الضوابط القانونية للإثبات الجنائي بالأدلة الرقمية
دراسة مقارنة

د. منصور عبد السلام عبد الحميد حسان العجيل

أستاذ القانون الجنائي المساعد– كلية الشريعة والقانون– جامعة الجوف- السعودية

مدرس بقسم القانون- الكلية التكنولوجية بجنوب الوادي- مصر

(ISSN: 2537- 0758)

الضوابط القانونية للإثبات الجنائي بالأدلة الرقمية
دراسة مقارنة

د. منصور عبد السلام عبد الحميد حسان العجيل

ملخص الدراسة:

إنَ تطور مجال المعلومات وتدخل الآلة كعنصر مهم في مختلف مجالات الحياة لم يؤدى الي تطور السوك الإجرامي فحسب بل ادى الي ظهور نمط جديد من الأدلة يعرف بالأدلة الرقمية، وتثير خصوصية هذه الادلة اشكالية القيود المتعلقة بقبولها واستخدامها، لذلك فإن القيمة لها في مجال الاثبات الجنائي تعتمد علي توافقها مع الشروط العامة التي وضعها المشرع فيما يتعلق بالأدلة بشكل عام، وتهدف هذه الدراسة الي الاجابة علي سؤال محدد حول فكرة قبول الدليل الرقمي في الاثبات الجنائي.

الكلمات المفتاحية: الدليل الرقمي– الاثبات الجنائي– اقتناع القاضي– حجية الدليل الرقمي.

Legal controls for digital forensic evidence
A comparative study

Abstract:

The evolution of information field and the intervention of the machine as an important element in various fields of life, does not only lead to the development of new forms and contents of criminal behavior. This evolution has led to the emergence of a new pattern of evidence known as digital evidence. The privacy of these evidences raise a clearly defined problematic issue in the field of criminal evidence. This problematic issue is based primarily on some restrictions set regarding the acceptance and use of the evidence. Therefore, the evidentiary value of the digital evidence in the field of criminal evidence depends on its compatibility with the general conditions developed by this system regarding evidences in general. In this context, the aim of this research is mainly to answer a specific question about the idea of accepting the digital evidence in the field of criminal evidence.

Keywords: Judge conviction- evidence electronic, legality- full authoritative.

مقدمة عامة

واكب التوسع في استخدام شبكة الإنترنت تطورا كبيرا في ظهور وسائل حديثة لارتكاب الجرائم، فظهرت نوعية جديدة من الجرائم المستحدثة يتم ارتكابها من خلال استخدام التقنيات الحديثة، أطلق عليها مسمى الجرائم المعلوماتية، ولاشك أن هذه الجرائم تتمتع بالدقة وتهدد أمن المجتمع وسلامته، ومع انتشار استخدام الإنترنت وتزايد المعلومات وأعمال التجارة الإليكترونية، وهو ما أدى إلي تزايد التهديدات وظهور أنماط جديدة من الجرائم.

ومع استفحال خطر هذه الجرائم وعدم فاعلية القوانين القائمة في مواجهتها، لاختلاف طبيعتها عن الجرائم التقليدية التي لها طبيعة محددة، وأبعاد واضحة، كان لزاماً علي الدول البحث عن كيفية مواجهتها القانونية، ولأهمية إثبات هذه الجرائم وعدم قدرة أدلة الإثبات التقليدية علي تحقيق ذلك، أصبحت الحاجة ملحة إلي إثباتها من خلال أدلة تنتمى إلي البيئة المعلوماتية نفسها، وهو ما فرضته الطبيعة الخاصة لتلك الجرائم، ولذا أصبح الإثبات بالأدلة الجنائية الرقمية من أبرز وسائل الإثبات، وهو ما يمكن تصنيفه علي أنه نوع جديد من الأدلة التي لها خصائصها وأساليب استخدامها.

وهو ما فرضته طبيعة تلك الجرائم وألقي علي عاتق القائمين علي مكافحة الجريمة عبئا شديدا لعدم ملائمة النظم التقليدية في إثبات تلك الجرائم سواءا من الناحيتين القانونية أو التقنية، ولذا كان لزاما أن يتم استحداث تشريعات تلائم هذا النوع من الجرائم، فضلا عن إنشاء أجهزة فنية متخصصة تعمل علي إثبات تلك الجرائم.

وهو ما دفع المشرع المصري إلي إصدار القانون رقم ١٧٥ لسنة ٢٠١٨م[١]، الخاص بتنظيم مكافحة الجرائم المعلوماتية وتقنية المعلومات، حيث نص من خلاله علي الجرائم المعلوماتية والعقوبات المقررة لها، كما نص علي استخدام الأدلة الجنائية الرقمية في إثبات تلك الجرائم، ونص كذلك علي أنَّ مَن يتولى استخلاص تلك الأدلة هم خبراء سواءًا كانوا من التقنين أو الفنيين التابعين للجهاز القومي للاتصالات، أو كانون خبراء "تقنين أو فنيين" من خارج الجهاز.

وبالرغم من إصدار الدول القوانين ذات الطبيعة الموضوعية، إلا أنَّ التطبيق العملي لهذه القوانين يصطدم بتحديات إجرائية قانونية تعود إلي طبيعة الجريمة، ومسرح الحادث، وهوما يزيد من صعوبة تطبيق بعض الإجراءات الجنائية "التفتيش، المعاينة،

---

[١] القانون المصري رقم ١٧٥ لسنة ٢٠١٨م، الجريدة الرسمية، العدد ٣٢ مكرر (ج)، الصادر بتاريخ ١٤ أغسطس سنة ٢٠١٨م، بشأن مكافحة الجرائم المعلوماتية وتقنية المعلومات.

(ISSN: 2537- 0758)

والضبط.....الخ" وهو ما يشكل عائقاً كبيراً أمام الاستفادة من الأدلة الجنائية الرقمية التي تثبت الواقعة أو تنفيها، وذلك نظرا لارتباط هذه الجرائم بأجهزة الحاسب الآلي وشبكة الإنترنت.

ونظرا لأهمية الموضوع التي تُعد من أهم الأسباب التي دفعتني لاختياره، ولظهور الأدلة الجنائية الرقمية والاعتداد بها كدليل في المجال الجنائي وهو ما يعد نقلة نوعية في الإثبات الجنائي، فبالرغم من اهتمام الكثير من الباحثين بدراسة الأدلة الجنائية الرقمية باعتبارها من وسائل الإثبات الحديثة، إلا أن التطور المستمر في مظاهر الحياة وعالم الجريمة يجعل منه موضوعاً متجدداً، وسوف نتناول الضوابط القانونية للأدلة الجنائية الرقمية وحجيتها في الإثبات بالتعريف والتأصيل باعتبارها أداة جديدة لمواجهة الجرائم المعلوماتية المستحدثة، كما تساعد الأدلة الجنائية الرقمية في كشف الجرائم التقليدية الغامضة بحسابات دقيقة لا يشوبها الشك.

مشكلة الدراسة:

شهدت السنوات الأخيرة ظهور نمطا جديدا للسلوك الإجرامي وهى الجرائم المعلوماتية التي شكلت تحديا جديدا في مواجهة أجهزة العدالة الجنائية، خاصة فيما يتعلق بإجراءات الضبط، وتكييف الجريمة، وإضفاء الوصف القانوني المناسب علي الوقائع التي تشكل هذه النوعية من الجرائم، ويرجع ذلك إلي الطبيعة الخاصة لهذه الجرائم.

فهذه النوعية من الجرائم تتم دائما في بيئة افتراضية تتميز بالتجدد والتغيير والانتشار الجغرافي، كما أن القدرات التخزينية في البيئة الرقمية لم تتفاعل مع القانون الجنائي، بحيث يتم فرز الملفات البريئة وتلك المجرمة والتي تعد دليلا جنائيا رقميا، فالمعلومات موجودة علي الشبكة العالمية "الإنترنت" ويتدخل فيها أشخاص ينتمون إلي دول مختلفة، فقد يكون المستخدم مقيم في دولة، ومقدم الخدمة في دولة أخرى كالشركة المختصة بتكنولوجيا معالجة البيانات وإدخالها وتحميلها عبر الشبكة. كما أن هذه الجرائم تتميز بتطورها وتجددها، وهو ما يستلزم مواجهتها بوسائل غير تقليدية.

واستجابة القواعد الإجرائية للتغيرات المستمرة التي صاحبت تغيير طريقة ارتكاب الجرائم ووسائلها والبيئة التي تتم فيها، ولاشك أن محاولة الاثبات للجرائم بالدليل الجنائي الرقمي يثير اشكالية تواجه العملية القضائية، فبكل ما يعترى تلك العملية من اشكاليات تخص اجراءات الاثبات ذاتها، ومدى قبول وحجية الدليل الرقمي، وامام اشكاليات تتعلق بالدليل الجنائي الرقمي ذاته وبمدى صحته وسلامته من التعديل، ومدى صلاحية هذا

الدليل في الاثبات الجنائي، ونظرا لأهمية مكافحة الجرائم المعلوماتية والحاجة الماسة الي الاستعانة بالأدلة الجنائية الرقمية تبرز مشكلة موضوع البحث.

أهمية الدراسة:

تكمن أهمية موضوع البحث في الطفرة الهائلة للتكنولوجيا التي صاحبت تحول الدول الي الاعتماد الكلي علي التقنية الحديثة في المعاملات والتجارة، وما ترتب علي ذلك من أثار يأتي في مقدمتها الاعتماد المتزايد علي النظام المعلوماتي وهو ما صاحبه تزايد ارتكاب الجرائم المعلوماتية، وقد أصبحت هذه الجرائم تهدد أمن وسلامة الأفراد والمؤسسات، خاصة أن المعلومات مصدرا للقوة الاقتصادية والسياسية، والعسكرية، والاجتماعية.

وهو ما أظهر الحاجة الملحة إلي مكافحة الجرائم المعلوماتية ومعاقبة مرتكبيها، وفقا لإجراءات تعتمد علي جمع الأدلة الجنائية الرقمية بشكل يساعد علي إثبات الجريمة، وبما يتناسب مع التحول الذى طرأ علي الدليل الجنائي التقليدي وهو ما أبرز الحاجة الي الاعتماد علي الأدلة الرقمية في إثبات الفعل المجرم، الذى نشأ في بيئة رقمية معقدة تتميز بالتغير والتطور المستمر وهو ما يظهر أهمية موضوع البحث.

أهداف الدراسة:

تهدف الدراسة الي تسليط الضوء علي أهمية الأدلة الجنائية الرقمية في إثبات الجرائم المعلوماتية التي تتميز بطبيعة خاصة، وتتمثل أهم أهداف الدراسة:

١- بيان ماهية الأدلة الجنائية الرقمية بما يشمل الخصائص والانواع، مع توضيح أهميتها في مواجهة الجرائم المعلوماتية في مصر والتشريعات المقارنة.
٢- إيضاح أهمية الإثبات بالأدلة الجنائية الرقمية.
٣- بيان الحجية القانونية للأدلة الرقمية في الإثبات الجنائي.
٤- تسليط الضوء علي مدى قبول الدليل الرقمي في الاثبات الجنائي.
٥- بيان مدى العمل بالدليل الرقمي في الاثبات الجنائي في التطبيق العملي بالمحاكم المصرية.
٦- توضيح ما توصلت إليه الدراسات والأبحاث الأجنبية فيما يتعلق باستخدام الأدلة الجنائية الرقمية في الإثبات.
٧- إيضاح الحماية الموضوعية والإجرائية للمعلومات الالكترونية.

التساؤلات التي تثيرها الدراسة:

يثير موضوع الدراسة عدة تساؤلات وهى:

١- هل تتميز الجريمة والمجرم المعلوماتي بسمات وخصائص خاصة؟

(ISSN: 2537- 0758)

٢- هل النصوص التقليدية قادرة علي الإيفاء بالغرض لمواجهة هذه الجرائم التي تمتاز بالتقنية الحديثة؟
٣- هل الجهات المختصة بالتحري والتفتيش قادرة علي مسايرة هذه الجرائم؟
٤- ما هو مفهوم الأدلة الجنائية الرقمية؟
٥- ما هي أهمية الإثبات بالأدلة الجنائية الرقمية؟
٦- مدى مشروعية الدليل الرقمي المستخلص من الوسائل الاليكترونية؟
٧- قيمة الدليل الرقمي في الإثبات الجنائي؟
٨- ماهي النصوص التي تتضمن الحماية الموضوعية والإجرائية للمعلومات في مصر والتشريعات المقارنة؟

منهج الدراسة:

قامت الدراسة علي عدة مناهج كالمنهج الوصفي التحليلي، من خلال الاعتماد علي تحليل القواعد القانونية والتشريعية المتعلقة بموضوع البحث، وكذلك الاعتماد علي القواعد العامة للإجراءات الجنائية، مسترشدا بآراء الفقهاء وأحكام القضاء، وكذلك المنهج الاستنباطي للبحث في القواعد والمبادئ القانونية وتطبيقات الجزئيات والفروع، بالإضافة الي استخدام المنهج المقارن وذلك للمقارنة بين التشريع المصري والتشريعات المقارنة والآراء الفقهية في المسائل محل الخلاف المتعلقة بالدليل الجنائي الرقمي.

خطة الدراسة:

قامت الدراسة علي مبحث تمهيدي وثلاثة مباحث، حيث يتناول المبحث التمهيدي تعريف الجريمة المعلوماتية وبيان صورها، أما المبحث الاول فيتناول مفهوم الدليل الجنائي الرقمي وأهميته في الاثبات الجنائي، ويتناول المبحث الثاني حجية الأدلة الجنائية الرقمية في الإثبات الجنائي في التشريع المصري والتشريعات المقارنة، ويتناول المبحث الثالث ذاتية الأدلة الجنائية الرقمية.

المبحث التمهيدي
ماهية الجريمة المعلوماتية

تمهيد وتقسيم:

تشكل الجرائم المعلوماتية خطرا كبيرا علي الجانب الاقتصادي، كما أنها تشكل تحديا لرجال الأمن والبحث الجنائي ورجال القضاء[٢]، حيث تتميز هذه الجرائم بطبيعة خاصة لكون مرتكبيها علي درجة عالية جدا من العلم والثقافة والحرفية، مما يصعب من

([2]) Carter David L and Datz A.J Computer Crime: An Emerging challenge for law Enforment " F.B,I.Law Eforcement Bulletin 1996.p.18

مواجهتهم وكشفهم وضبطهم وفقا للفكر الأمني التقليدي، وقواعد الإثبات الجنائي التقليدية، إضافة إلي ذلك تتمتع هذه الجرائم بتعدد أشكالها وصورها، وهو ما يدفعنا في هذا المبحث الي التعرض لتلك الجرائم.

وسنتناول هذا المبحث في ثلاثة مطالب، يتناول أولهما تعريف الجريمة المعلوماتية، أما المطلب الثاني فيتناول صور الجريمة المعلوماتية، بينما يتناول المطلب الأخير سمات الجريمة والمجرم المعلوماتي.

المطلب الأول
تعريف الجريمة المعلوماتية

مقدمة:

تعددت تعريفات الجريمة المعلوماتية، فجانب من الفقه عرفها كموضوع للجريمة، وعرفها جانب آخر باعتبارها وسيلة لارتكاب الجريمة وسوف نسلط الضوء علي أهم التعريفات التي تناولت الجريمة المعلوماتية، وقبل الخوض في ذلك نبدأ بتعريف الجريمة التقليدية:

الجريمة التقليدية تعرف بأنها "فعل غير مشروع صادر عن إرادة جنائية يفرض لها القانون عقوبة أو تدبيرا احترازيا"[٣]، فالجريمة وفقاً لهذا التعريف تقوم علي عدة عناصر، فلا جريمة بغير فعل مادى ظهر إلي العالم الخارجي وقام الدليل عليه من ناحية، ومن ناحية أخرى فإن الجريمة لا تقوم إلا إذا كان الفعل غير مشروع، فإذا كان الفعل مشروع فلا تتوافر الجريمة، وأخيرا تفترض الجريمة أن القانون يقرر عقوبة أو تدبيرا احترازيا علي من يرتكب الفعل[٤].

أما بخصوص الجريمة المعلوماتية فقد تعددت التعريفات بشأنها، ويرجع ذلك الي الاختلاف في وجهة النظر الفقهية التي تتناولها، وهو ما أدى إلي خلاف فقهى كبير

---

[٣] د. أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، الطبعة الخامسة، دار النهضة العربية مصر سنة ٢٠١٩ ص ٨ **للمزيد أنظر أيضا** د. محمود نجيب حسنى شرح قانون العقوبات القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدابير الاحترازية، الطبعة الثانية، دار النهضة العربية مصر سنة ٢٠١٨ ص٤٠، د. غنام محمد غنام، شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة، مكتبة المجلس الوطني الاتحادي سنة ٢٠٠٣، الإمارات ص ٩٧.

[٤] د. أشرف توفيق شمس الدين، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، مرجع سابق ص ٩.

(ISSN: 2537- 0758)

حول مفهوم الجريمة المعلوماتية والخصائص التي تتميز بها، ويمكن توضيح هذ الخلاف الفقهي من خلال المعيار أو الأساس الذى تم وضعه لتحديد تعريف هذا النوع من الجرائم:

أولا: **تعريف الجريمة المعلوماتية استناداً إلي موضوع الجريمة**:

عرف البعض الجريمة المعلوماتية وفقا لموضوعها بأنها "السلوك غير المشروع فيما يتعلق بالمعالجة الألية للبيانات"[٥]، ويري أنصار هذا الاتجاه أن الجريمة المعلوماتية ليست هي التي يكون النظام المعلوماتي أداة لارتكابها، بل هي التي تقع عليه أو في نطاقه.

وهذا الاتجاه سانده الاستاذ "روز بلات" وهو ما دفعه الي تعريف الجرائم المعلوماتية بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[٦]، وقد تم تعريف الجريمة المعلوماتية من خلال "G.O.A"[٧] بأنها الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات، من خلال إضافة أفعال تشكل جرائم أكثر تعقيدا من الناحية التقنية[٨].

وأخيراً عرفها جانب أخر من الفقه بأنها "كل فعل أو امتناع عمدى ينشأ عن نشاط غير مشروع لنسخ أو تغييرات أو حذف أو الوصول الي المعلومات المخزنة في الحاسب، أو تلك التي تحول طريقه"[٩]، ومن خلال استعراضنا للتعريفات السابقة نجد أنها عرفت الجريمة المعلوماتية اعتمادا علي السلوك الإيجابي أو السلبي الذى يقع باستخدام التقنية المعلوماتية علي مصلحة مشروعة بالاعتداء.

---

[٥] د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، ٢٠٠٦م، ص ٨٥.

[٦] د. هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، الطبعة الأولي سنة ١٩٩٢م، ص٢٤.

[٧] مكتب المحاسبة العامة بالولايات المتحدة الأمريكية.

[٨] د. كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة بتاريخ ٢٨ أكتوبر سنة ١٩٩٣م، ص ٢٧.

[٩] د. رامي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة فى ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، الطبعة الأولي، سنة ٢٠١١م، ص٥.

ثانيا: **تعريف الجريمة المعلوماتية استناداً إلي وسيلة ارتكابها**:

يعرف هذا الاتجاه الجريمة المعلوماتية بأنها "فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية"[١٠]، **وقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها** "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسياً" [١١]. وبالنظر إلي التعريفات السابقة نجد أنها تنصب علي الوسيلة التي ترتكب بواسطتها الجريمة.

ثالثا: **تعريف الجريمة المعلوماتية استناداً إلي شخص الجاني**:

تُعرف الجريمة المعلوماتية وفقاً لهذا الاتجاه بأنها "الجريمة التي تقع من فاعل له معرفة فنية بالحاسبات تمكنه من ارتكاب الجريمة"[١٢]، **كما عرفه أخرون بأنها** "الفعل غير المشروع الذى يكون الحاسوب أساساً لارتكابه والتحقيق فيه وملاحقته قضائيا"[١٣]، ولاشك أن هذا التعريف منتقد لاقتصاره علي المعيار الشخصي، وتوافر المعرفة التقنية وهو ما يجعل هذه التعريفات قاصرة عن وضع تعريف شامل لهذه الجريمة.

ونرى أن التعريف الأمثل للجريمة المعلوماتية هو الذى عرفها بأنها "الجريمة التي يمكن ارتكابها بواسطة نظام الحاسوب، وتشمل جميع الجرائم التي يمكن ارتكابها في بيئة إليكترونية"[١٤].

أطراف الجريمة المعلوماتية:

لكى تنهض الجريمة المعلوماتية لابد لها من أطراف، أي جانى يقوم بالفعل الإجرامي ومجنى عليه يلحق به الضرر.

أولاً: **الجاني** (**شخص طبيعي**):

المجرم المعلوماتي لكى يكون قادراً علي ارتكاب هذه الجريمة لابد أن يتمتع بالخبرة والدراية العملية بالحاسب الآلي، فهو بهذا المعنى لا يتصور إلا في صورة الشخص

---

[١٠] د. محمد الفيومي، مقدمة في علم الحاسبات الاليكترونية والبرمجة بلغة بيسك، دار الفرقان، عمان، الطبعة الثالثة سنة ١٩٨٩م ص ٦٠.

[١١] د. رامي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، مرجع سابق، ص٦.

[١٢] د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، سنة ٢٠٠٤م، ص ٣٤.

[١٣] د. هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق ص ٤٤.

[١٤] مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، فيينا، الفترة ١٠: ١٧ ابريل سنة ٢٠٠٠م.

(ISSN: 2537- 0758)

الطبيعي الذى يمتلك الأهلية والقدرة والقابلية لأن يكون محلاً لتوقيع الجزاء، وهو ما ينسجم مع الشخص الطبيعي دون المعنوي[١٥].

فالمجرم المعلوماتي شخصاً طبيعياً، ولا يمكن أن يكون من الأشخاص المعنوية، كما أنه يتميز بالخبرة والدراية في علوم الحاسب الآلي، سوءاً كان مستخدماً أم مبرمجاً أو حتى مجرد هاوٍ[١٦]. كما أنه يتمتع بالمهارة والذكاء والمعرفة، فهو علي قدر عالٍ من الثقافة، مما يؤهله للقدرة علي تبرير جرمه، عند شعوره بالقرب من الكشف عن جريمته[١٧]، وبإجراء البحث وجد أن معظم مرتكبي هذه الجريمة، ينتمون إلي الشباب[١٨].

ثانياً: **المجنى عليه**:

المجنى عليه في الجرائم المعلوماتية قد يكون شخصاً طبيعياً أو معنوياً، والغالب أن يكون المجنى عليه شخصاً اعتباريا كالبنوك والهيئات المالية وغيرها من الأشخاص الاعتبارية، التي تعتمد علي الحواسيب في أعمالها[١٩]، وبالرغم من أن التركيز ينصب في هذه الجرائم علي الأشخاص المعنوية إلا أنَّ ذلك لا يمنع وقوعها علي الأفراد العاديين.

خاصة عندما يكون المجنى عليه من الأشخاص الذين ينجذب إليهم الجناة، كأن يتمتع هذا الشخص بمكانة داخل المجتمع، كأصحاب الشهرة في قطاع من القطاعات الاقتصادية أو السياسية أو العسكرية أو الاجتماعية[٢٠]، وغالباً ما يكتشف المجنى

---

[١٥] د. محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية، مصر، سنة ٢٠٠٦م ص ٦٣.

[١٦] د. وليد كاصد الزيدى، القرصنة علي الإنترنت والحاسوب، القوانين المقارنة، دار أسامة للنشر، عمان، الطبعة الثالثة، سنة ٢٠٠٩م، ص ٣١.

[١٧] د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، سنة ٢٠٠٠م، ص٣١.

[١٨] د. خالد عياد الحلبي، إجراء التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن عمان، الطبعة الأولي، سنة ٢٠١١م ص٣٣.

[١٩] أ. محمد عبد الله قاسم، الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، طنطا، مصر، الطبعة الأولي، سنة ٢٠١٠م، ص ١٤٨.

[٢٠] د. محمد الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية،دراسة مقارنة دار الفكر العربي، القاهرة، الطبعة الأولي، سنة ٢٠٠٣م ص ٥٦.

عليهم هذه الجرائم بعد حصولها بفترات طويلة، الأمر الذى يدفعهم في الغالب إلي الإذعان لها، وعدم الإبلاغ عنها أو حتى التصريح بأن أجهزتهم وأنظمتهم المعلوماتية التي يفترض فيها الأمان والسرية، قد تعرضت للانتهاك والدخول غير المشروع، وهذا الموقف السلبي يعطى للجناة الفرصة لزيادة جرائمهم والاستمرار في نشاطهم الإجرامي، وهو ما يعد سبباً لتزايد معدلات ارتكاب الجرائم المعلوماتية[٢١].

