جامعة الأزهر
كلية الشريعة والقانون بدمنهور

مجلة البحوث
الفقهية والقانونية

مجلة علمية محكمّة
تصدرها كلية الشريعة والقانون بدمنهور

بحث مستل من
العدد السابع والأربعين - "إصدار أكتوبر ٢٠٢٤م - ١٤٤٦هـ"

الدليل الرقمي
ومعوقات إثبات الجريمة الإلكترونية

Digital Directory and Obstacles
To Proving Cybercrime

الدكتـــور
حسام أحمد كيلاني علي
دكتوراه في القانون الجنائي
محامي بنقابة جمهورية مصر العربية

مجلـة البحـوث الفقهيـة والقانونيـة
مجلة علمية عالمية متخصصة ومُحكمة
من السادة أعضاء اللجنة العلمية الدائمة والقارئة
في كافة التخصصات والأقسام العلمية بجامعة الأزهر

المجلة مدرجة في الكشاف العربي للإستشهادات المرجعية ARABIC CITATION INDEX
على Clarivate Web of Science
المجلة مكشّفة في قاعدة معلومات العلوم الإسلامية والقانونية من ضمن قواعد بيانات دار المنظومة
المجلة حاصلة على تقييم ٧ من ٧ من المجلس الأعلى للجامعات
المجلة حاصلة على المرتبة الأولى على المستوى العربي في تخصص الدراسات الإسلامية
وتصنيف Q2 في تخصص القانون حسب تقييم معامل "ارسيف Arcif" العالمية
المجلة حاصلة على تقييم ٨ من المكتبة الرقمية لجامعة الأزهر

رقم الإيداع
٦٣٥٩

الترقيم الدولي
(ISSN-P): (1110-3779) - (ISSN-O): (2636-2805)

للتواصل مع المجلة
+201221067852
journal.sha.law.dam@azhar.edu.eg

موقع المجلة على بنك المعرفة المصري
https://jlr.journals.ekb.eg

التاريخ: 2024/10/20

الرقم: L24/0260 ARCIF

سعادة أ. د. رئيس تحرير مجلة البحوث الفقهية و القانونية المحترم

جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر

تحية طيبة وبعد،،،

يسر **معامل التأثير والاستشهادات المرجعية للمجلات العلمية العربية (ارسيف – ARCIF)**، أحد مبادرات قاعدة بيانات "**معرفة**" للإنتاج والمحتوى العلمي، إعلامكم بأنه قد **أطلق التقرير السنوي التاسع للمجلات للعام 2024**.

يخضع معامل التأثير "ارسيف Arcif" لإشراف "مجلس الإشراف والتنسيق" الذي يتكون من ممثلين لعدة جهات عربية ودولية: (مكتب اليونيسكو الإقليمي للتربية في الدول العربية ببيروت، لجنة الأمم المتحدة لغرب آسيا (الإسكوا)، مكتبة الاسكندرية، قاعدة بيانات معرفة). بالإضافة للجنة علمية من خبراء وأكاديميين ذوي سمعة علمية رائدة من عدة دول عربية وبريطانيا.

ومن الجدير بالذكر بأن معامل "**ارسيف Arcif**" قام بالعمل على فحص ودراسة بيانات ما يزيد عن (**5000**) عنوان مجلة عربية علمية أو بحثية في مختلف التخصصات، والصادرة عن أكثر من (**1500**) هيئة علمية أو بحثية في العالم العربي. ونجح منها (**1201**) مجلة علمية فقط لتكون معتمدة ضمن المعايير العالمية لمعامل "**ارسيف Arcif**" في تقرير **عام 2024**.

ويسرنا تهنئتكم وإعلامكم بأن **مجلة البحوث الفقهية و القانونية** الصادرة عن **جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر، قد نجحت في تحقيق معايير اعتماد معامل "ارسيف Arcif"** المتوافقة مع المعايير العالمية، والتي يبلغ عددها (**32**) **معياراً**، وللاطلاع على هذه المعايير يمكنكم الدخول إلى الرابط التالي: http://e-marefa.net/arcif/criteria/

وكان **معامل "ارسيف Arcif" العام** لمجلتكم لسنة 2024 (**0.3827**). ونهنئكم بحصول المجلة على:

- **المرتبة الأولى في تخصص الدراسات الإسلامية من إجمالي عدد المجلات (103)** على المستوى العربي، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.082**). كما صُنفت مجلتكم في هذا التخصص ضمن الفئة (**Q1**) وهي الفئة العليا .
- كما صُنفت مجلتكم في **تخصص القانون** من **إجمالي عدد المجلات (114)** على المستوى العربي ضمن الفئة (**Q2**) وهي الفئة الوسطى المرتفعة ، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.24**).

راجين العلم أن حصول أي مجلة ما على مرتبة ضمن الأعلى (10) مجلات في **تقرير معامل "ارسيف" لعام 2024** في أي تخصص، لا يعني حصول المجلة بشكل تلقائي على تصنيف مرتفع كتصنيف فئة Q1 أو Q2، حيث يرتبط ذلك بإجمالي قيمة النقاط التي حصلت عليها من **المعايير الخمسة المعتمدة لتصنيف مجلات تقرير "ارسيف" (للعام 2024) إلى فئات في مختلف التخصصات**، ويمكن الاطلاع على هذه المعايير الخمسة من خلال الدخول إلى الرابط: http://e-marefa.net/arcif/

وبإمكانكم الإعلان عن هذه النتيجة سواء على موقعكم الإلكتروني، أو على مواقع التواصل الاجتماعي، وكذلك الإشارة في النسخة الورقية لمجلتكم إلى معامل "**ارسيف Arcif**" الخاص بمجلتكم.

ختاماً، في حال رغبتكم الحصول على شهادة رسمية إلكترونية خاصة بنجاحكم في معامل "**ارسيف**"، نرجو التواصل معنا مشكورين.

وتفضلوا بقبول فائق الاحترام والتقدير

أ.د. سامي الخزندار

رئيس مبادرة معامل التأثير

" ارسيف Arcif"

الدليل الرقمي
ومعوقات إثبات الجريمة الإلكترونية

Digital Directory and Obstacles
To Proving Cybercrime

الدكتـــــور

حسام أحمد كيلاني علي

دكتوراه في القانون الجنائي

محامي بنقابة جمهورية مصر العربية

بسم الله الرحمن الرحيم

﴿ سَنُرِيهِمْ آيَاتِنَا فِي الْآفَاقِ وَفِي أَنْفُسِهِمْ حَتَّى يَتَبَيَّنَ لَهُمْ أَنَّهُ الْحَقُّ أَوَلَمْ يَكْفِ بِرَبِّكَ أَنَّهُ عَلَى كُلِّ شَيْءٍ شَهِيدٌ ﴾ (١) .

صدق الله العظيم

(١) – سورة فصلت : الآية ٥٣.

الدليل الرقمي
ومعوقات إثبات الجريمة الإلكترونية

حسام أحمد كيلاني علي
قسم القانون الجنائي، كلية الحقوق، جامعة أسيوط، أسيوط، جمهورية مصر العربية.
البريد الإلكتروني: hosamkelany2024@gmail.com

ملخص البحث:

يشهد العالم في عصرنا الجاري تقدمًا عظيمًا، في الميدان المعلوماتي والاتصالات، باتت الدول معها تتسارع إلى استخدام التقنية في جميع المجالات ، وبقدر ما يحققه تطور التقنيات من فوائد كبيرة في مجال الرقي والتقدم الإنساني فإنها في الوقت ذاته مهدت السبيل إلى بروز أشكال جديدة من الجرائم الإلكترونية.

وأصبح هذا النوع المستحدث من الجرائم الإلكترونية يرتكب في وسط افتراضي غير متعارف عليه، ولا يشبه الوسط التقليدي للجرائم التقليدية ، حيث وجد المجرم تقنية عالية وأساليب حديثة تساعده في ارتكاب العديد من الجرائم دون أن يترك أثراً واضحاً لتلك الجرائم ، ولقد أدى الاستخدام غير المشروع للتقنية المعلوماتية إلى ظهور علم جديد في البحث الجنائي وهو علم البحث الجنائي الرقمي الذي يهتم بالدليل الرقمي بالنظر للآثار التي يتركها المتهم المعلوماتي أثناء ارتكابه لجريمة إلكترونية .

ولقد قمنا باختيار هذا الموضوع نظراً لأهميته البالغة ، فكلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم، وهذا ما شكل عائقا أمام القائمين على البحث وإثبات الجرائم الإلكترونية، حيث أن قواعد البحث والتحقيق وأسس الإثبات الجنائي في القوانين التقليدية لا تكفي، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلاءم مع طبيعتها الفنية .

وتعقد العملية الإثباتية في جرائم الانترنت لارتباطها بالسلوك الإنساني لطائفة من ذوى المهارات الفنية والعلمية وما يكتنف ذلك من تطور مستمر وتعقيدات.

لكل ذلك رأيت إلقاء الضوء على هذا الموضوع وذلك من خلال : تعريف الجريمة الإلكترونية ، وإلقاء الضوء على معوقات الحصول على الدليل الرقمي لإثبات الجرائم

الإلكترونية أثناء المعاينة والتحري والتفتيش لضبط الجرائم الإلكترونية ، وأخيراً الخبرة القضائية وضبط الدليل في الجرائم الإلكترونية .

الكلمات المفتاحية : الدليل الرقمي ، إثبات الجرائم الإلكترونية ، إثبات جرائم الإنترنت، الخبرة القضائية والجرائم الإلكترونية ، معوقات الحصول على الدليل الإلكتروني ، إثبات الجريمة المعلوماتية.

Digital Directory And Obstacles To Proving Cybercrime

Hossam Ahmed Kelany Aly
Department of Criminal Law , Faculty of Law, Assiut University, Assiut, Egypt.
E-mail: hosamkelany2024@gmail.com

Abstract:

The world is witnessing great progress in the field of information and communications, with which countries are accelerating the use of technology in all fields, and as much as the development of technologies achieves great benefits in the field of advancement and human progress, at the same time it has paved the way for the emergence of new forms of crimes.

This new type of cybercrime has become committed in an unrecognized virtual medium, and does not resemble the traditional medium of traditional crimes, where the criminal found high technology and modern methods that help him commit many crimes without leaving a clear trace of those crimes, and the illegal use of information technology has led to the emergence of a new science in criminal research, which is the science of digital criminal research, which is concerned with digital evidence in view of the effects left by the accused information while committing a cybercrime.

We have chosen this topic because of its great importance, the more electronic means develop, the more the method of committing this type of crimes develops, and this is what constituted an obstacle for those in charge of research and proof of electronic crimes, as the rules of research and investigation and the foundations of criminal evidence in traditional laws are not enough, but this type of crime needs to develop new legislation that suits its technical nature.

The evidentiary process is complicated in cybercrime because it is related to the human behavior of a range of people with technical and scientific skills and the continuous development and complexities surrounding this.

For all that, I saw shedding light on this topic through: the definition of cybercrime, shedding light on the obstacles to obtaining digital evidence to prove cybercrime, inspection, investigation and inspection to control cybercrimes, and finally judicial experience and evidence control in cybercrime.

Keywords: Digital Evidence, Proof Of Cybercrime, Proof Of Cybercrime, Judicial Experience And Cybercrime, Obstacles To Obtaining Electronic Evidence, Proof Of Information Crime.

مقدمة

الحمد لله رب العالمين ، والصلاة والسلام على أشرف الأنبياء والمرسلين ، سيدنا محمد وعلى اله وصحبه أجمعين ، أما بعد :

إن تقنية المعلومات تتصل في وقتنا الحاضر بشتى جوانب الحياة الإنسانية على وجه الأرض[١]، لأن هذا النظام لا يعترف بالمكان ويوفر الزمان والبحث، مما جعل تأثيره واضحاً في أنشطتنا اليومية سواء في محيط الأسرة أو العمل التجاري أو البنوك أو العمل الحكومي[٢].

ولقد جاء استخدام وسائل التكنولوجية في مناحي الحياة كافة؛ الى تحويل تلك المعمورة الى قرية إلكترونية صغيرة تتدفق المعلومات بين ارجائها في سهولة وسرعة، ويحصلون على آية معلومات يريدونها بسرعة فائقة وبدون أي عناء، والتي سميت بالثورة الإلكترونية أو المعلوماتية، وجاء هذا من خلال التطور الحافل السريع بالأجهزة الإلكترونية والتي أصبحت سهلة لمتناول الأفراد[٣] .

ولقد أصبحت تقنية الحاسوب تُستعمل كوسيلة لارتكاب الجرائم الإلكترونية، وأصبح هذا النوع المستحدث من الجرائم الإلكترونية يرتكب في وسط افتراضي غير متعارف عليه، ولا يشبه الوسط التقليدي للجرائم التقليدية[٤].

وهذه الجرائم الإلكترونية قد شكلت اعتداءات على الحياة الخاصة للأفراد وسببت في خسائر كبيرة لاقتصاد الدولة ألا وهي الجرائم الإلكترونية بشتى أنواعها، ذلك أن المجرم

---

(1) Computer Science Reflections on the Field. Reflections from the Field. National Research Council.2004.p5.

(٢) - محمد محيى الدين عوض، مشكلات السياسة الجنائية المعاصرة فى جرائم نظم المعلومات (الكمبيوتر)، قسم الجرائم الواقعة فى مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، من ٢٥ :٢٨ أكتوبر سنة ١٩٩٣، تقرير السعودية ص٣٥٨ومابعدها

(٣) - صالح بن سعد المقبل : بناء نموذج لمهارات التحقيق الاستدلالي في جرائم الابتزاز الالكتروني. ، رسالة ماجستير منشورة ، جامعة نايف العربية للعلوم الأمنية الرياض السعودية ٢٠١٥، ص٢ .

(٤) - يوسف صغير: الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير منشورة ، جامعة مولود معمري- كلية تيزي وزو ، الجزائر ، ٢٠١٣، ص ٥ .

اليوم وجد تقنية عالية وأساليب حديثة تساعده في ارتكاب الجرائم دون أن يترك أثر للكشف عنها ومعرفة مصدرها، وكما يستطيع أيضا أن يقترف جريمته ضد مجموعة من المجني عليهم في أي مكان يرغب فيه وفي نفس الوقت[١].

أولاً : موضوع البحث

موضوع البحث هو " الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية "

ثانياً : أهمية الموضوع :

تكمن أهمية هذه الدراسة في تحديد إجراءات الحصول على الدليل الرقمي لإثبات الجريمة الإلكترونية ومعوقات الحصول عليه .

ويحتاج إثبات الجرائم الإلكترونية إلى الدليل الرقمي كوسيلة لإثبات ارتكاب جريمة الاختراق والتعدي على البيانات والمعلومات سواء بسرقتها أو إتلافها أو تزويرها، أو سرقة المنظومة الإلكترونية الخاصة بفرد معين أو منظمة معينة لصالح الفرد أو الغير، والدليل العلمي يتطلب استخدام طرق غير تقليدية في الإثبات، والدليل العلمي يقتصر على إجراء تجارب علمية ومعملية على جهاز الحاسب الآلي الذي استخدم في الاختراق أو التعدي لتعزيز دليل سبق تقديمه سواء بالنفي أو الإثبات للواقعة التي ثار الشك بشأنها [٢] ، ويحتاج إجراء هذه التجارب إلى محقق جنائي وفني متخصص لديه مهارات فنية وتقنية لاستخلاص الأدلة الرقمية؛ لأن الفصل في الدعوى الجنائية في هذه الحالة يتوقف على الرأي الفني الذي يثبت أو ينفي ارتكاب الجريمة من قبل المشتبه به [٣].

---

(١) – سيدي محمد لبشير: دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية–، رسالة ماجستير في العلوم الشرطية تخصص التحقيق و البحث الجنائي، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية، الرياض، ، ٢٠١٠م ، ص ١٥ .

(٢) – عبد الفتاح بيومي حجازي : الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت. مرجع سابق،٢٠٠٥م ، ص ٤٩ ، ٥٠ .

(٣) – محمود نجيب حسني: شرح قانون الإجراءات الجنائية القاهرة، دار النهضة العربية، الطبعة الثانية،١٩٨٨م ص ٤٧٤ .

ولقد قمنا باختيار هذا الموضوع وجعلناه موضوع دراستنا في هذا البحث نظراً لأهميته البالغة ، وتظهر هذه الأهمية من خلال اعتبار أن موضوع الجرائم الإلكترونية حديث وكثير الانتشار حاليا، كما أنه من الموضوعات التي تثير جدلا فقهي لدى فقهاء القانون الجنائي، إضافة إلى تعلق هذا الموضوع بالوسائل الحديثة ذلك أنه كلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم، وهذا ما شكل عائقا أمام القائمين على البحث وإثبات الجرائم الإلكترونية، حيث أن قواعد البحث والتحقيق وأسس الإثبات الجنائي في القوانين التقليدية لا تكفي، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلاءم مع طبيعتها الفنية.

وتعقد المشكلات الفنية المتعلقة بالأسس العلمية لإثبات هذه الجرائم بالصورة التي تمكن الأجهزة الأمنية من مباشرة وظيفتها وعدم إفلات الجاني.

وتعقد العملية الإثباتية في جرائم الانترنت لارتباطها بالسلوك الإنساني لطائفة من ذوى المهارات الفنية والعلمية وما يكتنف ذلك من تطور مستمر وتعقيدات.

ثالثاً : أهداف البحث :

إن الغاية المرجوة من هذه الدراسة تتمثل أساساً في استخلاص أدلة إثبات الجرائم الإلكترونية ، والوقوف على معوقات استخلاص الدليل على ارتكاب تلك الجرائم وإزالتها .

رابعاً : إشكالية البحث :

أما عن إشكالية هذا الموضوع، فباعتبار أن صعوبة كشف وضبط الدليل الرقمي المستخلص من الجرائم الإلكترونية وما يصاحب الحصول عليه من خطوات معقدة، واتساع مسرح هذه الجريمة الذي يتخطى غالبا حدود الدولة الواحدة، وعدم ملائمة القوانين والأنظمة أحيانا لبعض القضايا المطروحة في هذا المجال، ونظرا لما قد يثيره قبول الدليل الرقمي من مشكلات في الإثبات كدليل جنائي ، وعليه من خلال هذه الدراسة نسعى للإجابة عن التساؤلات التالية:

١- ما الدليل الرقمي ومراحله في الإثبات الجنائي؟ ٢- ما هي الجريمة الإلكترونية وكيف يمكن إثباتها ؟ ٣- وما هي معوقات إثبات الجريمة الإلكترونية ؟ ٤- وكيفية تذليل تلك المعوقات ؟

خامساً : منهجية البحث:

سنتبع في بحث ودراسة موضوع **الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية** ؛ المنهج الوصفي التحليلي، من خلال تحليل أحكام النصوص العقابية لقانون العقوبات العراقي، وبيان صور الجرائم الماسة بالتعددية، ومن ثم نقارنها مع غيرها من تشريعات الدول الأخرى، لذلك سيكون منهج الدراسة تحليلي مقارن.

