة أصالة هذه السجلات. (٢)

كما قبلت إحدى المحاكم الدليل الرقمي رغم الدفوع المتعلقة بالعبث بهذا الدليل، لأن هذه الدفوع جاءت على شكل تخمين، دون أن يوجد أي دليل يدعمها.(٣) وفي إحدى القضايا قررت المحكمة "إن حقيقة وجود احتمال بتعديل البيانات الموجودة في الحاسب غير كافية للقول بعدم جدارة الدليل. (٤)

(1) Dr. Henry B. wolfe, Forensics and the emerging importance of electronic Evidence gathering, OTAGO university, 2001, P-4, available on line. www.e-evidence. info. Albert .J. Mercella, op-cit, 343.
(2) Eoghan casey,op-cit,p.170.
(3) Witaker, 127 F.3d 595, 601 (7th cir. 1997).
(4) Witaker, 127 F.3d at 602, Eoghan casey,op-cit,p.170.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

كما ذكرت وزارة العدل الامريكية في المرشد الفيدرالي لتفتيش وضبط الحواسب، وصولاً إلى الدليل الرقمي من مسرح الجريمة الالكترونية في التحقيقات الجنائية "إن غياب دليل واضح على حدوث العبث في الدليل، لا يؤثر على أصالة ودقة سجلات الحاسب.(١)

وفي عام ١٩٤٨ صدر في إنجلترا قانون الشرطة والاثبات الجنائي (Pace)، ويتناول آلية تفتيش الاماكن، وكيفية معاملة المشتبه بهم، والاعتقال وغير ذلك، وقد تم تعديل هذا القانون في ١٤ اكتوبر عام ٢٠٠٢. (٢)

وقد ركّز هذا القانون بصفة أساسية على قبول مخرجات الحاسب كدليل في الاثبات من مسرح الجريمة الالكترونية، حيث حدد المشرع الانجليزي في المادة ٦٩ من هذا القانون الشروط الواجب توفرها في المستند الناتج عن الحاسب، حتى يُقبل كدليل في الاثبات. (٣)

وهذه الشروط هي:

١- عدم وجود أسس معقولة للاعتقاد بأن البيان يفقد الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسب الموجود في مسرح الجريمة الالكترونية.

٢- أن الحاسب كان يعمل في جميع الاحوال بصورة سليمة، واذا لم يكن كذلك، فإن أي جزء لم يكن يعمل فيه بصورة سليمة، أو كان معطلاً عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته.

وقد علق مجلس اللوردات على المادة ٦٩ المشار إليها، بأنه يمكن للشهادة الشخصية الصادرة عن شخص على علم بطريقة تشغيل الحاسب، أن تعطي الثقة بالدليل، وليس بالضروري أن يكون هذا الشخص خبيراً بالحاسب.(٤) وبناءً على ذلك قبلت المحاكم الانجليزية - فيما يتعلق بسلامة نظام الحاسب- بشهادة أشخاص لديهم علم بطريقة عمل نظام الحاسب.(٥)

ويتناول الفقه في فرنسا حجية مخرجات الحاسب في المواد الجنائية، في إطار مسألة أوسع وأعم، هي مسألة قبول الأدلة الناشئة عن الالة أو الأدلة العلمية، مثل الرادارات، وأجهزة التصوير، وأشرطة التسجيل، وأجهزة التنصت.

---

(1) Bouallo, 858 F.2d 1427, 1436 (9th cir.1988). Eoghan casey, op-cit, p.170.

(2) Eoghan casey,op-cit,p.170.

(٣) متوفر على الانترنت على موقع القوانين البريطانية:

www.briTishlaw.org.uk .

(4) Eoghan casey,op-cit,p.170 .

(5) R.V. Shephard. 1933, Eoghan casey,op-cit,p.170.