المطلب الثاني
صور الجريمة المعلوماتية

مقدمة:

قبل التطرق لصور الجرائم المعلوماتية يجب أن نشير إلي أركانها، فالجرائم المعلوماتية تتطابق مع الجرائم التقليدية فهي تتكون من أركان تتصل فيما بينها، حيث أن هدم أي ركن يؤدى إلي زوال النموذج الإجرامي للفعل، و تتكون الجريمة المعلوماتية من الأركان الآتية:

الركن المادي

يتكون الركن المادي عادة من السلوك والنتيجة وعلاقة السببية[٢٢]، وهو ذاك السلوك الظاهر المحسوس للإنسان الذى ينشأ عند إحداث أثر في العالم الخارجي، ويترتب بذلك اعتداء علي مصلحة للغير يحميها القانون ويلزم إنزال العقاب بمن يلحق الضرر بها.

وعلي ذلك فالأمنيات والرغبات والنيات المستقرة داخلياً في النفس، والتي لا تفصح خارجياً عن الإخلال بالمبادئ الإنسانية، أو الاجتماعية أو الإخلال بالحقوق العامة، لا تعتبر من الجرائم المعاقب عليها.

علاقة السببية

علاقة السببية هي الصلة بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذى أدى إلي حدوث النتيجة، فالفعل شرط لوقوع الجريمة المعلوماتية مما يعنى بأن إسناد النتيجة

---

[٢١] د. محمد سليمان الخوالدة، جريمة الدخول غير المشروع إلي موقع الكترونى أو نظام معلوماتي وفق التشريع الأردني، دراسة مقارنة، دار الثقافة، الطبعة الأولي، عمان، الأردن، سنة ٢٠١٢م ص٥٠.

[٢٢] د. علي عبد القادر القهوجي، الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، خلال الفترة من ٢٦: ٢٨ أبريل، سنة ٢٠٠٣م، ص٩٨.

(ISSN: 2537- 0758)

إلي الفعل هو شرط أساسي لتقرير المسؤولية، وتُحقق علاقة السببية تلازماً ماديا بين الفعل والنتيجة وهو ما يؤدى إلي وحدة الركن المادي[٢٣].

الركن المعنوي للجريمة المعلوماتية

الركن المعنوي للجريمة المعلوماتية هو الوجه الباطني أو النفسي للسلوك الإجرامي الذى لا يتعدى نسبة هذا السلوك إلي صاحبه، فهو الرابطة النفسية بين الفعل والجاني، فالجاني عندما يرتكب الجريمة المعلوماتية يجب أن تتوافر العلاقة النفسية بينه وبين الفعل في صورة عناصر السلوك المادي، وأن تتوافر إرادة متجهة نحو ارتكاب الفعل المجرم.

فهذه الجرائم عمدية يجب أن يتوافر فيها القصد الجنائي[٢٤]، فالجاني عند دخوله إلي موقع أو نظام ليحذف بيانات أو معلومات، أو ليفشي أسرار، أو ليطلع علي بيانات ليس له الحق في الاطلاع عليها، يجب أن يكون عالماً ومريداً لسلوكه والنتائج المترتبة علي هذا السلوك وهوما يجعله خاضعاً للمسؤولية الجنائية.

صور الجرائم المعلوماتية:

تتعدد صور الجرائم المعلوماتية فمنها ما يتعلق بالاستيلاء علي البينات الموجودة بالحواسيب الآلية، ومنها ما يتصل بعمليات اختراق الحواسيب بشكل غير قانوني.

ومنها ما يعد انتهاكا للخصوصية، وقد أحسن المشرع المصري عندما نص عليها في قانون مكافحة الجرائم المعلوماتية وتقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م، وسوف نتعرض لبعض هذه الصور في النقاط التالية:

أولا: الاستيلاء علي البيانات المخزنة علي الحاسوب بشكل غير قانونيا.

تتمثل هذه الجريمة في سرقة المعلومات والبيانات بصورة غير شرعية، أو نسخ برامج بصورة غير مشروعة، أو الدخول إلي حسابات بعض المنظمات بهدف الاطلاع علي معلومات يجرم القانون الاطلاع عليها، أو التلاعب بقيود المصارف أو المؤسسات المالية، بهدف الإضرار بمصالح البلاد.

---

[٢٣] د. محمود نجيب حسنى علاقة السببية في قانون العقوبات، دار النهضة العربية، القاهرة، سنة ١٩٨٣م، ص٦.

[٢٤] د. أشرف شمس الدين توفيق، شرح قانون العقوبات، القسم العام، مرجع سابق، ص ٦٥.

ثانيا: **جرائم اختراق الحاسوب بطريقة غير قانونية**:

تتمثل هذه الجريمة في قيام الجاني باختراق الحاسوب لتدمير البرامج والبيانات والمعلومات المخزنة به من خلال الفيروسات الإليكترونية، التي تعمل علي تدمير البيانات والبرامج المخزنة علي الحاسوب، أو تقليل كفاءة أداء النظام[٢٥].

ثالثا: **استخدام الحاسوب في الجرائم التقليدية**:

قد يتم استخدام الحاسوب في الجرائم التقليدية، كالتهديد بالقتل، وجرائم السب والقذف[٢٦]، وكذلك جرائم تزييف العملات، أو قد تستخدم المعلومات المخزنة عليه في الجرائم الإرهابية.

أو تزوير المحررات الرسمية أو العرفية، وقد يستخدم في جرائم غسل الأموال، وجرائم الاحتيال بواسطة البريد الإليكتروني.

رابعا: **جرائم انتهاك الخصوصية**:

تعد جريمة إنتهاك الخصوصية هي الأوسع انتشارا بين الجرائم المعلوماتية، كجرائم انتهاك حرمة وخصوصية البيانات والمعلومات الشخصية، كذلك الجرائم المخلة بالآداب العامة، كجرائم الاستغلال الجنسي والتجاري للأطفال[٢٧].

---

[٢٥] د. حسام الدين الأهونى، د. جميل عبد الباقي الصغير، مقدمة في الحاسب الألي "دراسة عملية ونظرية"، دار النهضة العربية، مصر، سنة ٢٠٠٠م ص١٩٧.

[٢٦] **الطعن رقم ٤ لسنة ٢٠٢٠ قضائية، جلسة ٢٠٢٠/١٠/٢٤ م حيث أكدت محكمة النقض المصرية علي أنه** "ومن حيث إنه يبين من الاطلاع علي الأوراق أن الدعوى الجنائية رفعت ابتداء علي المتهم بطريق الادعاء المباشر أمام محكمة جنح كرموز بوصف تعدى بالسب والقذف علي المدعية بالحقوق المدنية عن طريق شبكة المعلومات الدولية "الانترنت" وعبر المحادثات الالكترونية (تطبيق الواتس آب)"، وإذا كانت واقعة الدعوى الجنائية تشكل جنحة تعمد الازعاج والمضايقة بإساءة استعمال أجهزة الاتصالات كما تشكل جنحة القذف والسب والمعاقب عليهما بالمواد ٣/١، ٧٠، ٢/٧٦ من القانون رقم ١٠ لسنة ٢٠٠٣م بشأن تنظيم الاتصالات، والمواد ١/٣٠٢، ١/٣٠٣، ٣٠٦ من قانون العقوبات المصري.

[٢٧] د. رامي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة مرجع سابق، ص١٢٠.

(ISSN: 2537- 0758)

خامسا: **جرائم الاعتداء علي سلامة شبكات وأنظمة وتقنيات المعلومات، وجريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها**[٢٨]:

المشرع المصري جعل الانتفاع بخدمة الاتصالات أو أي خدمة من خدمات قنوات البث المسموع أو المرئي جريمة معلوماتية يعاقب عليها بالحبس والغرامة.

سادسا: **جريمة تجاوز حدود الحق في الدخول**:

فكل من دخل الي موقع أو حساب خاص أو نظام معلوماتي، وتعدى الحق المخول له من حيث الزمان ومستوى الدخول يعد مرتكباً لجريمة معلوماتية، سواءاً كان الدخول الي الموقع المعتدى عليه عمداً أو خطأ غير عمدى، فإذا استمر المعتدى بدون وجه حق علي موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه كان مرتكباً لجريمة يعاقب عليها القانون.

سابعا: **جريمة الاعتراض غير المشروع**:

تعد جريمة اعتراض المعلومات أو البيانات أو ما يتم تداوله علي الشبكة المعلوماتية أو أحد أجهزة الحاسب الألي من الجرائم المعلوماتية التي يعاقب عليها المشرع المصري[٢٩].

فكل من اعترض بدون وجه حق أي معلومات أو بيانات، أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

ثامنا: **جريمة الاعتداء علي البريد الإلكتروني**:

فالجاني في هذه الجريمة يقوم بالاعتداء علي بريد الكتر ونى أو موقع أو حساب سواءًا كان ذلك مملوكا لأحد الأفراد أو مملوكا لأحد الأشخاص الاعتبارية الخاصة، فإذا وقع الاعتداء علي بريد إلكتروني أو موقع أو حساب خاص بأحد الأفراد.

فإن المشرع المصري قد نص علي أن عقوبة هذا الاعتداء هي الحبس مدة لا تقل عن شهر، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تزيد عن مائة ألف جنيه، أما في حالة الاعتداء علي بريدا الكترونيا أو موقعاً أو حساباً خاصاً بأحد الأشخاص

---

[٢٨] المادة (١١)، القانون المصري بشأن مكافحة الجرائم المعلوماتية وتقنية المعلومات، رقم ١٧٥ لسنة ٢٠١٨م، الجريدة الرسمية، العدد ٣٢ مكرر (ج)، ١٤ أغسطس سنة ٢٠١٨.

[٢٩] المادة (١٦)، القانون المصري بشأن مكافحة الجرائم المعلوماتية وتقنية المعلومات، رقم ١٧٥ لسنة ٢٠١٨م.

الاعتبارية الخاصة، فإنه يتم تشديد العقوبة حيث تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين.

تاسعاً: **الاعتداء علي تصميم موقع**:

تعد جريمة إتلاف أو تعطيل أو إبطاء أو تشويه أو إخفاء أو تغيير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير حق، جريمة معلوماتية يعاقب عليها المشرع المصري بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه، ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

عاشراً: **بيع أو جلب أو حيازة الأجهزة أو المعدات أو البرامج المصممة بدون تصريح أو مسوغا قانونيا**:

هذه الجريمة تتمثل في حيازة أو إحراز أو جلب أو بيع أو تصنيع أو استيراد أو تصدير أو تداول الأجهزة أو المعدات أو الأدوات أو البرامج المصممة أو المطورة، كذلك من استخدم الشفرات والأكواب الخاصة بالمرور أو الرموز أو أي بيانات مماثلة بدون تصريح من الجهاز القومي للاتصالات أو لم يكن لذلك مسوغاً قانونياً.

إذا كان ذلك بغرض استخدامها في ارتكاب أو تسهيل إرتكاب أي من الجرائم المعلوماتية، أو كان الهدف من استخدامها إخفاء آثار الجريمة المرتكبة أو للتخلص من الأدلة الجنائية الرقمية التي من الممكن أن تسهم في التوصل إلي مرتكب الجريمة، ويعاقب الجاني في هذه الحالة بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه مصري.

الحادي عشر: **الاعتداء علي أرقام أو بيانات بطاقات البنوك**:

الجاني في هذه الجريمة يقوم باستخدام الشبكة المعلوماتية للاعتداء بدون وجه حق علي أرقام أو بيانات بطاقات البنوك والخدمات أو غير ذلك من أدوات الدفع الإلكتروني، ويعاقب المشرع المصري علي هذه الجريمة بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسون ألف جنيه أو بإحدى هاتين العقوبتين.

أما إذا كان الغرض من هذا الاعتداء هو الحصول علي أموال الغير فإن العقوبة تُشدد، فيعاقب الجاني في هذه الحالة بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين. أما إذا توصل الجاني إلي الاستيلاء لنفسه أو لغيره علي تلك الخدمات أو الأموال فإن العقوبة

(ISSN: 2537- 0758)

تزيد إلي الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين.

الثاني عشر: إنشاء موقع أو حساب لتسهيل ارتكاب الجرائم المعلوماتية:

تتجلي هذه الجريمة في قيام أحد الأشخاص بإنشاء موقعاً أو حساباً خاصاً علي الشبكة المعلوماتية، بغرض ارتكاب أو تسهيل ارتكاب جريمة من الجرائم المعلوماتية التي يعاقب عليها القانون، وتكون العقوبة في هذه الحالة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد علي ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين.

المطلب الثالث
سمات الجريمة والمجرم المعلوماتي

مقدمة:

تتمتع الجريمة المعلوماتية بطبيعة قانونية خاصة، تميزها عن غيرها من الجرائم التقليدية، ونتيجة لذلك أصبحت تكتسب خصوصية غير عادية إذا ما قارناها بالجرائم التقليدية كما أن المجرم القائم بها يكون علي درجة عالية من العلم، وهو ما يدعونا إلي التعرف علي السمات التي تتميز بها الجرائم المعلوماتية، وكذا السمات التي تتوافر في المجرم المعلوماتي، **وهو ما نتناوله علي النحو التالي:**

اولاً: سمات الجريمة المعلوماتية:

١- صعوبة اكتشافها:

تتميز هذه الجرائم بصعوبة تعقبها واكتشافها، فإذا كانت الجرائم التقليدية تترك خلفها أثارا خاصة، فإن ذلك غير متوفر في إطار الجريمة المعلوماتية فهي تتركز علي تغيير أو تعديل أو مسح البيانات كليا أو جزئيا من خلال الدخول إلي السجلات المخزنة في ذاكرة الحاسب الآلي، الأمر الذى يجعل إمكانية اكتشافها تكتنفه الصعوبة[٣٠].

فالجناة يتميزون بالذكاء والإتقان الفني للعمل الذى يقومون به، والذى يتميز بالطبيعة الفنية، ولذلك فإنهم يتمكنون من إخفاء الأفعال غير المشروعة التي يقومون بها أثناء تشغيلهم لهذه الوسائل الإلكترونية، ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات من خلالها[٣١].

---

[٣٠] د. شمس الدين إبراهيم أحمد، وسائل الاعتداء علي الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، دراسة مقارنة، دار النهضة العربية، القاهرة، ط١، سنة ٢٠٠٥م، ص١٠٤.

[٣١] د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ص ١٦.

ومما يزيد من صعوبة العثور علي الأدلة الناجمة عن الجرائم المعلوماتية، سهولة إخفائها، حيث يمكن محو الدليل في زمن قصير، فالجاني يستطيع أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جداً، بحيث لا تتمكن السلطات من كشف الجريمة، كذلك يساعد المجنى عليهم في إخفاء الجريمة المعلوماتية، عن طريق امتناعهم عن تقديم الأدلة التي تكون بحوزتهم عن هذه الجرائم، وقد يرجع ذلك إلي رغبتهم في استقرار حركة التعامل الاقتصادي بالنسبة لهم، أو رغبتهم في إخفاء الأسلوب الذى ارتكبت به الجريمة، لكى لا تعلن للآخرين[٣٢].

٢- عدم وجود أثر مادى لتلك الجرائم:

هذا النوع من الجرائم لا يترك أثر خارجي ومرئي، فهي تتم بشكل خفى لا يلاحظه المجنى عليه، كما أن الجاني يعمل علي حجب السلوك المكون لها بحكم الخبرة والمعرفة التي يتمتع بها، مما يجعل من إثباتها وفقاً للطرق التقليدية في الإثبات تكتنفه الصعوبات[٣٣]، فالجرائم المعلوماتية " كالجرائم علي عمليات التجارة، والجرائم المتعلقة بعمليات الصرافة، والجرائم المتعقلة بأعمال الحكومة الإلكترونية " قد يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات[٣٤].

مما قد يصعب معه إقامة الدليل بالنسبة لها بسب الطبيعة المعنوية للمحل الذى وقعت عليه الجريمة المعلوماتية، كما أن الجرائم التي ترتكب علي العمليات الإلكترونية والتي تعتمد في موضوعها علي التشفير، والأكواد السرية، والنبضات، والأرقام، والتخزين الإلكتروني يصعب معه أن تخلف ورائها أدلة مرئية يستدل من خلالها علي الجناة.

٣- اتساع نطاق تلك الجرائم:

يطلق علي الجرائم المعلوماتية "جرائم عابرة للدول" أو جرائم غير وطنية، فقد تكون الجريمة المعلوماتية شاملة لأكثر من دولة، حيث تتسع إمكانية الاتصالات الإلكترونية بخلاف الجريمة التقليدية التي تتم في نطاق محدد، وتعتبر الجريمة المعلوماتية من الجرائم العابرة للحدود.

---

[٣٢] د. زكى أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، سنة ١٩٩٥م ص٤٧٦.

[٣٣] د. هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق١٦.

[34] Manfred Mohrenschlager Compouter crimes and other crimes against information technology in Germany Rev.Inter.De.Pen.1993.p351.

(ISSN: 2537- 0758)

فمن السهولة ارتكابها ليس فقط داخل حدود الدولة بل وعلي المستوى الدولي أيضاً، وحتى الآن لا يوجد اتفاق بين الدول علي مفهوم عام لهذه الجرائم[٣٥]، ويرجع ذلك لعدم التناسق بين قوانين الإجراءات الجنائية للدول المختلفة، خاصة فيما يتعلق بالتحري والتحقيق في هذه الجرائم، وهو ما يتطلب تتبع الاتصالات الإلكترونية عن طريق سلطات التحقيق لإقامة الدليل علي تلك الجرائم التي ترتكب في مجال الإنترنت[٣٦].

ولاشك أن اختلاف التشريعات فيما بينها وبخاصة فيما يتعلق بشروط قبولها للأدلة يؤدى لظهور العديد من المشكلات التي قد تعوق اتخاذ الإجراءات اللازمة لمواجهتها، فمازالت إجراءات البحث عن هذه الجرائم وضبطها تتم في إطار النصوص الإجرائية التقليدية التي تنص عليها القوانين العقابية، الأمر الذى ستترتب عليه الكثير من المشكلات بالنسبة لضبط هذه الجرائم المستجدة ذات الكيان المعنوي والتي تتعدد أماكن ارتكابها داخل الدولة الواحدة، أوقد يمتد نطاقها ليشمل العديد من الدول عبر شبكة الإنترنت، فيتعذر تبعاً لذلك اتخاذ إجراءات جمع الأدلة بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات[٣٧].

ثانيا: **سمات الجاني**:

يمكن أن نستخلص مجموعة من السمات التي يتميز بها المجرم المعلوماتي، والتي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين، فالمجرم المعلوماتي يتميز ببعض الصفات الخاصة، إلا أنه في الوقت ذاته لا يخرج عن كونه مرتكباً لفعل إجرامي يتطلب توقيع العقاب علية، وسوف نتعرض لبعض السمات التي يتميز بها، والتي تميزه في الغالب عن غيره من المجرمين التقليدين:

١- مجرم ذو مهارات عالية في مجال الحاسوب:

المجرم المعلوماتي يتمتع بمهارات تقنية عالية ودراية بأنظمة الحاسوب، وقد تبين في عديد من القضايا أنّ عدداً من المجرمين لا يرتكبون سوي جرائم الحاسب الآلي.

---

[٣٥] د. رامي القاضي، الجرائم المعلوماتية، مرجع سابق ص٨.

[٣٦] د. عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الألي، دار النهضة العربية للطباعة والنشر، القاهرة، الطبعة الثانية سنة ٢٠٠٦، ص٢٦٢.

[٣٧] د. جميل الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، الطبعة الاولي، سنة الشر ١٩٩٨م، ص ٤.

أي أنهم يتخصصون في هذا النوع من الجرائم دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأُخرى، مما يؤكد أن المجرم الذى يرتكب الجرائم المعلوماتية، هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

٢- العود الي الإجرام:

يتميز المجرم المعلوماتي بالعود، فالكثيرون منهم يعودون إلي ارتكاب الجرائم في مجال الكمبيوتر لسد الثغرات التي قد تؤدى إلي التعرف عليهم أو التي أدت إلي تقديمهم للمحاكمة، ويؤدى ذلك إلي العود إلي مسرح الجريمة لإخفاء الأدلة أو تدميرها.

٣- يتميز المجرم المعلوماتي بالذكاء العقلي والمعرفة:

المجرم المعلوماتي يتمتع باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الحاسب الآلي الأمر الذى يتطلب الكثير من الدقة، والتخصص، والاحترافية في هذا المجال، لكى يستطيع التغلب علي العقبات التي أنشأها المتخصصون لحماية أنظمة الحاسب، كما في حالة البنوك، والمؤسسات التجارية، والمؤسسات العسكرية.

٤- متكيف مع المجتمع:

المجرم المعلوماتي مجرم غير عنيف فهو لا يلجأ إلي العنف في تنفيذ جرائمه، حيث يتمتع بقدر كبير من الذكاء مما يساعده علي التكيف في المجتمع، فهو مسالم لا يدخل في عداء مع المحيطين به، بخلاف المجرم في الجرائم التقليدية[٣٨].

٥- المهارة:

يتطلب تنفيذ الجريمة المعلوماتية، قدراً من المهارة، والتي قد يكتسبها الجاني عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال الحاسب الآلي، أو بمجرد التفاعل مع الآخرين، وهذه ليست قاعدة وهو ما أثبته الواقع العملي، حيث تبين أن جانب من أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لإرتكاب هذا النوع من الإجرام.

٦- المعرفة:

المجرم المعلوماتي يستطيع أن يُكون تصوراً كاملاً لجريمته، ويرجع ذلك إلي أن المسرح الذى تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته علي أنظمة مماثلة وذلك قبل تنفيذ الجريمة.

---

[٣٨] د. محمد عبد الله قاسم، الحماية الجنائية للمعلومات الالكترونية، مرجع سابق، ص١٤٨.

(ISSN: 2537- 0758)

٧- الوسيلة:

الوسيلة التي يستخدمها المجرم المعلوماتي، قد تكون في الغالب وسائل بسيطة وسهلة الحصول عليها، خصوصاً إذا كان النظام الذى يعمل به من الأنظمة الشائعة، أما إذا كان النظام من الأنظمة غير المألوفة فتكون هذه الوسائل معقدة وعلي قدر من الصعوبة.

٨- السلطة:

قد يكون لمجرمي المعلوماتية سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلي النظام الذى يحتوى علي المعلومات، أو قد تكون السلطة أيضاً حق للجاني في الدخول إلي الحاسب الآلي وإجراء المعاملات، وقد تكون شرعية أو غير شرعية، كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

٩- الباعث:

الباعث هو الهدف الذى يسعى إليه المجرم المعلوماتي، وبمطالعة العديد من هذه الجرائم، وجدنا أن الباعث الأول وراء ارتكابها هو تحقيق الربح المادي، إلا أنه لا يعد هو الباعث الاوحد، فقد يكون الهدف من هذه الجرائم الاستغلال الجنسي أو إفشاء الأسرار الاقتصادية أو العسكرية....إلخ.

المبحث الأول
مفهوم الدليل الجنائي الرقمي

الدليل عند أهل اللغة:

عرف أهل اللغة الدليل بأنه "المرشد، أو الكاشف، وما يتم به الإرشاد، وما يستدل به، ويجمع علي أدلة"[٣٩]، **أما في الاصطلاح القانوني فيقصد بالدليل** "الوسيلة التي يستعين بها القاضي للوصول للحقيقة التي ينشدها" ويعتبر الإثبات أكثر عمومية من الدليل فيشمل "مجموعة الإجراءات الشكلية والموضوعية والقواعد اللازمة لكشف الحقائق وتحقيق العدالة".

وعرف البعض الدليل بأنه "كل ما يفيد في إثبات أو نفى مسألة معينة في القضية، أو كل ما يتصل اتصالا مباشرا بإدانة المتهم أو تبرئته استنادا إلي المنطق"[٤٠]. **وعرفه**

---

[٣٩] د. جميل صليبا، المعجم الفلسفي، دار الكتاب، الطبعة الأولي، سنة ١٩٧٠م، ص٢٣

[40] Charless R.Swanson, Neil Chamelin and Leonard Territo, Criminal Investigation (7th, ed.) London: Graw Hill, 2000, p.658.

آخرون بأنه "الوسيلة التي يستعين بها القاضي للوصول الي الحقيقة التي ينشدها"[٤١]، **كما عرفه البعض الأخر بأنه** "عملية الإقناع بأن واقعة حصلت أو لم تحصل بناءاً علي حصول أو وجود واقعة مادية ماضية أو حاضرة أو تقرير واقعة أو وقائع"[٤٢]، **وأخيراً عُرف الدليل بأنه** "إقامة الدليل لدى السلطات المختصة علي حقيقة واقعية ذات أهمية قانونية وذلك بالطرق التي حددها القانون وفقاً للقواعد التي أخضعها لها"[٤٣].