سادساً : الدراسات السابقة

أـ الدراسات العربية

١- دراسة أحمد محمود مصطفى : جرائم الحاسبات الآلية في التشريع المصري "دراسة مقارنة" للحصول على الدكتوراه ، جامعة القاهرة ،كلية الحقوق ، ٢٠٠٩م.

وخلصت الدراسة إلى مجموعة من النتائج أهمها :

- تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح، فمن ناحية، تتميز الجريمة المعلوماتية **بقلة** الحالات التي تم اكتشافها بالفعل بالمقارنة بالجريمة التقليدية، وتتميز الجريمة المعلوماتية أيضاً بكونها لا تتسم بالعنف الذى تتسم به غيرها من الجرائم .

- كما أن الأسباب أو العوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف أيضاً بالمقارنة بالجريمة التقليدية، فمجرد إظهار التقنية قد يكون واحداً من هذه الأسباب وهو ما لا نراه في الجرائم التقليدية، وقد انعكس ذلك على المجرم المعلوماتي الذى تميز أيضاً بمجموعة من السمات ميزته عن غيره من المجرمين، وكذلك على البواعث التي تحركه في بعض الأحيان.

وتختلف الجريمة المعلوماتية من حيث رد فعل المجنى عليه تجاهها وتجاه مرتكبها. كما أن أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية.

- تعانى جرائم الحاسبات الآلية بشكل كبير من مشكلة الرقم الأسود، حيث يرتفع الفارق بين الحجم الحقيقي للجريمة وبين ما هو مسجل بالإحصائيات، ويرجع ذلك إلى عدة أسباب يمكن تقسيمهما إلى طائفتين رئيسيتين، تضم الأولى العوامل التي تتعلق بالجريمة ذاتها، وتضم الثانية العوامل التي تتعلق بالمجنى عليهم.

- لابد أن تتوافر في المعلومة بعض الشروط حتى يمكن أن تتمتع بالحماية القانونية، وأهم هذه الشروط أن تتوافر في المعلومة صفتي التحديد والابتكار، وكذلك السرية والاستئثار ٠

- إن تحديد الطبيعة القانونية للمعلومة قد تنازعه اتجاهان، الأول: هو الاتجاه التقليدي الذى ينفى عن المعلومات كونها من القيم المالية، ويرى لها طبيعة قانونية من نوع خاص. والثاني : هو اتجاه أكثر حداثة، يرى أن للمعلومات قيمة مالية يمكن الاعتداء عليها شأنها فى ذلك شأن القيم المالية بشكل عام.

- تعددت الأحكام التي تناولت سرقة المعلومات في الدول المختلفة، اختلفت فيما بينها من حيث تطبيق النصوص الخاصة بجريمة السرقة في حالة الحصول غير المشروع على المعلومات . كما تباين موقف الفقه في هذا الخصوص وظهر اتجاه يذهب إلى صلاحية المعلومات كمحل فى جريمة السرقة. إلا أن تطبيق النصوص الخاصة بجريمة السرقة في قوانين الدول المختلفة يصطدم دائماً بمجموعة من العقوبات من أهمها ضرورة أن يكون الشيء محل الجريمة قابلاً للتملك وأن يكون ذا طبيعة مادية وأن يكون قابلاً للنقل من حيازة إلى أخرى ليتحقق بذلك الاختلاس المكون لجريمة السرقة، وهو ما لا يتفق مع الطبيعة غير المادية للمعلومات منفصلة عن إطارها المادي، والتي تتعارض أيضاً مع تطبيق النصوص الخاصة بجرائم خيانة الأمانة والنصب والحصول على المال بالتهديد وإخفاء الأشياء المتحصلة من جريمة، حيث تتطلب هذه الجرائم محلاً مادياً ينصب عليه النشاط الإجرامي.

- إن النصوص التقليدية التي تتعلق بإتلاف الأموال لا يمكن تطبيقها في مجال المعلوماتية، إذا لم ينصب الإتلاف على الحاسب الآلي ذاته أو أي من مكوناته المادية، أما الإتلاف الذى ينصب على المكونات المنطقية للحاسبات الآلية، وكذلك الأفعال التي تستهدف إعاقة أنظمة الحاسبات الآلية عن أداء وظيفتها، فإنه لا يمكن تطبيق النصوص التقليدية بشأنها.

- وقد تباينت اتجاهات التشريعات المختلفة في التعامل مع إتلاف المعلومات والبرامج من ناحية، وإعاقة أنظمة الحاسبات الآلية من ناحية أخرى، فبينما اتجهت بعض الدول إلى تجريم كل من السلوكيين بنصوص منفصلة، اتجهت دول أخرى إلى تعديل النصوص

التقليدية الخاصة بجريمة الإتلاف وإدراج السلوكيين معاً في هذه النصوص، كما اكتفت دول أخرى بتجريم الإتلاف الواقع على المعلومات والبرامج وتباينت فيما بينها من حيث مدى قابلية نصوصها للتطبيق في حالة إعاقة نظام الحاسب الآلي. وأخيراً اتجهت تشريعات أخرى إلى الاكتفاء بتجريم إعاقة أنظمة الحاسبات الآلية. كما تختلف النصوص التي تناولت جريمة الإتلاف المعلوماتي فيما بينها من حيث تناولها لأعمال الإتلاف التي يمكن إن تقع على المعلومات أثناء نقلها.

- تباينت الاتجاهات التشريعية للدول المختلفة في التعامل مع ظاهرة الجريمة المعلوماتية، ويمكن بصفة عامة التمييز بين اتجاهين رئيسيين: الاتجاه الأول: يذهب إلى اعتبار الجرائم المرتبطة بالحاسبات الآلية جرائم عادية، لا تتصف بخصائص تميزها عن غيرها من الجرائم، بحيث تتطلب نصوصاً خاصة بمواجهتها، أما الاتجاه الثاني فيذهب على عكس الأول إلى ضرورة التدخل التشريعي لمواجهة الجريمة المعلوماتية لما تتميز به من سمات تميزها عن غيرها من الجرائم. وقد اختلف الأساس الذى يرتكز عليه هذا التدخل التشريعي لمواجهة الجريمة المعلوماتية من دولة إلى أخرى أو من تشريع إلى أخر.

- تباينت السياسات التشريعية في تحديد المحل الذى يتخذه الركن المادي في جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي. فقد اتجهت بعض التشريعات إلى الجمع بين المعلومات وأنظمة الحاسبات الآلية وشبكات المعلومات. كما اتجهت التشريعات الأخرى إلى استبعاد شبكات المعلومات من نطاق التجريم. كما اتجهت تشريعات أخرى إلى تجريم الدخول غير المصرح به إلى أنظمة الحاسبات الآلية عبر شبكات المعلومات. بينما اتجهت بعض التشريعات إلى تجريم الدخول غير المصرح به إلى أنظمة الحاسبات الآلية وشبكات المعلومات، وتجريم اعتراض عملية نقل المعلومات بنصوص منفصلة.

- اختلفت التشريعات في الدول المختلفة حول تحديد الفعل الذى تقوم به جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي. فقد اتجهت بعض التشريعات في تجريم الدخول غير المصرح به إلى نظام الحاسب الآلي إلى استبعاد ما يسمى إلى الدخول الذهني المحض الذى يتمثل في الإلمام بالمعلومات دون أن يسبق ذلك أية عملية منطقية يقوم بها

الفاعل. بينما لم تتضمن تشريعات أخرى أية إشارة إلى تطلب نشاط ما يسبق الدخول إلى النظام، أو استلزام وسائل محددة.

- كما تسمح بعض التشريعات بتطبيق النصوص الخاصة بجريمة الدخول غير المصرح به بمجرد الدخول إلى نظام الحاسب الآلي، بينما تتطلب تشريعات أخرى أن يتم الوصول إلى المعلومات التي يتضمنها النظام لقيام الجريمة. ومن ناحية أخرى اتجهت بعض التشريعات إلى النص صراحة على تجريم البقاء غير المصرح به داخل نظام الحاسب الآلي، بينما لم تشر تشريعات أخرى إلى مثل هذا التجريم. واتجهت بعض التشريعات إلى إفراد نص خاص لتجريم اعتراض نظام الحاسب الآلي منفصلاً عن تجريم الدخول غير المصرح به.

- وقد انقسم الفقه والقضاء في الدول التي لا تتضمن تشريعات نصوصها تجرم الاستعمال غير المصرح به لنظام الحاسب الآلي حول مدى قابلية النصوص الخاصة بجرائم السرقة والنصب وخيانة الأمانة، للتطبيق على هذا الاستعمال.

- أن تطبيق النصوص التقليدية كالنصب والسرقة وخيانة الأمانة والتزوير على حالات الاحتيال المعلوماتي، سواء التحويل الإلكتروني غير المشروع للأموال أو الاستعمال غير المشروع لبطاقات الائتمان يعترضه الكثير من الصعوبات التي حالت في كثير من الأحيان دون تطبيقها، وكانت سبباً في كثير من الانتقادات عندما طبق القضاء في بعض الأحيان مثل هذه النصوص، ولعل من أكبر هذه العقوبات مشكلة الاحتيال على الآلة، والتي تتعارض مع اغلب التشريعات التي تتطلب أن يمارس الاحتيال في مواجهة شخص ما، وكذلك وجود المحرر الذى تتطلب النصوص الخاصة بجريمة التزوير والذى لا يتحقق في جريمة الاحتيال المعلوماتي.

- هناك مجموعة شروط معينة لقبول مخرجات الوسائل الإلكترونية كأدلة إثبات فى المواد الجنائية، فيجب أن تكون الأدلة يقينية، ويتعين مناقشتها تطبيقا لمبدأ شفوية المرافعة، ومتحصلة من وسائل الكترونية مشروعة.

٢- دراسة المقدم/ خالد حازم إبراهيم

تناولت الدراسة " دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية "الإنترنت" [دراسة مقارنة] رسالة مقدمة لكلية الدراسات العليا

بأكاديمية الشرطة للحصول على درجة الدكتوراه أكاديمية الشرطة كلية الدراسات العليا ، ٢٠١٤م .

وخلصت الدراسة إلى مجموعة من النتائج أهمها :

١- إن الدليل الرقمي تتعدد أنواعه بصورة يصعب حصرها ويستخلص من الحاسب وشبكاته والأجهزة التي تعمل بالتقنيات الرقمية، ويصنف ضمن الأدلة الفنية أو العلمية في الدليل الجنائي في ضوء ما يتميز بها من طبيعة وخصائص منفردة عن تصنيفات الدليل الجنائي الأخرى.

٢- اعتماد الخبرة كوسيلة في إثبات الجرائم المتعلقة بشبكة الإنترنت من خلال استخلاص الدليل الرقمي المعامل الجنائية للحاسبات الشرعية عبر الاختبارات التي تجرى للمكونات المادية والمنطقية لأجهزة التقنيات الرقمية.

٣- ضرورة التأكد من صحة الدليل الرقمي المستخلص إعمالا لقاعدة تفسير الشك لصالح المتهم، فيجب على القاضي أن يسير وفقاً لضوابط منهجية للوصول إلى اليقين في الدليل الذي يستند إليه في قضاءه.

٤- يجب إتباع الإرشادات الفنية التي تتناسب مع طبيعة البيئة الرقمية لمسرح الجريمة الرقمي عند تلقى البلاغ والمعاينة الرقمية لكشف حقيقة الواقعة المرتكبة وتحديد شخص المتهم والحفاظ على الأدلة والتحفظ عليها ونقلها للمعل الجنائي .

٥- يتطلب ضبط الأدلة الرقمية بعض القواعد الفنية للبيئة الرقمية أهمها أخذ بصمه للبيانات محل الضبط لضمان عدم التعديل بها أو تحريفها، نسخ البيانات بوسائل متخصصة بصورة طبق الأصل بحيث تكون لها الحجية بعد فحصها واستخراج الدليل مع ضرورة توقيع المتهم على هذه الإجراءات، مع إتباع المنهج العلمي في التحفظ على الأدلة الرقمية ونقلها للمعمل الجنائي.

٦- يتم استصدار إذن قضائي لتفتيش المكونات المنطقية إذا كانت لدى طرفا داخل الدولة، أما إذا كانت لدى أحد أطراف الجريمة خارج الإقليم فان الأمر يخضع للتعاون المتبادل بين الدول في ضوء المعاهدات الموقعة بين الطرفين.

بـ الدراسات الأجنبية:

١ـدراسة بروس ميدليتون (٢٠٠٠)

تناولت الدراسة موضوع الدليل التطبيقي للمحققين في جرائم الانترنت، فاستعرضت الإجراءات التى ينبغي على المحققين إتباعها من لحظة تلقى البلاغ والتوجه لمسرح الجريمة ثم إجراءات جمع الأدلة ثم الأدوات التي ينبغي الاستعانة بها في أعمال التحقيق، وكيفية معالجة البيانات المتحصلة من مسرح الجريمة[١] .

٢ـدراسة جودى ويستباى وآخرون (٢٠٠٣)

تناولت الدراسة موضوع الدليل الدولي لمكافحة جرائم الانترنت، فاستعرضت القوانين المنظمة للجوانب الموضوعية لجرائم الانترنت في العديد من الدول والممارسات القضائية في التعامل معها، وتحديات التي تواجه تطبيق القانون بشأنها، وتطبيق إجراءات التفتيش والضبط لهذه الجرائم ، والتعاون الدولي في مكافحة الجريمة[٢].

٣ـدراسة مارجى (٢٠٠٣)

تناولت الدراسة مقدمة في جرائم الانترنت ووسائل البحث الجنائي الشرعي للحاسبات، فاستعرضت في المقدمة الصعوبات التي تواجه تطبيق القانون على جرائم الانترنت من الناحية الموضوعية والإجرائية والعملية، كما تناولت مصطلحات وتاريخ الحاسب وتاريخ جرائم الانترنت، وألقت نظرة عامة على جهود الحكومة الأمريكية والدولية لمكافحة الجريمة وأثار التعديل الأول والرابع في الدستور الأمريكي على تطبيق النواحي الإجرائية لهذه الجرائم، ثم تناولت العلم الشرعي لتحقيق الحاسبات من حيث مصطلحات وإجراءات ما قبل الانتقال لمسرح الجريمة وكيفية فحص مسرح الجريمة وتحليل الأدلة ومعالجتها[٣].

---

(1) -Bruce Middletion Cyber crine invesyigator's field guide auevbach publication, New York, 2000

(2) -Jody R. and Westby. Project Chair & Editor, international Guide to Combating Cybercrime, defending liberty pursuing Justice, USA,2003

(3) -Marjie T. and Britz, PHD: computer Forensics and Cyper crime an introduction, pearson prentice Hall, USA,2003.

سادساً : خطه الدراسة

المقدمة

فصل تمهيدي: ما هيه الجريمة الإلكترونية

الفصـــل الأول : معوقات الحصول على الدليل الرقمي لإثبات الجرائم الإلكترونية

الفصـــل الثاني : المعاينة والتحري والتفتيش لضبط الجرائم الإلكترونية

الفصل الثالث : والخبرة القضائية وضبط الدليل في الجرائم الإلكترونية

الفصل التمهيدي
الأحكام العامة لماهية الجريمة الإلكترونية

تمهيد :

يوصف العصر الحالي بأنه العصر الرقمي أو ما يسمي بالعصر الإلكتروني الرقمي، فهو يتضمن تطورات تكنولوجية هائلة وكبيرة ومعقدة تخدم جميع المجالات العامة والخاصة داخل الإطار الضيق للدول، مما يؤدي إلي خدمة المجتمع الدولي بأكمله، فهذه التكنولوجيا تخدم جميع مجالات الحياة، حيث بات هذا العصر يتحرك من خلال تكنولوجيا المعلومات والاتصالات، التي واكبتها حركة إجرامية كبيرة، فانتشرت الجرائم الإلكترونية بشكل واضح وكبير في جميع دول العالم، فالجميع يستخدم الحاسب الآلي، والجميع معرض للوقوع تحت تهديد هذه الجرائم، وهي دون أدنى شك جرائم من نوع فريد تحتاج إلى تشريعات خاصة وقوية، وإلي وسائل إثبات مختلفة ومعقدة[1] ، لذا سوف نعرض هذا الفصل في ثلاث مباحث على النحو التالي :

المبحث الأول : تعريف الجريمة الإلكترونية
المبحث الثاني : خصائص وأركان الجريمة الإلكترونية
المبحث الثالث : سمات المجرم الإلكترونية

---

(١) - الأزرق عبد الله: مؤتمر البيئة المعلوماتية الأمنة الرياض جمعية المكتبات والمعلومات السعودية، ٢٠١٠م ص ٢.

المبحث الأول
تعريف الجريمة الإلكترونية

لقد تعددت تعريفات الجريمة الإلكترونية فعرفها الفقهاء على أنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها "[١].

وعرفت بأنها هي كل سلوك غير قانوني يتم باستخدام الأجهزة الالكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالباً ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات [٢].

وتعرف الجريمة الإلكترونية أيضاً بأنها أنماط من الجريمة تستخدم فيها التقنية الحديثة من أجل تسهيل عملية الإجرام [٣]. وتعرف بأنها " النشاط الإجرامي الذي تستخدم فيه التقنية الإلكترونية الرقمية بصورة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف [٤]

وعرفتها منظمة التعاون الاقتصادي والتنمية OECD عام ١٩٨٣م لمصطلح جرائم الكمبيوتر بأنها" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها[٥].

وقد عرفها خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD، بأنها " كل فعل أو امتناع من شأنه الاعتداء على

---

(١) – هشام محمد فريد رستم: قانون العقوبات و مخاطر تقنية المعلومات، سنة ١٩٩٢م ، ص٣٤ .

(٢) – أحمد عبد الحكيم عبد الرحمن شهاب : شروط قبول الأدلة الالكترونية أمام القضاء الجنائي الفلسطيني ، مجلة العلوم السياسية والقانون–العدد ٧٠ فبراير٢٠١٨ المجلد ٢ ، تصدر عن المركز الديمقراطي العربي ألمانيا– برلين،ص١٢٦،١٢٥ .