أما القضاء فقد قبل هذه الأدلة إذا توفرت فيها مجموعة من الشروط، من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة، وأن يتم مناقشتها حضورياً من قبل الاطراف، وقد قضت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة، التي يكون لها قيمة دلائل الاثبات، يمكن أن تكون صالحة للتقديم أمام القضاء الجنائى.(١) أما بالنسبة إلى قناعة القاضي الجنائي، فإن الأدلة الرقمية تخضع لحرية القاضي في الاقتناع الذاتي، بحيث يمكن أن يطرح مثل هذه الأدلة، رغم قطعيتها من الناحية العلمية، عندما يجد أن الدليل الالكتروني لا يتسق منطقياً مع ظروف الواقعة وملابساتها(٢).

الخاتمـــــة والتوصيـــــات

من المقرر ان هناك جملة من التوصيات التي انتهت الدراسة الي وجوب مراعاتها بشأن مسرح الجريمة الالكترونية والركون الي أدلته في الاثبات، نجملها ونوجزها فيما يلي.

١- أهمية مراعاة السرية وحماية الخصوصية ومراعاة النوع الاجتماعي في النصوص التشريعية وفي التطبيقات والاجراءات والممارسات ذات الصلة.

٢- التأكد من أن السياسات الحكومية والتشريعات المنظمة تحقق التوازن بين الحاجة إلى جميع المعاملات وتطوير المحتوى والخدمات الرقمية في مصر، وزيادة وتعزيز المحتوى العربي من جهة، وتوفير الحماية وضمان أمن المعلومات وحماية البيانات الشخصية والحد من جرائم تقنية المعلومات.

٣- تحديث دوري للقوانين لتتلاءم مع التكنولوجيات الجديدة، وعلى سبيل المثال، إن القوانين التي تنظم عمليات مزودي خدمات الانترنت تحتاج إلى تنظيم تحديث بشكل يتناسب والتطور التكنولوجى.

٤- ضرورة استحداث قواعد مناسبة فى مجال الاجراءات الجنائية لعدم ملائمة الاجراءات الجنائية الحالية فى مجال مسرح الجريمة الالكترونية.

٥- ضرورة الالتزام بأحكام الدستور بشأن حماية سرية المراسلات والخصوصية والحرية الشخصية ونشر المعرفة بها.

---

(١) Cass. Criw. 28 avr. 1987, Bull. Criw.no.173

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

٦- ضرورة النص صراحة في كافة القوانين المنظمة للإثبات الجنائي والمدني، بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الاثبات، طالما أن ضبط هذه الأدلة جاء وليد إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير، وبما يحقق مبدأ المواجهة بين الخصوم.

٧- ضرورة تخصيص شرطة متخصصة لمكافحة جرائم تقنية المعلومات، وذلك من رجال الشرطة المدربين على كيفية التعامل مع مسرح الجريمة الالكترونية، واستخلاص الأدلة الرقمية منه.

٨- ضرورة تعديل بعض التشريعات المصرية الحالية، وخاصة في مجال الملكية الفكرية والتوقيع الالكترونى، بما يتلائم مع طبيعة مسرح الجريمة الالكترونية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات وشرحها لهم بشكل واضح.

٩- النص على عدم جواز إفشاء أو تقديم بيانات تتجاوز حدود البيانات اللازمة في قضية ما والنص على وجوب تحديد طلبات الجهات الرسمية الادارية والقضائية بصورة شديدة التحديد والوضوح، وخاصة لجهة تحديد أطراف القضية لمنع سوء الاستخدام واقتصار الطلب على هذه البيانات دون تعميم.

١٠- يلزم أن تمتد إجراءات التفتيش إلى أية انظمة حاسبية أخرى، قد تكون بمسرح الجريمة الالكترونية، يمكن ان تكون ذات صلة بالنظام محل التفتيش وضبط ما بها من معلومات.

١١- يلزم تعديل قانون ونظم الاجراءات الجنائية، بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها حيال التفتيش لمسرح الجريمة الالكترونية على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الالكتروني حتى يستمد الدليل مشروعيته.

١٢- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الالكتروني وأية تقنية أخرى، قد تفيد في إثبات الجريمة والحصول على دليل، والكشف عن الحقيقة من مسرح الجريمة الالكترونية.