وتأسيسا علي ما تقدم من تعريفات الفقهاء للدليل يمكننا أن نعرفه بأنه "**كل ما يمكن الحصول عليه من معلومات، ويمكن الاستعانة بها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات صحة الواقعة أو نفيها**".

وسوف نتناول في هذا المبحث تعريف الدليل الجنائي الرقمي من خلال المطلبين التاليين:

المطلب الأول: تعريف الدليل الجنائي الرقمي.

المطلب الثاني: أهمية الدليل الجنائي الرقمي في الإثبات الجنائي.

المطلب الأول
تعريف الدليل الجنائي الرقمي

أصل مصطلح الرقمية (Digittal) يعود الي استخدام النظام الرقمي الثنائي (٠،١) وهى الصيغة التي تسجل بها البيانات (أشكال وحروف ورموز وغيرها) داخل الحاسب الآلي، حيث يمثل الصفر وضع الاغلاق (off)، ويمثل رقم (١) وضع التشغيل (on)، ويعرف الرقم (٠)، أو (١) بـ(Byte)[٤٤].

---

[٤١] د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثانية، سنة ٢٠٠٦م ص ٤١٨.

[٤٢] د. محمود نجيب حسنى، شرح قانون الإجراءات الجنائية، وفقا لأحدث التعديلات التشريعية دار النهضة العربية، القاهرة سنة ٢٠١٩ م، ص٤١٧.

[٤٣] د. محمد محى الدين عوض، القانون الجنائي، مبادئه الاساسية ونظرياته العامة دراسة مقارنة، مطبعة دار النهضة العربية، القاهرة، سنة ١٩٨١م ص ٤٥٦.

[٤٤] د. عبد الناصر محمد محمود، محمد عبيد سيف سعيد، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الاول لعلوم الادلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الامنية، الرياض، سنة ٢٠٠٧م، ص١١.

(ISSN: 2537- 0758)

وقد عرف المشروع المصري الدليل الرقمي بأنه "أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج تكنولوجية خاصة"[٤٥]، ووفقاً لهذا التعريف فقد اعتبر المشرع المصري الأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الالكترونية أو من النظام المعلوماتي أو من برامج الحاسب.

أو من أي وسيلة لتقنية المعلومات لها حجية الأدلة الجنائية المادية في الإثبات الجنائي، بشرط توافر الشروط المنصوص عليها، وهو ما أكدته محكمة النقض المصرية بقولها أن البريد الإلكتروني (E-MAIL) electronic mail هو وسيلة لتبادل الرسائل الالكترونية بين الاشخاص الذين يستخدمون الأجهزة الالكترونية من أجهزة كمبيوتر أو هواتف محمولة أو غيرها.

تتميز بوصول الرسائل الي المرسل اليهم في وقت معاصر لا رسالها من مُرسلها أو بعد برهة وجيزة، عن طريق شبكة المعلومات الدولية (الانترنت) أيًا كانت وسيلة طباعة مستخرج منها في مكان تلقي الرسالة، وسواءً اشتملت هذه الرسائل علي مستندات أو ملفات مرفقة attachments أم لا. ولقد أجازت القوانين الوطنية والاتفاقيات الدولية للقاضي استخلاص واقعتي الايجاب والقبول– في حالة التعاقد الإلكتروني– من واقع الرسائل الالكترونية دون حاجة لأن تكون مفرغة كتابياً في ورقة موقعة من طرفيها[٤٦].

وقد عرف بعض الفقهاء الدليل الجنائي الرقمي بأنه "الدليل الذى يجد له أساساً في العالم الافتراضي، ويقود الجريمة، وهو ذلك الجزء المؤسس علي الاستعانة بتقنية المعالجة التقنية للمعلومات، والذى يؤدى إلي إقناع قاضى الموضوع بثبوت ارتكاب شخص ما لجريمة الإنترنت"[٤٧].

كم عرف البعض الدليل الرقمي بأنه "البيانات المخزنة في أجهزة الحاسب الآلي وملحقاتها، أو المنقولة عبر شبكات الاتصال التي يمكن أن تكشف وقوع جريمة أو تثبت

---

[٤٥] الاحكام العامة المادة (١)، القانون المصري بشأن مكافحة الجرائم المعلوماتية وتقنية المعلومات، رقم ١٧٥ لسنة ٢٠١٨م، الجريدة الرسمية، العدد ٣٢ مكرر (ج)، ١٤ أغسطس سنة ٢٠١٨.

[٤٦] الطعن رقم ١٧٦٨٩ لسنة ٨٩ ق– جلسة ٢٠٢٠/٣/١٠م.

[٤٧] د. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر العربي، الاسكندرية، سنة ٢٠١٩، ص١٧٧.

وجود علاقة بين الجريمة والجاني أو الجريمة والمتضرر"[٤٨]، **وعرف الأستاذ (Eoghan Casey) الدليل الرقمي بأنه** "كافة البيانات الرقمية التي تستخدم في إثبات الجريمة المرتكبة، أو توضح العلاقة بين الجريمة والجاني، أو توجد علاقة بين الجريمة والمضرور"[٤٩].

وعرف التقرير الأمريكي المقدم الي ندوة الإنتربول العلمية الدليل الرقمي بأنه "بيانات يمكن إعدادها وتراسلها وتخزينها رقميا بحيث تمكن الحاسوب من تأدية مهمة ما"[٥٠]، **وذهب جانب آخر من الفقهاء إلي تعريف الدليل الرقمي بأنه** "الدليل المشتق بواسطة النظم البرامجية المعلوماتية الحاسوبية ومعدات وأدوات الحاسب الألي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، يتم تقديمها للقضاء، بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها"[٥١].

كما عُرف الدليل الرقمي بأنه "الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجمعيها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، لتظهر في شكل صور أو تسجيلات صوتية أو مرئية"[٥٢]، **وعلي ذلك فالدليل الرقمي**، ما هو إلا مرحلة متقدمة من الأدلة المادية الملموسة، التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان من خلال الاستعانة بجميع ما يبتكره العلم من أجهزة مخبرية.

---

[٤٨] د. محمد أمين البشري، الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، مجلد ١٧، العدد ٣٣، أبريل ٢٠١٢م ص٥٦.

[49] Eoghan Casey, Digital Evidence and Computer Crime, London: Academic Press, 2000, p.260.

[٥٠] د. عمر محمد بن يونس، الدليل الرقمي، دار النهضة العربية للطباعة والنشر، القاهرة، سنة ٢٠٠٨م، ص ٢٥.

[٥١] د. عبد الناصر محمد فرغلي، د. محمد عبيد سيف سعيد، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة مرجع سابق، ص١٣.

[٥٢] د. سوزان نور علي محمد، الإثبات في جرائم الإنترنت في القانون العراقي المقارن، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، سنة ٢٠١٥م، ص٥.

(ISSN: 2537- 0758)

ووسائل التقنية العالية ومنها الحاسوب محور الأدلة الرقمية، فهي لا تختلف عن آثار الأسلحة والبصمات أو البصمة الوراثية D.N.A[٥٣]، وتتميز هذه الأدلة بأنها نوع متميز من وسائل الإثبات، ولها من الخصائص العلمية والمواصفات القانونية ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية[٥٤]، فالدليل الجنائي الرقمي يعتمد علي استخدام كافة المعلومات والبيانات الحسابية المخزنة في أجهزة الحاسبات الآلية وملحقاتها.

وشبكات الاتصال، بشرط أن يتم الحصول عليها بإجراءات قانونية وعلمية تضمن سلامة ووضوح تلك البيانات، بحيث يمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات الواقعة، أو إثبات العلاقة بين الجريمة والجاني أو المجنى عليه.

مميزات الدليل الجنائي الرقمي عن الدليل التقليدي:

الدليل الرقمي دليل علمي:

فالعلم هو المحرك الرئيسي للأساليب التي تولد المزيد من خيوط التحقيق والوقائع من الأدلة، فهذه الأدلة عبارة عن دوائر مغناطيسية، ونبضات كهربائية غير ملموسة، ولا يدركها الرجل العادي بالحواس الطبيعية للإنسان، فالدليل الرقمي هو الواقعة التي تنبيئ عن وقوع جريمة، وهى واقعة مبناها علمي، فالعالم الرقمي هو مبنى علمي شيده التقنيين، وهو ما يحيطه بخاصية أنه لا يمكن الاطلاع عليه او التعرف علي فحواه بدون أساليب التقنية العلمية الحديثة، كما يوجب علي رجال الضبط والاستدلال وسلطات التحقيق أن يتخذوا عند البحث عن الادلة الرقمية أسس علمية، ووسائل تقنية تمكنهم من بناء مسرح الجريمة المعلوماتية[٥٥].

الدليل الرقمي نابع من بيئته التقنية:

الدليل الرقمي يختلف عن الدليل العادي، فهو ينتج في بيئة التقنية في شكل (نبضات رقمية تشكل قيمتها في امكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب علي أية حال يكون عليها)، فهذه البيئة تتطور بطبيعتها تطورا هائلاً، ويجب أن تكون الأدلة مسايرة لهذا التطور والتجدد، وعلي ذلك يجب أن يكون متوافقاً مع البيئة التي يعيش فيها، فالأدلة الرقمية تصل إلي درجة التخيلية في شكلها وحجمها ومكان وجودها غير معين.

---

(53) Eoghan Casey, Digital Evidence Op. Cit p.,5.

[٥٤] د. محمد أمين البشري، الأدلة الجنائية الرقمية، مرجع سابق، ص٢١.

[٥٥] د. عمر محمد بن يونس، الدليل الرقمي، مرجع سابق ص ٤٢.

وتأسيساً علي ما سبق يمكننا القول بأنه لا وجود للدليل الرقمي خارج بيئته، وانما يجب أن يستخلص أو يستنبط من البيئة التي نشأ بها وهى البيئة الرقمية، ونتيجة للطبيعة الخاصة التي تتمتع بها فإنها تتميز عن الادلة التقليدية من حيث القابلية للنسخ، فيمكن استخراج نسخ للأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهو مالا يتوافر في الأدلة بشكلها التقليدي.

وهو ما يشكل ضمانة لحفظ هذه الأدلة من الفقد أو العبث بها أو التلف، وكذلك يمكن التعرف علي ما اذا كانت هذه الادلة قد تم اتلافها أو تعديلها أو تغييرها من خلال مقارنتها بالأصل عن طريق استخدام التقنيات الحديثة من تطبيقات وبرامج[٥٦].

الدليل الجنائي الرقمي قد يتخذ أشكال عدة:

الدليل الرقمي قد يتخذ أشكال مختلفة حيث أن عبارة الدليل الرقمي شاملة كافة البيانات الرقمية التي يمكن تداولها، وهو ما يمكن الاستفادة منه من خلال تكوين رابطة بين الجريمة وهذه البيانات تتصل بالضحية علي النحو الذى يمكن من معرفة الجاني، فقد يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل، كما في حالة المراقبة عبر الشبكات أو الخوادم، وقد يتخذ شكلا مفهوما كما لو كان وثيقة معدة بنظام المعالجة الآلية للعبارات، كما أن الدليل الجنائي الرقمي قد يتخذ صورة ثابتة أو متحركة أو معدة بنظام التسجيل السمعي المرئي أو تكون مخزنة في email[٥٧].

الدليل الجنائي الرقمي لا يمكن التخلص منه:

يصعب التخلص من الأدلة الجنائية الرقمية، فعندما يتم حذف البيانات أو المعلومات من علي الحاسوب فإنه يمكن استردادها مرة أخرى فالمساحة التي كانت تشغلها هذه البيانات وتلك المعلومات مازالت متاحة وموجودة، فإذا لم يتم شغل هذه المساحة ببيانات أخرى فإنه يمكن استرداد ما حذف عن طريق برامج أو تطبيقات مخصصة لذلك، فالدليل الجنائي الرقمي يمكن استرجاعه في حالة التخلص منه من خلال برمجيات يمكن بمقتضاها استرداد كافة الملفات التي تم إزالتها من الحاسب الآلي.

وبذلك يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها[٥٨]، فيمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل، ولها ذات القيمة العلمية والحجية الثبوتية، وهو ما لا يتوافر في الأدلة التقليدية.

---

[٥٦] د. عمر محمد بن يونس، الدليل الرقمي، مرجع سابق ص ٤٢.

[٥٧] د. ناصر بن محمد بن مجول البقمي، أهمية الأدلة الرقمية في الإثبات الجنائي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، سنة ٢٠١٢م، ص٥٦.

[٥٨] د. حسين بن سعيد الغافرى، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، سنة ٢٠٠٩م، ص ٥٣٢.

(ISSN: 2537- 0758)

يتحدد الدليل الجنائي الرقمي بمساعدة العلوم الأخرى:

الدليل الجنائي الرقمي له علاقة وثيقة بالعلوم الأخرى، والتي تساعد بدورها علي استخلاص الأدلة الرقمية وتشمل هذه العلوم، علوم الحاسب التي تقدم المعلومات التكنولوجية الدقيقة.

وكذلك علوم الأدلة الجنائية التي من شأنها أن تقدم منظورا علميا لتحليل الأدلة الجنائية الرقمية. كما تساهم علوم التحليل السلوكي في الربط بين المعارف التكنولوجية، وبين الطرق العلمية لاستخلاص الدليل الرقمي، وعن طريق هذه العلوم يمكن تحريز الدليل الجنائي الرقمي لإثبات أنه أصيل وموثوق به، ويقع ضمن سلسلة الأدلة المقدمة في الدعوى، وتحديد كل جزء من الأدلة الرقمية، كالمستند الرقمي، والتطبيقات، والصور، والأصوات[٥٩].

دور الأدلة الرقمية الهامشية: ـ

الدليل الجنائي الرقمي الصحيح يتم من خلاله استخلاص المعلومات المتعلقة بالجريمة والمجرم، وكما ذكرنا فإن الأدلة الجنائية الرقمية التي تم محوها أو العبث بها، يمكن استعادتها باستخدام برامج خاصة تم تصنيعها خصيصاً لذلك، وأخيرا الأدلة الرقمية الهامشية تلعب دورا هاما في إعادة ترميم الأدلة الممحوة أو التي تم العبث بها، فهي تكمل أوجه النقص في الأدلة الجنائية الرقمية المستخلصة من الأدلة الصحيحة.

ويتوقف بناء الأدلة الجنائية الرقمية علي نوع الدليل، ونوع الحاسب، وأنظمة التشغيل، ومن خلال إصلاح الأدلة التالفة أو الممحوة، وربطها بالأدلة الرقمية الصحيحة، وسد ثغراتها من خلال الأدلة الرقمية الهامشية مما يؤدى إلي إعادة بناء مسرح الجريمة الرقمي[٦٠].

المطلب الثاني
أهمية الدليل الجنائي الرقمي في الإثبات

تساهم الأدلة الجنائية بوجه عام في إثبات الواقعة أو نفيها، فعن طريقها يمكن الإدانة أو البراءة، وتعتبر الأدلة الرقمية نوع من الأدلة الجنائية، ولكنها تتميز بطبيعتها

---

[٥٩] د. ناصر بن محمد بن مجول البقمي، أهمية الأدلة الرقمية في الإثبات الجنائي دراسة وفق الأنظمة السعودية، مرجع سابق ص٣٣.

[٦٠] د. سعد أحمد محمود سلامة، مسرح الجريمة، دار النهضة العربية، القاهرة، الطبقة الأولي، سنة ٢٠٠٧م، ص٢٦٥.

الخاصة التي تميزها عن الأدلة التقليدية المتعارف عليها، من حيث مكان وجود الدليل والبيئة التي تحكمه وإجراءات التقنية اللازمة لجمعه والعوائق المصاحبة له.

وعلي مدى السنوات القليلة الماضية أدخلت تحسينات كبيرة بواسطة مزودي الخدمات والبرمجيات على أدوات التحليل الجنائي الرقمي[٦١]، لذلك فإن ما كان في يوم من الايام عملية تحليل يتم تنظيمه يدويا الآن بشكل تلقائي بفضل وسائل التقنية الحديثة، حيث لم نعد في حاجة الي سنوات الخبرة العديدة كما أن التدريب علي استخلاص هذه الأدلة بشكل يدوى لم يعد ضرورياً[٦٢].

ولاشك أن الدليل أحد المشكلات التي يثيرها موضوع الجرائم المعلوماتية التي فجرتها ثورة الاتصالات عن بعد، والتي تتعلق بصعوبة إثبات هذه الجرائم بالأدلة المتحصلة من الوسائل الإلكترونية في إطار الإثبات الجنائي، ومن هنا تظهر أهمية الدليل الجنائي الرقمي، فهو يرتبط بالبيئة الرقمية التي تقع فيها الجريمة، ويعتمد علي البصمة الرقمية التي تميزه وتجعله ظاهرة جديدة في الإثبات الجنائي.

فالأدلة التقليدية لا تتلأم مع طبيعة الجرائم المعلوماتية، مما يجعل الاعتماد علي الأدلة الجنائية الرقمية أمراً حتمياً لمواجهة تلك الجرائم، وهو ما جعل الكثير من الدول تشجع البحث العلمي في هذا المجال، وتعمل علي ابتكار وسائل علمية جديدة تساعد في كشف الجرائم وإزالة غموضها، وتبرز أهمية استخدام الدليل الرقمي الجنائي في الإثبات عندما تقف الأدلة التقليدية عاجزة عن إثبات هذه الجرائم،

فالجاني يستخدم ويستحدث وسائل مبتكرة لا تترك أثراً محسوساً يمكن التعامل معه، مع عدم ظهور الأسلوب الإجرامي المستخدم[٦٣]، وإذا كانت الأدلة الجنائية في إطار الجرائم التقليدية هي التي تحدد الإدانة أو البراءة، فإن الأدلة الجنائية الرقمية هي أهم أدلة الإثبات التي تظهر الإدانة أو البراءة خاصة في الجرائم المعلوماتية.

---

(61) ewa huebner et al, computer forensics- past,present and future, 8 INFO, Security technical, 2007.p32.

(62) of the costs of digital forenssic investigations,see tylre moore,the economies of digital forensies, fifth workshop on the econ-of info.see.(june 26, 2006, available at http//weis,2006.econinfosec.org/ docs/ 14 .

[٦٣] د. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعلميات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، سنة ٢٠٠٣م، ص٤.

(ISSN: 2537- 0758)

ولاشك أنَ للقاضي الحرية في الاستناد إلي أي دليل من الأدلة التي يقتنع بحقيقتها، فالعبرة في المحاكمات الجنائية باقتناع القاضي بناءًا علي الأدلة المطروحة عليه، وعلي ذلك لا يجوز مطالبته بالأخذ بدليل بعينه (مالم يقيده القانون)، فله الأخذ بأي بينة أو قرينة يرتاح اليه دليلاً لحكمه[٦٤]، وبذلك يجوز للقاضي أن يستخدم الوسائل العلمية.

وكذلك بأهل الخبرة وخاصة مع ظهور أنواع جديدة من الجرائم لم تكن معروفة من قبل ويجب حماية الأفراد والمجتمع منها، وعلي الرغم من قصور التشريعات التي تنظم التعامل مع الحاسوب وتقنية المعلومات، لم يواجه القضاء مشكلة في تعامله مع الأدلة الجنائية الرقمية.

استخلاص الدليل الجنائي الرقمي:

يمكن استخلاص الدليل الجنائي الرقمي من خلال أجهزة الكمبيوتر المتعلقة بالجريمة، سواءًا التابعة للجاني أو المجنى عليه، وذلك من خلال فحص الحاسوب، فهو المصدر الذى يشتمل علي هذه الادلة، حيث يحوى الكثير من المعلومات المتعلقة بنشاط الجاني، كما أن الوصول الي الادلة الرقمية يتطلب الفحص المادي والمعنوي للارتباط القائم بين مكونات الحاسوب ككل فيتم فحص القرص الصلب الذى يضم بداخله البيانات الرقمية ذات الطابع الثنائي[٦٥].

ويتم فحص هذا القرص جزئيا عن طريق استرداد المعلومات التي تم حذفها، وهو ما يتوقف علي أمر هام كحالة ضبط الحاسوب محل الواقعة، ومهارة من يقوم باستخلاص هذه البيانات والمعلومات دون اتلافها أو العبث بمحتوياتها حسب الجريمة المرتكبة والاثر المترتبة عليها، وبفحص القرص الصلب للحاسوب تظهر البيانات التي استخدمها الجاني.

وكذلك الصور ومخابئ صفحات الانترنت، و يمكن التوصل الي صفحات وعناوين مواقع الانترنت التي استخدمها الجاني، بالإضافة الي رسائل البريد الإلكتروني ورؤوس الصفحات التي ارسلها أو استقبلها وهو ما يمكن من معرفة شركاء الجاني إن كان له شركاء.

بالإضافة الي فحص الجزء المادي للحاسوب وهو القرص الصلب، يجب أيضا فحص المكون المعنوي له وهو عبارة عن البرمجيات، وينبغي الا تكون معطوبة أو تالفة

---

[٦٤] الطعن رقم ٢٠٤٩٩ لسنة ٨٧ قضائية، الدوائر الجنائية، جلسة ٢٠٢٠/٧/٩.

[٦٥] د. عمر محمد بن يونس، الدليل الرقمي، مرجع سابق ص ٨٧.

حيث ينعكس ذلك علي قوة الدليل وضعفه، فإذا كانت تالفة أو معطوبة فمن شأن ذلك ان يقلل من قيمة الدليل الجنائي الرقمي المستخلص من خلالها.

بالإضافة لما سبق فانه ينبغي للوصول الي الدليل الجنائي الرقمي فحص النظام المعلوماتي للحاسوب، حيث أنه يحتوى علي بيانات في هيئة رقمية متبادلة، وكذلك فحص ذاكرة التخزين والتي تمثل قدرة الحاسوب علي الاحتفاظ بنسخة كاملة ممن قام به الجاني خلال ارتكابه للجريمة المعلوماتية[٦٦]، ويتم فحص النظام المعلوماتي من أجل ضبط كافة ما يشتمل عليه الحاسوب من بيانات ومعلومات.

كما يمكن الحصول عليها أو استرجاعها باستخدام البرامج والتطبيقات المتخصصة علي أية شاكلة يمكن أن تكون عليها طريقة استردادها ما دامت هذه البيانات تشكل جريمة معلوماتية، و اخيرا من اجل الحصول علي الادلة الرقمية يجب فحص ملحقات الحاسوب كالطابعة التي تحتفظ بتخزين الصفحات التي تم استخراجها من الحاسوب، فهناك برامج تقوم باسترداد مخرجات الطابعة وهو ما يمكن جهات التحقيق من معرفة ما قام الجاني بطباعته.

ويمكن ايضا فحص لوحة المفاتيح لاستخلاص الدليل الجنائي الرقمي، حيث ان مرتكب الجرائم المعلوماتية يمكن ان يتحكم في لوحة المفاتيح ومن ثم يمكن الاعتماد عليها في استخلاص الدليل[٦٧]، وتضم الجريمة المعلوماتية في الغالب الي جانب الجاني والمجنى عليه مقدم الخدمة، فيجب عند البحث عن الادلة الرقمية أن نبدأ بفحص الحاسوب الخاص بالمتهم بكل ما يحتويه من وحدات التخزين.

ثم بعد ذلك يتم فحص معاينة مسرح الجريمة الافتراضية لتتبع بعض الآثار التي قد يكون الجاني خلفها، وهذا يتم بتفتيش الأنظمة مع اتخاذ كافة الاجراءات اللازمة للحفاظ علي الادلة الجنائية الرقمية، ثم يتم فحص مزود الخدمة.

حيث يتم تسجيل وحفظ البيانات الخاصة بالمشتركين على الشبكة المعلوماتية، بالإضافة الي كيفية استخدامهم للخدمة المقدمة من قبل مزود الخدمات[٦٨]، بالإضافة

---

[٦٦] د. عمر محمد بن يونس، الجرائم الناشئة عن الانترنت، الاحكام الموضوعية والاجرائية، رسلة دكتوراه، كلية الحقوق جامعة عين شمس، سنة ٢٠٠٤م، ص١٧.

[٦٧] د. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مرجع سابق، ص ١٩.

[٦٨] د. سعد أحمد محمود سلامة، مسرح الجريمة، مرجع سابق ص١٤٢.

(ISSN: 2537- 0758)

الي امكانيات الاستعانة بشركات الانترنت للتوصل الي الملفات المحملة والتي استخدمها الجاني في جريمته والمواقع التي دخل اليها.