(٣) – عبد الله بن عبد العزيز اليوسف : الظواهر الإجرامية المستحدثة وسبل مواجهتها الرياض جامعة نايف العربية للعلوم الأمنية، ١٩٩٩م، ص ١٣ .

(٤) – مصطفى محمد موسى: أساليب إجرامية للتقنية الرقمية: ماهيتها مكافحتها، القاهرة، دار النهضة العربية ، ٢٠٠٣م ص٥٦.

(5) Urich sieber, the international handbook on computer crime, UK, 1986, John Wiley & Sons Ltd, p19.

الأموال المادية أو المعنوية، يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "[١].

ولقد عرف الفقيه الألماني (تيدمان) الجريمة الإلكترونية على أنها:" كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب " [٢] .

ويمكننا من خلال التعريفات السابقة تعريف الجريمة الإلكترونية بأنها : النشاط غير مشروع الذي تستخدم فيه التقنية الإلكترونية من شأنه الاعتداء على الأموال المادية أو المعنوية .

ثانياً : تحديد الطبيعة القانونية للمال المعلوماتي

ينقسم المال المعلوماتي إلى نوعين منفصلين وفقاً لطبيعته، فهو إما مال معلوماتي ذو طبيعة معنوية ويتمثل في البرامج والمعلومات أياً كان نوعها، وإما أن يكون المال المعلوماتي ذو طبيعة مادية ويتمثل في أدوات وآلات الحاسب الآلي الملموسة، إذ قد يترتب على اختلاف هذه الطبيعة القانونية للمال المعلوماتي اختلافاً في النتائج المترتبة على تطبيق بعض نصوص القانون الجنائي التقليدي، ولذلك ظهرت هذه الخلافات الفقهية وتبعها في ذلك عدم استقرار الأحكام القضائية، فالاعتداء على برامج ومعلومات الحاسب الآلي يجعلنا أمام مشكلة تقنية ذات طبيعة خاصة يتطلب فيه البحث في تطبيق الجزاء الجنائي الواجب في حالة الاعتداء على المال المعلوماتي المعنوي أي المحتوى الداخلي للشريط الممغنط أو الاسطوانة الممغنطة، وهي ما سميت في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات وهي جريمة مستحدثة تناولها المشرع الفرنسي بموجب القانون رقم (١٩) لسنة ١٩٨٨م بشأن بعض جرائم المعلوماتية في مادته (٢/٤٦٢)[٣].

---

(١) – الدكتور : هشام فريد رستم، المرجع السابق، ص٣٥ .

(٢) – قارة أمال : الجريمة المعلوماتية، رسالة لنيل الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، بن عكنون ، ٢٠٠٢ م ، ص ١٧ ، نقلاً عن :

Tiedemann, Traude et autres délits d'affaires commis à l'aide d'ordinateurs éléctroniques. R.D.P.C. 1984 .n°7 ;61

(٣) – محمد سامي الشواء: ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، القاهرة، ص٥٢١ .

ثالثاً : تاريخ الجريمـة المعلوماتية

يرى البعض أن البداية الحقيقية للاهتمام بهذه الظاهرة تمثلت في ثلاث وقائع رئيسية هي[١]

الواقعة الأولي عام ١٩٨٦ عندما اكتشف موظفو رصد النتائج في جامعة كاليفورنيا أن هناك خطأ في الأرصدة الخاصة بهم في أقل من دولار، كما كشفت التحقيقات الداخلية عن اختراق هاكر ألماني يعمل في KGB لقاعدة بيانات عسكرية والتحصل منها على معلومات مهمة باستخدام الحاسب الشخصي له ومودم فقط، وباختراقه الحاسب الرئيسي للجامعة عن طريق توصيل مودم وكابل منفصل به لنقل المعلومات، وبمجرد حدوث الاتصال بالحاسب أصبح قادراً على التجول عبر نظام MILNET بسهولة فائقة وبدون معوقات، وفى أغلب الأحوال يحدث ذلك بسبب عدم دراية مدير نظام المعلومات بإجراءات أمن الحاسب وتكتشف بالصدفة، فبدون ملاحظة موظفى الجامعة لهذه الاختلافات الموجودة في رواتبهم فلن يكتشف أن النظام المعلوماتي مفتوح ومن ثم تكتشف الواقعة الأخرى، ونتيجة لذلك تشددت الحكومة الأمريكية فى اتخاذ الإجراءات اللازمة لتأمين المعلومات وخاصة العسكرية.

والواقعة الثانية كانت في ٢٣ نوفمبر ١٩٨٨ حيث بداية استخدام شبكة الإنترنت في معمل (Los Alamos)[٢] للربط بين عدد صغير من الجامعات الأمريكية والمؤسسات الحيوية، عندما قام أحد الطلبة في جامعه كورنيل (Cornell) بتطوير برنامج سمي دودة مورس (Morris Worm) والتي تسببت في تعطيل أكثر من ٦٠٠٠ جهاز حاسب مرتبطة ببعضها البعض مما تسبب بأضرار تتراوح ما بين ٥ و١٠ ملايين دولار، وتعد بداية ظاهرة الإجرام عبر الإنترنت، وكان الهدف من تصميم البرنامج اكتشاف نقاط الضعف والاختراق في نظام UNIX وتسبب ذلك في إصابة ١٠٪ من المتصلين بشبكة الإنترنت في هذا الوقت.

---

(1) Marjie T. Britz, PHD, computer Forensics and Cyper crime an introduction, Op-Cit, p 24, 25.

(٢) هذا المعمل يتبع جامعة كاليفورنيا ويعد أهم المعامل العلمية فى الولايات المتحدة الأمريكية ويتمتع بمكانة علمية بالغة في شتى فروع العلم وأشهر ما تم به إنتاج القنبلة الذرية التى ألقيت على اليابان أبان الحرب العالمية الثانية.

والواقعة الثالثة كانت السبب في الاتجاه لإجراء التعديل الرابع للدستور الأمريكي الخاص بالحاسبات، نتيجة انتقاد القضاء لإجراءات عدم الحصول على إذن لما كشفت عنه تحقيقات أجهزة الأمن لنظام الحاسب الخاص للوحه اللعبة (illuminati) لشركة ستيفن جاكسون، حيث قام العملاء لجهاز الأمن في هذه القضية بالتحفظ على كل البيانات المنطقية وما يتضمنه ذلك من التسجيلات التجارية ورسائل البريد الإلكتروني ولوحة البيانات الخاصة باللعبة والنسخة المتقدمة من اللعبة والسرد النصي لقصة اللعبة.[١]

(١) في عام ١٩٩٦ صمم ستيفن جاكسون لعبة تسمى Illuminati وهي عبارة عن لعبة يتم استخدام مجموعة من البطاقات التي تصور الهجمات الإرهابية، والأوبئة، وخلقت بشكل مصطنع بين الأمراض، والحد من عدد السكان، والهدف من اللعبة هو تعبئة الموارد الخاصة بك لخلق الحروب، والثورات، والهجمات الإرهابية، والتأثير على الجمهور، والإطاحة بالحكومات.

المبحث الثاني
خصائص وأركان الجريمة الإلكترونية

أولاً : خصائص الجرائم الإلكترونية

يقوم بهذا النوع من الجرائم مجرمون يتمتعون بمعرفة وخبرة فنية عالية وأساليب احترافية[١].

وهي جرائم ناعمة ومغرية للمجرمين فالجريمة الإلكترونية تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي[٢].

فالجرائم الإلكترونية تبرز بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها، فالجرائم الإلكترونية هي جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في الأفعال غير المشروعة، وقد تحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة[٣] .

وغالباً ما يتمثل الركن المادي فيها باستعمال جهاز الحاسب الآلي، مع إمكانية تنفيذ ذلك عن بعد، دون اشتراط الوجود في مسرح الجريمة. فضلاً عن ضخامة الفوائد والمكاسب التي يستطيع الجاني تحقيقها باقتراف مثل هذه الجرائم، دون جهد يذكر، ودون أن يخاف أن يكتشف أمره[٤].

الجرائم الإلكترونية تتجاوز الحدود، حيث أنه يمكن عن طريق الحاسب الآلي اختراق حواسيب عن بعد بين الدول كأن يرتكب الجاني جريمته المتمثلة في غسل الأموال أو التزوير أو سرقة المعلومات وهو موجود في أوروبا، أما المجني عليه سواء كان الشخص طبيعي أو معنوي موجود في الولايات المتحدة الأمريكية، ولهذا فالجريمة الإلكترونية خطورتها بأنها تتخطى حدود الدول [٥] .

---

(١) – قارة أمال: مرجع سابق، ص ٢٥ .

(٢) – مصطفى سليمان أبكر: جرائم الحاسوب وأساليب مواجهتها مجلة الأمن والحياة، العدد ٢١٠، ١٤٢٠هـ السنة١٩،ص ٤٧.

(٣) – ثنيان ناصر آل ثنيان : إثبات الجريمة الإلكترونية ، رسالة ماجستير مقدمة كلية الدراسات العليا قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، عام ١٤٣٣هـ – ٢٠١٢م ، ص ٢٨ .

(٤) – مصطفى سليمان أبكر : مرجع سابق ، ص ٤٧ .

(٥) – محمود أحمد عبابنة : مرجع سابق، ص٣٤ .

ويطلق على تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية للدول ، وفي عصر الحاسب الآلي، ومع انتشار شبكة الاتصالات العالمية (الإنترنت)، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يعدو أمر التنقل والاتصال فيما بينها أمراً سهلا، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة أو غير مشروعة. لذلك يمكن أن توصف الجريمة الإلكترونية بأنها جرائم عابرة للدول إذ غالباً ما يكون الجاني في بلد والمجني عليه في بلد آخر[١].

الجريمة الإلكترونية تمثل اعتداء على برامج وبيانات الحاسب الآلي، سواء بالتغيير أو المحو أو التعديل كلياً أو جزئياً في الملفات المخزنة داخل نظام الحاسب الآلي، ويقوم الجاني بهذه الأفعال بسرعة فائقة وفي مدة قصيرة لا تتعدى الثواني لذا يكون من الصعب اكتشاف الجريمة، وغالبا ما تكون للصدفة دور رئيسي في اكتشاف الجريمة ، حيث أن الجاني في تلك الجرائم لا يترك آثار مادية ملموسة ولا أدلة كتابية، وهذه الجرائم الإلكترونية تحتاج إلى دراية فنية وطرق خاصة لإثباتها[٢] .

وتتم الجريمة الإلكترونية أثناء عملية المعالجة الآلية للبيانات، حيث أنها لا ترتكب في أي مراحلها سواء أثناء إدخال البيانات، أو أثناء المعالجة، أو في مرحلة إخراج المعلومات[٣] .

ومن خصائص الجريمة الإلكترونية سرعة التنفيذ بحيث يمكن تنفيذها خلال جزء من الثانية وبصورة خفية لا يلحظها المجني عليه، كما أنها تتم في بيئة خاصة هي بيئة المعالجة الآلية للبيانات[٤] .

فالجريمة الإلكترونية في أكثر صورها خفية لا يلحظها المجني عليه أو لا يدري حتى بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي

---

(١) – محمود عبد الله حسين : سرقة المعلومات المخزنة في الحاسب الألي القاهرة، دار النهض العربية، الطبعة الثانية ، ٢٠٠٢م ، ص٣٦١ ، ٣٦٢ .

(٢) – عادل يوسف عبد النبي الشكري: الجريمة المعلوماتية وأزمة الشرعية الجزائية ، كلية القانون، جامعة الكوفة، ٢٠٠٨ م ، ص ١١٦ .

(٣) – عادل يوسف عبد النبي الشكري: مرجع سابق، ص ١١٥ .

(٤) – ناصر محمد البقمي : مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، أبو ظبي، مركز الإمارات للدراسات والبحوث الاستراتيجية ،٢٠٠٨م ، ص١٢ .

في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمر ليس عسيراً في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات لدى مرتكبيها [١].

كما أن المجني عليه يلعب دوراً رئيسياً في صعوبة اكتشاف وقوع الجريمة الإلكترونية، حيث تحرص أكثر الجهات التي تعرضت أنظمتها المعلوماتية للانتهاك أو منيت بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها [٢].

وإلى جانب ذلك، فإن المجني عليه يتردد أحياناً في الإبلاغ عن هذه الجرائم، خوفاً من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين، كما أن الإعلان عن هذه الجرائم يؤدي إلى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي، مما يسهل عملية اختراقه [٣].

ويعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية في الجريمة الإلكترونية، حيث أن اكتشاف الجريمة الإلكترونية أمر ليس بالسهل، ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من الصعاب، فالجريمة الإلكترونية تتم في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر محو الدليل كلياً من قبل الفاعل أمراً غير مستحيل [٤].

---

(١) – هشام محمد فريد رستم : الجوانب الإجرامية للجوانب المعلوماتية مجلة الأمن والقانون، العدد الثاني، شرطة دبي ، ١٩٩٤م ، ص ١٦

(٢) – هشام محمد فريد رستم : المرجع السابق ، ص ٢٥.

(٣) – محمد حماد الهيتي: التكنولوجيا الحديثة والقانون الجنائي، عمان، دار الثقافة للنشر والتوزيع،٢٠٠٤م ، ص١٦٦ .

(٤) – هشام محمد فريد رستم : المرجع السابق ، ص ٢٣.

ثانياً : أركان الجريمة الإلكترونية

أـ الركن المادي في الجريمة الإلكترونية

إن النشاط أو السلوك الإجرامي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت ويتطلب أيضًا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب؛ لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، وتحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها [١].

فالركن المادي بصورة عامة هو : " مجموعة من العناصر المادية التي تتخذ مظهراً خارجياً للحواس، ويرتب القانون لها عقوبة حين تظهر بالخروج"[٢] ، كما أنه سلوك إجرامي يرتكب الجاني فعلاً أو الامتناع عن فعل أمر به القانون وعاقب على مخالفته، فهو السلوك المادي الخارجي الذي ينص القانون على عقوبة له[٣].

ويتمثل الركن المادي في الجريمة الالكترونية في الولوج والبقاء الذي يهدف من خلاله انتهاك نظام الحماية الأمنية للمواقع والأنظمة الإلكترونية[٤].

بـ الركن المعنوي

ويدخل الركن المعنوي في أركان الجريمة ويقصد به الجانب الإرادي المتعلق بالجاني ومسئوليته عن الفعل أو الامتناع المنسوب إليه[٥]. وبعبارة أخرى، يلزم لقيام الجريمة في هذا

---

(١) – ثنيان ناصر آل ثنيان : إثبات الجريمة الإلكترونية ، رسالة ماجستير مقدمة كلية الدراسات العليا قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، عام ١٤٣٣هـ – ٢٠١٢م ، ص ٢١ .

(٢) – ناصر بن محمد البقمي: جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، ط ١: السعودية: مطابع الحميضي ٢٠٠٩م–١٤٣٠ هـ ، ص ٢٢١.

(٣) – زين الدين بلال أمين: جرائم نظم المعالجة الآلية للبيانات، ط ١ . الإسكندرية: دار الفكر الجامعي، ٢٠٠٨م ص٢٧١ .

(٤) – معن احمد الحياري : الركن المادي للجريمة، ط١ . لبنان : منشورات الحلبي ٢٠١٠، ص ٩٣ .

(5)James W. H. McCord. Sandra L.. Criminal Law and Procedure for the Paralegal: A Systems Approach. Op.cit.51.

التحليل أن يأتي الجاني الفعل أو الامتناع وهو متمتع بإرادة حره – أي قادرة على الاختيار وواعية وقادرة على الفهم والإدراك ومذنبه أو آثمة – أي جديرة باللوم[١].

وتعد هذه الجرائم من الجرائم القصدية (العمدية) : فهي لا تقوم إلا بتوافر القصد الجرمي لدى الجاني، والقصد هنا قصد عام يندرج تحت عنصر العلم والإرادة، أما العلم فهو ثبوت ما يقوم الجاني بإتيانه من إشارات أو عبارات أو ألفاظ أو صور أو رموز، من شأنها أن تمس بكرامة المعتدى عليه وحياته وسمعته، وأما الإرادة فهي نية الفاعل وتوجيهها إلى إحداث هذه الأفعال بإرادته الحرة دون إكراه أو تشويش[٢] .

فالقصد الجنائي إذن هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويتحدد الركن المعنوي للجريمة المعلوماتية من خلال مبدأ الإرادة ومبدأ العلم، فالمجرم المعلوماتي تارة يستخدم الإرادة للتخطيط للجريمة، وتارة أخرى يستخدم العلم من أجل تنفيذ الجريمة الإلكترونية [٣].

فالقصد الجنائي هو إرادة اتجهت على نحو معين وسيطرت على ماديات الجريمة وعبرت عن خطورة شخصية الجاني وكانت سبباً لان يوجه القانون لومه إليه[٤].

---

(١) – أحمد عوض بلال: الآثم الجنائي، القاهرة، دار النهضة العربية، سنة٢٠٠٣م، ص٢١ .

(٢) – عادل سقف الحيط : جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية دراسة قانونية مقارنة، ط١ ، عمان ، دار الثقافة للنشر والتوزيع ، ٢٠١١م ، ص٨٠.

(٣) – محمد علي العريان : الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، ٢٠٠٤م ، ص١٥٧.

(٤) – محمود نجيب حسنى : النظرية العامة للقصد الجنائي، القاهرة، دار النهضة العربية، الطبعة الرابعة، سنة٢٠٠٤، ص١٦ .

المبحث الثالث
سمات المجرم الإلكترونية

المجرم الذي يقترف الجريمة الإلكترونية، والذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية ، فالجرائم المعلوماتية هي جرائم فنية تقنية في الغالب الأعم ، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدني من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت[١].

وتتميز الجرائم الإلكترونية عن غيرها من الجرائم العادية من ناحية الفعل ذاته ومن ناحية الفاعل، ومن الأهمية بمكان تحديد الفاعل ومدى مسئوليته الجنائية عن ارتكاب الفعل، واختلافها في حالة كون الفاعل شخص طبيعي أو شخص معنوي[٢].

موقف القضاء المصري من مساءلة الشخص المعنوي

استقر القضاء المصري في قضائية على عدم مساءلة الشخص المعنوي جنائياً ما لم ينص القانون على ذلك صراحة، ولا تقع المسئولية الجنائية إلا على عاتق ممثلي الشخص المعنوي أو أعضائه أنفسهم، وقضت بذلك محكمة النقض[٣]، وهذا يعنى أن الشركات المنتجة للمعلوماتية وتعمل في مجال البرامج والمعالجات المعلوماتية إذا ارتكبت جريمة من الجرائم التي تقع في نطاق عملها فلا تسأل جنائياً عن الجريمة على ممثلي الشخص المعنوي لما يقترفونه من جرائم أثناء قيامهم بالعمل لحساب الشخص المعنوي[٤].