١٣- ينبغي أن ينص على اعتبار أن الانترنت وسيلة من وسائل العلانية في قانون العقوبات والقوانين ذات الصلة بجرائم تقنية المعلومات، مع الأخذ بالاعتبار أن الانترنت أوسع انتشارا من سائر وسائل النشر والعلانية الاخرى.

١٤- إنشاء قسم جديد بكليات الحقوق على مستوى كافة الجامعات العربية لدراسة أوجه الحماية القانونية للمعلوماتية أو تحت مسمي مسرح الجريمة الالكترونية، مع وجوب بيان الأدلة الرقمية وقيمتها وقوتها في الاثبات.

١٥- إنشاء مجموعات عمل ميدانية عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مسرح الجريمة الالكترونية.

١٦- التدخل التشريعي لمواجهة القصور في التشريعات والقوانين الجنائية العربية الحالية أو تحديثها بالنص صراحة على تجريم إساءة استخدام بطاقة الائتمان الالكترونية اعمالا لمبدأ شرعية الجرائم والعقوبات حتى نصل إلى إقامة بني قانونية للتصدي لمثل هذا النوع من الجرائم.

١٧- الدعوة إلى إنشاء قسم خاص داخل إدارات مكافحة الجريمة بوزارات الداخلية العربية، يكون متخصصاً في مسرح الجريمة الالكترونية، مع تدريب العاملين به على أساليب التحري والضبط في هذا النوع من الجرائم.

١٨- الاهتمام بالطرق الفنية لتحقيق مسرح الجريمة الالكترونية، وذلك بعمل دورات تدريبية للقائمين على ذلك وتوعيتهم بالأساليب المتطورة والمستحدثة فى هذا المجال.

١٩- ضرورة التعاون الدولي بتبادل المعلومات والخبرات، والتعاون في المجال الأمني والقضائي بصوره المختلفة، فضلا عن التعاون بينها وبين الدول الاخرى في هذا المجال لتوقيع اتفاقيات مع دول أخرى لتسليم مقترفي هذا النوع من الجرائم، وهو الأمر الذي انتبهت إليه السلطات وتحاول جاهدة تجاوزه، لاسيما مع حداثة جرائم تقنية المعلومات، والمتسمة بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها.

٢٠- استحداث إدارات أمنية خاصة تعنى بمسرح الجريمة الالكترونية وتزويدها بالكوادر المؤهلة في الشق الأمني والتقني للاهتمام بجمع المعلومات وإجراء التحريات والتواصل مع الجهات المماثلة لها في الدول الاخرى، مع تأهيل وتدريب سلطات المكافحة تدريباً وافياً لمواكبة التغير السريع في مجالات التقنية المعاصرة، لكي تتوافر لدى هذه السلطات القدرة على المكافحة الفعالة وتتواكب بقدراتها وكفاءتها مع ما يسعى إلى تحقيقه أطراف الجريمة المنظمة.

٢١- الاستعانة بالمتخصصين والخبراء القادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية والمحققين مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أفضل صورة.

٢٢- إنشاء مختبر للأدلة الرقمية الجنائية لجرائم تقنية المعلومات (Digital Forensic Lab) وهو مختبر جنائي مشترك بالتعاون مع اتحاد المصارف، بغية اجراء التحقيقات المطلوبة والحصول على الأدلة، وتحليل الفيروسات، والحد من انتشارها محليا ودوليا واجراء الأبحاث العلمية في هذا المجال، والاهتمام بمكافحة جرائم تقنية المعلومات والتصدي لها، نظرا لما تشكله من تهديد لسمعة المصرف فضلا عن الخسائر التي قد تنتج عن هذه الجرائم.

٢٣- تأهيل القائمين على أجهزة إنفاذ القانون لتطوير معلوماتهم في مجال مسرح الجريمة الالكترونية، وذلك من خلال تدريب وتأهيل القائمين بالضبط والخبراء وسلطات التحقيق والقضاة، وخاصة تدريب القضاة على التعامل وتفهم هذا النوع من القضايا التي تحتاج إلى خبرات فنية عالية لملائمة قبول هذا النوع من الأدلة في الاثبات وتقديرها، حتى يتمكن قاضى الموضوع من الفصل في القضايا المتعلقة بهذا النوع من جرائم تقنية المعلومات.