أنواع الأدلة الجنائية الرقمية التي يمكن الاعتماد عليها في الاثبات الجنائي:

١- أدلة أعدت لتكون وسيلة إثبات:

وهذه الأدلة عبارة عن السجلات التي تم إنشاؤها تلقائيا كسجلات الجوال والحاسب الألي[٦٩]، ومن الأدلة التي أعدت لتكون وسيلة للإثبات، السجلات التي جزء منها تم إنشاؤه بواسطة الإدخال وجزء تم إنشاؤه بواسطة الأجهزة ذاتها، كما هو الحال في البيانات المدخلة إلي الألة والتي تمت معالجتها من خلال برامج خاصة، ويتميز هذا النوع من الأدلة الجنائية الرقمية بسهولة الحصول عليه فهو معد ليكون دليلا في الأصل ووسيلة لإثبات الواقعة، فعادة ما يتم حفظ هذه الأدلة للاحتجاج بها لاحقا.

٢- الأدلة التي لم تعد لتكون وسيلة إثبات:

هذه الأدلة تعد الأثر الذى يتركه المجرم دون رغبته، وهذا النوع من الأدلة الرقمية يعرف بأنه (أدلة البصمة الرقمية)[٧٠]، كالرسائل المرسلة من الجاني أو التي يستقبلها، وكافة العمليات الالكترونية التي تمت من خلال شبكة الانترنت[٧١]، ويُعد النوع الثاني من الأدلة الجنائية الرقمية أكثر أهمية لتضمنه معلومات أكثر دقة تفيد في كشف الجريمة المرتكبة ومرتكبيها، ويمكن الحصول علي هذا النوع من الأدلة من خلال استخدام التقنيات الحديثة.

ولاشك أن وسائل التقنية الخاصة تُمكن من اكتشاف هذه الأدلة وضبطها حتى بعد فترة زمنية من إنشائها بواسطة وسائل التقنية الحديثة[٧٢]، حيث يتم الاعتماد في الكشف عن هذه الأدلة علي بروتوكول (IP)، والذى يمكن من خلاله ضبط تحركات المتهم،

---

[٦٩] د. خالد ممدوح إبراهيم، امن الجرائم الالكترونية، الدار الجامعية للطباعة والنشر، سنة ٢٠٠٩م، ص٢.

[٧٠] د. ممدوح عبد الحميد عبد المطلب،، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب الوطنية، مصر، ٢٠٠٦م، ص ٢٣٨.

[٧١] أ. طارق محمد الجملين– الدليل الرقمي في مجال الاثبات الجنائي، مجلة الحقوق جامعة البحرين، مجلد ١٢ ا، العدد ١، سنة ٢٠١٥ ص ١٢٣.

[٧٢] د. عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة معمقة في جرائم الحاسب الألي والإنترنت، بهجات للطباعة والتجليد، مصر، ٢٠٠٩م، ٦٣.

وتحديد الجهاز الذى يستعمله من خلال بيانات الجهاز عند مزود الخدمة، وان كان هذا البروتوكول لا يحدد شخصية الجاني ولكن يمكن من خلاله تحديد الجهاز الذى استخدمه في جريمته، وهو ما يعد قرينة[٧٣].

وقد يأخذ الدليل الجنائي الرقمي شكل صورة رقمية والتي عادة ما تكون في شكل ورقي أو مرئي عن طريق الشاشة المرئية، والحقيقة أن الصورة الرقمية هي أكثر تطورا من الصورة الفوتوغرافية التقليدية، كذلك قد يأخذ الدليل الجنائي الرقمي شكل التسجيلات الصوتية، وهى التي تخزن بواسطة الجهاز المستخدم، وأخيرا قد يأخذ شكل النصوص المكتوبة، وهى التي تكتب بواسطة الجهاز كالرسائل المرسلة عبر البريد الإلكتروني والهواتف النقالة[٧٤].

أسباب اللجوء للأدلة الرقمية:

١- **الثقة والكفاءة:**

اكتسبت الأدلة الجنائية الرقمية أهمية كبيرة نظر للثقة في الحاسب والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات.

٢- **الارتباط بين الأدلة الرقمية وبيئة الجريمة:**

فالأدلة الجنائية الرقمية ترتبط بالجريمة وأثارها، فهذه الأدلة من نفس بيئة الجرائم المعلوماتية.

٣- **الوضوح:**

تتميز الأدلة الجنائية الرقمية بالوضوح والدقة في إثبات العلاقة بين الجاني والمجنى عليه أو بين الجاني والجريمة.

٤- **يقنيه الأدلة الجنائية الرقمية:**

فالأدلة الجنائية الرقمية تقوم علي نظريات حسابية مؤكدة لا يتطرق إليها الشك، والتي تبنى علي الدراسات والتقنية العلمية.

٥- **الخبرة في الدليل الجنائي الرقمي:**

يعتمد الإثبات بالأدلة الجنائية الرقمية علي رأى الخبراء، حيث يساعد ذلك في الكشف عن الأدلة، وفحصها، وتقييمها، ثم تعرض النتائج التي توصل إليها الخبراء علي

---

[٧٣] د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص١٠٨.

[٧٤] د. ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، أكاديمية شرطة دبي، سنة ٢٠١٥م، ص٩.

(ISSN: 2537- 0758)

جهة التحقيق، وفقاً لشروط وقواعد نظمها النظام، وقد أحسن المشرع المصري صنعاً عندما نص[٧٥]، علي إنشاء سجلان بالجهاز القومي للاتصالات، لقيد الخبراء، يُقيد بأحدهما الفنيون والتقنيون العاملون بالجهاز، ويُقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به، وتطبق عليهم في ممارسة أعمالهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام التي تنظم الخبرة أمام جهات القضاء.

٦- تَمَّيز الأدلة الجنائية الرقمية:

حيث تقوم علي حقائق وأسس علمية، كما أنها تتميز بنتائج دقيقة وواضحة.

٧- مواجهة الجرائم المعلوماتية المتطورة:

تطور الجريمة المعلوماتية، يفرض علينا مواجهتها بالأسلوب نفسه، سواءًا في مجال الضبط أو التحقيق أو المحاكمة. ونرى أن الأدلة الجنائية الرقمية أصبحت جزءا لا يتجزأ من أدلة الإثبات، لكونها تتناسب مع تطور الجريمة المعلوماتية.

المبحث الثاني
حجية الأدلة الجنائية الرقمية في الإثبات

تمهيد

العلوم الجنائية تقدم لنا الأدوات والتقنيات والأساليب النظامية التي يمكن من خلالها تحليل الأدلة الرقمية للاستفادة منها في إثبات الواقعة أو نفيها وذلك من خلال الربط بين الجريمة والجاني أو بين الجاني والمجنى عليه، وسوف نتناول هذا المبحث من خلال مطلبين نخصص أولهما لحجية الدليل الرقمي في التشريع المصري والقوانين الوضعية المقارنة، ويتناول المطلب الثاني الأدلة الجنائية الرقمية ووسائل الإثبات التقليدية.

المطلب الأول
حجية الدليل الجنائي الرقمي في التشريع المصري والتشريعات المقارنة

تمهيد:

مواجهة الجرائم الإلكترونية لاقى اهتماما عالمياً فقد عقدت المؤتمرات والندوات المختلفة، وصدرت من خلالها قوانين وتشريعات تجرم هذه الجرائم، وتعد السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب حيث صدر قانون البيانات السويدي سنة

---

[٧٥] **نصت المادة ١٠ من قانون رقم ١٧٥ لسنة ٢٠١٨م بشأن مكافحة جرائم تنقية المعلومات المصري علي أن** "ينشأ بالجهاز سجلان لقيد الخبراء، يقيد بأولهما الفنيون والتقنيون العاملون بالجهاز، ويقيد بالأخر الخبراء من الفنيون والتقنيين من غير العاملين به.....الخ".

١٩٧٣م، والذى عالج قضايا الاحتيال عن طريق الحاسب الآلي، كما عمل هذا القانون علي مكافحة جرائم الدخول غير المشروع إلي البيانات أو تزويرها أو تحويلها أو الحصول عليها بطريق غير المشروع.

ثم جاءت الولايات المتحدة الأمريكية وشرعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي في الفترة من ١٩٧٦م إلي ١٩٨٥م، وفى عام ١٩٨٥م اكد معهد العدالة القومي علي خمسة جرائم معلوماتية وهى "جرائم الحاسب الآلي الداخلية، وجرائم الاستخدام غير المشروع عن بعد، وجرائم التلاعب بالحاسب الآلي، وجرائم دعم التعاملات الإجرامية، وجرائم سرقة البرامج الجاهزة".

وقد استقر الفقه والقانون الوضعي علي أن للقاضي سلطة واسعة في تقدير الأدلة واستنباط القرائن وما تحمله الوقائع من دلالات، شريطة أن يكون الدليل ثابتاً بيقين ومرتبطاً بالواقعة الرئيسية، ومنسجما مع التسلسل المنطقي للأحداث، ومن الطبيعي أن ينسحب هذا الرأي علي الأدلة الجنائية الرقمية باعتبارها أحد أقسام الأدلة المادية العلمية بل أكثرها حجية في الإثبات.

فالأدلة الرقمية محكمة بقواعد علمية وحسابية قاطعة لا تقبل التأويل، كما أنها معالجة بوسائل التقنية المعلوماتية التي أصبحت تستغل في الجرائم المستحدثة[٧٦]، ولقد تضمنت أحكام محكمة النقض المصرية مبدأً هاماً وهو "إذا كانت المسألة المعروضة عليها من المسائل الفنية البحتة التي لا تستطيع المحكمة أن تشق طريقها إليها لإبداء الرأي فيها، فالمحكمة ملزمة بندب خبير، بل إنها ملزمة بالأخذ برأي هذا الخبير، إذا كان العلم قد انتهى برأي قاطع إلي صحة النتائج التي تم التوصل إليها"[٧٧].

ولاشك أن إخضاع كافة الجرائم لقواعد إجرائية مماثلة كانت هي النظرة التقليدية السائدة، فلا يكون لسلطات الضبط والتحقيق سلطات استثنائية في نوع معين من الجرائم، ولكن ذلك لم يعد مسلماً به، فقد اتجهت التشريعات المقارنة خلال الربع الأخير من القرن العشرين إلي التوسع في حالات المساس بالحرية الشخصية.

كما اتجهت إلي تقرير صلاحيات واسعة لسلطات الضبط والتحقيق والاتهام، ويرجع ذلك إلي انتشار الجرائم المنظمة، وجرائم العنف السياسي والديني، وهو ما شكل ظاهرة

---

(76) Amadt, B.L and plaza, E., "case, based Reasoning: Foundational Issues, Mathodalogical Variations, and system Approaches", Alcom, Artficial intelligence Communications, 7 (1), 1994, p.18.

(٧٧) نقض ١٣ مايو ١٩٦٨م، مجموعة الأحكام رقم (١٠٧) حكم رقم ٣٠٣ لسنة ١٩٦٨م، ص٣٨.

(ISSN: 2537- 0758)

استتبعت مواجهتها التوسع في السلطات المخولة للجهات القائمة علي ضبط هذه الجرائم وتعقبها، وهو ما أدى في النهاية إلي استقلال الجرائم المنظمة، كالجرائم المعلوماتية التي تتميز بصفات خاصة، وتحتاج لإثباتها أدلة نابعة من بيئتها كالأدلة الرقمية. وسوف نتناول حجية الدليل الجنائي الرقمي في التشريع المصري والتشريعات المقارنة في النقاط التالية:

أولاً: حجية الدليل الجنائي الرقمي في التشريع المصري:

نظرا لأهمية الأدلة الرقمية في الاثبات الجنائي فإن المشرع المصري في القانون رقم ١٧٥ لسنة ٢٠١٨م، والخاص بمكافحة جرائم تقنية المعلومات، قد أعطى لها قيمة وحجية في الإثبات، حيث اعتبر أن الأدلة المستمدة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو أي من برامج الحاسب.

أو من أي وسيلة لتقنية المعلومات لها حجية الأدلة الجنائية المادية في الإثبات[٧٨]، وهو ما أكدت عليه محكمة النقض المصرية بقولها " لما كانت جناية التهديد المنصوص عليها في الفقرة الأولي من المادة ٣٢٧ من قانون العقوبات المصري تتوافر إذا وقع التهديد كتابة بارتكاب جريمة ضد النفس أو المال، وكان التهديد مصحوباً بطلب أو تكليف بأمر.

وكان الحكم قد أورد بأسبابه قيام الطاعن بتهديد المجنى عليهما عبر وسائل التواصل الاجتماعي، وتمكن من خدعاهما وتحصل منهما علي صور ومقاطع مرئية في أوضاع مخلة بالحياء وهددهما بنشرها، وإذ كان مصطلح الكتابة قد ورد في المادة ٣٢٧ من قانون العقوبات المصري سالفة الذكر علي سبيل البيان في صيغة عامة لتشمل كافة وسائل الكتابة المختلفة سواءاً بالطرق التقليدية أو بإحدى الوسائل الالكترونية الحديثة.

فإذا أثبت الحكم علي الطاعن إرساله عبارات التهديد عن طريق الوسائط الالكترونية الحديثة (لوحة المفاتيح) بقصد إيقاع الخوف في نفس المجنى عليهما لحملهما علي اداء ما هو مطلوب، فإنه قد استظهر أركان جريمة التهديد كما هي معرفة به في القانون "وبناءاً عليه فإن جناية التهديد مناط توافرها إثبات ارسال الطاعن عبارات التهديد كتابة عن طريق الوسائط الإلكترونية الحديثة بقصد إيقاع الخوف في نفس المجنى عليهما لحملهما علي أداء ما هو مطلوب يتوافر به أركان جريمة التهديد".

---

[٧٨] الطعن رقم ٢٢٦٢٠ لسنة ٨٨ قضائية، الدوائر الجنائية، جلسة ٢٠٢٠/٧/٩م.

ولكن ربط ذلك بأن يكون استخلاص تلك الأدلة وفقا للشروط المنصوص عليها، وتمر الأدلة الجنائية الرقمية منذ نشأتها بمراحل متعددة تتطلب مهارات خاصة للتعامل معها، (مرحلة تلقى البلاغ لوقوع الجريمة، مرحلة التحقيق، مرحلة حفظ الأدلة، مرحلة المحاكمة).

ففي مرحلة تلقى البلاغ يقتصر دور أجهزة الضبط في التعرف علي مسرح الجريمة والمحافظة عليه والتحفظ علي الأدلة الموجودة من خلال التفتيش في بيئة الإنترنت، والتفتيش هو إجراء تحقيقي ووسيلة للإثبات المادي فهو يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وهو ما يتعارض مع الطبيعة غير المادية لبرامج وبيانات الحاسبات الآلية.

فهي عبارة عن برامج أو بيانات إلكترونية ليس لها مظهر مادى محسوس في العالم الخارجي، وهو ما يلزم خضوع الجرائم المعلوماتية لأحكام مستقلة تتناسب مع طبيعتها الخاصة، ويعد نظام تفتيش الحاسبات الآلية، كتفتيش وسائط وأوعية حفظ وتخزين البيانات المعالجة الكترونياً، إجراءاً يندرج ضمن التفتيش بمعناه القانوني ويخضع بالتالي لأحكامه، ويتم ذلك من خلال ضبط الوعاء المادي لهذه المعلومات كالأقراص والأسطوانات الممغنطة[٧٩].

وتخضع عملية التفتيش في العالم الافتراضي لشروط موضوعية وآخري شكلية، وتتمثل الشروط الموضوعية للتفتيش في السبب، والمحل، والسلطة المختصة، فالنسبة للسبب يجب أن تكون هناك جناية أو جنحة وقعت بالفعل، وإتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، وقيام قرائن وأمارات قوية علي وجود أشياء تفيد في كشف الحقيقة سواء امع شخصه أو مسكنه أو مع شخص أو مسكن غيره.

أما المحل فيقصد به الحاسب الآلي، ويشمل مكوناته (الخادم، والمزود الآلي، والمضيف، وملحقات التقنية)، ولا شك أنَّ محل الجريمة المعلوماتية لا يكون قائماً بذاته، بل يشمل المكان أو العقار الذى يوجد فيه الحاسب الآلي، الذى يعد بطبيعته حرزاً كالمنزل أو حتى المجرم نفسه، كما في حالة الحاسوب المحمول[٨٠].

---

[٧٩] د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ص٦٨.

[٨٠] د. سامى حسين الحسيني، النظرية العامة للتفتيش في القانون المصري والقانون المقارن دار النهضة العربية، سنة ١٩٧٢م، ص ٢١٠.

(ISSN: 2537- 0758)

ويشترط لصحة تفتيش محل الجرائم المعلوماتية، أن يكون الإذن محدداً خصوصاً في محله والأشياء المراد البحث عنها، كأن يتضمن الإذن بتفتيش ذاكرة الحاسب الآلي والأدوات الأخرى لتخزين البيانات، وعلي ذلك يقع التفتيش في جرائم الإنترنت علي مكونات الحاسب الآلي المادية والمعنوية.

كذلك الشبكة وما تتضمنه من مكونات وفيما يتعلق بالسلطة المختصة بالتفتيش في الجرائم المعلوماتية، فهي النيابة العامة، فلها أن تندب مأمور الضبط القضائي مع مراعاة قواعد الاختصاص المكاني والنوعي، وللقاضي سلطة تقدير الأدلة والقرائن وما تحمله الوقائع من دلالات، بشرط أن يكون الدليل ثابت بيقين ومرتبطا بالواقعة محل الدعوى.

ومنسجماً مع التسلسل المنطقي للأحداث، وهو ما يمكن أن نطبقه في حالة الأدلة الجنائية الرقمية فهي محكمة بقواعد علمية وحسابية قاطعة لا تقبل التأويل[٨١]، ولاشك أن الأدلة الجنائية الرقمية معالجة بوسائل التقنية المعلوماتية التي أصبحت تستغل في الجرائم المستحدثة فيمكن استخلاصها من ندب خبراء وهو ما أكدته محكمة النقض المصرية.

فقد بينت أنه إذا كانت المسألة المعروضة عليها من المسائل الفنية البحتة التي لا تستطيع المحكمة أن تشق طريقها إليها لإبداء الرأي فيها فالمحكمة ملزمة بندب خبير، بل إنها ملزمة بالأخذ برأي هذا الخبير، إذا كان العلم قد انتهى برأي قاطع إلي صحة النتائج التي تم التوصل إليها[٨٢].

كما أن الغلبة في إثبات الجرائم المعلوماتية ستكون للقرائن والخبرة، وهو ما يزيد من أهمية الدليل الرقمي الجنائي في الإثبات، ويزيد من أهمية دور القاضي، من خلال السلطة التقديرية التي يجب أن يتمتع بها، ولأشك أن الجريمة في السنوات القليلة الأخيرة تطورت بشكل هائل، وهو ما يستلزم أن يكون الدليل الذى تقوم به هو الآخر متطوراً لكى يقوم علي إثباتها، ومن هنا تظهر أهمية الدليل الرقمي، الذى يتطلب وسائل علمية لاستخلاصه، كما يتطلب قدرات خاصة في المحققين والخبراء.

وهو ما يؤدى بدوره إلي تطور الحقيقة القضائية ويستطيع أن يجعل الحقيقة العلمية عادلة، مما يؤدى إلي نتائج محددة وواضحة، فتؤثر علي اقتناع القاضي بشكل أكبر من

---

(81) Amadt, B.L and Plaza, E., case, based Reasoning: Foundational Issues, MAthodagical Variations, and system Approaches, Alcom,Artfical intelligence Communications, op cit p.18

[٨٢] نقض ١٣ مايو، مجموعة الأحكام رقم (١٠٧) حكم رقم ٣٠٣، لسنة ١٩٦٨م.

الأدلة الأخرى، فهي تعتمد علي الخبير المختص الذى يستخدم العلم في الكشف عن الجريمة، مما يجعل للدلالة طبيعة موضوعية وفق ضوابط ومعايير علمية محددة.

فرأى الخبير في حد ذاته دليلاً متى كان مباشرا وقد يكون ما توصل إليه غير مباشر في إثبات الواقعة، فيساعد حينئذ علي إقامة الدليل وتقديره، مع احتفاظ القاضي في هذه الحالة بسلطته التقديرية في الأخذ بما توصل إليه الخبير أو طرحه، ولا يمكن مراجعته في ذلك لآن رأيه في كافة المسائل الموضوعية نهائي[٨٣]، ويجب أن يكون هناك ملائمة للدليل الجنائي بحيث يكون الدليل المقدم لإثبات الواقعة ذو قيمة إثباتية، فيجب أن يقوم الدليل علي المنطق ويتجه إلي إثبات الواقعة التي من أجلها قُدم واتجاه الدليل إلي إثبات الواقعة أو عدم إثباتها لا يكون إلا عن طريق المنطق والعقل، فيكون ملائماً إذا اتجه طبقا لمقتضيات العقل والمنطق إلي إثبات الواقعة أو نفيها.

كما يجب أن يكون الدليل قادراً بذاته علي إثبات العناصر المادية للجريمة ويكتسب الدليل الأهمية إذا كان يفصل في الواقعة المنظورة، بحيث يمكن من خلاله تحديد وقوع الجريمة أو عدم وقوعها فالأدلة الرقمية تنتمى إلي القرائن، وغالبا ما تكون نتيجة لتقارير الخبراء التي تعد مجرد أراء في شأن دليل الإثبات.

وتتضمن هذه التقارير بيان الدليل وتفصيل عناصره، ثم اقتراحا من وجهة نظر فنية لما يمكن أن يكون له قيمة في إثبات الواقعة وعلي اعتبار أن الدليل الرقمي من باب القرائن التي تعد أهم الأدلة المؤثرة في الدعوى الجنائية، فهي تعتمد علي الجانب العلمي والعقلي في مجال الإثبات، كما أنها تبتعد عن العناصر النفسية غير المستقرة[٨٤]، مما يُمكن من الوصول إلي الحقيقة وتحديد العلاقة بين الجاني والجريمة أو الجاني والمجنى عليه.

ثانيًا: الدليل الجنائي الرقمي في التشريع الإنجليزي:

أقر المشرع الإنجليزي بالأدلة الرقمية في قانون مكافحة التزوير والتزييف عام ١٩٨١م، والذى شمل تعريف التزوير الذى يتم من خلال وسائط التخزين الحاسوبية أو أي أداة أخرى يتم بها التسجيل سواء تم ذلك بالطرق التقليدية أو الإلكترونية أو بأي

---

[٨٣] د. رأفت عبد الفتاح حلاوة، الإثبات الجنائي، قواعده وأدلته، دار النهضة العربية، القاهرة، سنة ١٩٩٦م ص ١٥٨، **وأنظر أيضاً** د. عبد الحكيم فودة، حجية الدليل الفني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، سنة ١٩٩٦م ص ٢٦.

[٨٤] د. رمزي رياض عوض، مشروعية الدليل الجنائي فى مرحلة المحاكمة وما قبلها، دراسة تحيلية وتأصيلية مقارنة، دار النهضة العربية، القاهرة، سنة ١٩٩٧م، ص٢٥.

(ISSN: 2537- 0758)

طريق أخر[٨٥]، كما أنه أصدر تشريعاً في بداية التسعينات خاصاً بالحاسب الآلي، وعُرف هذا التشريع باسم "إساءة استخدام الحاسب" الصادر بتاريخ ١٩٩٠/٦/٢٩م. **وقد نص هذا القانون علي ثلاث جرائم جديدة هي:**

- الدخول غير المصرح به للكمبيوتر للأضرار أو اتلاف البرامج أو حتى مجرد التطفل.
- الدخول غير المصرح به بقصد ارتكاب أو تسهيل ارتكاب جريمة.
- القيام بما من شأنه التعديل غير المصرح به لنظام الحاسوب بقصد اضعاف النظام أو تعطيله.

ولم يتطرق لقواعد قبول الأدلة الرقمية، ويرجع ذلك إلي أنّ قانون البوليس والإثبات الجنائي لسنة ١٩٨٤م، والذى حل محل قانون الإثبات الجنائي لعام ١٩٦٤م قد احتوى تنظيماً محدداً لمسألة قبول الأدلة الجنائية الرقمية[٨٦]، فالمادة ٦٩ من هذا القانون قد تضمنت مجموعة من الشروط، التي يجب أن تتوافر في الأدلة المستخلصة من الحاسب الآلي.

وقد يُرفض الدليل الجنائي الرقمي لكونه غير دقيق أو بياناته غير سليمة أو أنّ الحاسب الآلي الذى أُستخرج منه الدليل الجنائي الرقمي لا يعمل بكفاءة وبصورة سليمة، وقد حدد المشرع الإنجليزي مجموعة من القواعد لكى يصبح الدليل الرقمي مقبولاً أمام القضاء ومنها عدم قيام الخبير المنتدب لفحص الحاسب الآلي بأي تغيير في البيات الموجودة في هذا الحاسب[٨٧]، كما اشتراط أن يتم تسجيل وتوثيق كل الخطوات التي قام بها الخبير في عملية جمع الأدلة وتحليلها وإخضاعها للاختبار للتحقق من مصداقية النتائج.