وفي فرنسا رتب القانون الفرنسي الجديد المسئولية الجنائية على الشخص المعنوي بجانب الشخص الطبيعي وفسر الفقهاء تلك المسئولية بقولهم : أنها لا تستبعد مسئولية الأشخاص الطبيعيين الفاعلين أو الشركاء في الجريمة نفسها لمجرد قيام مسئولية الشخص

---

(١) – ثنيان ناصر آل ثنيان : إثبات الجريمة الإلكترونية ، رسالة ماجستير مقدمة كلية الدراسات العليا قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، عام ١٤٣٣هـ – ٢٠١٢م ، ص ٢٨ ، ٢٩ .

(2) Andrea Campbell. Making Crime Pay: The Writer's Guide to Criminal Law. 2002.P.15.

(٣) – مجموعة احكام الدائرة الجنائية لمحكمة النقض، السنه الثامنة عشرة، العدد الثاني ،قاعدة ١٣١،ص٦٨١.

(٤) – ادوار غالى الدهبي: المسئولية الجنائية للشخص المعنوي، المرجع السابق، ص١٩ .

المعنوي فالمشرع لم يرد بهذه المسئولية أن يعفي الشخص الطبيعي من تحمل مسئوليته عن الجريمة، وإنما أراد أن يجنب هذا الشخص تحمل الأثر القانوني للجريمة بمفرده، مع أنها تعد نتيجة لقرار جماعي صدر عن شخص معنوي، مما يعني أن المسئولية تتعدد بين الشخص الاعتباري والشخص الطبيعي[١].

(١) – إدوارد غالي الدهبي : مجموعة بحوث قانونية، المسئولية الجنائية للأشخاص الاعتباريين، الطبعة الأولى، دار النهضة العربية، ١٩٧٨م ، ص٥.

الفصـــل الأول
معوقات الحصول علي الدليل الرقمي

تمهيد وتقسيم:

ترتكز قواعد الإثبات على إقامة الدليل على الواقعة التي يستند إليها، ويعد هو الوسيلة التي يتوصل بها صاحب الحق إلى إثباته وتقديمه إلى القضاء ليمكنه منه، ويحتل الدليل الجنائي مكان الصدارة في نظرية الإثبات باعتباره النتيجة التي تهدف إلى تحقيقها، والأساس المحرك لقواعد الإثبات الجنائي.[١]

وبظهور جرائم الحاسب والإنترنت برز الدليل الرقمي من أدلة الإثبات لها، ويشمل مصطلح الدليل الرقمي كافة البيانات الرقمية التي من شأنها تأكيد ارتكاب الجريمة أو تأكيد وجود علاقة بين الجريمة والمجني عليه والمتهم، ويتبوأ مكان الصدارة لإقامة الدليل على الوقائع المرتكبة في البيئة الرقمية لنظم الحاسب الآلي وقواعد نظم الاتصال بالإنترنت.[٢]

وعليه سوف نقسم هذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول: ماهية الدليل الرقمي .

المبحث الثاني: معوقات الحصول على الدليل الرقمي.

---

(١) -أحمد ضياء الدين محمد خليل: مشروعية الدليل في المواد الجنائية ، رسالة دكتوراة ، جامعة عين شمس ، ١٩٨٢ ، ص ٣٥٩.

(2) Eoghan Casy: Digital Evidence forensics Science computer and the internet computer crime, Academic Press, USA, 2003, p 2.

المبحث الأول
ماهية الدليل الرقمي

أولاً: تعريف الدليل الرقمي

يعد الدليل هو الثمرة التي تنتج عن المرور بمراحل العملية الإثباتية، ويشتق دليل الإثبات الجنائي الرقمي عن الدليل الجنائي الذى يعد الأساس العام للإثبات الجنائي الذى يهدف إلى إثبات وقوع الجريمة بوجه عام ونسبتها إلى المتهم بوجه خاص إن كان هو الجاني.[١]

ويُعرف الدليل الرقمي بأنه هو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون[٢] .

ويُعرف الدليل الرقمي أيضاً بأنه:" الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة[٣] .

وفى صورة أكثر تفصيلاً يعرف الدليل الرقمي بأنه هو ذلك الدليل المشتق من نُظم البرمجة المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها إلى القضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور أو أشكال أو أصوات، لإثبات وقوع الجريمة أو لتقرير البراءة أو الإدانة فيها[٤] .

---

(١) – على ذكى العرابي: "المبادئ الأساسية للتحقيقات والإجراءات الجنائية"، مطبعة لجنة التأليف والترجمة والنشر، القاهرة، ١٩٤٥، ص٥٥٨.

(٢) – ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، ط ١ ، دار الكتب القانونية، مصر،٢٠٠٦م ، ص٨٨.

(٣) – عمر محمد أبو بكر بن يونس: عمر محمد أبو بكر بن يونس : الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٤ م ، ص٩٦٩ .

(٤) – محمد عبيد سيف سعيد المسماري والخبير ،عبد الناصر محمد محمود فرغلى: "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة"، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، ١٢-١٤/ ١١/ ٢٠٠٧ م ، ص ١٣.

ويمكن من خلال التعريفات السابقة استخلاص تعريف للدليل الرقمي شامل وواضح ونقول أن الدليل الرقمة هو : مكون رقمي مشتق من نظم البرمجة المعلوماتية يجد له أساساً في العالم الافتراضي يربط بين الجريمة والمجرم والمجني عليه ويقود إلى الجريمة ، لتقديم المجرم إلى القضاء لإثبات وقوع الجريمة ، أو لنفي وقوع جريمة يحاكم بها شخص أمام القضاء .

ثانيا: تقسيمات الدليل الرقمي:

للدليل الرقمي أشكال مختلفة، وقد قسمها البعض إلى الأقسام الأساسية التالية : ١- أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها. ٢- أدلة رقمية خاصة بالشبكة الدولية للمعلومات "الانترنت". ٣- أدلة خاصة ببروتوكولات تبادل ونقل المعلومات بين أجهزة الشبكة العالمية للمعلومات[١].

وتتكون الأدلة الرقمية من بيانات ومعلومات إلكترونية غير مرئية وغير ملموسة، بحيث يتطلب لإدراكها استخدام أجهزة ومعدات الحاسب الآلي واستعمال نظم برمجيات الحاسوب[٢].

ويعد الدليل الرقمي من طبيعة تقنية تنتج التقنية نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه ويتميز الدليل الرقمي على أنواع الأدلة الأخرى أنه يمكن أن يستخرج نسخ من الدليل الرقمي مماثلة ومطابقة الأصل ولها نفس القيمة العلمية والثبوتية، وهذا ما يكفل وجود ضمانة قوية وفعّالة للحفاظ على الدليل ضد الفقدان والتلف والتغيير من خلال وضع نسخ طبق الأصل من الدليل[٣] .

---

(١) - ممدوح عبد الحميد عبد المطلب: مرجع سابق ، ص٨٨.

(٢) - عبد الناصر محمد محمود فرغلي : محمد عبيد سيف سعيد المسماري: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٧م ، ص١٤ .

(٣) - عبد الناصر محمد محمود فرغلي : محمد عبيد سيف سعيد المسماري : مرجع سابق ، ص١٥ .

فموضوع التخلص من الدليل الرقمي باستعمال أو الاستعانة بخصائص التخلص من المستندات في الحاسب الآلي والشبكة الإلكترونية لا تعتبر من العوائق التي تحيل دون استرداد الملفات، حيث أنه تتوافر برمجيات من ذات الطبيعة الرقمية يمكن من خلالها استرجاع كامل الملفات التي تم من قبل إلغاؤها أو محوها من الحاسب الآلي أو إظهارها، وهذا ما يعني صعوبة إخفاء الجاني لجريمته[١] .

ويُمكّن الدليل الرقمي من تسجيل المعلومات على الجاني ورصدها وتحليلها في الوقت نفسه، لأن الدليل الرقمي يمكن أن يقوم بتسجيل تحركات الأفراد وسلوكاتهم وعاداتهم وبعض الأمور الخاصة بهم لذلك فالبحث الجنائي عن الدليل الرقمي يكون بسهولة مقارنة مع الدليل المادي[٢] .

والدليل الرقمي هو مفهوم يحتوي التطور والتنوع، ذلك لأن هذا مصطلح يتضمن كافة أشكال وأنواع البيانات الرقمية التي يمكن تداولها رقمياً ، بحيث يكون بين هذه البيانات والجريمة رابطة أو علاقة من نوع ما تلك التي تتصل بالضحية أو المجني عليه على النحو الذي يحقق هذه الرابطة[٣] .

---

(١) – عمر محمد أبو بكر بن يونس: مرجع سابق، ص٩٨١ ، ٩٨٢ .

(٢) – ممدوح عبد الحميد عبد المطلب: مرجع سابق، ص٨٩.

(٣) – عمر محمد أبو بكر بن يونس: مرجع سابق، ص ٩٨٠ .

المبحث الثاني
معوقات الحصول على الدليل الرقمي

أولاً: معوقات متعلقة بالدليل ذاته:

إن الوسيلة المستخدمة لضبط دليل الإثبات في الجريمة الإلكترونية هو عبارة عن نبضات إلكترونية غير مرئية تتم عبر أجزاء الحاسب الآلي والشبكة، كما تنساب الكهرباء عبر الأسلاك، فهي غير مرئية، ولا يقف الأمر عند حد عدم الرؤية، لكنها غالباً مشفرة بحيث لا يمكن للإنسان العادي قراءتها، بل تقرأها الآلة وتظهر على شاشة الحاسب الآلي، ولذلك يمكن للمجرم أن يطمس دليل جريمته طمساً كاملاً ولا يترك وراءه أي أثر ، ومن ثم يتعذر إن لم يسكن مستحيلاً ملاحقته أو كشف شخصيته[١].

ويعد انتحال الشخصية، وكذلك التسلل الإلكتروني من أبرز أمثلة السلوك الإجرامي في الجرائم الإلكترونية، وذلك كدليل على عدم رؤية دليل الجريمة، فكلاهما يستخدم أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية إلكترونياً أو الوصول إلى مراكز الحاسب الآلي والدخول إلى قواعد المعلومات، ويكون الدخول شخصياً أو إلكترونياً، فالدخول أو التسلل الإلكتروني، يتم عن طريق قيام الجاني بتوصيل جهازه إلى جهاز آخر له حق الدخول وذلك عن طريق خط هاتفي، وعندما يفتح الجهاز المتصل بمركز المعلومات والمسموح له بذلك، نجد أن جهاز الجاني يمارس نشاطه ويحصل على ذات المعلومات دون أن يراه أحد إلى أن يغلق الجهاز الأصلي صاحب الحق في الدخول، وهذه الجريمة وإن أمكن السيطرة عليها بوسائل متطورة وحراسة شخصية ومراقبة إلكترونية، فإن محاولات القراصنة والمحتالين في الجرائم الإلكترونية تتجاوز هذه الحراسات [٢].

ثانياً: معوقات ترتبط بفقدان آثار الجريمة الإلكترونية

تظل الجريمة الإلكترونية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها للجهات الخاصة بالاستدلالات أو التحقيق الجنائي، والمشكلة التي تواجه أجهزة العدالة الجنائية أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات،

---

(١) – هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ،١٩٩٢م ص٢٨.

(٢) – عبد الناصر محمد محمود فرغلي : محمد عبيد سيف سعيد المسماري : مرجع سابق ، ص٢٦ .

فهي جرائم غير تقليدية، لا تُخلف آثاراً مادية كتلك التي تخلفها الجريمة العادية ، ويرجع ذلك إلى صعوبة اكتشاف الجريمة الإلكترونية عن طريق الحاسب الآلي، ذلك أن الجهات التي تستخدم الحاسب الآلي في معاملاتها اليومية كالشركات التجارية أو المؤسسات لا تراجع أعمالها يومياً، وحتى تلك التي تقوم بالمراجعة اليومية أو الأسبوعية أو الشهرية، قد لا تكتشف الجريمة وتبدو لها وكأنها خسائر عادية على أثر ممارسة نشاطها ، وحتى في حال اكتشافها فإن بعض الجهات المجني عليها لا تقدم على الإبلاغ خوفاً من الأثر السلبي الذي ينعكس عليها من جراء هذا الإبلاغ[١].

وقد يرجع السبب في افتقاد الآثار التقليدية للجريمة الإلكترونية عن طريق الحاسب الآلي ما يلاحظ من أن هناك بعض العمليات التي يجرى إدخال بياناتها مباشرة في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معداً و مخزناً على جهاز الحاسب، ويتوافر أمام المتعامل عدة اختيارات وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك، أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى حيث يتم ترصيد الأشياء المخزنة أو حسابات العملاء، أو نقلها من مكان لآخر بطريقة آلية وحسب الأوامر المعطاة لجهاز الحاسب الآلي، ويمكن ارتكاب بعض أنواع الجرائم الإلكترونية كالاختلاس أو التزوير وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكمبيوتر ، وتكون النتيجة مخرجات على حسب متطلبات مستخدم الجهاز الذي أدخل البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات ورقية وبالتالي تفقد الجريمة آثارها التقليدية [٢] .

---

(١) – محمد الأمين البشري : التحقيق في جرائم الحاسب والإنترنت. المجلة العربية للدراسات العربية والتدريب العدد ٣٠ ، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ٢٠٠١م ، ص ٢٠ .

(٢) – علي محمود حمودة :الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية مركز البحوث والدراسات أكاديمية شرطة دبي محور القانون الجنائي في الفترة من ٢٦ – ٢٨ أبريل ٢٠٠٣م، ص ٢٨١ .

ولذلك يتعين عند البحث عن آثار الجريمة الإلكترونية عن طريق الحاسب الآلي وأدلتها بمعرفة سلطات الاستدلال والتحقيق أن توجه تحرياتها إلى دائرة المتعاملين في نطاق المؤسسة أو الجهة التي وقعت بها الجريمة سواء كانوا موظفين بتلك الجهة أو من المتعاملين معها، وذلك برصد حركة المعاملات الإلكترونية ومراقبة المشبوهين داخل المؤسسات وحولها [١].

ثالثاً: معوقات ترتبط بتعذر الحصول على الأدلة بسبب نظم الحماية الإلكترونية

الجريمة الإلكترونية عبارة عن حرب ما بين المجني عليه وهو ربما يكون فرد أو مؤسسة أو شركة وتكون هدفاً للاعتداء على نظامها المعلوماتي ومن ثم الإضرار بها، وما بين المجرم المعلوماتي أو الجناة في حال تعددهم، لذلك فإن الهيئات عن طريق تخزين هذه البيانات والمعلومات بعيداً عن أيدي محترفي الجريمة الإلكترونية عن طريق الحاسب الآلي ولذلك تحاول الجهات المعنية بالتجارة حماية عملية التحويلات المالية، ويتبع في ذلك طريقتين هما استخدام أسلوب التشفير والتحقق من شخصية المتعاقدين. وفيما يتعلق بالشفرة فهي متفق عليها بين الطرفين ويعرف كلاهما مفتاح هذه الشفرة لضمان عدم قراءة الرسالة إلا لمن هو مصرح له بذلك[٢] .

أما التحقق من شخصية المتعاقدين فيتم عن طريق استخدام شفرة المفتاح العام حيث يمكن للطرفين المتعاقدين أن يوقعا على المستندات بطريقة رقمية، ويتأكد كل طرف من توقيع الطرف الآخر باستخدام المفتاح العام للشفرة [٣] .

وعلى الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها عن طريق الترميز والتشفير وغيرها من طرق الحماية الإلكترونية، فإن قراصنة الحاسب الآلي والعاملين في ذات المؤسسات يستطيعون اختراق هذه الأنظمة ومن ثم يجعلون حمايتها عديمة الجدوى،

---

(١) – جودة حسين محمد جهاد: المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١ – ٢ مايو ٢٠٠٠م، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون، ص ٤ .

(٢) – سمير حجازي : التهديدات الإجرامية للتجارة الالكترونية دبي ، مركز البحوث والدراسات بإدارة شرطة دبي ١٩٩٩م ، ص٣.

(٣) – سمير حجازي : مرجع سابق ، ص٤ .

لا سيما لو كانوا من العاملين داخل المؤسسة، وذلك بالدخول إلى المعلومات السرية أو الأسرار التجارية بغرض بيعها أو استخدامها في مؤسسات جديدة يسعون إلى إنشائها أو يكون هدفهم فقط تغيير الأرقام والبيانات أي تخريب المعلومات، كما أن الأمور لا تقف عند هذا الحد، بل إن هؤلاء يقومون بفرض تدابير أمنية لمنع التفتيش المتوقع بحثاً عن أدلة إدانة ضدهم، وذلك كاستخدام كلمات سر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة الاطلاع على أي دليل يخلفه نشاطهم الإجرامي، الأمر الذي يعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود الدولة، حيث إنه بعد تقدم شبكة الإنترنت الدولية، لم تعد الحدود الجغرافية عائقاً في الاختراق، بل أكثر من هذا يلجأ الجاني إلى أسلوب حماية لمنع ضبطه أو الإيقاع به الأمر الذي يشكل تهديداً لحرمة البيانات الشخصية المخزنة، وكذلك أسرار التجارة الإلكترونية وكذلك تدابير الدفاع والأمن[١].

رابعاً: معوقات عدم الإبلاغ عن الجريمة ونقص خبرات سلطات الاستدلال والتحقيق

١- عدم الرغبة في الإبلاغ عن الجريمة الإلكترونية

تظل الجريمة الإلكترونية مستترة ما لم يتم الإبلاغ عنها، ومن ثم عمل الاستدلالات أو تحريك الدعوى الجنائية حسب النظام السائد والصعوبة التي تواجهه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية - كما هو الحال في الجريمة التقليدية - وذلك لصعوبة اكتشافها من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات التي أصبحت مجني عليها في هذه الجرائم، أو لأن هذه الجهات تحاول إخفاء الأثر السلبي للإبلاغ عما وقع لها وحرصاً على ثقة العملاء فلا تبلغ عن تلك الجرائم التي ارتكبت ضدها[٢].