٢٤- توظيف محققين ذوى معرفة تقنية عالية ومواكبة أحدث التقنيات في مجال مسرح الجريمة الالكترونية، وينبغي إنشاء مختبرات الطب الشرعي على الحاسب لجمع الأدلة الرقمية من أجهزة الحاسب وتوفير التدريب للمحققين.

٢٥- ضرورة إعداد الكوادر الأمنية، وسلطات التحقيق من الناحية الفنية للبحث والتحقيق وجمع الأدلة في مجال مسرح الجريمة الالكترونية، مما يستلزم إنشاء مراكز متخصصة في المعهد القضائي وكلية الشرطة تحقيقا لهذا الغرض.

٢٦- اعتماد السياسات والاجراءات والنظم المناسبة للتصدّي لجرائم تقنية المعلومات، ورصد الميزانيات والبرامج الواجّبة لذلك، وتدريب الموظفين على تطبيقها.

٢٧- الالتزام بتطبيق الاجراءات الوقائية الضرورية، لا سيما لجهة التحقيق من موضوع العملية من حيث السبب والعلاقة بالمستفيد وبالبلد، والتيقن من المعلومات المطلوب تنفيذها.

٢٨- عقد دورات مكثفة للكوادر البشرية من العاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسب، والجرائم المرتبطة بها، والنظر في ادراج مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن مسرح الجريمة الالكترونية.

٢٩- يتعين تدريب وتحديث أعضاء النيابة العامة والقضاء بشأن التعامل مع مسرح الجريمة الالكترونية، وما قد تتواجد به من أجهزة الحاسب والانترنت بصفة عامة، والأدلة الرقمية بصفة خاصة.

٣٠- الاستمرار دوريا في تحديث الدليل الارشادي للوقاية من الأفعال الاجرامية بواسطة البريد الالكتروني الذي يحدد المؤشرات الدالة لطرق الاحتيال التي قد يتعرض لها القطاع المالي والتجار والمؤسسات والأفراد.

٣١- إشراك القطاع الخاص في مسرح الجريمة الالكترونية، لأنها ضرورية لمساعدة السلطات العامة من خلال تحسين الحماية الذاتية كخط دفاع أولى لهذا القطاع، واعتماد الحلول التقنية المتقدمة والخطوات الادارية الضرورية لحماية أمن المعلومات.

٣٢- التقيّد بإرشادات الدليل الارشادي للوقاية من الافعال الاجرامية بالوسائل الالكترونية والمُمارسات السلوكية المثلى Best Practices التقنية والقانونية.

٣٣- ضرورة خلق ثقافة اجتماعية جديدة تندد بجرائم تقنية المعلومات، مع تفعيل اسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية وحثهم على الاستخدام الأمثل لهذه التقنيات.

٣٤- ضرورة نشر الوعي الرقمي بين المستخدمين، وكيفية تفادي التعدي على بياناتهم الشخصية، وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.

٣٥- ضرورة نشر الوعي بين صفوف المواطنين– ولا سيما الشباب – بمخاطر التعامل مع المواقع السيئة علي شبكة الانترنت، مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للانترنت وتكثيف التوعية عن الآثار السلبية الصحية المترتبة عن الممارسات الجنسية الشاذة، وذلك بأسلوب غير مباشر من خلال المواد الدرامية.

٦١- الدليل التقني المستمد من مسرح الجريمة الالكترونية

٣٦- ضرورة مشاركة المجتمع المدني في مناقشة مشروعات القوانين المتعلقة بمسرح الجريمة الالكترونية وأمن المعلومات الشخصية وضمانات الحق في الخصوصية دون مساس بحرية الرأي والتعبير ودون تضييق على المساحة التي يتيحها الانترنت للحصول على المعرفة والمعلومات ولتسهيل التواصل الاجتماعي.