ثالثاً: الدليل الجنائي الرقمي في التشريع الأمريكي:

تضمنت القواعد الاتحادية للبينة في الولايات المتحدة الأمريكية نصاً يعتبر السجلات والبيانات المنظمة بدقة بينة مقبولة أمام المحاكم الجنائية استنادا للبينة السماعية، وعلي

---

[٨٥] د. عبد الرحمن عبد العزيز الشنقيطي، أمن المعلومات وجرائم الحاسب الآلي، ط١، المكتبة الأمنية جامعة نايف، الرياض سنة ١٩٩٤م ص١٠٨.

[٨٦] د. أحمد عبد اللاه هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والإنترنت، المجلد ٢، ط٣، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، سنة ٢٠٠٤م ص١٣٥.

[87] Association of Chief Police Officers (of England, Wales, Northern, Ireland), for Computer Based Electronic Evidence, Version5, October 2011, p.6.

ذلك تعتبر التقارير والمعلومات والبيانات المحفوظة في أي شكل وكذا الوقائع والأحداث والآراء ونتائج التحليل المنقولة بواسطة أشخاص ذو معرفة وخبرة في نطاق الأنشطة والممارسات المنظمة.

تُعد بينة مقبولة أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، ولاشك أن الأدلة الجنائية الرقمية من هذا النوع لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آلياً بأسلوب علمي(٨٨).

وقد أخذت الولايات المتحدة الأمريكية بالأدلة الرقمية، ونصت علي ذلك في عدة قوانين منها قانون الحاسب الآلي لسنة ١٩٨٤م، والصادر بولاية آبوا الأمريكية، الذى اعتبر أن الأدلة الناتجة عن الحاسب الآلي مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة(٨٩)، كما تضمن ذلك قانون الإثبات لسنة ١٩٨٣م الصادر بولاية كاليفورنيا والذى نص علي أن النسخ المستخرجة من البيانات التي يحتويها جهاز الحاسب الآلي، تكون مقبولة بوصفها أفضل وأنسب الأدلة المتاحة لإثبات هذه البيانات(٩٠).

وقد اشترط المشرع الأمريكي لقبول الأدلة الجنائية الرقمية أمام المحاكم في الولايات المتحدة الأمريكية، أن يكون جهاز الحاسب الآلي يؤدى وظائفه بصورة سليمة وان يكون الدليل الرقمي له صلة وطيدة بالقضية المعروضة، وأوجب الارتباط بين الجريمة والأشخاص المشتبه بهم(٩١).

وإضافةً إلي ما تقدم يجب أن يكون الدليل الرقمي محل ثقة ومعتمد كشرط لقبوله، وعلي ذلك يقوم القضاة بتحديد درجة مصداقية وفاعلية هذا الدليل عن طريق إخضاعه لإختبارا قانونيا لتقرير صلاحية الدليل العلمي وصلته بالواقعة، ونشأ هذا الاختبار بموجب القرار الصادر من المحكمة العليا في الولايات المتحدة الأمريكية، والتي أصدرته

---

(88) Icove, D., Seger, K, and Vonstorch, W. Computer crime, A crime fighter's Handbook, Sebastpol, CA: O'Reilly and Associates 1995, p.61.

(٨٩) د. علي حسن الطوالبة، التفتيش الجنائي علي نظم الحاسوب والإنترنت، دراسة مقارنة، الطبعة الأولي، عالم الكتب الحديث، الأردن، سنة ٢٠٠٤م ص١٩٧.

(٩٠) د. علي حسن الطوالبة، التفتيش الجنائي علي نظم الحاسوب والإنترنت، مرجع سابق ص١٩٨.

(91) Peter Sommer, Digital Evidence, Digital Investigation and E-Disclosure (A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers), Third Edition, Information Assurance Advisory Council (I,A,A,C), United Kingdom, 2011, p.30.

(ISSN: 2537- 0758)

في قضية "داوبورت" ضد "ميريل دو للصناعات الدوائية" في سنة ١٩٩٣م[٩٢]، ويخضع الاختبار لأربعة معايير أساسية:

المعيار الأول: التجربة والاختبار.

المعيار الثاني: نسبة الخطأ.

المعيار الثالث: النشر.

المعيار الرابع: القبول.

وقبل ظهور اختبار "داوبورت" كان هناك اختبار يسمى "فراي" لتقرير صلاحية الدليل العلمي بصفة عامة، والذى صدر بقرار المحكمة العليا للولايات المتحدة الأمريكية في سنة ١٩٢٣م، وكان يقتصر علي معيارين فقط هما "التجربة والاختبار"، ومعيار القبول، إلا أن هذا المعيار قد ثبت فشله في مواجهة أنواع جديدة من الأدلة العلمية والتي من بينها الأدلة الرقمية[٩٣].

لذا كان لزاماً علي الخبراء والمتخصصين إيجاد معايير أخرى تتماشي مع تطور الأدلة الجنائية، فإذا لم تتوافر هذه الاشتراطات التي قررها القانون، يقوم القاضي باستبعاد الدليل الجنائي الرقمي، حيث يفقد هذا الدليل قدرته علي تحديد العلاقة بين الجاني والجريمة أو بين الجاني والمجنى عليه وقد اعتبر المشرع الأمريكي الافعال التالية من قبيل الجرائم المعلوماتية التي يجوز استخلاص الدليل الجنائي الرقمي بشأنها:

- الدخول الي أجهزة الحواسيب الحكومية والاطلاع علي المعلومات السرية بها.
- الكشف عن المعلومات المخزنة بأجهزة الكمبيوتر الحكومية الي جهات غير مصرح بها تلقيها.
- ارتكاب جرائم احتيالية من خلال الدخول غير المشروع الي اجهزة الكمبيوتر الحكومية.
- الحاق ضرر بالأجهزة أو البرامج أو المعلومات نتيجة الدخول غير المشروع.
- التهديد بارتكاب جرائم ابتزاز (أموال– منافع) من أي شخص طبيعي أو معنوي.
- نقل مواد فاحشة عبر الولايات المتحدة أو الجهات الاجنبية.
- توظيف القُصر في جرائم منافية للآداب.
- تزوير الوثائق أو انتاج وثائق مزورة من خلال الحواسيب.

---

(92) Stive Bunting and William Wei, Encase Computer forensic,Wiley Publishing (inc), United States of America, 2006.p 500.

(93) Linda Volonino and Reynaldo Anazaldua, Computer Forensics For Dummies Wiley Publihing, United States of America, 2008, p.83.

وكل ولاية من الولايات الامريكية تملك حرية التشريع الخاص فيما يتعلق بالجرائم المعلوماتية، علي الرغم من وجود الاطار العام لجرائم الكمبيوتر يعتمد علي مشروع قانون نموذجي تم وضعه من قبل هيئة أكاديمية سنة ١٩٩٨م، وتم تقسيم الجرائم المعلوماتية الي ثماني طوائف.

رابعاً: الدليل الجنائي الرقمي في التشريع الفرنسي:

أما المشرع الفرنسي فقد اهتم بتطوير القوانين الجنائية لمواجهة الجرائم المعلوماتية، حيث أصدر في عام ١٩٨٨م القانون رقم (٨٨– ١٩) والذى أضاف إلي قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، كما قام بتعديل قانون العقوبات عام ١٩٩٤م ليشمل مجموعة جديدة من القواعد الخاصة بالجرائم المعلوماتية، وقد أوكل إلي النيابة العامة سلطة التحقيق بما في ذلك طلب التحريات وسماع أقوال الشهود[٩٤].

وقد أخذ المشرع الفرنسي بمبدأ الاقتناع الشخصي للقاضي الجنائي لاستخلاص الأدلة الرقمية في الاثبات الجنائي، وهو ما اكد عليه في قانون الاجراءات الجنائية الفرنسي في المادة ٣١٠ أ. ج الفرنسي[٩٥] مع تجريمه الاعتداء علي الحق في الحياة الخاصة.

فقد عالج المشرع الفرنسي في قانون العقوبات، كما نص صراحة علي ضرورة توافر الخبرة في قانون التحقيق الجنائي وذلك في المواد ٤٤،٤٣ كما نظمها في قانون الاجراءات الجزائية في المواد ١٥٦ الي ١٦٩[٩٦]، فضلا عن القانون رقم ٧٨– ١٧ لسنة ١٩٧٨م المتعلق بالمعالجة الالكترونية للبيانات الرسمية، حيث تضمن هذا القانون بعض صور الجرائم الالكترونية التي تنتهك بواسطتها الخصوصية ومن هذه الجرائم[٩٧]:

١– جريمة المعالجة الالكترونية للبيانات الشخصية دون ترخيص.

٢– جريمة التسجيل غير المشروع للبيانات الرسمية.

---

[٩٤] د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، سنة ١٩٩٨م، ص٢٠٠.

[٩٥] حيث خول المشرع لرئيس محمة الجنايات سلطة تفويضية بمقتضاها يمكنه أن يتخذ كافة الاجراءات التي يعتقد أنها مفيدة للكشف عن الحقيقة، حيث لا يقدم عليه سوى ضميره وشرفه.

[96] PIERRE Chamabon.Lejuge d'instuction théorie et pratique de la procédure.4ème, edition DALLOZ, 1997, P307.

[٩٧] د. سوزان عدنان الاستاذ، انتهاك حرمة الحياة الخاصة عبر الانترنت، دراسة مقارنة، مجلة دمشق للعلوم الاقتصادية والقانونية، العدد ٣، مجلد ٢٩، سنة ٢٠١٣م، ص٤٣٧.

(ISSN: 2537- 0758)

٣- جريمة الحفظ غير المشروع للبيانات الاسمية.
٤- الانحراف عن الغرض أو الغاية من المعالجة الالكترونية للبيانات الاسمية.
٥- الإفشاء غير المشروع للبيانات الاسمية.

واتساقا مع ذلك نجد أن هناك تشريعات نصت علي إجراءات استخلاص الأدلة الرقمية من خلال النص علي قواعد خاصة بتفتيش الحاسب الآلي، كالتشريع اليوناني الذى نص علي ذلك في المادة ٢٥١ من قانون الإجراءات الجنائية[٩٨]، وكذلك المشرع الكندي الذى أولي الجرائم المعلوماتية أهمية خاصة حيث قام بتعديل القانون الجنائي بحيث يشمل قواعد خاصة بجرائم الإنترنت كما شمل القانون الجديد تحديد العقوبات والمخالفات الحاسوبية وجرائم الدخول غير المشروع لأنظمة الحاسب وقد أوضح هذا القانون صلاحيات جهات التحقيق[٩٩].

كما أن المشرع الكندي تناول الجرائم المعلوماتية واستخلاص الأدلة الرقمية بقانون المنافسة وأكد علي حق مأمور الضبط القضائي متى صدر أمر قضائي أن يقوم بتفتيش أنظمة الحاسب الآلي والتعامل معها، وقد تناول قواعد تفتيش الحاسب الألي في المادة ٤٧٨من القانون الجنائي[١٠٠].

خامسا: الدليل الجنائي الرقمي في التشريعات العربية:

- **الدليل الجنائي الرقمي في التشريع الجزائري:**

المشرع الجزائري أخذ بمبدأ حرية الإثبات، ونص علي ذلك في المادة ٢١٢ من قانون الإجراءات الجزائية الصادر سنة ١٩٦٦م والمعدل بالقانون رقم ٧/١٧ لسنة ٢٠١٧م، حيث اكد علي أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها علي غير ذلك وللقاضي أن يصدر حكمه تبعاً لاقتناعه الشخصي[١٠١]، ومما سبق يتضح أن المشرع الجزائري أكد علي مبدأ حرية الإثبات،

---

(98) Irini Vassilaki, computer crime and other crimes against information technology in Greece. Rev.Intern De.Dr.pen1998.p.371.

(99) Frédéric Debove, François Falletti,précis de droit pénale et procédure pénale2 ème ed,, P.U.F, paris 2001

(100) Donald K Piragoff, Computer crimes and other crimes against information technology in Canda: Rev.Intern.De.Dr.Pen.1993.p.241.

(١٠١) الأمر رقم ١٥٥/٦٦ بتاريخ ٨ يونيو ١٩٦٦م، والمتضمن قانون الإجراءات الجزائية الجزائري، جريدة رسمية، عدد ٤٨ والصادر بتاريخ ١١ يونيو ١٩٦٦م، والمعدل والمتم بالقانون رقم ٠٧/١٧ الصادر بتاريخ ٢٧ مارس ٢٠١٧م، جريدة رسمية، عدد ٢٠، الصدارة بتاريخ ٢٩ مارس ٢٠١٧م.

ولعل من أسباب الأخذ بهذا المبدأ ظهور الأدلة العلمية الحديثة كالبصمة الوراثية والدليل الرقمي فهذا الدليل شأنه في ذلك شأن الأدلة الجنائية الأخرى.

ويعد الدليل الرقمي مقبولاً مبدئياً في إثبات الجرائم التقليدية بصفة عامة، وكذلك يعد دليل إثبات في مجال الجرائم المعلوماتية بصفة خاصة[١٠٢]، وقد أجاز المشرع الجزائري للقاضي أن يوجه إلي مزودي الخدمة من أجل الوصول الي كشف العلميات التي تمت من خلاله والتي تساعد القاضي في استنباط الأدلة التي تساهم في كشف وقائع الجريمة ومرتكبيها.

- **حجية الدليل الجنائي الرقمي في النظام السعودي:**

المملكة العربية السعودية كانت في طليعة الدول التي واكبت التطور السريع في النظام المعلوماتي فشيدت البنية التحتية وفتحت سوق الاتصالات وتنظيم المعاملات الإلكترونية، وتطبيق الحكومة الإلكترونية والتحول إلي مجتمع معلوماتي وهو ما يعنى اعتماد المملكة علي النظام المعلوماتي في كافة المعاملات الرسمية والفردية.

وهو ما دفع المملكة إلي العمل علي اعتبار حماية المعلومات من أهم الأولويات التي تسعى الدولة لتحقيقها من خلال الاتفاقات الدولية والأنظمة المحلية التي يجب أن تواكب التطور في النظام المعلوماتي وما صاحبه من جرائم مستحدثة، لذا لجأت المملكة إلي إصدار نصوص خاصة تواكب هذا التحول وتناسب البيئة التقنية التي تتم من خلالها هذه الجرائم.

وقد أصدر المنظم السعودي نظاما خاصا لحماية المعلومات[١٠٣]، هدف من خلاله إلي الحد من وقوع الجرائم المعلوماتية وذلك بتحديدها والعقوبات المقررة لكل منها، ونص المنظم السعودي علي حجية الأدلة الرقمية في المادة الخامسة من نظام التعاملات الإلكترونية[١٠٤]، وقد أجاز المنظم السعودي للقاضي استنتاج القرائن من خلال مناقشة وقائع الدعوى المنظورة، أو من خلال مناقشة الخصوم أو الشهود، ليكون مستنداً لحكمه بعد اقتناعه، ليحكم بها أو يكمل بها دليلاً ناقصاً ثبت لديه.

---

[١٠٢] د. سامى جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، سنة ٢٠١٤م ص٨١.

[١٠٣] نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/١٧) بتاريخ ٧/ ٣/ ١٤٢٨هـ.

[١٠٤] (يكون للتعاملات والسجلات والتوقيعات الإلكترونية حجيتها الملزمة، ولا يجوز نفى صحتها، أو قابليتها للتنفيذ، ولا منع تنفيذها بسبب أنها تمت– كلياً أو جزئياً– بشكل إلكتروني، بشرط أن تتم تلك التعاملات والسجلات والتوقيعات الالكترونية بحسب المنصوص عليها في النظام).

(ISSN: 2537- 0758)

وهو ما تضمنه نظام المرافعات الشرعية والذى نص علي أنه يجوز للقاضي أن يستنتج قرينة أو أكثر من وقائع الدعوى أو مناقشة الخصوم أو الشهود[١٠٥].

ليكون ذلك مستندا لحكمه أو ليكمل به دليلاً ناقصاً ثبت لديه ليُكون بهما معاً اقتناعه بثبوت الحق لإصدار الحكم"[١٠٦]، كما أكد المنظم السعودي علي قبول القرينة في الإثبات من خلال اعتبار حيازة المنقول قرينة بسيطة للملكية[١٠٧]، وأجاز للمحكمة أن تقرر ندب خبير، لتقديم تقرير عن الواقعة أو تكلفه بإبداء رأيه شفويا في جلسة المحاكمة.

ويتم إثبات رأيه في دفتر الضبط وإذا كان المنظم أعطى للمحكمة الحق في انتداب خبير، فكذلك منح هذا الحق للمحقق، فله أن يستعين بخبير مختص لإبداء الرأي في المسألة المتعلقة بالتحقيق لوجود بعض المسائل العلمية والفنية التي لا يستطيع المحقق التعامل معها، وتتطلب رأى خبير مختص[١٠٨]، كذلك أعطى نظام الإجراءات الجزائية السعودي للخصوم الحق في تقديم تقرير من خبير آخر بصفة استشارية غير ملزمة[١٠٩].

---

[١٠٥] القضية رقم ١٤٣١/٤/٢٩٠هـ اشتملت هذه القضية علي جريمة الكترونية وذلك من خلال توجيه الاتهام الي المتهم بمخالفة الفقرة الثالثة والخامسة من المادة الثالثة من نظام جرائم المعلوماتية السعودي، وذلك من خلال قيام المتهم باختراق موقع المؤسسة عن طريق استخدام الشبكة المعلوماتية من خلال هواتف ثابتة تعود للمتهم تحت اسم مستعار يطلق عليه (عرب فيروس) ومن ثم قام بنقل استضافة الموقع المؤسسة الي صفحات مخترقة وقام بنشر ذلك في المنتديات الحوارية كموقع (سوالف سوفت) معلنا ذلك صراحة والتشهير بمؤسسته والحاق الضرر بها، حتى استرجاع نطاق المؤسسة بواسطة مكتب محاماة تولي القضية، وهو ما ترتب عليه ضرر مادى يقدر بمليون ريال سعودي وضرر معنوي بتشويه سمعة المؤسسة لدى عملائها بأنها لا تستطيع حماية نطاقها الإلكتروني فكيف لها أن تقدم خدمات الحماية لهم، ومن خلال ما تقدم فإن المدعى عليه قد ارتكب فعلا مجرما.

[١٠٦] مادة ١٥٥ من نظام المرافعات الشرعية الصادر بالمرسوم الملكي رقم (م/٢١) بتاريخ ١٤٢١/٥/٢٠هـ.

[١٠٧] مادة ١٥٦ من نظام المرافعات الشرعية.

[١٠٨] **نص المادة ٧٦ من نظام الإجراءات الجزائية السعودي رقم (م/٢) بتاريخ ١٤٣٥/١/٢٢هـ علي أنه:** "للمحقق أن يستعين بخبير مختص لإبداء الرأي في أي مسألة متعلقة بالتحقيق الذى يجريه".

[١٠٩] المادة ٧٨ من نظام الإجراءات الجزائية السعودي.

واعتبر المنظم السعودي الخبراء أعواناً للقضاء وهو ما يجعل الاستعانة بهم أمر تقره النظم السعودية، وهو ما يُمكن من مسايرة التطور العلمي وما صاحبه من ظهور أنماط جديدة للجريمة تتطلب الاستفادة من أراء الخبراء في مسائل لا يمكن للقاضي أن يتوصل إليها إلا من خلال هذا الرأي حتى يستطيع أن يُكون عقيدته للفصل في الدعوى[١١٠].

يتضح لنا مما سبق أن المملكة العربية السعودية تأخذ بالقرائن باعتبارها من الأدلة التي يمكن أن يأخذ بها القاضي في الإثبات وفقاً للضوابط التي نص عليها المنظم السعودي، مما يؤكد حجية الأدلة الرقمية في الإثبات، فيمكن الاستعانة بالخبراء في المسائل العلمية التي لا يستطيع القاضي أو المحقق الفصل فيها إلا من خلال تقرير الخبير المختص.

- **حجية الدليل الرقمي في التشريع الإماراتي:**

أخذ المشرع الإماراتي بمبدأ اقتناع القاضي بالأدلة ونص علي ذلك في المادة ٢٠٩ من قانون الاجراءات الجزائية[١١١]، وبناءا علي ذلك فان القاضي غير مقيد بما تضمنه محضر الاستدلال أو التحقيق الابتدائي ويحكم في الدعوى بناءًا علي قناعته المتكونة لديه من الأدلة المعروضة امامه والمتعلقة بالدعوى، والحقيقة أن الدليل الرقمي يتميز بطبيعة خاصة عن غيره من الادلة التقليدية، فأعمال التفتيش والاستدلال عن الادلة الرقمية يختلف كلية عن باقي الادلة بصفته دليل غير مادى.

وعليه فتكوين قناعة القاضي بالدليل الرقمي مبناها كون هذا الدليل قد تم الحصول عليه بطريق مشروع وهو ما أكدت عليه المادة ٥٣ من قانون الإجراءات الإماراتي[١١٢]، فالقاضي له الحرية في الاستعانة بكافة الطرق لتكوين قناعته للوصول الي الحقيقة ولا يجوز الزامه بقبول الادلة المقدمة من أطراف الدعوى.

دون بحثها وفحصها، ولاشك أن الطبيعة الخاصة للأدلة الرقمية قد تمكن من العبث بها بالإضافة الي أن الخطأ وارد في استخلاص هذه الادلة كونها تحتاج الي خبراء

---

[١١٠] المادية ٨١ من نظام القضاء الصادر بالمرسوم الملكي رقم (م/٧٨) بتاريخ ١٤٢٨/٩/١٩هـ.

[١١١] نصت المادة ٢٠٩ من قانون الاجراءات الجزائية الإماراتي علي "يحكم القاضي في الدعوى حسب قناعته التي تكونت لدية ومع ذلك لا يجوز له أن يبنى حكمه علي أي دليل لم يطرح علي الخصوم أمامه في الجلسة".

[١١٢] **نصت المادة ٥٣ من قانون الاجراءات الجزائية الإماراتي علي** ".....، والجرائم الالكترونية عموما يستحيل التلبس بها والامر الثاني هو ضمانة الحفاظ عليه من التلاعب وهذا يتم من الخبراء واستخلاص الدليل دون اكراه والحفاظ عليه من التلاعب والا اعتبر الدليل باطلا".

(ISSN: 2537- 0758)

متخصصين، وهو ما يوجب علي المحكمة عند نظرها للأدلة الرقمية أن تنظر اليها كوحدة واحدة، ومن خلال هذه الادلة يستطيع القاضي أن يكون قناعته الكاملة بالأدلة المقدمة وهو ما أخذت به المحكمة الاتحادية العليا الامارتية في الطعن رقم ٤١٦ لسنة ٢٠١٤م[١١٣].

فالمحكمة تعاملت مع الأدلة الجنائية الرقمية المتمثلة في مخرجات الحاسب الألي كما تعاملت مع دليل الاعتراف، وهو ما يظهر قيمة الأدلة الرقمية المتحصلة عليها من الحاسوب كدليل مقبول للإثبات الجنائي والدليل الرقمي عادة ما يكون نتيجة تفتيش الحاسوب للجاني أو المجنى عليه من قبل رجال الضبط القضائي وبصحبة الخبراء الذين تتوافر فيهم الحيادية والنزاهة والاستقلال.

ومما تقدم نستخلص ان المشرع الإماراتي قد أعطى الحجية الكاملة للدليل الرقمي في الاثبات الجنائي وساوى بينه وبين الدليل التقليدي، ولكن اشترط في هذا الدليل شروط معينة يجب توافرها مجتمعة بالسجل الإلكتروني ليكون ذو حجية كاملة[١١٤]، وحدد قانون المعاملات الالكترونية الإماراتي في مادته العاشرة عناصر محددة يجب أن تتوافر في الدليل الرقمي لضمان قبوله في الاثبات الجنائي.

---

[١١٣] الطعن رقم ٤١٦ لسنة ٢٠١٤ م جزائي، جلسة الاثنين ٢ فبراير ٢٠١٥ م المحكمة الاتحادية العليا "لما كان المقرر في قضاء هذه المحكمة أن لمحكمة الموضوع السلطة التامة فى تكوين عقيدتها مما تطمئن إليه من أدلة الدعوى، ولها أن تأخذ باعتراف المتهم متى اطمأنت مت اطمأنت اليه لصدوره عن ارادة حرة وأن تستخلص من ذلك الاعتراف الصورة الصحيحة للواقعة، ولا يشترط في الادلة ومنها الاعتراف الذى اعتمدت عليه المحكمة فى حكمها واتخذه سندا لقضائها بالإدانة أن ينبئ في جزئياته عن الواقعة بل للمحكمة أن تعضده بأدلة أو قرائن أخرى ذلك أن الادلة فى الجنائية متساندة يكمل بعضها بعضا حيث تكون المحكمة مجتمعة عقيدتها ولا ينظر الي الدليل بعينه دون باقي الادلة بل يكفى أن تكون تلك الادلة في مجموعها مؤدية الي ما قصده الحكم منها.