وتدخل هذه المؤسسات في اعتباراتها أن الإبلاغ عن الجريمة الإلكترونية عن طريق الحاسب الآلي التي وقعت ضدها ربما يؤدى إلى إحاطة المجرمين علماً بنقاط الضعف في أنظمة الجهات المجني عليها، والجريمة في صورتها التقليدية تصل إلى علم سلطات الضبط عن طريق الشكوى أو الإبلاغ والتي يجب على المحقق قبولها متى وردت في شأن

---

(١) - جودة حسين محمد جهاد: المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، مرجع سابق، ص ٦.

(٢) - هشام محمد فريد رستم: قانون العقوبات و مخاطر تقنية المعلومات، سنة ١٩٩٢م، ص٤٢.

جريمة ويحرر بها محضراً يرسله فوراً إلى الجهة المختصة، حتى يتسنى لها مراقبة مشروعية أعمال الاستدلال والشكوى كالبلاغ، إلا أنها توجه ضد شخص معين، وتقدم من المجني عليه أو المضرور من الجريمة، بينما البلاغ يقدم من غيرهما أو يخلو من تعيين اسم من تنسب إليه الجريمة[١] .

٢ـ نقص خبرة سلطات الاستدلال والتحقيق في الجريمة الإلكترونية

ومن المعوقات التي تواجه عملية استخلاص الدليل في الجريمة الإلكترونية كذلك نقص الخبرة لدى المحقق، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة الإلكترونية عن طريق الحاسب الآلي وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظراً لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخراً عن أوربا وكندا والولايات المتحدة الأمريكية ، وأن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ في التكوين والتشكيل عقب ظهور هذه الجرائم، وهو أمر يستغرق وقتاً أبطأ من وقت انتشار الجريمة لان هذه الجريمة تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها، وحتى الآن فإن الحركة التشريعية، أو الثقافية الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلباً على فنية إجراء الاستدلالات والتحقيقات في الدعوى الجنائية عن الجريمة الإلكترونية عن طريق الحاسب الآلي، ومن هنا تأتي الدعوة إلى وجوب تأهيل المختصين في جهات التحقيق والادعاء تأهيلاً مناسباً في شأن هذه الجرائم [٢].

وتتطلب الطبيعة الافتراضية لبيئة الجريمة محققين ذوي مهارات فنية عالية وخبراء في مجالات الشبكات والأدلة الجنائية فيما يتعلق بتكنولوجيا الاتصالات والمعلومات فيختلف مسرح الجريمة الرقمية عن مسرح الجرائم التقليدية، فلا يرتبط الدليل الرقمي بالمحيط

---

(١) – عمر السعيد رمضان : مبادئ قانون الإجراءات الجنائية القاهرة، دار النهضة العربية، المجلد الأول، ١٩٩٠م ، ص ٢٨٠ .

(٢) – ممدوح عبد الحميد عبد المطلب : جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية الشارقة دار الحقوق، ٢٠٠١م، ص ١٧ .

المادي لمسرح الجريمة، فيمكن جمعه من عدد كبير من أجهزة الحاسب الموجودة في العديد من الدول، كما إنه لا يتم حفظ الملفات التي تسجل عمليات اتصال الأجهزة عبر شبكة الإنترنت وحركة المعلومات التي تتدفق من خلالها، ولذلك يتم خسارة عدد من الأدلة وحتى مع وجود الدليل تواجه عملية التحصيل عليه مشكلات التطبيق للقانون بالإضافة إلى إنه بعد الحصول على الدليل يتطلب تحليله العديد من العمليات غاية في التعقيد كما تتطلب وقتا طويلاً وأن يكون أفراد عملية الضبط القضائي لديهم مهارة فنية عالية وخبراء في البحث والحصول عن الأدلة الإلكترونية في مجال الأدلة الجنائية [١] .

لذلك تتطلب أعمال التحقيق في جرائم الإنترنت دعم التطوير والتجهيز وتوفير العناصر المدربة لجهات الضبط القضائي حتى يمكنها الوفاء بمتطلبات التحقيق الجنائي الرقمي والتعاون على المستوى الإقليمي والدولي في التحقيقات المشتركة في إطار منظومة دولية [٢] .

خامسا: معوقات متعلقة بصعوبة التعاون الدولي في مكافحة الجريمة الإلكترونية

رغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية عن طريق الحاسب الآلي، إلا أن هناك عوائق تحول دون ذلك، وتجعل هذا التعاون [٣]:

أ- عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي: ذلك أن الأنظمة القانونية في بلدان العالم لم تتفق على صور محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب إتباعها، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه، وذلك نتاج طبيعي القصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي

---

(1) Jody R. and Westby. Project chair & Editor, international Guide to Combating Cypercrime, Op-Cit, p87.

(2) Marjie T. and Britz, PHD: computer Forensics and Cyper crime an introduction, Op-Cit, p9.

(٣) - إسماعيل عبد النبي شاهين: أمن المعلومات في الانترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من (١ - ٢) مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون ٢٠٠٠م ،ص٢٢٨-٢٢٩.

ب- عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة الإلكترونية بين الدول المختلفة خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، خاصة وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق الضبط أو التفتيش في نظام معلوماتي معين هو أمر غاية في الصعوبة، فضلاً عن الصعوبة الفنية في الحصول على الدليل ذاته.

ت- عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم برامج الحاسب وشبكة الإنترنت ومن ثم تطور الجريمة الإلكترونية عن طريق الحاسب الآلي بذات السرعة على نحو يؤدي إلى إرباك المشرع في الدول، ومن ثم يظهر الأثر السلبي في التعاون الدولي وهو ما حاولت الأمم المتحدة الاهتمام به، وكذلك بلدان أوربا.

ث- مشكلة الاختصاص في الجريمة الإلكترونية: وهي من المشكلات التي تعرقل الحصول على الدليل في الجريمة الإلكترونية عن طريق الحاسب الآلي، ذلك أن هذه الجرائم من أكثر الجرائم التي تثير مسالة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع جريمة الحاسب الآلي في مكان معين، ومن هنا تنشأ مشكلة البحث عن الأدلة الجنائية على شبكة الإنترنت وهذا ما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدول.

ج- ترتكب الجريمة الإلكترونية في مسرح غير قابل للتحديد الجغرافي، إلا أنه يضم أكبر خلق آليات خاصة لفرض تجمع إنساني يتميز بارتباط وتشابك معقد ، وتتمثل أهم خصائصه بالالتزامات والإذعان لها مثل قطع الاتصال على مخترقي بعض القواعد، أو طردهم من المنتديات، لكن هذا التجمع الإنساني الضخم يفتقر إلى المعايير الأخلاقية المشتركة، وهو ما حداً المجلس الأوروبي إلى عقد اتفاقية بودابست عام ٢٠٠١م بشأن الجرائم الإلكترونية، والتي قدمت صوراً لمكافحة الجرائم الإلكترونية، ونصت المادة (٢٢) منها على أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمه لكي يحدد

اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من (٢) إلى (١١) من الاتفاقية عندما تقع الجريمة :

أ- داخل النطاق المحلي للدولة.

ب- على ظهر سفينة تحمل علم تلك الدولة.

ت- على متن طائرة مسجلة في هذه الدولة.

ث- بواسطة أحد رعاياها، إذا كانت الجريمة معاقباً عليها جنائياً في المكان الذي ارتكبت فيه، أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

سادساً : معوقات متعلقة بضخامة البيانات المتعلقة بالجريمة الإلكترونية

لعل من الصعوبات الكبيرة التي تواجه رجال الضبط وسلطات التحقيق الجنائي في الجرائم الإلكترونية عن طريق الحاسب الآلي كمية المعلومات والبيانات الضخمة والتي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل هذه الجريمة، ففضلاً عن ضرورة توافر الخبرة الفنية في مجال الحاسب الآلي والمعلوماتية لدى رجل الضبط أو المحقق، يتعين كذلك أن يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي أو على ديسكات أو اسطوانات منفصلة[1].

(١) - هشام محمد فريد رستم : قانون العقوبات و مخاطر تقنية المعلومات، سنة ١٩٩٢م ، ص٣٦ .

الفصـــل الثاني
المعاينة والتحري والتفتيش للبحث عن أدلة الجريمة الإلكترونية

سوف نتناول هذا الفصل في ثلاث مباحث على النحو التالي:

المبحث الأول : معاينة مسرح الجريمة الإلكترونية .

المبحث الثاني : التحري الرقمي عن الجريمة الإلكترونية .

المبحث الثالث : التفتيش عن الجريمة الإلكترونية .

المبحـــث الأول
معاينة مسرح الجريمة الإلكترونية

أولاً: تعريف المعاينة:

يقصد بالمعاينة هي ذلك الإجراء الذى يتضمن وصف مكان الحادث بما فيه من أشياء أو أشخاص والفحص الدقيق لكافة المحتويات، بهدف كشف مخلفات وآثار الجاني بالمكان والتي تشير إلى شخصيته أو شركائه وما قد يفيد في إثبات الجريمة، وتوضيح قدر من الاستنتاجات المنطقية تشكل الأساس الذى تقام عليه عملية التحقيق والبحث[١].

وعرف بعض الفقه المعاينة بأنها إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة ومرتكبها.[٢]

ويقصد بمعاينة مسرح الجريمة المعلوماتية معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسب والإنترنت[٣].

---

(١) – هشام فريد رستم: "الجوانب الإجرائية في الجرائم المعلوماتية"، مرجع سابق، ص٥٨.

(٢) –عمر السعيد رمضان: مبادئ قانون الإجراءات الجنائية ، ج١، دار النهضة العربية، ١٩٩٣،القاهرة، ص٣٧٣.

(٣) – خالد ممدوح على إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الإسكندرية ، ٢٠١٠م ، ص ١٦٥عن

Henry,J.F, "Testimony befor permanent Subcommmittee On Governmental Affairs, The United States Senate, Ninety Ninth congress, 1984.
http://www.igc.apc.org.nemesis/aclu/nudishallofshame/henry.html.

ثانياً: محل المعاينة:

محل المعاينة في الجرائم التقليدية يتمثل في معاينة المكان بمسرح الحادث والأشخاص المتواجدين به وأى شيء موجود به سواء كانت ثابتة أو منقولة، كذلك رصد جميع الآثار أو المخلفات المتعلقة بالواقعة محل الحادث وتفيد في كشف الحقيقة.

وبعد الانتقال إلى مسرح الجريمة يعمل المحقق على السيطرة ويضع خطة دقيقة لجمع الأدلة حيث على المحقق أن يتعامل بحذر شديد مع الأدلة الرقمية وأن تكون من خلال أيد خبيرة ومتخصصة في رفعها وتحريزها، ومن ثم يقوم خبراء التصوير بتصوير المكان بالكاميرات الفوتوغرافية تصويراً ثلاثي الأبعاد وذلك قبل البدء بالتفتيش مع التأكيد على وجود ضرورة أخذ صور فوتوغرافية لما كانت عليه الشاشات وقت حضور مأمور الضبط القضائي إلى مسرح الجريمة، ومع وجود سلطات التحقيق عليهم أن يأخذوا البصمات مع الأخذ بعين الاعتبار الموجودة على لوحة المفاتيح والفأرة[١].

لعل من أهم العناصر التي ترتبط بالجريمة هو مسرحها أو مكان وقوع أركانها، وهو العنصر الرئيسي لضبط وتحري الجريمة وملاحقة مرتكبيها، وهذا هو الحال نفسه فيما يتعلق بالجريمة الإلكترونية، حيث إن مسرحها متوفر وحتى إن كان مختلفا عن المسرح المادي للجريمة التقليدية كونه مسرحاً معنوياً، فتجول الشخص في الشبكة العنكبوتية يعني أن يترك آثار أقدامه وبصماته المعنوية في الموقع الذي يزوره، إذ يتم تحديد عنوانه الإلكتروني الدائم له، ويتم تحديد نوع الجهاز الذي يستخدمه والمكان الذي يدخل منه[٢].

ويمكن التقرير بصلاحية مسرح الجريمة الإلكترونية للمعاينة من قبل سلطة التحقيق، للضبط والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها لفاعل معين[٣]

---

(١) – محمد أمين البشري: التحقيق في جرائم الحاسب الآلي والانترنت، مرجع سابق، الصفحة ٣٦٠ .

(٢) – كامل السعيد: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات دراسات جنائية معمقة في القانون والفقه والقضاء المقارن، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٢م ، ص ٤٦ .

(٣) – ممدوح عبد الحميد عبد المطلب : أدلة الصور الرقمية ، مرجع سابق ، ص ٥٣٣ .

ويمكن تتبع هذه العناصر بطرق بسيطة أحيانا وبعضها متوفر للمستخدمين العاديين والتي تكشف معلومات المستخدم ويجعلها متاحة لأي شخص يود تتبع تحركات المجرم، فضلاً عن أن يقوم بذلك المتخصصون، وحتى أن جهاز المجرم الشخصي نفسه يحتفظ بملفات الكوكيز للمواقع التي دخلها[١].

ولكن الأمر ليس بهذا القدر من البساطة بالنسبة المجرمين المتخصصين بل وحتى الهواة منهم يقومون بمحو آثارهم التي تم تسجيلها من خلال عدة طرق، منها مسح ملفات الكوكيز الموجودة على أجهزتهم، وأيضاً القيام بإخفاء عناوينهم الإلكترونية الخاصة بأجهزتهم بطرق مختلفة[٢].

وتحاول مختلف الدول والشركات المقدمة لخدمات الإنترنت التغلب على هذه الاختراقات عبر برامج خاصة أحياناً وعبر رموز أخرى، وهذا يتطلب عند محاولة الاستفادة منه لغايات التحري تعاوناً من مزودي الخدمة، لأن هذه الرموز تخص مزود الخدمة ويتعرف من خلالها على هوية المتصلين عبر خطوطهم[٣].

وقد يلجأ بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج فيصعب إثباتها[٤].

وتنقسم المعاينة في مسرح الجريمة الرقمي إلى قسمين:[٥] الأول هو معاينة المكونات المادية للأجهزة التي تم بها ارتكاب الواقعة، ومن أمثلة هذه المكونات الحاسب بمكوناته

---

(١) – عبدالله دغش العجمي : المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة ، رسالة ماجستير ، جامعة الشرق الأوسط ، ٢٠١٤م ، ص ٧٤ .

(٢) – مصعب القطانة : مرجع سابق، ص ٧٤ .

(٣) – محمد موسى مصطفى : دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، ٢٠٠٥م ،ص٤٨ .

(٤) – هلالي عبد اللاه أحمد : تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، الطبعة الأولى، سنة ١٩٩٧م ص٤٨ .

(٥) محمد بن نصير السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت ، رسالة ماجستير ، مقدمة بجامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا ، قسم العلوم الشرطية ، سنة ١٤٢٥هـ ، ٢٠٠٤م ، ص٧٦.

المختلفة والأقراص والكابلات المتصل بها الحاسب وشاشات العرض....إلخ، وكل ذلك مما يعتبر من المكونات المادية والتي لها ذات الطابع ذاته المادي المحسوس للأدلة المادية، وتنطبق عليها القواعد نفسها المتعارف عليها للمعاينة التقليدية للأدلة المادية.

أما القسم الثاني فهو المتمثل في المكونات المنطقية للواقعة الإجرامية المرتكبة ومن أمثلة هذه المكونات برامج الحاسب بأنواعها المختلفة مثل برامج التشغيل والتأمين ومعالجة البيانات...إلخ، والبيانات المعالجة أليا باستخدام الحاسب بأشكالها المتعددة مثل النصوص والصور والفيديو...الخ، وكذلك النظم الرقمية التي يتم من خلالها اتصال شبكات الحاسب وأيضا النظم الرقمية التي يتم اتصال الحواسب الشخصية وشبكات الحاسب من خلالها بشبكة المعلومات الدولية الإنترنت وهي التي تجعل من معاينتها شكلاً بالغ الاختلاف بينها وبين معاينة الأدلة المادية.

ولا توجد صعوبة مادية لتقرير صلاحية مسرح الجريمة الإلكترونية الذي يضم المكونات المادية، كأشرطة الحاسب، مفاتيح التشغيل، والأقراص وغيرها لمعاينتها من طرف مأمور الضبط القضائية، وكذا وضع الأختام في الأماكن التي تمت معاينتها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها مع إخطار وكيل النيابة العامة بذلك[١].

ثانياً: أهمية المعاينة:

الأصل في المعاينة أن لها الصدارة والأولوية في كشف الجرائم التقليدية[٢] ويبرز أهميتها في أنها مرآة صادقة تعكس بأمانة الفعل الذى قام به الجاني بلا تزييف ودون شطط أو نقصان.

وجوهر المعاينة في كونها ملاحظةً وفحصاً حسياً مباشراً لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والكشف والتحفظ على كل ما يفيد في كشف الجريمة[٣] وأن كانت إجراء يجوز الالتجاء إليه إلا أنها ليست مجدية أو صالحة للكشف عن الجريمة في كل الجرائم[٤]

---

(١) – عبد الفتاح بيومي حجازي : مرجع سابق، ص ١٨٢ .

(٢) –محمد محمد عنب: معاينة مسرح الجريمة ، ج١،جامعة نايف للعلوم الامنية، الرياض،١٩٩١، ص٤٥.

(٣) –هشام فريد رستم: الجوانب الإجرائية في الجرائم المعلوماتية، مرجع سابق، ص٥٧.

(٤) – محمد ذكى أبو عامر: الإجراءات الجنائية ، منشأة المعارف ، الاسكندرية، ١٩٩٤، ص٦٠٤ .

ويرى جانب من الفقه أن معاينة مسرح الجريمة الرقمي لا ترقى إلى الأهمية نفسها في مجال كشف غموض الجرائم التقليدية، وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبها. ويرجع هذا الجانب في عدم أهميتها إلى سببين: الأول عدم تخلف آثار مادية عن الجرائم التي تتم باستخدام الحواسب الآلية و شبكة الإنترنت، والثاني هو عدم القدرة على حصر الأفراد الذين ترددوا على مسرح الجريمة الرقمي لطول الفترة الزمنية الفاصلة بين ارتكاب الجريمة واكتشافها، وذلك مما يفتح المجال أمام التغيير أو العبث بالآثار المادية أو زوالها، وهو ما يلقى بظلال الشك حول الآثار المادية المتولدة عنها[١].