٣٧- إعداد ونشر مواد توعية وتثقيف وتوزيعها على نطاق واسع وإتاحتها إلكترونياً لنشر الوعي بالاستخدام الآمن لتكنولوجيا المعلومات والاتصال ومسألة الخصوصية ووسائل الوقاية من جرائم تقنية المعلومات، وإنشاء وإتاحة برامج وخدمات متخصصة موجهة للفئات الأكثر عرضة لمثل هذه الجرائم.

٣٨- ضرورة نشر المعرفة والمعلومات حول جهات الارشاد والمساعدة القانونية والفنية للمتضررات والمتضررين والجهات الرسمية التي تستقبل الشكاوى المتعلقة بمسرح الجريمة الالكترونية .

٣٩- نشر الاحصائيات والارقام المتعلقة مسرح الجريمة الالكترونية والأحكام القضائية الصادرة به لتحقيق المزيد من الردع وللتوعية وتحفيز المزيد من الحذر من الاستخدام الخاطئ لوسائل التواصل الاجتماعي والانترنت.

٤٠- تعزيز التعاون مع وسائل الاعلام بما فيه الاعلام الالكترونية لمتابعة ورصد وتطوير مواثيق وأخلاقيات ومدونات سلوك وآليات محاسبة ذاتية بشأن استخدام وسائل المعلومات والاتصال الالكتروني ومواجهة جرائم تقنية المعلومات.

٤١- ضرورة المتابعة بالتنسيق مع الأجهزة المعنية والقطاع الخاص وجهات انفاذ القانون في الخارج والمنظمات الدولية والسعي للانخراط في المعاهدات الدولية للتمكن من مواجهة هذه الجريمة الأسرع تناميا والأكثر تعقيدا.

٤٢- تطوير منهج تدريبي وتنفيذ تدريب متخصص للمعنيين والمعنيات وخصوصاً لجهة بناء قدرات الموظفين المعنيين في الجهات الرسمية والأهلية وشركات الاتصالات ومزدي الخدمة لمعرفة القوانين والاجراءات ذات الصلة وتطبيقها بدقة وخاصة لجهة سرية المعلومات وحماية الخصوصية والمعلومات والبيانات الشخصية .

٤٣- العمل على إدخال مادة " مسرح الجريمة الالكترونية " فى مناهج التدريس لطلبة كلية الشرطة، كمادة مستقلة عن نظم التشغيل، وذلك حتى يستطيع الدارسون التعرف على

الجرائم المتعلقة به والالمام بها، وكذا تعميم دراستها لطلاب كليات الحقوق بكافة الجامعات بالجمهورية.

٤٤- حث الجامعات والمراكز البحثية العربية للبحث والدراسة في مسرح الجريمة الالكترونية والجرائم عبر الانترنت، ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمسرح الجريمة الالكترونية.

٤٥- ضرورة تضمين المناهج الدراسية كافة المعارف والمعلومات والقيم السلوكية المتعلقة بإستخدام تكنولوجيا المعلومات والاتصال الحديثة ومتطلبات صيانة الخصوصية والأمن الشخصي وسبل مواجهة مخاطرها.

٤٦- التوعية بأساليب التحايل والنصب المعلوماتى والجوانب السلبية لعدم الاستخدام الآمن لوسائل التواصل الاجتماعي والانترنت بشكل عام.

المراجع والمصادر

أولاً: المراجع العربية:

- القرآن الكريم.
- الحديث الشريف.

أ) المراجع والمؤلفات العامة:

١. إبراهيم حامد طنطاوى، علي محمود حمودة، شرح الاحكام العامة لقانون العقوبات - الجزء الاول النظرية العامة للجريمة، دار النهضة العربية، سنة ٢٠٠٨.

٢. إبراهيم حامد طنطاوي، سلطات مأمور الضبط القضائي، الطبعة الأولى، ١٤١٣هـ.

٣. إبراهيم محمد إبراهيم، النظرية العامة للقبض على الأشخاص في قانون الإجراءات الجنائية، دار النهضة العربية، ١٤١٦هـ.

٤. ابن فارس، معجم مقايس اللغة، للمحقق عبدالسلام محمد هارون، دار الفكر، بدون دار نشر، سنة ١٩٧٩.