[١١٤] اشترطت المادة ٥ من قانون المعاملات الالكترونية في الدليل الرقمي ليكون له الحجية في الاثبات الجنائي أن يتم حفظ مستند أو سجل أو معلومات لأى سبب، وهذا الشرط يكون متوافرا في الحالات التالية: ١- حفظ السجل الإلكتروني بالشكل الذى انشئ به أو ارسل أو استلم به أو بشكل يمكن من اثبات أن يمثل بدقة المعلومات التي أنشئت أو أرسلت أو استلمت في الاصل. ٢- بقاء المعلومات محفوظة علي نحو يتيح استخدامها والرجوع اليها. ٣- حفظ المعلومات ان وجدت التي تمكن من تحديد منشأ الرسالة الالكترونية وجهة وصولها وتاريخ ووقت استلامها وارسالها.

وتتمثل هذه العناصر في مدى امكانية الاعتداد بالطريقة التي تم بها تنفيذ واحدة أو اكثر من عمليات ادخال المعلومات أو تجهيزها أو انشائها أو تخزينها أو تقديمها أو ارسالها، بالإضافة الي مدى امكانية الاعتداد بالطريقة التي استخدمت في المحافظة علي سلامة المعلومات ومدى امكانية الاعتداد بمصدر المعلومات اذا كان معروفا، وكذلك مدى امكانية الاعتداد بمصدر المعلومات ان كان معروفا.

المطلب الثاني
الأدلة الجنائية الرقمية ووسائل الإثبات التقليدية

تمهيد:

يقصد بالإثبات القواعد الخاصة بالبحث عن الأدلة، وإقامتها أمام القضاء وتقديرها من جانبه[١١٥]، وعلي ذلك فالإثبات في المواد الجنائية ما هو إلا كافة الأدلة التي تؤكد وقوع الجريمة، وتحقق حالة اليقين لدى القاصي للفصل في الدعوى فيقضى بالإدانة، أو ترجح حالة الشك لديه فيقضى بالبراءة، ولأجل الحكم بإدانة المتهم في المواد الجنائية يجب ثبوت وقوع الجريمة في ذاتها وأن المتهم هو المرتكب لها، أي وقوع الجريمة بشكل عام ونسبتها للمتهم بوجه خاص[١١٦].

وحتى يتحقق الإثبات فإنه لابد من جمع عناصر التحقيق والدعوى وتقديم هذه العناصر إلي سلطة التحقيق، فإذا أسفر هذا التحقيق عن دليل أو أدلة ترجع معها إدانة المتهم قدمته إلي المحكمة، فإذا توافر الدليل أو الأدلة، واقتنع القاضي بها قضى بإدانة المتهم،أما إذا لم يقتنع بالأدلة المقدمة فإنه يقضى ببراءته[١١٧]، وتخضع الأدلة الجنائية الرقمية لوسائل الإثبات، بالإضافة إلي انضمام الخبرة التقنية إلي علم الخبرة المتميزة بتصنيف التعامل مع موضوع الدعوى.

من حيث الاستعانة بالمختصين في مجال النزاع[١١٨]، وتعد المعاينة والتفتيش والشهادة، من وسائل جمع الأدلة، ولكل منها قواعده التي يجب إتباعها، وهو ما سوف نتناوله في النقاط الآتية:

---

[١١٥] د. محمد زكى أبو عامر، الإثبات في المواد الجنائية، دار المطبوعات الجامعية، الإسكندرية، سنة ٢٠١٢م، ص١٩.

[١١٦] د. محمود محمود مصطفى، الإثبات فى المواد الجنائية فى القانون المقارن، الجزء الأول النظرية االعامة، الطبعة الأولي، مطبعة جامعة القاهرة، سنة ١٩٧٨م ص١٣.

[١١٧] د. محمود محمود مصطفى، الإثبات فى المواد الجنائية فى القانون المقارن، مرجع سابق ص١٧.

[١١٨] د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ص١٤١.

(ISSN: 2537- 0758)

أولاً: المعاينة:

تتضاءل أهمية المعاينة فيما يتعلق بالأدلة الجنائية الرقمية ويرجع ذلك لندرة الآثار المادية للجريمة المعلوماتية، كما أن طول الفترة بين وقوع الجريمة واكتشافها يكون له التأثير السلبي علي الآثار الناجمة عنها بسبب قيام الجاني بالعبث بها أو إتلافها أو حتى محوها[١١٩]، ولكن في كل الأحوال عند تلقى البلاغ عن وقوع الجريمة المعلوماتية، وبعد التأكد من البيانات الضرورية في هذا البلاغ، يتم الانتقال إلي مسرح الجريمة لمعاينته، ولاشك أن مسرح الجريمة المعلوماتية يختلف عن مسرح الجرائم التقليدية، فقد تكون الجريمة المعلوماتية مستمرة كما في جرائم السرقة وجرائم الاحتيال.

وقد تكون كالجرائم التقليدية وقتية كالتزوير وإتلاف البرامج والجرائم الإرهابية، فإذا كانت الجريمة مستمرة فإن الهدف من المعاينة يكون بغرض المداهمة وضبط الأدلة، أما إذا كانت الجريمة وقتية فيتوقف الأمر علي اعتراف الجاني متى تم القبض عليه وكذلك شهادة الشهود والقرائن.

الضوابط التي يجب مراعاتها عند المعاينة[١٢٠] في الجرائم المعلوماتية:

١- تصوير الحاسب محل الواقعة والأجهزة المتصلة به.
٢- تسجيل وقت وتاريخ ومكان التقاط الصور الخاصة بالحاسب محل الواقعة.
٣- وضع الخطة المناسبة لضبط الأدلة الرقمية من خلال الفريق الذى سيتولى المعاينة.
٤- الاهتمام بالطريقة التي تم بها إعداد النظام.
٥- إجراء عمليات المقارنة والتحليل من خلال إثبات حالة التوصيلات والكابلات بكل مكون من مكونات النظام.
٦- إجراء الاختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن تسبب في محو البيانات المسجلة.
٧- التحفظ علي الشرائط والأقراص الممغنطة غير السليمة وفحصها ورفع ما بها من بصمات ذات الصلة، وكذا التحفظ علي الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة.
٨- التحفظ علي مستندات الإدخال والمخرجات الورقية ذات الصلة بالواقعة محل المعاينة.

---

[١١٩] د. محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، مرجع سابق ص٤٣.

[94] Robert Taylor: Computer Crime, "in criminal investigation" edited by Charles swanson, N. chamelin and L. Territto, Hill inc. 5th edition 1992. p.450

٩- يقوم بالمعاينة الخبراء من التقنين والفنيين الذين تتوافر لهم الكفاءات العلمية والخبرة الفنية في مجال الحاسب الآلي.

١٠-خضوع كافة الإجراءات لمبدأ المشروعية ووفقا لما تنص عليه التشريعات الجنائية.

وينبغي عند إجراء المعاينة أن نتعامل مع مسرح الجريمة المعلوماتية علي أنهما شقان، فالأول منهما مسرح تقليدي يقع خارج بيئة الحاسوب، وهو بشكل رئيسي يتكون من المكونات المادية المحسوسة للمكان الذى وقعت فيه الجريمة، فقد يترك المتهم آثار كالبصمات وبعض الاثار التي تدل عليه، أما الشق الثاني فهو متعلق بالمسرح الافتراضي الذى يقع في البيئة الافتراضية بالإنترنت، ويتكون من البيانات والمعلومات المخزنة داخل الحاسوب(١٢١).

كما يتكون المسرح الافتراضي من ذاكرة الاقراص الصلبة بداخل الحاسوب، ويكون التعرف علي هذا المسرح عبر الافتراضي، ونظرا لخصوصية الادلة الرقمية وهو ما يستوجب التقنيات الحديثة للكشف عنها من قبل خبراء وذلك باتباع القواعد الفنية كتوفير معلومات مسبقة عن مكان وقوع الجريمة ونوع الاجهزة وشبكات الاتصال، بالإضافة الي ضرورة توافر أجهزة وبرامج كبرامج معالجة الملفات (La plink) ويستخدم هذا البرنامج للكشف عن حقيقه الادلة الجنائية الرقمية، وهو ما تستخدمه المبحث الفيدرالية الأمريكية في التحقيقات الجنائية(١٢٢).

ولاشك أن المعاينة وإن كانت غير ذات جدوى في بعض الجرائم،إلا أنها تساعد في الكشف عن الكثير من الجرائم من خلال معاينة مسرح الجريمة المعلوماتية، ويتمثل ذلك في تصور كيفية وقوع الجريمة وظروف وملابسات ارتكابها وتوفر الأدلة المادية التي يمكن تجميعها، وإن كان ذلك قليل بالنسبة للجرائم المعلوماتية(١٢٣).

ثانيًا: **التفتيش**:

يُعد التفتيش أحد أخطر وأهم إجراءات التحقيق الابتدائي، فهو خطير بطبيعته لأنه يمس السر لدى المشتبه فيه أو حق في المحافظة علي أسراره الخاصة، وذلك بالتنقيب

---

(121) Robert Taylor: Computer Crime, "in criminal investigation" edited by Charles swanson, N. chamelin and L,op cit. 504.

(١٢٢) د. سامى جلال فقي حسين، الادلة المتحصلة من الحاسوب وحجيتها في الاثبات الجنائي مرجع سابق، ص ٢١٢.

(١٢٣) د. هشام فريد رستم، الجرائم المعلوماتية، أصول التحقيق الفني واقتراح بإنشاء ألية عربية موحدة للتدريب التخصصي، بحث مقدم إلي مؤتمر القانون والحاسب الآلي والإنترنت، خلال الفترة ١:٣ مايو، سنة ٢٠٠٠م، كلية الشريعة والقانون، العين، دولة الإمارات العربية المتحدة، ص١٠١.

(ISSN: 2537- 0758)

في شخصه أو مسكنه أو رسائله أو متاعه، ولا يخفى أن الحق في السرية هو الوجه الآخر لحق الإنسان في الحياة الخاصة[١٢٤]، ويجب علي المحقق الجنائي المبادرة لإجراء التفتيش وذلك قبل قيام الجاني بطمس معالم الجريمة وإخفاء كل ما يتعلق، والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية.

فيقصد به إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلي نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلي أدلة تفيد في إثبات الجريمة ونسبتها إلي المتهم[١٢٥]، فالتفتيش علي ذلك يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وهو ما قد يتنافر مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي، مما يتعين إخضاع الجرائم المعلوماتية لإجراءات مستقلة تلاءم الطبيعة الخاصة لها، فيجوز التفتيش في هذه الجرائم من خلال ضبط الوعاء المادي لهذه المعلومات كالأقراص والأسطوانات الممغنطة[١٢٦].

لكن توجد بعض الصعوبات الإجرائية التي تعيق خضوع البيانات المخزنة آلياً لقواعد التفتيش التقليدية والتي منها تعدد الأماكن التي يوجد بها النظام المعلوماتي داخل أو خارج الدولة، وهناك صعوبة في تحديد الأشياء التي يهدف إلي ضبطها من عملية التفتيش وغيرها من الصعوبات مثل عدم اكتمال المعرفة المعلوماتية والتقنية لتنفيذ عملية التفتيش[١٢٧]، ولذلك يخضع التفيش في الجرائم المعلوماتية لشروط شكلية وآخري موضوعية:

الشروط الموضوعية للتفتيش في بيئة الإنترنت:

التفتيش يجب أن يكون له محل وقد يكون هذا المحل مكان أو شخص ويشترط أن يكون محدداً أو قابلاً للتحديد وأن يكون مشروعاً، أي يرد التفتيش علي محل جائز

---

[١٢٤] د. أحمد فتحي سرور، القانون الجنائي الدستوري، الشرعية الدستورية في قانون العقوبات، الشرعية الدستورية في قانون الإجراءات الجنائية، دار الشروق، القاهرة، سنة ٢٠٠٦م، ص٢٠٥.

[١٢٥] د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، سنة ١٩٩٧م، ص ٧٣.

[١٢٦] د. هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق ص٦٨.

[١٢٧] د. عفيفي كامل عفيفي، جرائم الحاسب الآلي وحقوق المؤلف والمصنفات الفنية، مرجع سابق ص٣٤٤.

قانوناً، وبناءاً علي ذلك لا يجوز تفتيش السفارات ومنازل السفراء ورجال السلك الدبلوماسي، ولا يجوز تفتيش المدافع عن المتهم أو الخبير الاستشاري لضبط أوراق أو مستندات سلمه له المتهم لأداء مهمته الدفاعية[١٢٨]، ومحل التفتيش في جرائم الإنترنت هو الحاسب الآلي الذى يعتبر النافذة التي يستخدمها الجاني لتنفيذ جرائمه.

ويشمل ذلك مكونات الخادم والمزود الآلي والمضيف وملحقات التقنية، ولا يكون ذلك قائما بذاته بل يشمل عقار أو مكان ما، وقد يكون بصحبة مالكه أو حائزه أي أنَّ الحرز الذى يوجد فيه الحاسب الآلي هو بطبيعته حرز مادى[١٢٩].

ويجب علي مأمور الضبط القضائي عند استصداره لأذن التفتيش أن يحدد محل ذلك الإجراء تحديداً دقيقاً وكذا الغرض منه، وأن يتأكد من جواز تفتيشه وإلا كان هذا الإجراء باطلاً، كما يجب أن يكون للتفتيش سبب ولا يقوم هذا السبب إلا إذا كانت هناك جريمة وقعت بالفعل، سواءا كانت جناية أو جنحة وأن تكون هناك قرائن وأمارات قوية علي وجود أشياء تفيد في كشف الحقيقة، سواءاً مع المتهم أو مسكنه أو شخص آخر أو مسكن غيره، فالجريمة المعلوماتية قد تقع علي الشبكة ذاتها أو تقع باستخدامها.

الشروط الشكلية للتفتيش في الجرائم المعلوماتية:

النيابة العامة هي سلطة التحقيق والمختصة بالتفتيش وبالتالي فالتفتيش في هذه الجرائم يخضع للخصائص العامة التي تخضع لها كافة إجراءات التحقيق الابتدائي، كوجوب التدوين بمعرفة كاتب والسرية عن الجمهور والخصوم ووكلائهم، ولابد أن يكون أمر التفتيش مسبباً وهذا التسبيب ضمان لتوافر العناصر الواقعية التي بها سبب التفتيش.

وللنيابة العامة أن تندب مأمور الضبط القضائي مع مراعاة الاختصاص المكاني والنوعي، فإذا وجدت أجهزة استدعاء إلكترونية في حوزة المتهم جاز للمحكمة أن تسمح لمأمور الضبط القضائي بالاطلاع عليها[١٣٠]، وفى حالة وجود أجهزة تخزين إلكترونية تحتوى معلومات أكثر من جهاز الاستدعاء في حوزة المتهم فإنه يجوز لمأمور الضبط القضائي تفتيشها بالقياس علي الأشياء المادية في الجرائم التقليدية[١٣١].

---

[١٢٨] د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، مرجع سابق ص٤٢٣.

[١٢٩] د. سامى حسين الحسيني، النظرية العامة للتفتيش في القانون المصري والقانون المقارن مرجع سابق، ص٢١٠.

[١٣٠] د. هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي، مرجع سابق ص ٧٨.

[١٣١] د. هلالي عبد اللاه أحمد، تفتيش نظام الحاسب الآلي، مرجع سابق ص١٥٧.

(ISSN: 2537- 0758)

والتفتيش لاستخلاص الأدلة الجنائية الرقمية، يكون محله كل مكونات الحاسب الآلي سواءاً كانت مادية أو معنوية، وكذا شبكات الاتصال الخاصة به بالإضافة الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش، وتشمل برامج النظام وبرامج التطبيقات سابقة التجهيز، ويتم ذلك بمعرفة الخبراء الفنيين والتقنيين الذين تنتدبهم سلطات التحقيق، والذين يتمتعون بالخبرة والمهارة التقنية في نظم الحاسب الآلي[١٣٢].

ثالثاً: الشهادة:

الشهادة في الجرائم المعلوماتية لا تختلف من حيث ماهيتها عن الجرائم التقليدية، فللخصوم أن يطلبوا سماع من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية وله أن يسمع من يتقدم بشهادته من تلقاء نفسه.

والشاهد في الجريمة المعلوماتية هو الفني أو التقني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذى تكون لدية معلومات جوهرية أو هامة متعلقة بموضوع الجريمة، إذا كانت مصلحة التحقيق تقضى ذلك.

ويتميز الشهود في الجريمة المعلوماتية بأنهم خبراء في تقنية الحاسب أي لهم دراية تامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به، واستخدام لوحة المفاتيح في إدخال البيانات وتكون لديهم معلومات عن قواعد كتابة البرامج[١٣٣]، كما يتميز الشاهد المعلوماتي بأنه محلل يقوم بتحليل الخطوات ويقوم بتجميع بيانات النظام وتحليلها إلي وحدات منفصلة واستنتاج العلاقات الوظيفية منها. كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب الآلي، كما أن من الشهود في الجرائم المعلوماتية المبرمجون وهم الأشخاص المتخصصون في كتابة أوامر البرامج[١٣٤]، ويشمل مهندسو الصيانة والاتصالات وهم

---

[١٣٢] د. عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول، حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، خلال الفترة ٢٦: ٢٨ أبريل، سنة ٢٠٠٣م، ص٦١٠. **وأنظر في هذا الشأن** د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والإنترنت، مرجع سابق ص ٣٨٨.

[١٣٣] د. محمد فهمى، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، سنة ١٩٩١م، ص٢٣.

[١٣٤] د. هلالي عبد اللاه أحمد، التزام الشاهد بالأعلام في الجرائم المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، سنة ٢٠٠٠م، ص ٢٤.

المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به، ومديرو النظم وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[١٣٥].

فكلاً من التفتيش والمعاينة وسماع الشهود في الجرائم المعلوماتية يقود إلي الكشف عن الأدلة الجنائية الرقمية، من خلال إجراء الاختبارات التكنولوجية والعلمية عليه لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنقاذ وتطبيق القانون، وتحديد الخصائص الفريدة للدليل الرقمي، وإصلاح الدليل وإعادة تجمعيه من المكونات المادية للكمبيوتر.

كما يؤدى ذلك إلي عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل، وجمع الآثار المعلوماتية الرقمية التي قد تكون تبدلت خلال الشبكة المعلوماتية، وتحريز الدليل الرقمي لإثبات أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة فى الدعوى.

المبحث الثالث
ذاتية الأدلة الجنائية الرقمية

مقدمة:

عمدت العديد من الدول إلي استخدام الأدلة الجنائية الرقمية في الإثبات من خلال إجراء تعديلات علي القواعد الإجرائية لتطوير أساليب مكافحة الجرائم المعلوماتية، إلا أن هناك مجموعة من الصعوبات والمعوقات التي تعترض عملية استخلاص الأدلة الجنائية الرقمية، وسوف نقسم هذا المبحث إلي ثلاثة مطالب يتناول الاول الدليل الرقمي والحق في الخصوصية ويتناول الثاني صعوبة الاثبات الجنائي بالأدلة الرقمية، ونخصص الأخير لطبيعة الدليل الرقمي.

المطلب الأول
الدليل الرقمي والحق في الخصوصية

القواعد الجنائية التي تمثل اعتداءًا علي الحقوق والحريات التي يتمتع بها اطراف العلاقة الجنائية تكون باطلة، ولما كانت الاجراءات الجنائية هي مصدر الأدلة التي يؤسس القاضي عليها اقتناعه بالإدانة، فقبول هذه الادلة يتوقف علي مشروعية

[١٣٥] د. خالد محمد المهيري، التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، الطبعة الثانية، دار الغرير للطباعة والنشر، بدون سنة نشر، دبي، الإمارات العربية المتحدة، ص٥٠٨.

(ISSN: 2537- 0758)

الاجراءات التي تم وفقها تم الحصول عليها ومخالفة هذه الاجراءات في الحصول علي الادلة يترتب عليه البطلان[١٣٦].

ولقد تضمن الدستور المصري الصادر ٢٠١٤ م ضوابط لشرعية الاجراءات الجنائية الماسة بالحريات الفردية حيث نص علي أنه "للحياة الخاصة حرمة وهى مصونة لا تمس، وللمراسلات البريدية، والبرقية، والالكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الاحول التي يبنها القانون.

كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة اشكالها، ولا يجوز تعطيلها أو وفقها أو حرمان المواطنين منها بشكل تعسفي[١٣٧]، ولقد وضعت الاتفاقيات الدولية والدساتير الوطنية والقوانين الإجرائية نصوصا تتضمن الحماية للحق في الخصوصية[١٣٨]، ومن ثم فإن مخالفة الدليل الجنائي الرقمي لهذه النصوص يضفى عليه عدم المشروعية، فلا يجوز الاعتماد علي الادلة الجنائية الرقمية التي تم تحصيلها بطريقة غير مشروعة، أو التي تم التوصل اليها بطرق تتعارض مع القواعد القانونية العامة[١٣٩].

ومقتضى ما تقدم فإن الادلة الجنائية الرقمية لا تكون صالحة للاستدلال بها الا اذا جرت عملية البحث عنها والحصول عليها في اطار أحكام القانون وقيم العدالة واخلاقياتها[١٤٠]، فإجراءات جمع الأدلة الرقمية اذا خالفت القواعد القانونية والمبادئ التي نصت عليها الاتفاقيات الدولية لحماية الحريات والحقوق تكون باطلة، الا ان مصلحة المجتمع أو المصلحة العامة تعد في ذات الوقت قيمة دستورية لا يجوز التضحية بها.

---

[١٣٦] د. احمد فتحي سرور، القانون الجنائي الدستوري، الشرعية الدستورية في قانون العقوبات، الشرعية الدستورية في قانون الاجراءات الجنائية، دار الشروق، مرجع سابق، ص ٥٥٠.

[١٣٧] المادة ٥٧ من الدستور المصري ٢٠١٤م.

[١٣٨] **أنظر المواد** من ٢: ١٠ من الدستور الألماني ١٩٤٩م، المواد ١٠: ١٣ من الدستور السويسري ١٩٩٩م، والمواد ٥، ١١، ١٢ من الاعلان العالمي لحقوق الانسان ١٩٤٨م، والمواد ٣، ٨، ٣٨ من الاتفاقية الاوربية لحقوق الانسان والحريات الاساسية ١٩٥٠.

[١٣٩] كالمبادئ العامة التي توجب احترام قيم العدالة وأخلاقيتها، النزاهة في الحصول علي الادلة أو احترام حقوق الدفاع.

[١٤٠] د. احمد فتحي سرور، القانون الجنائي الدستوري مرجع سابق، ص ١٢٣.

وارى أن الاستعانة بالأدلة المستخرجة من شبكة الانترنت أو الحواسيب كدليل علي وقوع الجريمة يستهدف المصلحة العامة حتى تتمكن الدولة من حماية النظام الاجتماعي كي لا ينهار بسبب الاحترام المبالغ فيه للحقوق والحريات ولا يمكن الاعتراض علي هذه الادلة بحجة عدم مشروعية الدليل الرقمي.

وقد أكدت التشريعات الفيدرالية في الولايات المتحدة الأمريكية علي حق السلطات المختصة في إجبار شركات التواصل الاجتماعي علي تقديم الأدلة الجنائية الرقمية المتعلقة بالواقعة التي يتم التحقيق بشأنها، وذلك دون حاجة لأمر قضائي(١٤١).

ويسمح قانون الاتصالات المخزنة الأمريكي الحصول علي سجلات العملاء من خلال الحصول علي إذن من الشركة المسؤولة، ويوفر القانون الحماية التشريعية للحق في الحياة الخاصة، من خلال تحديد الفترة الزمنية التي يجوز للسلطات خلالها الحصول علي هذه الأدلة وهى ستة أشهر من تاريخ الحصول علي الإذن(١٤٢).

وقد قضت محكمة نيويورك الأمريكية بأنه لا توجد توقعات معقولة للحق في الحياة الخاصة فيما يتعلق بالتغريدات التي ترسل علانية من خلال توتير، فالكشف عن محتوى الحساب الخاص للجاني علي "توتير" لا يشكل انتهاكا للحق في الحياة الخاصة وذلك لأنه لم يتم الاعتداء ماديا علي حقوق الملكية، كما لا يوجد انتهاكاً للحياة الخاصة فالمتهم أرسل تغريداته عبر منصة توتير للجميع(١٤٣).