وقد تكون المعاينة إجراء تحقيق أو استدلال، يستهدف إلى إظهار الحقيقة في واقعة يبلغ أمرها إلى السلطات المختصة، بحيث لا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه إجراؤها من مساس بحقوق الأشخاص، فإذا تم إجراء المعاينة في مكان عام كانت إجراء استدلال، أما إذا اقتضت دخول حرمة مسكن خاص كانت إجراء تحقيق[٢]

وتظهر أهمية المعاينة في كونها تقوم بإحاطة صورة شاملة لموقع الجريمة لجهة التحقيق والمحاكمة، وبكل ما يحتويه من تفصيلات سواء تعلقت بمكانه أو وصفه من الداخل أو الآثار الموجودة به، وهذا حتى يتسنى لضباط الشرطة القضائية والقضاة وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها[٣].

وعادة لا يوجد مسرح للجريمة الإلكترونية باعتبار مكان الإغارة هو العالم الافتراضي أو عالم الفضاء الإلكتروني والذي يكون عادة الموقع أو المكتب الذي توجد فيه مكونات الحاسب الآلي المادية والمعنوية، والتي تكون محلا للجريمة أو أدلتها وهي تتمثل في الأجهزة والأنظمة والبرامج[٤].

---

(١) -جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة، ٢٠٠١م، ص٢٩.

(٢) - خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، ط. ، ١دار الفكر الجامعي، الإسكندرية، ٢٠٠٩م ص١٥٠.

(٣) - عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، د ط.، دار الكتب القانونية مصر، ٢٠٠٧م، ص١٨٠.

(٤) - نبيلة هبه هروال: الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، ط. د دار الفكر الجامعي الإسكندرية، ص ٢١٧

ويتم إجراء معاينة الجريمة الإلكترونية المرتكبة عبر الانترنت كأي جريمة أخرى، عن طريق الانتقال إلى مكان الجريمة، غير أن الانتقال لا يكون إلى العالم المادي وإنما إلى الفضاء الإلكتروني، وبالتالي يتم الانتقال إلى العالم الافتراضي لمعاينة الجريمة إما من قبل قاضي التحقيق أو مأمور الضبط القضائية[١]

ومن هنا يستوجب على سلطة التحقيق الانتقال إلى العالم الافتراضي بالسرعة الكافية من أجل منع زوال ومحو آثار الجريمة[٢].

رابعاً: معاينة المكونات المنطقية:

هيأت شبكة الإنترنت وسيلة الانتقال لمسرح الجريمة للتعامل مع المكونات المنطقية بمحل الواقعة بصورة مختلفة عن تلك التي في العالم المادي، فيمكن في الوقائع التي تتم عبر الإنترنت الانتقال عبرها للفحص.[٣]

فيمكن في هذه الحالة انتقال مأمور الضبط القضائي للواقعة محل الفحص من المكتب أو عبر أحد مقاهي الإنترنت أو عبر فحص مزود الخدمة المشترك لديه أطراف الواقعة.[٤]

ونظراً لأن تأمين مسرح الجريمة يتضمن اعتبارات تتعلق ليس فقط بالمخاطر التقليدية وإنما تتعلق بالمخاطر الإلكترونية أيضا، فينبغي أن يحدد المحققون المخاطر التي قد تأتي من مصادر غير تقليدية وأماكن بعيدة، وتتضمن المخاطر المحتملة تفخيخ محرك الأقراص والدخول على الحاسوب عن بعد، وينبغي أن يتم التعامل مع أنظمة الهاكر أو القرصنة على الإنترنت بحرص شديد، وأن مثل هذه الأنظمة من السهل نسبياً التعرف عليها، كما أن سلوكيات المشتبه به في مسرح الجريمة يعد مؤشراً على طبيعته، فبقايا المأكولات والمشروبات المبعثرة في أماكن العمل أو وجود أي دليل على أن شخصاً ما كأن يمضي ساعات طويلة أمام أجهزة الحاسوب قد تشير إلى وجود نظام هكر، وتعد الأنظمة المبرمجة

---

(١) -عمر محمد أبو بكر بن يونس : الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٤، ص٨٩٥.

(٢) - خالد ممدوح إبراهيم : فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص١٥٦ ، ١٥٧ .

(3) David Johnston&Sunny Handa, Cyber Law – second edition, Stoddart Publishing, New York, U.S.A., 1997, p17.

(٤) - خالد ممدوح ابراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية ، مرجع سابق، ص ١٥٧

محلياً، وتصنيف أجهزة الحاسوب غير التقليدية أو صناديق الحاسبات المفتوحة مؤشراً أو دليلاً إضافيا في التحقيق[١].

ويمكن الاستعانة بالمجنى عليه أو الشخص الذى يساعد في التحقيق سواء كان المدير أم المسئول عن إدارة النظام أم المسئول عن الأمن في النظام المعلوماتي والاستفسار منهم عن أي شيء متعلق بالمعاينة، لمواجهة أي موقف يستجد أثناء إجراء المعاينة[٢].

جمع معلومات أثناء المعاينة الرقمية:

تتنوع الوقائع في مسرح الجريمة الرقمي، وتتطلب كل منها الاستعداد الخاص بها والتحري عن المعلومات التي لدى المجنى عليه قبل الانتقال، كما إنه يجب أن يوضع في الاعتبار أنه لن يجيب على كافة التساؤلات لذلك يجب الاستعداد بأسئلة بديلة يمكن الوصول بها إلى الهدف نفسه، كما ينبغي أن تكون الأسئلة قصيرة قدر الإمكان، وينبغي تأمين وسيلة الاتصال بالمجنى عليه سواء أكانت عن طريق التليفون أم البريد الإلكتروني ...[٣]

فيطرح المحقق بعض التساؤلات التي تساعد في إجراء المعاينة ويكلف بها أحد أعضاء الفريق الذى يقوم بدورة بإعداد تقرير عن نتيجة الإجابة عن هذه الأسئلة ، وفيما يلى نموذج لبعض الأسئلة التي يمكن الاستعانة بها وفقاً للحالة محل المعاينة ويتم اختيار المناسب منها في إجراء المعاينة كالتالي:[٤]

هل المشتبه به من الطبيعي أن يلج إلى النظام في ٢٤ ساعة التي تسبق حدوث الواقعة؟

من آخر شخص ولج إلى النظام المعلوماتي؟

هل من الطبيعي أن يعمل المشتبه به في وقت ولوجه إلى النظام المعلوماتي؟

هل من عادة أحد الأشخاص أن يعمل لوقت متأخر أو أن يعمل في الإجازة الأسبوعية أو أن يحضر مبكراً إلى العمل؟

ما هو العمل القائم به المبلغ في المؤسسة و صلاحياته بالنسبة إلى النظام؟

متى حدثت هذه الواقعة؟

---

(1) Marjie T. Britz, computer Forensics and Cyper crime an introduction, Op-Cit,p66.
(2) Ibid, p 67.
(3)Ibid, p2.
(4) Bruce Middleton, cybercrime investigation field guid, Op-Cit,p5-6-7.

ما الذى كان على شاشة الحاسب وقت حدوث الواقعة؟

متى تمت آخر عملية حفظ للبيانات Backup للنظام المعلوماتي؟

كم امضى هذا الشخص في العمل مع المنظمة؟

هل تلاحظ أي شيء غير طبيعي على الشبكة في الـ ٣٠ يوماً التي سبقت حدوث الواقعة؟

ما الذى حدث للنظام المعلوماتي تحديداً؟

ما هي العقود والبرامج المتداخلة مع النظام المعلوماتي محل المعاينة ومن الأشخاص المتداخلين بالنظام في هذا الأمر؟

ما هي المستويات التي تم تقسيمها للتصريح للولوج إلى النظام والأشخاص المحددون للتعامل مع كل مستوى؟

هل توجد كاميرات أو أجهزة تسجيل للمراقبة يمكن الرجوع إليها لملاحظة ما تم من أحداث في المكان الموجود به النظام المعلوماتي؟

هل يوجد تصاريح للدخول إلى المكان الموجود به النظام وهل هذا التصريح يعمل من خارج المبنى أم داخل المبنى؟

هل يوجد كلمة السر للولوج إلى مستويات التقسيم بالنظام المعلوماتي وكم شخص مشترك في كلمة السر؟

هل المؤسسة يوجد بها مشاكل مادية أو برنامج معقد به خلل Slippage؟

هل يوجد أي شخص حصل على إجازة استثنائية أو تغيب بشكل غير مبرر أو سافر إلى أحد الدول الأجنبية للعمل أو للسياحة في الـ ٩٠ يوماً التي سبقت الواقعة؟

هل يوجد أي شخص يعمل في المؤسسة لديه مشكلات مادية وهل هي متعلقة بأحد الموظفين أو المتعاقدين مع المؤسسة؟

ما هو مستوى الموظفين العاملين على النظام المعلوماتي الواقع عليه الضرر في علوم الحاسب وشبكاته وشبكة المعلومات الدولية؟

ما هو طبيعة النشاط الذى تمارسه المؤسسة حالياً وسابقاً؟

من ومتى أول من كتب تقرير بشأن الحادثة؟

هل قام أحد الأشخاص بأي إجراء عقب الحادثة (لمس أحد الأشياء أو أجرى اتصال تليفوني...الخ)؟

من الأشخاص الذين تم إخطارهم بالحادثة؟

ما هي عناصر وأسس التأمين المادي للمؤسسة وتسجيل ذلك أثناء العمل يومياً؟

هل توجد أي ملاحظات لأفراد الأمن المادي عن أحد الأشخاص وهل هذه الملاحظات تسير وفقاً للمجرى الطبيعي للعمل؟

هل تم إنهاء عمل أحد الموظفين في المؤسسة في أخر ٩٠ يوماً قبل الحادث؟

هل يمكن التحصيل على نسخه من نظام التسجيل الأمني؟

لماذا تعتقد أن هناك اختراقا ما تم للمؤسسة؟

هل يمكن التحصيل على نسخه من التسجيلات العادية للنظام الذى تم اختراقه مثل تسجيلات عمليات البيع أو الشراء أو العمليات العادية التي تم حفظها والخدمات العادية التي تقدمها المؤسسة ويتم تسجيلها والتعديلات التي تم إجراؤها ...الخ؟

متى تمت آخر عملية صيانة للنظام ومن الذى قام بإجرائها؟

هل تم أي تحديث أو إضافة أي شيء للنظام في الوقت القريب من حدوث الاختراق؟

أين كان المشتبه بهم في آخر ٣٠ يوماً قبل الحادثة؟

هل تم إعطاء أحد الأشخاص حق الدخول للنظام استثناءات في آخر ٩٠ يوماً قبل الحادث؟

هل يوجد شخص في المؤسسة يعتقد إنه غير أمين من المعينين؟

ما هي آخر التعاقدات التي تمت للتعيين في آخر ٣٠ يوماً؟

طريقة التعامل مع المسرح الرقمي:

قد تتضمن مخرجات الحاسوب الآلي والحزم البرمجية والمذكرات التي يتم ترحيلها أدلة جنائية، فمرتكبو الجرائم الإلكترونية يستخدمون الأوراق لأغراض حفظ السجلات، وقد يقدم دليل البرامج على سبيل المثال الكثير من المساعدة في التحقيقات الجنائية كما قد يتم فيها إخفاء كلمات المرور، وقد يتضمن هذا الملف أرقام الاتصال الخاصة بالدعم الفني أهمية كبري بالنسبة للمحققين عند التعامل مع برمجيات قديمة لا تستخدم أو تعجز خبرتهم

عن التعامل معها، ويتطلب أن يكون المحققون على مستوي مناسب من الحذر والحيطة واليقظة للتعامل مع البرامج المخبئة[1].

(1) Marjie T. Britz, computer Forensics and Cyper crime an introduction, Op-Cit, p191.

المبحث الثاني
التحري الرقمي عن الجريمة الإلكترونية

تمهيد

يستقى رجل البحث أو مأمور الضبط القضائي معلوماته في الجرائم التقليدية باستخدام وسائل متعددة منها البيانات والمعلومات التعريفية أو التوضيحية من خلال العالم المادي مثل الاستعانة بالمرشدين أو المصادر السرية ... أما بالنسبة للتحري عبر شبكة الإنترنت فيتم البحث بالبيئة الرقمية للحواسب الآلية المرتبطة ببعضها البعض عبر شبكة الإنترنت، وهو ما يتطلب منه القدرة الفنية على الولوج للوصول للمعلومات بفاعلية وتحليلها، تلك القدرة الفنية تعنى ضرورة التخصص في تكنولوجيا الحاسب الآلي وشبكاته وارتباطها بشبكة الإنترنت ومواكبة المتغيرات في تطويرها والتعامل عليها[١].

أولاً: تعريف التحري الرقمي:

يعرف البعض **التحري الرقمي** أنه "عمل أمنى وقانوني يقوم به المتحرى عبر شبكة الإنترنت بواسطة التقنية الإلكترونية الرقمية تحت تغطية للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها للحد من الجرائم الإلكترونية أو ضبطها لتحقيق الأمن الإلكتروني أو لأى غرض آخر".[٢]

ثانياً : أهمية التحري

وتؤدى البرامج التطبيقية في تحقيق الاتصال بين الأفراد والمؤسسات دور بالغ الأهمية في جمع المعلومات عبر الإنترنت، فينبغي على المتحري عبر الإنترنت أن تكون له القدرة على الولوج عبر تلك التطبيقات واكتساب مهارة استعمالها والتعرف على أساليب التواصل من خلالها[٣].

وقد وجدت أجهزة الشرطة والتحقيق صعوبات جمة منذ ظهور هذا النوع المستحدث من الجرائم، سواء في كشف غموضها أو إجراء التفتيش والضبط اللازمين، أو التحقيق فيها

---

(١) – مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت، مرجع سابق، ص ٢٣.

(٢) – ده شيء صديق محمد : مرجع سابق، ص ٢٢.

(٣) – مصطفى محمد موسى : مرجع سابق، ص٢٤.

على نحو تطلب إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية على نحو يمكنها من تحقيق المهمة المطلوبة منها وبالكفاءة المطلوبة[١].

ففي الفترة الأولى لظهور هذا النوع من الجرائم، وقعت الشرطة في أخطاء جسيمة أدت إلى الإضرار بالأجهزة أو الملفات، أو الأدلة الخاصة بإثبات الجريمة[٢].

وترجع أهمية التحريات إلى دورها في التحقق من صحة ما ورد في البلاغات والشكاوي، كما أن بعض إجراءات التحقيق لا يمكن مباشرتها إلا إذا توافرت تحريات جدية أمام سلطة التحقيق لكي تأذن بها، فلا يمكن إصدار إذن بتفتيش المتهم أو مسكنه في الجريمة الإلكترونية إلا بعد توافر تحريات جدية على ارتكابه الجريمة أو الواقعة الإجرامية، وذلك باستخدام تقنيات التتبع والتأكد من وقوع الاختراق والتعدي على جهاز المجني عليه أو موقعه الإلكتروني سواء كان فرداً أو هيئة[٣] .

وتؤدى البرامج التطبيقية في تحقيق الاتصال بين الأفراد والمؤسسات دور بالغ الأهمية في جمع المعلومات عبر الإنترنت، فينبغي على المتحرى عبر الإنترنت أن تكون له القدرة على الولوج عبر تلك التطبيقات واكتساب مهارة استعمالها والتعرف على أساليب التواصل من خلالها[٤].

ثالثاً : أساليب التحري

وتتخذ أساليب تحرى الإنترنت صورتين: الأولى العلنية أو الاتصال المباشر مع الأشخاص أو الجهات أو المواقع المتعلقة بالواقعة محل الفحص، والثانية السرية كالتخفي أو انتحال الصفة (التغطية) حتى يأنس الجاني للقائم بالتحري ويأمن جانبه بالصورة التي لا تخل بإرادة الجاني الحرة.[٥]

---

(١) – أحمد حسام طه تمام :الجرائم الناشئة عن استخدام الحاسب الآلي، القاهرة، دار النهضة العربية، سنة ٢٠٠٠م ص١٨ .

(2) Bruce MiddletonCyber Crime Investigator's Field Guide.computers–2002. P.52.

(٣) – إبراهيم حامد مرسي طنطاوي: سلطات مأمور الضبط الجنائي. دار النهضة العربية ، ١٩٩٧م ، ص ٢٦٦–٢٦٧ .

(٤)) د مصطفى محمد موسى : مرجع سابق، ص٢٤.

(٥) نقض اول ديسمبر ١٩٩٥ مجموعة أحكام النقض س١٥ رقم ١٩٩، ص ٩٧٠، ٢٤/ ٢/ ١٩٨٠/ س ٣١ رقم ٥٢، ص ٢٦٢، عن د. إدوارد غالى الذهبي: "الإجراءات الجنائية"، القاهرة، مكتبة غريب، ط٢،

ويستقى رجل البحث أو مأمور الضبط القضائي معلوماته في التحري عن الجرائم الإلكترونية عبر شبكة الإنترنت فيتم البحث بالبيئة الرقمية للحواسب الآلية المرتبطة ببعضها البعض عبر شبكة الإنترنت، وهو ما يتطلب منه القدرة الفنية على الولوج للوصول للمعلومات بفاعلية وتحليلها، تلك القدرة الفنية تعنى ضرورة التخصص في تكنولوجيا الحاسب الآلي وشبكاته وارتباطها بشبكة الإنترنت ومواكبة المتغيرات في تطويرها والتعامل عليها[١].

وتبرز مظاهر التحريات الوقائية لمأموري الضبط القضائي في قيامهم بالتخفي وهو ما يجد بيئة مناسبة في شبكة الإنترنت لجمع المعلومات وضبط الجرائم في حالة التلبس، ويعد هذا النوع من التحريات له بالغ الأثر في تحقيق الأمن بالنظر إلى طبيعة المجرم الذى يستخدم هذه التقنيات الحديثة الذى لا تتوافر عنه المعلومات الكافية ، وسهولة قيامه بالتخفي عبر شبكة الإنترنت، هذا بالإضافة إلى إحجام الضحايا عن الإبلاغ عن الجريمة[٢].

رابعاً : مصادر التحري

يقوم مأمورو الضبط القضائي في التحريات القابعة باستخدام مصادر متعددة لجمع المعلومات عن الجريمة المرتكبة باستخدام شبكة الإنترنت، عن طريق الاتصال بمزود الخدمة ISP والذى يساهم بشكل فعال في الوصول إلى Ip address والذى يمكن من خلاله تحديد المشتبه به، وكما تعد البؤر الإجرامية ومسرح الجريمة ومراكز حفظ المعلومات من مصادر التحريات المهمة بالنسبة للجرائم التقليدية فإن مواقع الإنترنت ومنتديات الحوار وغرف الدردشة الصوتية والنصية من الأماكن التي يمكن التوصل منها على المعلومات عن الجريمة[٣].