٥. أحمد الخمليشي، شرح قانون المسطرة الجنائية، الجزء الاول، مطبعة المعارف الجديدة - الرباط، الطبعة الخامسة، سنة ١٩٩٩ .

٦. أحمد المهدي وأشرف شافعي، القبض والتفتيش والتلبس، دار العدالة، الطبعة الأولى، سنة ٢٠٠٥م .

٧. أحمد جاد منصور، حقوق الإنسان في ضوء المواثيق الدولية والإقليمية والتشريعات الداخلية ودور الشرطة في حمايتها، أكاديمية الشرطة، القاهرة، سنة ٢٠٠٦.

٨. احمد شوقى عمر ابوخطوة، شرح الاحكام العامة لقانون العقوبات لدولة الامارات العربية المتحدة، الجزء الاول، مطابع البيان التجارية، دبى، الطبعة الاولى، سنة ١٩٨٩ .

٩. أحمد عوض بلال، الإجراءات الجنائية المقارنة والنظام الإجرائي في المملكة العربية السعودية، دار النهضة العربية، القاهرة، سنة ١٩٩٠.

١٠. أحمد فتحى سرور، القانون الجنائي الدستورى، دار الشروق، الطبعة الثانية، سنة ٢٠٠٢.

١١. احمد فتحي سرور، الوسيط في الإجراءات الجنائية، دار النهضة العربية، الطبعة السابعة، ١٩٩٣ .

١٢. إدوار غالي الذهبي، الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، الطبعة الأولى، سنة١٩٨٠.

١٣. أسامة عبدالله قايد ومحمد علي كومان، النظام الإجرائي في المملكة العربية السعودية، طبعة دار النهضة العربية، سنة ١٤١٩هـ.

١٤. أسامة علي مصطفى الفقير الربابعة، أصول المحاكمات الشرعية الجزائية، دار النفائس، الأردن، الطبعة الأولى، سنة ١٤٢٥هـ.

١٥. بندر بن عبدالعزيز اليحيى، التحقيق الجنائي في الفقه الإسلامي، طبعة كنوز إشبيليا، الرياض، الطبعة الأولى، سنة ١٤٢٧هـ.

١٦. جلال ثروت، شرح قانون العقوبات القسم العام، منشاة المعارف، الاسكندرية، سنة ١٩٨٩.

١٧. جلال ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة، سنة ٢٠٠٣م.

١٨. جميل عبدالباقي الصغير، أدلة الإثبات والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، سنة ٢٠٠٠.

١٩. حسن صادق المرصفاوي، أصول الإجراءات الجنائية، منشأة المعارف، الإسكندرية، سنة ١٩٨٢.

٢٠. حسن صادق المرصفاوي، المرصفاوي في أصول الإجراءات الجنائية، منشأة المعارف بالإسكندرية، سنة ٢٠٠٠م .

٢١. حسنى الجندى، شرح قانون العقوبات، هدى حامد قشقوش دن، سنة ١٩٩٩.

٢٢. خليفة كلندر عبدالله حسين، ضمانات المتهم في مرحلة التحقيق الابتدائي في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الأولى، سنة ١٤٢٣هـ.

٢٣. رفاعي سيد سعد، ضمانات المشتكى عليه في التحقيق الابتدائي، منشورات جامعة آل البيت، الطبعة الأولى، سنة ١٤١٧هـ.

٢٤. رمسيس بهنام، الإجراءات الجنائية تأصيلاً وتحليلاً ، منشأة المعارف، سنة ١٩٧٧.

٢٥. روؤف عبيد، المشكلات العملية الهامة في الاجراءات الجنائية، دار الفكر العربي، الجزء الاول، سنة ١٩٨٠م.

٢٦. رؤوف عبيد، جرائم الاعتداء على الاشخاص والاموال، دار الفكر العربي، الطبعة الثانية، سنة ١٩٨٥.

٢٧. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، طبعة دار الفكر العربي بالقاهرة، ١٤٢٥هـ.

ب) المراجع والمؤلفات المتخصصة:

١. إبراهيم حامد طنطاوي، سلطات مأمور الضبط القضائي، الطبعة الأولى، ١٤١٣هـ.