كما قضت المحكمة العليا بنيويورك بأنه لا مجال للتمسك بالحق في الحياة الخاصة بالنسبة للمراسلات التي يتم ارسالها عبر مواقع التواصل الاجتماعي لأنها علنية ويطلع عليها الجميع(١٤٤). وفى قضية أخرى أدين المتهم بجريمة الاعتداء البدني علي صديقته،

---

(١٤١) يمنح قانون الاتصالات المخزنة الأمريكي "the Stored Communication Act of1986" السلطات المختصة الحق في إجبار مزودي الخدمة علي تسهيل مهمة الحصول علي الأدلة الجنائية الرقمية من خلال اطلاع رجال السلطات المختصة علي المراسلات والتغريدات بالإضافة الي السجلات المتعلقة بالمستخدمين كالاسم والعنوان وذلك في حالات محددة.

(١٤٢) د. سامى حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الاثبات الجنائي دراسة مقارنة في القانونين الإنجليزي والأمريكي، دار جامعة حمد بن خليفة للنشر والطباعة، ٢٠١٧م.

يمكن الاطلاع علي البحث عبر الموقع

https://www.qscience.com/docserver/fulltext/irl/2017/3/irl.2017.14.pdf?expires=1609578014&id=id&accnam

(143) People Homis,945.N.Y.Crime2012.

(144) Romano v.Steelcase Inc 907N.Y.S.2d650 SUP 2010.

(ISSN: 2537- 0758)

وأثناء المحاكمة قدمت النيابة العامة دليلا رقميا يتمثل في رسائل أرسلها من حسابه عبر مواقع التواصل.

تفيد بأنه قد ندم علي هذا الاعتداء طالبا من المجنى عليها الصفح عنه، وقد أقرت محكمة الاستئناف أن المراسلات الالكترونية عرضة للتحريف والتلاعب، ولكنها طلبت التحقق من أصالة الدليل وأن الرسائل المرسلة من الحساب الخاص للمتهم(١٤٥).

ولاشك أن الدليل الجنائي الرقمي المستخلص من مواقع التواصل الاجتماعي قد يرتبط مباشرة بالواقعة المرتكبة أو مصداقية الشهادة أو معرفة إذا ما كان هناك تلاعب بالأدلة، وتعتمد قيمة هذه الأدلة علي أصالته من خلال اقتناع المحكمة بأن الدليل الرقمي يتمتع بالمصداقية المطلوبة، فالأدلة الجنائية الرقمية المستخلصة من تلك الوثائق يمكن الاعتماد عليها في الاثبات الجنائي في حال تقديم الوثيقة ذاتها أو نسخة من الوثيقة تمت المصادقة عليها بأي طريقة تجيزها المحكمة(١٤٦).

وقد أعطى قانون العدالة الجنائية الإنجليزي لمحكمة الموضوع سلطة تقديرية واسعة فيما يتعلق بقبول الدليل الجنائي الرقمي، بالرغم من أنه لم يوضح الكيفية التى من خلالها يقوم القاضي بتقييم أصالة هذه الادلة، وفى المقابل نجد القوانين الأمريكية نصت صراحة علي أنه يجب علي الخصم عند تقديمه دليلا رقميا أن يثبت صحة ما يدعيه(١٤٧).

وعادة ما يتم تقديم الدليل المتحصل من مواقع التواصل الاجتماعي من قبل الجهة المختصة، ولكن في بعض المناسبات يقدم الدليل من المجنى عليه أو من محاميه، أما إذا كان الحساب عاماً، فإن الدليل يكون قريبا جدا من الحقيقة

الادلة المتحصلة من وسائل التواصل الاجتماعي

استخدام وسائل التواصل الاجتماعي أصبح أمراً شائعاً، حيث أن ٩١% من البالغين يستخدمونها بصورة منتظمة، وأصبح أفراد المجتمع المصري يمضون وقتا طويلا على مواقع التواصل الاجتماعي، وتشير الدراسات لي أن استخدام هذه المواقع زاد في مصر بنسبة ٤٦٥% منذ عام ٢٠١١م، وتعد المعلومات التي تتوفر علي مواقع التواصل الاجتماعي ذات أهمية.

---

(145) Compbll v.State, 382 SW.3d 545, 546.

(١٤٦) المادة ١٣٣ من قانون العدالة الجنائية الإنجليزي لسنة ٢٠٠٣.

(١٤٧) المادة ٩٠١ من قواعد الاثبات الفيدرالية في الولايات المتحدة الأمريكية تنص علي "لغايات استيفاء متطلبات الأصالة أو تحديد الدليل، يتعين علي الخصم دليلا كافيا لإثبات صحة ما يدعيه".

فهي قادرة علي تزويد أجهزة التحقيق بمعلومات كاملة عن صاحب الحساب، اضافة الي المراسلات الموجودة والصور التي تم تحميلها علي الموقع، وقائمة الاصدقاء.

ولم يعد سراً القول بأن أجهزة التحقيق قد تقوم بطلب تفتيش مواقع التواصل الاجتماعي بحثاً عن أدلة متعلقة بالواقعة محل التحقيق، بما يفيد في كشف الجريمة ومرتكبيها[١٤٨]، وهو ما أكده المشرع المصري في القانون رقم ١٧٥ لسنة ٢٠١٨م، من ان السلطات المصرية تعمل مع نظيراتها بالبلاد الاجنبية في اطار الاتفاقيات الدولية والاقليمية والثنائية المصدق عليها، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنية المعلومات.

والمساعدة علي التحقيق فيها وتتبع مرتكبيها، علي أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن وتوجد بالمركز الوطني إدارة خدمات التحليل الجنائي الرقمي (الطب الشرعي الرقمي)[١٤٩].

وقد أعطى قانون الجرائم المعلوماتية المصري الحق لجهة التحقيق المختصة في اصدار امر بضبط أو سحب أو جمع أو التحفظ علي البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو دعامة الكترونية أو حاسب تكون موجودة فيه، علي أن يتم تسليم أدلتها الرقمية الي الجهة مصدرة الأمر[١٥٠].

كذلك لجهة التحقيق المختصة أن تصدر أمراً بالبحث والتفتيش والدخول والنفاذ الي برامج الحاسب وقواعد البيانات وغيرها من الاجهزة والنظم المعلوماتية، تحقيقا لغرض الضبط، ولها ان تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي. أو جهاز تقنى موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وما تم من اتصالات علي ذلك النظام أو الجهاز التقني.

---

[١٤٨] تملك ادارة الشرطة في ولاية نيويورك بالولايات المتحدة الأمريكية وحدة خاصة لمواقع التواصل الاجتماعي، تكون مهمتها البحث في فيسبوك وتوتير وغيرهما من مواقع التواصل من أجل البحث عن أدلة أو ضبط أي نشاط إجرامي. **للمزيد راجع**

Rocco Parascandola, NYPD forms new social media unit to mine Facebook and Twitter for mayhem, N.Y.DAILY News, 10 Aug. 2011.

[١٤٩] **تهدف هذه الادارة الي:** ١) المحافظة علي سلامة المصنوعات الرقمية كدليل للكيانات المسؤولة، ٢) استرجاع وتحليل وتحديد الأدلة لتقدير التأثيرات المحتملة للأنشطة الخبيثة علي الضحية، ٣) تقييم نوايا وهوية مرتكبي الجرائم، ٤) اتخاذ الإجراءات الخاصة بعملية الطب الشرعي الرقمي في وقت قصير مع مراعاة تحقيق اعلي جودة في التحليل واعداد التقارير.

[١٥٠] المادة رقم ٦ من القانون رقم ١٧٥ لسنة ٢٠١٨م بشأن الجرائم المعلوماتية.

(ISSN: 2537- 0758)

المطلب الثاني
صعوبة الاثبات الجنائي بالأدلة الرقمية

مقدمة:

هناك مجموعة من الصعوبات التي تواجه استخدام الأدلة الجنائية الرقمية سوف نوضحها من خلال العناصر التالية:

أولاً: **الأدلة الجنائية الرقمية غير مرئية**:

تتميز الجرائم المعلوماتية بأنها تتم في بيئة مختلفة عن الجريمة التقليدية، وهو ما يجعل الدليل الجنائي الرقمي غير مرئي، وهو ما يزيد من صعوبة جمعه وتحليله[١٥١]، إذ تكون الأدلة الرقمية عبارة عن بيانات ومعلومات في البيئة الافتراضية، وهو ما يستلزم أن يقوم علي إثبات تلك الأدلة محققين ذو خبرة فنية ودراية كافية ومهارة كبيرة في التعامل مع التقنية المعلوماتية[١٥٢].

ثانياً: **سهولة محو الأدلة الرقمية**:

الصعوبة الأكبر التي تواجه استخدام الأدلة الجنائية الرقمية في الإثبات هي سهولة تدميرها، فالجاني في الجرائم المعلوماتية يتمتع بقدر كبير من الذكاء.

والخبرة والثقافة مما يؤهله إلي إتلاف وتدمير أو تعديل أي دليل رقمي يؤدى إلي إدانتهم[١٥٣].

ثالثا: **صعوبة الوصول إلي الدليل الرقمي علي وجه الدقة**:

تعد عملية استخلاص الأدلة الجنائية الرقمية معقدة وتكتنفها صعوبة بالغة، نظراً لكم المعلومات والبيانات الهائل التي يجب فحصها وتحليلها، حتى يتم الوصول إلي الدليل المتعلق بالواقعة، فيجب علي من يتولى التحقيق أن يكون خبيرا بأعمال التقنية، كذلك يكون له القدرة علي فحص كم هائل من المعلومات والبيانات المخزنة علي الحاسب الآلي أو في دعائم التخزين الرقمية[١٥٤].

---

(151) Schneider, Brent, High: Technology Crim Investigating Cases Involving Computers, San Jose: K.S.K publications, 1999, P. 27.

[١٥٢] د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولي، دار الفكر الجامعي، مصر، سنة ٢٠٠٦م ص ٧٨.

[١٥٣] د. هشام محمد فريد رستم، أصول التحقيق الجنائي الفنى، مرجع سابق ص٤٢٩.

[١٥٤] د. هشام محمد فريد رستم، أصول التحقيق الجنائي الفني، ص٤٣١.

رابعاً: **انعدام الأثر المادي للجريمة في بعض الجرائم**:

هناك صعوبة كبيرة تتعلق بإثبات الجريمة المعلوماتية، فغياب الدليل المرئي وسهولة وسرعة إخفاء الجريمة، وكذلك صعوبة الوصول إلي الدليل بوسائل الحماية الفنية، إضافةً إلي إحجام العديد من المؤسسات المعتدى عليها عن الإبلاغ عن جرائم الحاسب وكذلك أمكانية ارتكاب الجرائم المعلوماتية عبر مجموعة من الدول أو قد تتعدى تلك الجرائم من قارة إلي قارة أخرى.

خامساً: **صعوبة استعادة البيانات المخفية**:

يستطيع الجاني في الجرائم المعلوماتية، أن يقوم بإخفاء المعلومات أو البيانات، عن طرق أنشاء نظام ملفات أمن عبر الإنترنت وهو ما يجعل عملية استعادتها أو تركيبها في غاية الصعوبة.وهو ما يجعل عملية استعادتها أو تركيبها في غاية الصعوبة أمام المحقق أو القاضي، وهو ما يزيد من صعوبة الحصول علي الأدلة الجنائية الرقمية[١٥٥].

سادساً: **قلة خبرة المحققين في الجرائم المعلوماتية**:

يواجه الخبير الجنائي بعض الصعوبات في سبيل جمع الادلة الجنائية الرقمية والتي تتمثل في فقدان جزء من المعلومات والاوامر التي تتكون منها الأدلة الرقمية حال اغلاق الحاسوب.

بطريقة غير صحيحة أو في حالة انقطاع التيار الكهربي عن الحاسوب، فيؤدى هذا الي ازالة بعض المعلومات من ذاكرة الجهاز أو تحريفها أو منع نظام التشغيل من إعادة التحميل وهو ما يؤدى إلي فقدان الأدلة الرقمية[١٥٦].

كما أن المتهم قد يقوم بتهيئة الحاسوب للتدمير بمجرد البدء في تشغيله، كما أنه من الصعوبات التي تواجه الخبير عند جمعه للأدلة الرقمية طبيعة مسرح الجريمة، فهو عبارة عن شبكات الانترنت المنتشرة علي المستوى الدولي، وهو ما يصعب من الحصول علي الأدلة في حالة توزيع مسرح الجريمة بين أكثر من دولة.

بسبب تعقد الاجراءات أو وجود مشاكل عملية وتشريعية في بعض الدول مما يحول دون الحصول علي الدليل الجنائي الرقمي، بالإضافة الي تعمد الجناة في الجرائم

---

[١٥٥] د. عبد الناصر محمد فرغلي، الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، مرجع سابق ص ٣٢.

[١٥٦] د. هشام محمد فريد رستم، أصول التحقيق الجنائي الفني، مرجع سابق ص٣٧.

(ISSN: 2537- 0758)

المعلوماتية اخفاء هويتهم حال ولوجهم الي شبكة الانترنت، سوآءا باستخدامهم بعض البرامج والتطبيقات التي تؤدى الي طمس هويتهم، وهو ما يشكل عائقا أمام الخبير.

كذلك قد يلجأ الجناة الي إخفاء المعلومات أو البيانات وهو ما يجعل عملية بناء الأدلة الرقمية أو استعادتها في غاية الصعوبة أمام الخبير، كذلك تشكل قلة خبرة المحققين وعدم مسايرتهم للتطورات الهائلة في مجال الحاسب الآلي، وعدم تدريبهم علي معرفة الأساليب والتقنيات المستخدمة والمستحدثة في الجرائم المعلوماتية، عائقاً أمام الوصول إلي الأدلة اللازمة للفصل في الدعوى.

وهو ما دفع المشرع المصري إلي النص علي أن من يتولى استخلاص هذ الأدلة مختصين وخبراء في أجهزة الحاسب الألي، ويقيد هؤلاء الخبراء والفنيين في سجلان، فيخصص أولهما للخبراء من الفنيين والتقنيين بالجهاز[١٥٧]، ويخصص الآخر الخبراء من الفنيين والتقنيين من غير العاملين به[١٥٨]، وطيق عليهم في ممارسة عملهم وتحديد التزاماتهم، وحقوقهم، والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء، وهو نفس ما انتهجته فرنسا، حيث أنشأت المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات.

والاتصالات بموجب المرسوم الوزاري رقم ٢٠٠٠/٤٠٥ الصادر بتاريخ ٢٠٠٠/٥/١٥م، والذى أنشأ وحدات متخصصة وغير متخصصة ضمن جهازي الشرطة والدرك لمكافحة الجريمة المعلوماتية.

سابعاً: طمس الهوية:

عند استخدام المجرم المعلوماتي الإنترنت يتعمد إخفاء هويته عن طريق استخدام بعض البرامج أو التطبيقات التي تعمل علي طمس الهوية، مما يشكل صعوبة كبيرة أمام المحققين أو القضاء لاستخلاص الأدلة الجنائية الرقمية كذلك قد يلجأ الجناة الي إخفاء المعلومات أو البيانات وهو ما يجعل عملية بناء الأدلة الرقمية أو استعادتها في غاية الصعوبة أمام الخبير، كما تشكل قلة خبرة المحققين وعدم مسايرتهم للتطورات الهائلة في مجال الحاسب الآلي، وعدم تدريبهم علي معرفة الأساليب والتقنيات المستخدمة والمستحدثة في الجرائم المعلوماتية، وهو ما يتطلب استخلاص الأدلة الجنائية الرقمية، عائقاً أمام الوصول إلي الأدلة اللازمة للفصل في الدعوى.

---

[١٥٧] الجهاز القومي للاتصالات.

[١٥٨] مادة (١٠) من قانون مكافحة جرائم تقنية المعلومات المصري، رقم ١٧٥ لسنة ٢٠١٨م.

ثامنا: صعوبة التعاون الدولي في مجال الادلة الجنائية الرقمية:

تتمثل معوقات التعاون الدولي في مجال تبادل الأدلة الجنائية الرقمية نظرا لعدم وجود نموذج واحد متفق عليه من المجتمع الدولي يتعلق بالنشاط الإجرامي، فالتشريعات في سائر دول العالم لم تتفق عل صور محددة يندرج في اطارها، ما يسمى بالجرائم المعلوماتية "اساءة استخدام نظم المعلومات الواجب اتباعها"[١٥٩].

بالإضافة الي عدم وضع تعريف دولي متفق عليه للنشاط الناتج عن الجريمة المعلوماتية، بالإضافة الي أنه لا يوجد تنسيق فيما يتعلق بالإجراءات الجنائية في شأن الجريمة المعلوماتية الدولية، خاصة فيما يتعلق بأعمال الاستدلال أو التحقيق، فعملية الحصول علي الأدلة الجنائية الرقمية خارج حدود الدولة أمر في غاية الصعوبة، خاصة أن هذه الأدلة تكتنفها صعوبة فنية في الحصول عليها، يضاف الي ما سبق عدم وجود معاهدات دولية للتعاون في مجال الأدلة الجنائية الرقمية.

وان كانت بعض الدول قد اتجهت الي الانضمام الي المعاهدات الثنائية أو الجماعية، فإن هذه المعاهدات قاصرة عن الهدف منها نظرا للتطور السريع للجريمة الالكترونية وهو ما يؤدى الي ارباك المشرع الوطني، وهو ما ينعكس سلبيا علي التعاون الدولي فى مجال تبادل الأدلة الجنائية الرقمية[١٦٠]، بالإضافة الي مشكلة تنازع الاختصاص التي تحول دون الحصول علي الادلة الرقمية عن طريق الحاسوب.

حيث أن هذه الجريمة من اكثر الجرائم التي تثير مشكلة الاختصاص سوآءا علي المستوى الوطني أو علي المستوى الدولي، وهو ما يجعل البحث عن الأدلة الجنائية الرقمية عبر شبكة الانترنت من الصعوبة بمكان، وهو ما يجعلنا ننادى بضرورة توحيد المواجهة التشريعية الدولية للجرائم المعلوماتية.

المطلب الثالث
طبيعة الدليل الجنائي الرقمي

مقدمة:

نظر للأهمية التي تتمتع بها الأدلة الجنائية الرقمية كان لزاما علينا أن نتعرض للطبيعة التي تمتع بها تلك الأدلة، ويثير ذلك بعض المسائل نتناولها في النقاط التالية:

---

[١٥٩] د. هشام رستم محمد فريد، قانون العقوبات ومخاطر تقنية المعلومات، ص ٣٦.

[١٦٠] د. إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت، خلال الفترة من ١: ٢ مايو ٢٠٠م، كلية الشريعة والقانون، الامارات العربية المتحدة، ص ٢٢٩.

(ISSN: 2537- 0758)

أولاً: **الدليل الجنائي الرقمي والواقعة الافتراضية**:

تعرف الجريمة الافتراضية بأنها "الواقعة التي تبدأ وتنتهى في اطار العالم الافتراضي" وبذلك تشكل الواقعة الافتراضية الإجرامية البناء الحقيقي للجريمة المعلوماتية.

فالعلاقة بين الدليل الرقمي، والجريمة الافتراضية، تظهر في أن كليهما يعد صورة للآخر، فالدليل الرقمي هو الواقعة الرقمية ذاتها، والتقنية تمثل وسيلة ضبط الدليل، إلا أنها ليست الوحيدة التي تحدد صفة التجريم في الواقعة، فجريمة الاختراق يتم ارتكابها وكذلك اكتشافها من خلال التقنية ذاتها.

حيث يقوم الجاني باستخدام تكنولوجيا المعلومات وهى نفسها التي تعتمد عليها جهات التحقيق والقضاء للفصل في الدعوى وكشف واقعة الاختراق[١٦١].

ثانيًا: **الدليل الرقمي والواقعة المادية**:

قد تقع جريمة معلوماتية وتستخدم الأدلة الرقمية للكشف عنها، وبالتالي فإنها تساهم بشكل فعال في كشف الواقعة المادية بحيث يكون الدليل الرقمي دليلاً له وجود في كشف الجريمة ومرتكبيها، وتعتمد هذه الجرائم علي التخزين الرقمي في الواقع، ولكى يتم الكشف عن الدليل الرقمي يجب اتخاذ إجراءات ملائمة ومشروعة، وإلا فقد الدليل قيمته في الإثبات.

فالكشف عن الادلة الجنائية الرقمية يعتمد علي علاقات التحزين الرقمي، ولكى يتم الكشف عنه ويقدم كدليل يعتد به أمام القضاء يجب أن تكون اجراءات الكشف عنه ملائمة ومشروعة، والا فقد الدليل قيمته في الاثبات، و أصبح مجرد واقعة مادية بحتة، فيتعين أن يتم استخلاص الدليل الرقمي وفقا لإجراءات قانونية مشروعة، كأن يكون هناك إذناً للتفتيش، فإذا لم يتم مراعاة الإجراءات القانونية المنصوص عليها عند استخلاصه، فإن ذلك يؤدى إلي الدفع أمام القضاء ببطلان ذلك، ويصبح هذا الإجراء قابلاً للبطلان.

ثالثًا: **الشراكة المادية والرقمية**:-

الدليل الرقمي قد يؤدى إلي التعرف علي مدى أهمية الاستعانة بالحاسب الألي لارتكاب الجرائم المادية، وهنا نكون بصدد دليل ممزوج بين المادية والرقمية، وفى كل الأحوال ليس من السهولة الحصول علي تصنيف لعلاقة الواقعة المزدوجة والدليل

---

[١٦١] د. عمر محمد بن يونس، مذكرات الإثبات الجنائي عبر الإنترنت مرجع سابق، ص ٥.

الرقمي، ويتوقف ذلك علي مراعاة المصلحة من حيث مكافحة الإجرام والتبليغ عن الجرائم ومرتكبيها.

شروط الدليل الرقمي الملائم والمشروع:

١- المنطقية:

يجب أن يكون الدليل الرقمي المستخدم مؤيداً بالمنطق والعقل بحيث يقود إلي النتائج المترتبة علي الأخذ به موضوعياً، فيشترط أن يؤدى الدليل عقلاً إلي صحة ما ينتهى إليه القاضي، حيث يحظر علي القاضي الحكم بعلمه الشخصي.

٢- مشروعية استخلاص الدليل الرقمي:

يجب أن يتم استخلاص الدليل الرقمي ضمن إجراءات قانونية مشروعة تضمن صحة ودقة هذا الدليل، والتأكد منه بإجراء اختبارات الثقة والتي تشمل من ناحية الكفاءة الفنية في الشخص المسؤول، حيث يتم التأكد من أن استخراج الدليل الرقمي قد رُعى فيه توافر الشروط الشكلية والموضوعية والقانونية المنصوص عليها، كما تشمل مشروعية استخلاص الدليل الرقمي تحديد الحاسب الآلي محل الجريمة، والتي تمت من خلاله الأفعال الإجرامية، وأخيراً يجب التأكد من البرامج أو التطبيقات التي تكشف وقوع الفعل الإجرامي من عدمه.

٣- الطرق الفنية في تحديد الدليل الرقمي:

يجب أن يتم تحديد الدليل الرقمي وفقاً للإجراءات المعيارية التي تضمن الموضوعية والحيادية والكفاءة، حيث يساعد ذلك في اقتناع أجهزة التحقيق والقضاء بالدليل، ويتم ذلك من خلال تقدير الأدلة الرقمية، من خلال التحقيق ومناقشة الظروف والملابسات التي وجد بها الدليل الرقمي.

ولا يتم قبوله إلا بعد خضوعه لاختبارات الدقة للتأكد من صحة هذه المخرجات، ودقتها، وصحة وكفاءة الحاسب الآلي المستخرج منه الدليل، ومدى توافر الثقة والاطمئنان في الخبير القائم علي عملية استخراج الدليل الرقمي[١٦٢].

٤- قيمة الدليل الرقمي الجنائي غير المشروع:

ينبغي أن تكون الأدلة الجنائية الرقمية التي يؤسس عليها الحكم مشروعة، فان كانت هذه الادلة قد تم الحصول عليها بطريقة غير مشروعة أو بصورة مخالفة للنصوص

---

[١٦٢] د. عبد الرؤوف محمد أحمد مهدى، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، سنة النشر ٢٠١٧م ص ١٩٣.

(ISSN: 2537- 0758)

القانونية تكون غير مقبولة فى عملية الاثبات، لا نه اذا سمح بقبول الادلة التي تكون وليدة اجراءات باطلة، فان الضمانات المقررة لحماية الحقوق والحريات لا قيمة لها.

وبناءا عليه لا يجوز القبول بالأدلة الرقمية التي تم الحصول عليها دون مراعاة النصوص القانونية اللازمة في ذلك، فاذا تم الحصول علي البيانات والمعلومات من خلال التجسس المعلوماتي او المراقبة الالكترونية عن بعد دون مسوغا قانونيا، فان هذه الادلة لا يمكن استخدامها كدليل ادانة ضد المتهم، أما عن مدى اشتراط مشروعية الادلة الرقمية كدليل للبراءة، فقد وقع خلاف بين الفقهاء فى هذا الشأن، حيث يري الاتجاه الاول بأن المشروعية لازمة في الادلة الرقمية، سواءا أكانت ادلة ادانة أم ادلة براءة، فإثبات البراءة كالإدانة لا يكون الا من خلال سبل مشروعة، ولا يصح أن يتلف إثبات من قيد المشروعية الذى هو شرط أساسي في أي تشريع لكل اقتناع قضائي سليم[١٦٣].