١٩٩٥، هامش ص ٣٣٢ عن د. مصطفى محمد موسى: "دليل التحري عبر شبكة الإنترنت"، مرجع سابق، ص٢٥.

(١) – مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت، مرجع سابق، ص ٢٣.

(٢) – عمر محمد ابو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية) ، مرجع سابق، ص ٨٢٧.

(٣) –عمر محمد ابو بكر بن يونس: مرجع سابق، ص ٨٢٨.

خامساً : التصنت على المراسلات الإلكترونية

لقد نص دستور جمهورية مصر العربية لسنة ٢٠١٤ في المادة ٥٧ على أن "للحياة الخاصة حرمة، وهى مصونة لا تمس، وللمراسلات البريدية، والبرقية، والإلكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، أو في الأحوال التي بينها القانون".

سادساً : الإرشاد الجنائي في البيانات الرقمية

يستعين مأمور الضبط القضائي بالمرشد الجنائي في قيامه بالبحث عن جريمة ومرتكبيها لإمداده بالمعلومات التي تفيد في كشف الحقيقة، وتقوم العديد من المؤسسات الضبطية حول العالم باستخدام نظام الإرشاد الجنائي عبر شبكة الإنترنت حيث تدفع العناصر وتجند الغير أيضًا للدخول في العالم الافتراضي عبر حلقات النقاش وقاعات البحث والاتصال المباشر مستخدمين في ذلك اسماء وصفات وهيئات مستعارة بقصد البحث عن الجرائم ومرتكبيها وتقديم الجناة إلى المحاكمة[١].

ويقوم أيضًا مأمورو الضبط القضائي بالعمل وفق نظام الإرشاد الجنائي عبر شبكة الإنترنت بذاته بدور المرشد أو يكلف غيره ممن هم على اتصال بالإنترنت فله أن يشرع في الولوج إلى الشبكة سعيًا وراء اكتشاف الجريمة ومرتكبيها باليات مختلفة فله أن يلج إلى قاعات الدردشة أو حلقات النقاش أو برمجيات الاتصال المباشر المستقل والتنكر في هيئات مختلفة واتخاذ أسماء مستعارة وتناول الأحاديث المختلفة وبشكل عام الظهور بمظهر طبيعي، ومن الأمثلة على ذلك قيام المباحث الفيدرالية FBI بضبط أول تشكيل عصابي منتشر حول العالم امتهنوا قرصنه البرمجيات وتحميلها على مواقع الهكرة عبر الإنترنت Warez وتحصلوا على أرباح وصلت لمليون دولار في فترة زمنية قصيرة وتم ضبط تسعة منهم في الولايات المتحدة الأمريكية وأدانتهم هيئة المحلفين العليا في شيكاغو، وقد استخدم فريق المباحث الفيدرالية أسلوب التسلل Infiltrste بدس عضو الضبطية القضائية إلى أن تم ضبط التشكيل العصابي[٢].

---

(١) سليمان احمد محمد فضل : المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الإنترنت، دار النهضة للنشر، ص٢٧٣.

(2)USDOJ-9indicated in chicago in $ 1 million"fastan" software piracy conspiracy feb,16,2001,http//www.Cybercrime.gov/fastane.htm.

كذلك قامت أجهزة التحري في المباحث الفيدرالية بالقبض على أحد الأشخاص أطلق على نفسه مافيابوى Mafiaboy لقيامه بتعطيل خدمات الموزع DDOS لعدد من الشركات مما سبب في انخفاض أسهمها في البورصات العالمية، وقد تمت عملية اكتشاف الجريمة في مواقع المحادثة المباشرة Chatting room حيث رصدت بالمصادفة حديث هذا الشخص مع أعضاء الحوار بشأن كيفية ارتكابه للجريمة فتم القبض عليه[١].

سابعاً: تتبع أثر المشتبه به عبر الإنترنت:

يجب على فريق جمع المعلومات أن يستخدم الأدوات Tools والبرمجيات التقنية التي تساعده على جمع المعلومات، ومثال ذلك برامج تتبع مصدر الاتصال الشبكي Tracing-Back ومنها برنامج Visual route ويمكن تشبيه استخدام برامج التتبع بعملية تتبع آثار المتهم في الجرائم التقليدية، فيمكن عن طريق استخدام هذه البرامج معرفة الطريق الذى سلكه المتهم للوصول إلى الحاسوب الذى وقع عليه الاعتداء.[٢]

ويستخدم المشتبه به شبكة الإنترنت بالاتصال بها من خلال مقدم الخدمة ISP، ويقوم بعد ذلك بالدخول على الخادم المخصص له أحد المواقع على الشبكة، وتعمل المواقع من خلال أكواد مثل [HTML (Hyber Text Markup Language وذلك حتى يتحقق الاتصال من خلال الشبكة بموقع الخادم، ثم يتم تحميل أشكال النصوص الكتابية والصور ومقاطع الفيديو أو أي شكل من أشكال المعلومات التي يتم تداولها عبر شبكة الإنترنت من حاسب المستعمل إلى حاسب الخادم، ويتم نقل هذه المعلومات بصورة مجزأة Packets ثم يعاد تجميعها لدي حاسب المستعمل، ويتولى حاسب الخادم إصدار التعليمات إلى صفحة الإنترنت بكيفية إرسال المعلومات عبر الشبكة، ويتولى حاسب مقدم

(1) Neal Kumar Katyal,Criminal Law in Cyberspace,University of Pennsylvania Law Review,Vol. 149, No. 4 (Apr., 2001), pp. 1003-1114, The University of Pennsylvania Law Review http://www.jstor.org/stable/3312990

(٢) – ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر الإنترنت، مرجع سابق، ص ٧١.

الخدمة ISP التعليمات الخاصة بتحديد العنوان IP الذي يتم التعامل معه في الإرسال والاستقبال، ويقوم الخادم الخاص بمقدم الخدمة بتخزين المعلومات الخاصة بعمليات الاتصال والإرسال والاستقبال في ملف Log File.[١]

كما يمكن باستخدام برمجيات جافا أو جافا سكريبت أو اكتيف اكس معرفة عنوان بريد إليكتروني وبعض المعلومات الأخرى عنه، كما يمكن زيارة موقع للتعرف على المواقع التي زارها مستخدم الشبكة[٢].

وتحتفظ أغلب المواقع بالبيانات الشخصية للقائمين بزيارتها، وتضع بعض المواقع على القرص الصلب لحاسب المستخدم ملف كوكى(cookie) لتسجيل المعلومات الشخصية عن المستخدم واستعمالها عند كل محاولة دخول للموقع، مثل حفظ كلمة المرور للموقع و الولوج إليها عبر الملف دون قيام المتصفح بإدخالها[٣].

ويسجل المتصفح لمواقع الشبكة معلومات يكتبها ضمن المجموعات الاخبارية تحفظ ضمن أرشيف يمكن لأى شخص الاطلاع عليها، كما يقوم البعض بالكتابة لدى المنتديات والتي تحتفظ بالمعلومات لديها ولكن ليس لفترات طويلة مثل المجموعات الإخبارية، تلك المعلومات يمكن الرجوع إليها في إطار البحث الجنائي عن الجرائم المرتكبة عبر شبكة الإنترنت[٤].

وبعض المواقع تمكن المتصفح من إخفاء هويته عن مزود الخدمة المشترك معه من خلال مزود خدمة آخر يتحكم في توجيه المتصفح باستخدام تقنيات تشفير متطورة، تضمن سرية إرسال الرسائل عبر البريد الإلكتروني والدردشة عبر الإنترنت فيمكن عبر استخدام البرمجيات المجانية مثل Ghost Mail إمكانية إرسال البريد الإلكتروني دون الكشف عن

---

(1) Albert J. Marcella Robert s. Greenfield, Cyber forensics a Field Manual for collecting, Examining, and preserving evidence of Computer crime, CRC Press, USA, 2001, p 87.

(2) www.consumer.net/analyze.

(٣) ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت مرجع سابق، ص٦٩ .

(٤) ممدوح عبد الحميد عبد المطلب: مرجع سابق، ص٧٠.

عنوان IP للمتصل، وفى هذه الحالة(بروكسى) لا يمكن الوصول لمعلومات المستخدم إلا عبر الولوج للجهة الوسيطة التي تقدم هذه الخدمة وعندما يثبت قيام المستخدم بأعمال تخالف القانون عبر الإنترنت، والعديد من الدول تمنع الولوج للمواقع التي تقدم هذه الخدمة[١].

ويقوم المحقق الجنائي بالوصول لمتصفح الموقع المتهم بارتكاب جريمة عبر تحديد IP للمستخدم من خلال البرمجيات المتعددة مثل برنامج الأوت لوك ثم يلجأ لمزود الخدمة الذى قام المستخدم بالولوج من خلاله والذى يحدده رقم IP المشار إليه، وعن طريق مد مزود الخدمة بالمعلومات عن تاريخ ومدة واسم الموقع الذى قام المستخدم بالولوج إليه يمكن تحديد اسم المشترك، وتقدم شركة الهاتف الرقم الذى قام المستخدم بالولوج من خلاله ثم يتم بالطرق التقليدية تحديد المكان المستخدم لتحقيق الاتصال والشخص الذى قام بالاستخدام لتحقيق الاتصال.[٢]

(١)- ممدوح عبد الحميد عبد المطلب: مرجع سابق، ص٧١.

(٢)- ممدوح عبد الحميد عبد المطلب: مرجع سابق، ص ٧٢.

المبحـــث الثالث
التفتيش للبحث عن أدلة الجريمة الإلكترونية

إن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة الإلكترونية الرقمية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها، وتعد التفتيش من بين الإجراءات التي تباشرها سلطات التحقيق والتي تؤدي للوصول إلى الدليل المستمد من الواقعة الإجرامية، عن طريق التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه، لذا سوف نعرض في هذا المبحث للتفتيش لضبط الجرائم الإلكترونية.

فالتفتيش لضبط الجرائم الإلكترونية لابد أن يتم بناء على مذكرة قضائية ولابد أن تشتمل المذكرة القضائية على ما مفاده جواز تفتيش أنظمة الكمبيوتر والقواعد التي ترعى التعامل عبر الإنترنت، وأما إجراء التفتيش دون مذكرة قضائية أو الحصول على بيانات من جهات ليست محلاً للاشتباه لتعلقها بالمشتبه به فإنها مسائل تثير الكثير من المعارضة خاصة في ظل ما تقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد، وتوجب مشروعية الدليل وسلامة مصدره، أو تبطل كل إجراء يتم خلافاً للقواعد الأصولية المتعلقة بالتفتيش والضبط المنصوص عليها في القانون، لذلك يجب أن يتضمن إذن التفتيش الإجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات[١] .

وتبدأ المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيا وكيانات منطقية غير مادية، وبالتالي يصعب من ناحية كشف هذه الجرائم، ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة الإجراءات في هذا المجال ، سرعة ودقة تنفيذ الجرائم الإلكترونية وإمكانية محو آثارها، وإخفاء الأدلة المتحصلة عنها عقب التنفيذ مباشرة[٢].

---

(١) – محمد محيي الدين عوض : مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ، دار الفكر العربي ، القاهرة ، ٢٠١١م ، ص ١٤٦ .

(٢) – أحمد حسام طه تمام : الجرائم الناشئة عن استخدام الحاسب الآلي، القاهرة، دار النهضة العربية، سنة ٢٠٠٠م ، ص١٨ .

وباعتبار أن التفتيش من أخطر الحقوق التي منحت للمحقق لكونه يمس بالحريات التي تكفلها وتصونها الدساتير عادة لذا فالقوانين قد وضعت له عدة ضوابط سواء فيما يتعلق بالسلطة المختصة بمباشرته، أو التي تأذن بإجرائه، أو الأحوال التي تجوز فيها مباشرته وشروط اتخاذه، وكل هذا يمثل ضمانات الحرية الفردية أو حرمة المسكن. وهذا ما سوف نتطرق إليه من خلال أولاً: الإطار العام للتفتيش في الجرائم الإلكترونية ثانياً : ضوابط تفتيش الجرائم الإلكترونية.

وتعد إحدى المسائل الشائكة المتعلقة بقضايا الجريمة الإلكترونية أن مستخدم الشبكة يمكن أن ينتحل أي شخصية يريدها، حيث يمنح جهاز الحاسوب والإنترنت للمستخدم ميزة لا مثيل لها وهي القدرة على إخفاء الهوية، وقد أدى ذلك إلى التأثير على طبيعة المحاكمة الجنائية في ضوء الخدمات العديدة التي تقدم عبر الإنترنت وتمكن المشتبه به من التخفي بسهولة خلف هويات زائفة وأسماء مستعارة تخفي هويتهم الحقيقية عند القيام بأنشطة غير مشروعة على الحاسوب[١].

أولاً: الإطار العام للتفتيش للبحث عن أدلة الجرائم الإلكترونية

يقع التفتيش على محل منح له القانون حرمة خاصة باعتباره مستودع السر، وقد يكون المحل شخص أو مسكن أو محل ألحقه القانون في حكم المسكن، ويباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أدلة أو أشياء يكون كشفها مفيدا لإظهار الحقيقة [٢].

وسوف نعرض لتعريف التفتيش، وخصائصه، ومدى قابلية جرائم الحاسب والشبكات الإلكترونية للتفتيش عن أدلة الجريمة .

تعريف التفتيش

لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة الإلكترونية، وبالتالي يقصد به إجراء من إجراءات التحقيق الذي يهدف للوصول إلى أدلة تفيد إظهار الحقيقة وإسنادها

---

(1) Michael Froomkin, Flood Control On The Information Ocean: Living With Anonymity, Digital Cash, And Distributed Databases, Published at 15 U. Pittsburgh Journal of Law and Commerce. 15 J.L. COM.395,398(1996 .)

(... يؤثر توافر إمكانية إخفاء الهوية في الاتصالات الإلكترونية بشكل مباشر علي قدرة الحكومة علي مراقبة الصفقات الإلكترونية علي الإنترنت (سواء المشروعة أو غير المشروعة) ".

(٢) – خالد ممدوح إبراهيم : فن تحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص١٨٠.

إلى المتهم المنسوب إليه التهمة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات وتخزين ومخرجات، وذلك من أجل البحث عن الأفعال والسلوكيات المرتكبة وغير المشروعة والتي تشكل جناية أو جنحة[١] .

والشاهد في الجريمة الالكترونية هو ذلك الشخص الفني صاحب الخبرة العالية في علوم الحاسب الالي وصاحب التخصص الذي لديه العلم والدراية عن ماذا سوف يدلي بوقائع شهادته، والذي يكون لديه معلومات جوهرية هامة او لازمه للدخول الى نظام المعالجة الآلية للبيانات اذا كانت مصلحة التحقيق تقتضي ذلك للتنقيب عن ادلة الجريمة الالكترونية[٢] .

مدى قابلية برامج الحاسوب والشبكات الإلكترونية للتفتيش عن أدلة الجريمة الإلكترونية ؟

فيما يتعلق بالبرامج الإلكترونية لا يحتاج الأمر إلى قواعد جديدة للتفتيش عن التي يكون محلها سرقة أو إتلاف أو استعمال هذه البرامج للتزوير أو التلاعب بالبيانات المخزنة، وذلك لكفاية القواعد التقليدية الموضوعية والإجرائية لإثبات وقوع الجريمة عن طريق الالتجاء إلى المتخصصين فـ مجال المعلوماتية. أما فيما يتعلق بالبيانات الإلكترونية، فإن الأمر تكتنفه بعضاً من الصعوبات العملية والإجرائية نظراً لتجرد هذه الأخيرة من الكيان المادي المحسوس في المحيط الخارجي، وهو ما يعيق عملية إخضاعها لقواعد التفتيش التقليدية، ففي هذا النمط من الجرائم التي تتم عادة على شبكات المعلومات، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة به [٣] .

---

(١) – علي محمود حموده : "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ، " المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، ع ،١ دبي– الإمارات العربية المتحدة– ٢٨–٢٦نيسان ، ٢٠٠٣ م ،ص٢٤.

(٢) – عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري: الاثبات الجنائي بالأدلة الرقمية من الناحية القانونية والفنية دراسة تطبيقه مقارنة ، رسالة ماجستير ، جامعة نايف العربية للعلوم الامنية. الرياض ، السعودية، ٢٠٠٧م ، ص ٢١.

(٣) – محمد دباس الحميد ، ماركو إبراهيم ونينو: حماية أنظمة المعلومات عمان، دار الحامد للنشر والتوزيع، ص١٠٥ – ١٠٦ .

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ذهب رأي إلى أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها[١].

وفي هذا المعنى نجد المادة ٢٥١ من قانون الإجراءات الجنائي اليوناني تعطي سلطات التحقيق إمكانية القيام (بأي شيء يكون ضروريا لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أي شيء بأنها تشتمل بالضبط البيانات المخزنة أو المعالجة إليكترونيا، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان، إذ بمقدور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية[٢].

وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم ٣٤ من القواعد الفيدرالية الخاصة بالإجراءات الجنائية عام ١٩٧٠، لتنص على السماح بتفتيش أجهزة الحاسب والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس[٣].

ويرى الفقه الألماني ضرورة وجود اتفاق خاص بين الدول المعنية للولوج الى أنظمة المعلومات لضبط البيانات المخزنة فيها[٤]، ويمكن أن يتحقق ذلك من خلال التماس المساعدة المتبادلة كما ذهب الفقه الألماني request for matual assistance، أو كما يرى الفقه المجرى[٥] بالاشتراك في شبكة اتصالات الانتربول

---

(1) John R. Vacca .Computer Forensics: Computer Crime Scene Investigation. -computers- 2005. P.85

(2) VASSiLAKi (Irini): " Computer crimes and other crims against information Technology in Greece." R.I.D.P.1993. P.355.

(٣) – هلالي عبداللاة أحمد : مرجع سابق، ص٤٨.

(4) Mohens Chlager (MOnfred) " Computer Crim and other crimes Against information Technology in Germany " R.I.D.P.1993.P.351

(5) KERTESZ (I mre) and PUSZTAI(Lasz10)computer crimes and technology in Hungary R.I.D.P.1993.P.387.

ولقد ذهب بعض الفقهاء الفرنسيين بالتفسير إلى أن برامج الحاسب الآلي ذات كيان مادي يشمل على نبضات وذبذبات إلكترونية ممغنطة قابلة للتخزين داخل الجهاز أو على الأقراص الصلبة، كما يجب الأخذ بعين الاعتبار القيمة التي يتمتع بها شيء محل الحماية الجنائية والتي قد تكون غالبا مصلحة اقتصادية يصل إليها صاحبها لذلك فالأشياء المعنوية مثلها مثل الأشياء المادية[١] .