٢. إبراهيم محمد إبراهيم، النظرية العامة للقبض على الأشخاص في قانون الإجراءات الجنائية، دار النهضة العربية، ١٤١٦هـ

٣. احمد خليفة الملط، الجرائم المعلوماتية ، الاسكندرية ، دار الفكر الجامعي، سنة ٢٠٠٥.

٤. احمد عبد اللطيف الفقهي، الدولة وحقوق ضحايا الجريمة، دار الفجر، القاهرة، ط١، سنة ٢٠٠٣.

٥. أحمد عوض بلال، الجرائم المادية والمسؤولية الجنائية دون خطأ، دراسة مقارنة، دار النهضة العربية، سنة ١٩٩٣.

٦. أحمد كامل سلامة، الحماية الجنائية لاسرار المهنة، دار النهضة العربية، القاهرة، سنة ١٩٨٨.

٧. أروى الفاعوري وإيناس قطيشات، جريمة غسل الاموال (المدلول العام والطبيعة القانونية) دار وائل، الاردن، الطبعة الاولى، سنة ٢٠٠٢.

٨. أسامة أبو الحجاج – دليلك الشخصي الى الانترنت – دار نهضة مصر – القاهرة – سنة ١٩٩٨.

٩. امال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة للنشر، سنة ٢٠٠٧.

١٠. أيمن عبد الحفيظ: الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، بدون دار نشر، سنة ٢٠٠٥.

١١. بندر بن عبدالعزيز اليحيى،التحقيق الجنائي في الفقه الإسلامي، طبعة كنوز إشبيليا، الرياض، الطبعة الأولى، سنة ١٤٢٧هـ.

١٢. جعفر الجاسم، تكنولوجيا المعلومات، عمان، دار أسامة للنشر، سنة ٢٠٠٥ .

١٣. جعفر حسن جاسم الطائي: جرائم تكنولوجيا المعلومات، دار البداية، ليبيا، سنة ٢٠٠٧.

١٤. جمال محمود الكردي: المحكمة المختصة والقانون الواجب التطبيق بشأن دعاوى المسؤولية والتعويض عن مضار التلوث البيئة العابرة للحدود، ط ١، دار النهضة العربية، الاسكندرية، سنة ٢٠٠٣.

١٥. جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنولوجيا الحديثة ، دار النهضة العربية ، القاهرة ، سنة ٢٠٠٢.

١٦. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي ، دار النهضة العربية ، القاهرة ، سنة ٢٠٠١ .

١٧. جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، سنة ١٩٩٨م.

١٨. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، سنة ١٩٩٢.

١٩. حاتم عبد الرحمن منصور، الإجرام المعلوماتي ، دار النهضة العربية ، ط١، سنة ٢٠٠٢.

٢٠. حسن صادق المرصفاوى، الأساليب الحديثة في التحقيق الجنائي، المجلة الجنائية القومية، المجلد العاشر، سنة ١٩٦٧.

٢١. حسن طاهر داوود، جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم الأمنية ، الطبعة الاولى، الرياض، سنة ٢٠٠٠ .

٢٢. حسنين عبيد، التعاون الدولي في مكافحة الجريمة، دار النهضة العربية، الاسكندرية، سنة ٢٠٠١.

٢٣. حسنين عبيد، الجريمة الدولية - دراسة تحليلية وتطبيقية، دار النهضة العربية، الاسكندرية، سنة ١٩٨٩.

٢٤. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت دراسة مقارنة، دار النهضة العربية، سنة ٢٠٠٩.

٢٥. حمدي عبد العظيم، غسل الاموال في مصر والعالم، الجريمة البيضاء، أبعادها، آثارها، كيفية معالجتها، الطبعة الاولى، القاهرة ، سنة ١٩٩٧.

٢٦. خالد المختار واسماعيل ببكر محمد، التحقيق الجنائئ فى جرائم الحاسب – دراسة سيكولوجية – اساليبه القانونية وادواته العلمية - دار عزة للنشر والتوزيع، السودان، سنة ٢٠١٠م.