بينما يري الاتجاه الثاني بأن المشروعية شرط في دليل الادانة دون البراءة، فالمحكمة المختصة لا تحتاج الي اليقين في الحكم بالبراءة بل يكفى في ذلك الشك وهو ما يمكن الحصول عليه من أي دليل حتى ولو كان الدليل الجنائي الرقمي قد تم الحصول عليه بطريق غير مشروع، بالإضافة الي أن المتهم له الحرية الكاملة في اختيار وسائل دفاعه.

كما ان القول بضرورة مشروعية البراءة أسوة بدليل الادانة يعرقل حق المتهم في الدفاع عن نفسه، وهناك اتجاه ثالث ينادى بضرورة التفرقة بين ما اذا كان دليل البراءة الرقمي قد تم الحصول عليه نتيجة سلوك يعد جريمة جنائية، وما اذا كان قد تم الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة اجرائية، فان تم الحصول علي الدليل الجنائي الرقمي نتيجة سلوك يمثل جريمة وجب اهدار الدليل وعدم الاعتداد به.

فالقول بغير ذلك مفاده استثناء بعض الجرائم من العقاب والدعوى الي ارتكابها، أما اذا كانت طريقة الحصول علي الدليل الرقمي تخالف قاعدة اجرائية فحسب الاعتداد بالدليل، وبهذا يصح الاستناد الي هذه الادلة في البراءة تحقيقا للغاية من تشريع البطلان[١٦٤].

---

[١٦٣] د. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، سنة ٢٠٠٩م ص٢٢٠.

[١٦٤] د. عمر محمد بن يونس، مذكرات الإثبات الجنائي عبر الإنترنت، مرجع سابق، ص ٢٣١.

الخاتمة

استخدام الأدلة الجنائية الرقمية في الإثبات موضوعات يتسم بالأهمية خاصة في ظل التطور الهائل الذى تشهده الجرائم المعلوماتية، فالغرض الأساسي من الدراسة هو معرفة طبيعة الأدلة الجنائية الرقمية، ومدى حجيتها في الإثبات خاصة أنها لا تستخدم لإثبات الجرائم المعلوماتية فقط بل يمكن من خلالها إثبات الجرائم التقليدية.

فالدليل الرقمي من الأدلة الرقمية الجنائية التي ظهرت بظهور الجرائم المعلوماتية وأصبح الاستدلال به ضرورة ملحة، فرضتها الحاجة إلي أدلة تنتمى إلي البيئة نفسها التي ترتكب فيها أو من خلال هذه الجرائم، وأصبح هناك اعتراف قانوني بهذه الأدلة وهو ما نراه جلياً في إصدار المشروع المصري للقانون رقم ١٧٥ لسنة ٢٠١٨م والخاص بمكافحة الجرائم المعلوماتية وتقنية المعلومات والذى نص علي اعتبار الدليل الجنائي الرقمي من أدلة الإثبات.

كما نص هذا القانون علي الجرائم المعلوماتية والعقوبات المقررة لها، وأكد علي ضرورة انتداب خبراء "فنيّن أو تقنيّن" من خلال إنشاء سجلان بالجهاز القومي للاتصالات يقيد بأولهما الفنيون والتقنيون العاملين بالجهاز، والآخر يقيد به الفنيين والتقيين من غير العاملين به، وطبق عليهم فيما يتعلق بالحقوق والالتزامات، القواعد والأحكام الخاصة بتنظيم عمل الخبرة أمام جهات القضاء.

وأعطى لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين بضبط أو سحب أو جمع أو التحفظ علي البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة به الأدلة الجنائية الرقمية.

كذلك البحث والتفتيش والدخول والنفاذ إلي برامج الحاسب وقواعد البيانات وغيرها من الأجهزة ونظم المعلوماتية للوصول إلي كشف الجريمة محل الواقعة، كما لها أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي، أو جهاز تقنى موجود تحت سيطرته أو مخزنة لديه.

ويجب علي مقدم الخدمة تقديم البيانات المستخدمة وحركة الاتصالات التي تمت علي ذلك النظام التقني، وفى جميع الأحوال يجب أن يكون أمر جهة التحقيق المختصة مسبباً، وينعقد الاختصاص في استئناف الأوامر السابقة للمحكمة الجنائية المختصة منعقدة في غرفة المشورة في المواعيد ووفقاً للإجراءات المقررة بقانون الإجراءات الجنائية.

(ISSN: 2537- 0758)

وقد اكتسي هذا الموضوع أهمية بالغة كونه يتعلق بأحد المواضيع المستحدثة في إطار الأدلة الجنائية، فهو يعالج أحد أهم الجرائم المنتشرة حاليا، والتي تقوم علي التقنية المعلوماتية خاصة مع تطور المجتمعات والوسائل العلمية والمستجدات التكنولوجية، وقد تبين من خلال البحث تزايد الجرائم المعلوماتية التي تستهدف مستخدمي الحاسب من أفراد ومؤسسات.

وهذه الجرائم تتميز بطبيعتها الخاصة التي تميزها عن الجرائم التقليدية من حيث الوسائل والبيئة التي تقع فيها، وكذلك نوعية مرتكبيها، وهو ما يجعل من الأدلة الرقمية هي الأصلح للكشف عن تلك الجرائم، فهي أدلة ذات طبيعة فنية خاصة تنشأ من نفس بيئة الجريمة المعلوماتية،وبالرغم من أن هذه الأدلة غير مادية ويسهل إخفاؤها وتدميرها ومحوها، إلا أنها تتميز بسهولة إثباتها واسترجاعها في نفس الوقت من خلال الخبرة الفنية والتقنية.

وقد تطرقت الدراسة إلي ماهية الجرائم المعلوماتية، وما تتميز به من خصائص، كذلك التطرق إلي سمات المجرم المعلوماتي، وتضمنت ايضا تعريف الدليل الرقمي والخصائص التي يتميز بها وحجيته في الإثبات سواءاً في التشريع المصري الوضعي أو التشريعات المقارنة، **وكذلك أهمية الأدلة الجنائية الرقمية في الإثبات، وقد توصلنا من خلال الدراسة إلي النتائج والتوصيات الآتية:**

أولاً- النتائج:

١- أفرز التقدم العلمي والتكنولوجي جرائم مستحدثة وهى الجرائم المعلوماتية والتي تتمتع بالخطورة علي الأفراد أو المؤسسات، فهي تعتمد علي التقنية الرقمية في شتى الميادين.

٢- الجرائم المعلوماتية تتميز عن الجرائم التقليدية بأنها تقع في بيئة تقنية مما يكسبها خصائص تجعل من اكتشافها وإثباتها أمرا يصعب بالأدلة التقليدية.

٣- يتميز الدليل الرقمي بطبيعة غير مرئية تتطلب برامج تقنية معينة يمكن من خلالها استرجاع تلك الأدلة التي تم تدميرها أو إتلافها أو محو أثرها.

٤- احسن المشرع المصري صنعاً بإصداره القانون رقم ١٧٥ لسنة ٢٠١٨م، بشان مكافحة الجرائم المعلوماتية، وإن جاء ذلك متأخراً عن بعض الدول كالولايات المتحدة وإنجلترا وكندا واليونان وغيرها من الدول التي بادرت بإصدار التشريعات لمواجهة تلك الجرائم الخطيرة.

٥- يستخدم الدليل الرقمي في إثبات الجرائم المعلوماتية وكذلك الجرائم التقليدية، فهو يتميز بالدقة واليقينية بخلاف الأدلة التقليدية.

٦- يخضع الدليل الجنائي الرقمي كباقي الأدلة للسلطة التقديرية للقاضي الجنائي.
٧- الدليل الجنائي الرقمي له علاقة وثيقة بالعلوم الأخرى، فعلوم الحاسب تقدم المعلومات التكنولوجية الدقيقة، وكذلك علوم الأدلة الجنائية من شأنها أن تقدم منظورا علميا لتحيل الأدلة الجنائية الرقمية.
٨- ضرورة الاعتماد علي الأدلة الجنائية الرقمية في إثبات الجرائم المعلوماتية، خاصة مع تحول الدول إلي النظام المعلوماتي.
٩- هناك بعض العقبات أمام الأخذ بالأدلة الجنائية الرقمية يجب علي المشرع المصري التغلب عليها من خلال تشريعات تتناسب مع التحول إلي النظام التقني.
١٠-الأخذ بالأدلة الجنائية الرقمية يساعد في توفير الحماية الموضوعية للمجتمعات المعلوماتية.
١١- يتم الحصول علي الأدلة الجنائية الرقمية من خلال الاستعانة بالخبراء من الفنيين والتقنيين والمتخصصين في أنظمة الحاسب الآلي.

ثانياً- التوصيات:

١- أحسن المشرع المصري صنعاً بإصدار القانون رقم ١٧٥ لسنة ٢٠١٨م، والخاص بمكافحة الجرائم المعلوماتية، إلا أن تلك الجرائم متطورة وهو ما يتطلب مراجعة التشريعات الخاصة بها بشكل دوري.
٢- نشر الوعى لدى المجتمع المصري بالمخاطر الاجتماعية والسياسية والاقتصادية والثقافية الناجمة عن الاستخدام غير الامن لوسائل التواصل الاجتماعي.
٣- تبنى الدولة المصرية استراتيجية قومية لتنمية الرصد والتحقيق والتثقيف بخطورة الجرائم المعلوماتية.
٤- التواصل مع المجتمع الدولي لتحقيق استراتيجية موحدة لمواجهة الجرائم المعلوماتية، والعمل علي التعاون مع سائر دول العالم للاستفادة من خبراتها في مجال مكافحة الجريمة المعلوماتية.
٥- إنشاء مراكز متخصصة لتدريب الخبراء علي استخلاص الأدلة الجنائية الرقمية، مع توفير كافة الأجهزة والمعدات التي تساعد في ذلك.
٦- تدريب المختصين بالتحقيق في الجرائم المعلوماتية علي التعامل مع الأدلة الجنائية الرقمية واتباع القواعد الفنية الصحيحة.
٧- إنشاء المعامل التي تسهم في عملية استخلاص الأدلة الجنائية الرقمية.
٨- استحداث مناهج تساعد في تأهيل الخبراء "الفنيين والتقنيين" المختصين باستخلاص الأدلة الجنائية الرقمية للعمل مع جهات التحقيق.

(ISSN: 2537- 0758)

المراجع

أولاً: المراجع العربية:

- **د. أحمد حسام طه تمام:** الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، سنة ١٩٩٨م.
- **د. أحمد خليفة الملط:** الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، سنة ٢٠٠٦م.
- **د. أحمد عبد اللاه هلالي:** حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والإنترنت، المجلد ٢، ط٣، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، سنة ٢٠٠٤م.
- **د. أحمد فتحي سرور:**الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ط٢، سنة ٢٠٠٦م.

– القانون الجنائي الدستوري، الشرعية الدستورية في قانون العقوبات، الشرعية الدستورية فى قانون الإجراءات الجنائية، دار الشروق، القاهرة، سنة ٢٠٠٦م

- **د. أشرف توفيق شمس الدين:** شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، الطبعة الخامسة، دار النهضة العربية مصر سنة ٢٠١٩.
- **د. إسماعيل عبد النبي شاهين:** امن المعلومات في الانترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت، خلال الفترة من ١: ٢ مايو ٢٠٠م،، كلية الشريعة والقانون، الامارات العربية المتحدة
- **د. جميل عبد الباقي الصغير:** الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ط١، سنة الشر ١٩٩٨م.

– مقدمة في الحاسب الألي "دراسة عملية ونظرية"، دار النهضة العربية، مصر، سنة ٢٠٠٠م.

- **د. حسين بن سعيد الغافرى:** السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، سنة ٢٠٠٩م.
- **د. خالد عياد الحلبي:** إجراء التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن عمان، الطبعة الأولي، سنة ٢٠١١م.
- **د. خالد محمد المهيري:** التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية، الطبعة الثانية، دار الغرير للطباعة والنشر، بدون سنة نشر، دبي، الإمارات العربية المتحدة.

- **د. خالد ممدوح إبراهيم:** الجرائم المعلوماتية، دار الفكر العربي، الاسكندرية، سنة ٢٠١٩.

– امن الجرائم الالكترونية، الدار الجامعية للطباعة والنشر، سنة ٢٠٠٩م

- **د. رأفت عبد الفتاح حلاوة:** الإثبات الجنائي، قواعده وأدلته، دار النهضة العربية، القاهرة، سنة النشر ١٩٩٦م.
- **د. رامي متولي القاضي:** مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفى ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، الطبعة الأولي سنة ٢٠١١م.
- **د. ر مزى رياض عوض:** مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحيليه وتأصيلية مقارنة، دار النهضة العربية، القاهرة، سنة ١٩٩٧م.
- **د. زكى أمين حسونة:** جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، سنة ١٩٩٥م.
- **سامى جلال فقي حسين:** الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، سنة ٢٠١٤م.
- **د. سوزان عدنان الاستاذ،** انتهاك حرمة الحياة الخاصة عبر الانترنت، دراسة مقارنة، مجلة دمشق للعلوم الاقتصادية والقانونية، العدد٣، مجلد ٢٩، سنة ٢٠١٣م.
- **د. سوزان نور علي محمد:** الإثبات في جرائم الإنترنت في القانون العراقي المقارن، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، سنة ٢٠١٥م.
- **د. شمس الدين إبراهيم أحمد:** وسائل الاعتداء علي الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، دراسة مقارنة، دار النهضة العربية، القاهرة، ط١، سنة ٢٠٠٥م.
- **د. سعد أحمد محمود سلامة:** مسرح الجريمة، دار النهضة العربية، القاهرة، الطبقة الأولي، سنة النشر، ٢٠٠٧م.
- **د. سامى حسين الحسيني:** النظرية العامة للتفتيش في القانون المصري والقانون المقارن دار النهضة العربية، سنة ١٩٧٢م.
- **د. سامى حمدان الرواشدة:** الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الاثبات الجنائي دراسة مقارنة في القانونين الإنجليزي والأمريكي، دار جامعة حمد بن خليفة للنشر والطباعة، ٢٠١٧م.

(ISSN: 2537- 0758)

- **د. سامى جلال فقي حسين:** الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، سنة ٢٠١٤م.
- **د. عائشة بن قارة مصطفى:** حجية الدليل الإلكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، سنة ٢٠٠٩م.
- **د. عبد الحكيم فودة:** حجية الدليل الفني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، سنة ١٩٩٦م.
- **د. عبد الرحمن عبد العزيز الشنقيطي:** أمن المعلومات وجرائم الحاسب الآلي، ط١، المكتبة الأمنية جامعة نايف، الرياض سنة ١٩٩٤م.
- **د. عبد الرؤوف محمد أحمد مهدى:** شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، سنة النشر ٢٠١٧م.
- **د. عبد الفتاح بيومي حجازي:** الدليل الرقمي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة معمقة في جرائم الحاسب الألي والإنترنت، بهجات للطباعة والتجليد، سنة ٢٠٠٩.

– مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولي، دار الفكر الجامعي، مصر، سنة ٢٠٠٦م.

- **د. عبد الله حسين علي محمود:** سرقة المعلومات المخزنة في الحاسب الألي، دار النهضة العربية للطباعة والنشر، القاهرة، الطبعة الثانية سنة ٢٠٠٦.

– إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، بحث مقدم للمؤتمر العلمي الأول، حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، خلال الفترة ٢٦: ٢٨ أبريل، سنة ٢٠٠٣م

- **د. عبد الناصر محمد فرغلي، د. محمد عبيد سيف سعيد:** الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي للعلوم الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة ٢٠٠٧.
- **د. عفيفي كامل عفيفي:** جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، سنة ٢٠٠٠م.
- **د. عمر محمد بن يونس:** الجرائم الناشئة عن الانترنت، الاحكام الموضوعية والاجرائية، رسلة دكتوراه، كلية الحقوق جامعة عين شمس، سنة ٢٠٠٤م.

– مذكرات الإثبات الجنائي عبر الإنترنت، ندوة الدليل الرقمي، جامعة الدول العربية، القاهرة، مصر، سنة ٢٠٠٦.

- **د. علي حسن الطوالبة:** التفتيش الجنائي علي نظم الحاسوب والإنترنت، دراسة مقارنة، الطبعة الأولي، عالم الكتب الحديث، الأردن، سنة ٢٠٠٤م.
- **د. علي عبد القادر القهوجي:** الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، المؤتمر العلم الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، خلال الفترة من ٢٦: ٢٨ أبريل، سنة ٢٠٠٣م.
- **د. علي محمود علي حمودة:** الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعلميات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، سنة ٢٠٠٣م.
- **د. غنام محمد غنام:** شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة، مكتبة المجلس الوطني الاتحادي، الإمارات، سنة ٢٠٠٣.
- **د. كامل السعيد:** جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ٢٨ أكتوبر سنة ١٩٩٣م.
- **د. محمد أحمد الفيومي:** مقدمة في علم الحاسبات الاليكترونية والبرمجة بلغة بيسك، دار الفرقان، عمان، الطبعة الثالثة سنة ١٩٨٩م.
- **د. محمد أمين البشري:** الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، مجلد ١٧، العدد ٣٣، أبريل ٢٠١٢م.
- **د. محمد زكى أبو عامر:** الإثبات في المواد الجنائية، دار المطبوعات الجامعية، الإسكندرية، سنة النشر ٢٠١٢م.
- **د. محمد سليمان الخوالدة:** جريمة الدخول غير المشروع إلي موقع الكترونى أو نظام معلوماتي وفق التشريع الأردني، دراسة مقارنة، دار الثقافة، عمان، الأردن، الطبعة الأولي، سنة ٢٠١٢م.
- **د. محمد عبد الله أبو بكر سلامة:** جرائم الكمبيوتر والإنترنت، موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية، مصر، سنة ٢٠٠٦م.
- **محمد عبد الله قاسم:** الحماية الجنائية للمعلومات الإلكترونية، دار الكتب القانونية، طنطا، مصر، الطبعة الأولي، سنة ٢٠١٠م.
- **د. محمد عبيد الكعبي:** الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، سنة ٢٠٠٤م.

(ISSN: 2537- 0758)

- **د. محمد فهمى:** الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، القاهرة، سنة ١٩٩١م.
- **د. محمد كمال محمد الدسوقي:** الحماية الجنائية لسرية المعلومات الإلكترونية، دراسة مقارنة دار الفكر العربي، القاهرة، الطبعة الأولي، سنة ٢٠٠٣م.
- **د. محمد محى الدين عوض:** القانون الجنائي، مبادئه الاساسية ونظرياته العامة دراسة مقارنة، مطبعة دار النهضة العربية، القاهرة، سنة ١٩٨١م.
- **د. محمود محمود مصطفى:** الإثبات في المواد الجنائية في القانون المقارن، الجزء الأول النظرية العامة، الطبعة الأولي، مطبعة جامعة القاهرة، سنة ١٩٧٨م.
- **د. محمود نجيب حسنى:** شرح قانون العقوبات القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدابير الاحترازية، الطبعة الثانية، دار النهضة العربية مصر سنة ٢٠١٨م- علاقة السببية في قانون العقوبات، الطبعة الأولي، دار النهضة العربية، القاهرة، سنة ١٩٨٣م.

- شرح قانون الإجراءات الجنائية، وفقا لأحدث التعديلات التشريعية دار النهضة العربية، القاهرة، ٢٠١٩م.

- **د. ممدوح عبد الحميد عبد المطلب:** البحث والتحقيق الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب الوطنية، مصر، ٢٠٠٦.

- أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، أكاديمية شرطة دبي، سنة ٢٠١٥م.

- **د. ناصر بن محمد بن مجول البقمي:** أهمية الأدلة الرقمية في الإثبات الجنائي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، سنة ٢٠١٢م
- **د. هشام محمد فريد رستم:**أصول التحقيق الجنائي الفني، مؤتمر القانون والكمبيوتر والإنترنت، المجلد رقم ٢، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، سنة ٢٠٠٤م.

- قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر الطبعة الأولي سنة ١٩٩٢م.

- الجرائم المعلوماتية، أصول التحقيق الفني واقتراح بإنشاء ألية عربية موحدة للتدريب التخصصي، بحث مقدم إلي مؤتمر القانون والحاسب الآلي والإنترنت، خلال الفترة ١:٣ مايو، سنة ٢٠٠٠م، كلية الشريعة والقانون، العين، دولة الإمارات العربية المتحدة.

- **د. هلالي عبد اللاه أحمد:** تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، سنة ١٩٩٧م.

– التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، سنة ٢٠٠٠م.

- **د. وليد كاصد الزيدى:** القرصنة علي الإنترنت والحاسوب، القوانين المقارنة، دار أسامة للنشر، عمان، الطبعة الثالثة، سنة ٢٠٠٩م.

ثانياً: **المراجع الأجنبية**:

- **Association of Chief Police Officers:** (of England,Wales, Northern, Ireland), for Computer Based Electronic Evidence, Version5, October 2011
- **Amadt, B.L and plaza, E**: "case, based Reasoning: Foundational Issues, Mathodalogical Variations, and system Approaches", Alcom, Artficial intelligence Communications, 7 (1), 1994.
- **Carter David L and Datz A.J Computer Crime**: An Emerging challenge for law Enforment "F.B, I.Law Eforcement Bulletin 1996.
- **Carter David L and Datz A.J**: Computer Crime: An Emerging challenge for law Enforment "F.B. I.Law Eforcement Bulletin 1996.
- **Charless R.Swanson, Neil Chamelin and Leonard Territo:** Criminal Investigation (7^{th}, ed.) London: Graw Hill, 2000.
- **Donald K Piragoff:** Computer crimes and other crimes against information technology in Canda: Rev.Intern.De.Dr.Pen.1993.
- **ewa huebner et al** " computer forensics- past,present and future, 8 INFO, Security technical, 2007.
- **Eoghan Casey:** Digital Evidence and Computer Crime, London: Academic Press, 2000.
- **Frédéric Debove, François Falletti**:, précis de droit pénale et procédure pénale2 ème ed,, P.U.F, paris 2001.
- **Linda Volonino and Reynaldo Anazaldua**: Computer Forensics For Dummies Wiley Publihing, United States of America, 2008.
- **Manfred Mohrenschlager**: Compouter crimes and other crimes against information technology in Germany Rev.Inter.De.Pen.1993.

(ISSN: 2537- 0758)

- **PIERRE Chamabon.Lejuge d**'instuction théorie et pratique de la procédure.4ème, edition DALLOZ,1997,
- **Peter Sommer:** Digital EvidenceDigital Investigation and E-Disclosure (A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers), Third Edition, Information Assurance Advisory Council (I,A,A,C), United Kingdom, 2011.
- **Icove, D., Seger, K, and Vonstorch, W**: Computer crime, A crime fighter's Handbook, Sebastpol, CA: O'Reilly and Associates 1995
- **Irini Vassilaki:** computer crime and other crimes against information technology in Greece. Rev.Intern De.Dr pen, 1998.
- **Robert Taylor**: Computer Crime, "in criminal investigation" edited by Charles swanson, N. chamelin and L. Territto, Hill inc. 5th edition 1992.
- **Schneider, Brent**: High Technology Crim: Investigating Cases Involving Computers, San Jose: K.S.K publications, 1999.
- **Stive Bunting and William Wei**: Encase Computer forensic, Wiley Publishing (inc), United States of America, 2006.
- **tylre moore**: the economies of digital forensies, fifth workshop on the econ-of info.see.(june 26,2006, available at http //weis,2006.econinfosec.org / docs.

ثالثا: **كتب التراث**

- **جميل صليبا:** المعجم الفلسفي، دار الكتاب، ط١، سنة ١٩٧٠م.

رابعا: **أحكام القضاء**

- الطعن رقم ٤ لسنة ٢٠٢٠قضائية، جلسة ٢٠٢٠/١٠/٢٤م.
- الطعن رقم ١٧٦٨٩ لسنة ٨٩ ق– جلسة ٢٠٢٠/٣/١٠م.
- الطعن رقم ٢٠٤٩٩ لسنة ٨٧ قضائية، الدوائر الجنائية، جلسة ٢٠٢٠/٧/٩.
- نقض ١٣ مايو ١٩٦٨م، مجموعة الأحكام رقم (١٠٧) حكم رقم ٣٠٣ لسنة ١٩٦٨م.
- الطعن رقم ٢٢٦٢٠ لسنة ٨٨ قضائية، الدوائر الجنائية، جلسة ٢٠٢٠/٧/٩م.