وتتصل هذه المسألة مباشرة بالبعد الدولي فلا يمكن الحديث عن القضاء عليها إلاَ في ظل تعزيز وتبادل التعاون الدولي في إطار اتفاقيات دولية أو إقليمية أو ثنائية مع تفعيل آليات المساعدة الدولية في مجال القضائي وتسليم المجرمين، وذلك باحترام مبدأ المساواة بما يفضي أنه لا مجال للدول المتقدمة في المجال الإلكترونية الرقمية أن تتحكم في أنظمة الغير والتجسس عليها بحجة ما يقتضه إجراء التحقيق من تمديد التفتيش عن بعد بين الدول[٢] .

ثانياً : أسلوب تنفيذ التفتيش:

عادتاً وضع فريق يتكون من خبيران فنيان أجاز لهم القاضي بالتفتيش، فالأول يسمى بالمكتشف ؛ مهمته نزع مقبس الكهرباء الخاص بسائر الأجهزة، ويقوم بالبحث عن الأقراص والمستندات وغير ذلك، والثاني يسمى بالمسجل مهمته تصوير كامل الأجهزة والأدوات المتصلة بها على الحالة التي تم ضبطها، كما يقوم أيضا بتصوير جميع الغرف الأخرى المتواجدة في المكان كضمانة لعدم ادعاء أحد المشتبه فيهم بسرقة منزله وقت التفتيش، بالإضافة إلى أجهزة الفيديو والتسجيل الصوتي التي يتم من خلالها ترقيم الأشياء المضبوطة[٣].

يجوز إجراء تفتيش أنظمة المعالجة الآلية للمعطيات فيها في كل ساعة من ساعات الليل والنهار بناء على إذن مسبق من وكيل الجمهورية المختص، ذلك لأن المكونات المعنوية للحاسب الآلي وشبكة الاتصال قد تكون عرضة لإخفاء أو تغيير أو تدمير أو تلاعب بالبيانات المخزنة والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي

---

(١) – علي محمود علي حموده : مرجع سابق، ص٢٥ .

(٢) – فايز محمد راجح غلاب: مرجع سابق، ص ٣١٥، ٣١٦ .

(٣) – عبد الله حسين على محمود: مرجع سابق، ص ٣٨٢ .

بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضافة الجريمة الإلكترونية كاستثناء عن أوقات التفتيش نظرا لطبيعة أدلتها الخاصة [١].

ثالثاً : محل التفتيش في جرائم الإنترنت

يطلق البعض في الفقه على عملية البحث عن أدلة الجريمة في العالم الرقمي مصطلح الولوج أو النفاذ باعتباره أكثر دقه من التفتيش الذى يعنى البحث والفحص والتدقيق في البيانات.[٢]

أ- تفتيش مكونات منطقية لدي غير أطراف الجريمة داخل الدولة:

تبرز هذه الحالة في المكونات المنطقية محل التفتيش في متناول طرف ثالث مثل موفر خدمة الاتصالات أو مدير النظام، ولا يكون هناك حاجة إلى التصنت الفوري للحصول على الدليل واعتراض انتقال البيانات الفوري، فيكون للسلطة المختصة أن تأمر بتسليمها أي معلومات ذات علاقة في حوزته، ويعد الكشف اقتحاما لخصوصية المتهم فيحتاج لإذن من السلطة المختصة.[٣]

ويرى البعض في الفقه الألماني امتداد التفتيش لسجلات البيانات التي تكون في موقع آخر استناداً إلى مقتضيات القسم (١٠٣) من قانون الإجراءات الجنائية الألماني.[٤]

ونص قانون تحقيق الجنايات البلجيكي في المادة ٨٨ على أنه "إذا أمر قاضى التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقاً لضابطين: الأول أن يكون ضرورياً لكشف الحقيقة والثاني أن توجد مخاطر تتعلق بضياع بعض الأدلة نظراً لسهولة عملية محو أو إتلاف أو تحريف أو نقل البيانات محل البحث[٥].

---

(١) - فايز محمد راجح غلاب: مرجع سابق، ص٣٢٩ ، ٣٣٠ .

(٢) - نبيلة هبة هروال: "الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات"، مرجع سابق ، ص٢٢٤.

(3) Jody R. Westby, Project chair&Editor, international Guide to Combating Cybercrime,OP-Cit, P125.

(٤) -هلالي عبداللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ص ٧٧ .

(٥) - هلالي عبداللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع سابق، ٧٨.

رابعاً: تطبيقات تفتيش المكونات المنطقية لأطراف خارج نطاق الدولة: في مصـــــر[١]:

بفحص الإدارة العامة لمباحث الأموال العامة لبلاغ إنتربول واشنطن قيام مصري بارتكاب وقائع احتيالية على العديد من التجار أصحاب المحلات التجارية بالولايات المتحدة الأمريكية عن طريق اختراق العديد من المواقع الالكترونية على شبكة الإنترنت وسرقة بيانات بطاقات ائتمان واستخدامها في الدخول على مواقع التجار الأمريكيين على شبكة الإنترنت وانتحال شخصية أصحاب البطاقات وطلب منهم شراء بضائعهم على أن تسدد قيمة البضائع من حسابات البطاقات الائتمانية المسروقة بياناتها، وقام هؤلاء التجار بأرسال البضائع المشتراه وهي عبارة عن كتب ومجلات وبرامج كمبيوتر واسطوانات وأشياء أخرى ذات قيمة إلى المذكور بعالية، الذي قام باستلامها من مكاتب البريد بمصر حيث تم اكتشاف تلك الوقائع حالة رفض أصحاب البطاقات سداد قيمة تلك البضائع لعدم قيامهم بتلك العمليات أو طلبها وأنها تمت بالأسلوب الاحتيالي المشار إليه.

تمكن الجانب الامريكي من تحديد الشخص القائم على ذلك النشاط بعدما تمكنوا من التتبع الفني للرسائل المرسلة من مصر إلى التجار الأمريكيين بمعرفة المتهم المذكور.

حيث أسفرت التحريات عن صحة ما جاء بالبلاغ المشار إليه وأن المذكور هو وراء ارتكاب تلك الواقعة وانه سبق ضبطه واتهامه في قضيتين مماثلتين وأنه يزاول نشاط تزوير البطاقات الائتمانية وسرقة بياناتها واستخدامها في الاحتيال على الشركات المصرية والأجنبية والاستيلاء على بضائعهم من خلال شبكة المعلومات الدولية الإنترنت حيث إن المذكور يعد من العناصر الإجرامية النشطة في مجال القرصنة على شبكة الإنترنت، تم استصدار إذن بالتفتيش لشقته والذي تبين وجوده بالشقة وبالإفصاح له عن شخصية مأموري الضبط وطبيعة مأموريتهم وإذن النيابة العامة بتفتيش شخصه ومسكنه عثر داخل حجرة نومه الخاصة على عدد ثمانية إخطارات بوصول طرود من الخارج باسم المذكور وصادرة عن الهيئة القومية للبريد – مكتب المنشية، حيث اعترف حال مناقشته أن تلك الاخطارات خاصة

---

(١) – خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية ، مرجع سابق، ص ٤٩٢ وما بعدها.

بوصول طرود من الخارج له وأن تلك الطرود عبارة عن بضائع وكتب وبرامج تمكن من الاستيلاء عليها بعدما احتال على التجار أصحاب الشركات الأجانب وقدم إليهم بيانات بطاقات ائتمانية منتحلاً شخصية أصحابها وذلك لخصم قيمة تلك البضائع من حساباتها موضوع بلاغ انتربول واشنطن، والعديد من الكتب والقواميس والبرامج الكمبيوترية والتي تمكن المتهم من الحصول عليها باتباعه الأسلوب الاجرامي الوارد بالبلاغ وبالتحريات، وأقر المتهم حال مناقشته بأن تلك البضائع جزء من البضائع التي تمكن من الاستيلاء عليها بإتباعه الأسلوب الاجرامي المشار إليه وانه في طريقه لإعادة بيع تلك البضائع والكتب والحصول على مقابلها النقدي مثلها مثل البضائع الأخرى التي تمكن من الاستيلاء عليها الأسلوب الإجرامي ذاته وقام ببيعها.

وبسؤاله عن كيفية حصوله على بيانات البطاقات الائتمانية التي تمكن من سرقتها واستخدامها في الاحتيال على أصحاب المحلات التجارية بالعديد من الدول الأجنبية والحصول على بضائعهم قرر أنه نظرا لما لديه من خبرة عالية في مجال استخدامات الحاسب الالي وكيفية اختراق المواقع الالكترونية الخاصة بالشركات والبنوك والأشخاص، فقد تمكن من الحصول عليها من تلك المواقع التي اخترقها على بيانات البطاقات الائتمانية والبيانات الشخصية الخاصة بأصحابها.

وأضاف أنه أيضًا تمكن من الحصول على أرقام بطاقات ائتمانية خاصة بأجانب عن طريق تخليق الأرقام بان يحصل على رقم بطاقة صادرة عن أحد البنوك ويقوم بتخليق مجموعة من الأرقام الأخرى والتي تكون البنوك قد اصدرتها من قبل بأرقام مسلسلة وأنه كان يتمكن من تخليق تلك الأرقام باستخدام برنامج خاص بذلك وأضاف بأن جهاز الكمبيوتر الخاص به والمضبوط محمل عليه ذلك البرنامج والمواقع التي كان يخترقها وبيانات البطاقات الائتمانية التي قام باستخدامها في الاستيلاء على البضائع، وكذا مواقع التجار الأجانب الذين كان يتعامل معهم منتحلاً شخصية صاحب البطاقة ويمدهم ببيانات البطاقة ثم ترسل البضائع له بموجب ذلك.

الفصل الثالث
ضبط الدليل في الجرائم الإلكترونية والخبرة القضائية

تمهيد وتقسيم:

بتطور أساليب ارتكاب الجريمة اصبح اكتشاف الجاني أمرا عسيراً ولذلك كان لزاماً على المجتمع أن يستخدم ذات السلاح (سلاح العلم)، باستخدام وسائل علمية حديثة للكشف عن الجريمة وإثباتها. فالأدلة العلمية هي وسائل لإيجاد الصلة بين الجريمة والجاني، وهى من أهم مقومات الإثبات الجنائي وتقليل فرص الخطأ القضائي.[١]

فتلعب الخبرة دوراً مهماً في الإثبات حينما لا يكون متاحاً الإلمام بالواقعة الإجرامية، لكونها مرتبطة بمسائل ذات طبيعة فنية أو متخصصة تتطلب قدراً من الإلمام والدراية بمجال المعرفة أو الناحية الفنية التي تنطوي على تلك المسائل، مما يتطلب اللجوء إلى الخبرة لاستجلاء حقيقة ظروف وملابسات ارتكاب الجريمة[٢].

ومنذ بدء ظهور الجرائم ذات الصلة بالحاسب الآلي فإن الشرطة وسلطات التحقيق وسلطات المحاكمة تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، وذلك بغرض كشف غموض الجريمة، أو تجميع أدلتها والتحفظ عليها ، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[٣] .

وقد يكون التحفظ على المواد المتعلقة بوسائل الحاسب الأخرى أمراً أكثر تعقيداً مثل : الأشرطة الممغنطة ، الأسطوانات، البرامج ويحتاج إلى معونة أحد الخبراء الموثوق فيهم، حتى يتمكن المحقق من الإلمام بمحتويات الأشرطة أو الاسطوانات دون إحداث أي تغيير فيها[٤].

---

(١)) جميل عبد الباقي الصغير: أدله الإثبات الجنائي والتكنولوجيا الحديثة (اجهزة الرادار – الحاسبات الالية – البصمة الوراثية)، دار النهضة العربية، القاهرة، ٢٠٠١، ص٤.

(٢) نقض ٨/ ١/ ١٩٦٨، مجموعة أحكام النقض، الطعن رقم ١٩٣٤، لسنه ٣٧ق، س١٩، ص٣٤.

(٣) – مدني عبد الرحمن تاج الدين : أصول التحقيق الجنائي وتطبيقاتها في المملكة العربية السعودية، الرياض، معهد الإدارة العامة، ٢٠٠٤م ، ص ٢١ .

(4) Bruce Middleton .Cyber Crime Investigator's Field Guide. Op.cit. P.55.

ويتم الاستعانة بالخبرة في مجال الجرائم المعلوماتية من أجل **وصف** تركيب الحاسبات وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به، وكلمات المرور أو السر ونظام التشفير.... الخ[١].

ويتم الاستعانة بالخبرة في مجال الجرائم المعلوماتية من أجل بيان كيفية تجسيد الأدلة في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة[٢].

لذا سوف نتناول هذا الفصل في مبحثين :

المبحث الأول: ضبط الدليل في الجرائم الإلكترونية

المبحث الثاني: الخبرة القضائية في الجرائم الإلكترونية

(1) http://www.al-jazirah.com/digimag/11042004/wr35.htm
(2) Eoghan Casey. Digital Evidence and Computer Crime.Op.cit.P.71

المبحث الأول
ضبط الدليل في الجرائم الإلكترونية

فالغاية من التفتيش ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأن الجريمة الإلكترونية، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة، ونظراً لكون الضبط في مجال الجرائم الإلكترونية هو ضبط البيانات المعالجة إلكترونياً، فقد ثار التساؤل: هل يصلح ضبط هذا النوع من البيانات[١] ، في البداية نعرف الضبط .

أولاً: تعريف الضبط

يعرف **الضبط** : بأنه بحث وتنقيب[٢] يرتبط عادة بتطلب معارف علميه أو فنية خاصة لا تتوافر سواء لدى المحقق أو القاضي[٣] .

وإجراء الضبط قد يكون من إجراءات الاستدلال أو التحقيق وذلك وفقاً للطريقة التي تم بها وضع اليد على الشيء المضبوط، فإذا كان في حيازة شخص واقتضى الأمر تجريده من حيازته كان إجراء تحقيق، أما إذا تم دون الاعتداء على حيازة قائمة فإنه يكون إجراء استدلال، كأن يتم بناءً على معاينة مسرح جريمة[٤].

وفى أعمال التحقيق يجرى التفتيش بغرض ضبط الأدلة المادية لكشف حقيقة الواقعة المرتكبة، فعرف البعض الضبط بأنه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في

---

(١) – فتوح الشاذلي : عفيفي كامل عفيفي : جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. بيروت، منشورات الحلبي الحقوقية،٢٠٠٣م ، ص ٩٢،٩٣ .

(٢) نقض ٣١أكتوبر سنة١٩٧١ ، مجموعة أحكام محكمة النقض،س٢٢،رقم ١٤٢،ص٥٩٠ .

(٣) – محمد ابراهيم زيد : تنظيم الاجراءات الجزائية في التشريعات العريقة جـ٢،الرياض،المركز العربي للدراسات الامنيه،سنة١٩٩٠م ، ص٢٤٤ .

(٤) –عبدالله حسين على محمود: "سرقة المعلومات المخزنة على الحاسب الآلي ، دار النهضة العربية ، ٢٠٠٤م ، ص ٣٨٨.

كشف الحقيقة عنها،[١] وأنه العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، ونتيجة لذلك فأنه يتطلب توافر نفس القواعد التي تنطبق على التفتيش[٢].

ثانياً : ضبط المكونات المادية للحاسب الآلي:

بالنسبة للجرائم الواقعة على المكونات المادية للبيئة الإلكترونية فإن الأمر لا يثير أي صعوبة تذكر، ذلك أن الضبط يرد بالأساس على الأشياء المادية محل الجريمة المرتكبة[٣] فالضبط يرد على أشياء مادية كالدعامة المادية للبرامج والأسطوانات والأشرطة[٤] .

ثالثاً : ضبط المكونات المعنوية للحاسب الآلي:

تكمن المشكلة في الأشياء المعنوية للحاسب الآلي التي تتضمن البرامج والبيانات[٥] .

فالضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، وأي أدوات دفع إلكترونية أو أي أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف[٦].

أ- برامج الحاسب الآلي:

إن الأمر يتعلق بكيفية ضبط الأدلة في حالة استخدام الوسائل الفنية في نسخ أو إتلاف البرنامج كالفيروسات مثل حصان طروادة، وهذا من الناحية الأولى، ومن الناحية الثانية تتمثل في قيام عملية ضبط الوسائل التقنية بواسطة الأنظمة والشبكات الإلكترونية الكبيرة، حيث

---

(١) تنص المادة ٥٢ إجراءات جنائية "إذا وجت في منزل المتهم أوراق مختومة أو مغلقة بأية طريقة أخرى، فلا يجوز لمأمور الضبط القضائي أن يفضها."

(٢) -مصطفى محمد موسى: التحقيق الجنائي في الجرائم الالكترونية ، مرجع سابق، ص ٢٠٨.

(٣) - عبد الفتاح مصطفى الصيفي: تأصيل الإجراءات الجنائية الإسكندرية، دار المعرفة الجامعية، ٢٠٠٢م ، ص١١٩.

(٤) - عفيفي كامل عفيفي: جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط٢ منشورات الحلبي الحقوقية، بيروت- لبنان، ٢٠٠٧م ، ص٣٧٣ .

(٥) - عفيفي كامل عفيفي : مرجع سابق، ص٣٧٨ .

(٦) - عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، ط١، الإسكندرية ، دار الفكر الجامعي ،٢٠٠٧م ، ص١٤٨ .

يؤدي الضبط إلى عزل النظام المعلوماتي بالكامل عن دائرته لفترة زمنية يمكن أن تطول أو تقصر[١].

ب- بيانات الحاسب الآلي

تتميز الجرائم التي يكون محلها بيانات الحاسب بعدم وجود أثار مادية يمكن من خلالها الاستدلال على أدلة في ارتكاب الجريمة ويظهر ذلك بشكل أوضح في جرائم الاختلاس والتزوير باستخدام الحاسب الآلي، كذلك فالبيانات التي يمكن التوصل إليها يستطيع الجاني تدميرها أو محوها في مدة قصيرة، وهو ما يلزم للمحقق من فحص البيانات مع ضخامتها، ناهيك عن نقص الخبرة الفنية لعملية الفحص وما تتطلبه من تحديد البيانات التي تصلح كأدلة إدانة من عدمه، والأمر يزداد تعقيداً في حالة الأنظمة الإلكترونية المتصلة بنهاية طرفية أخرى تتعدى حدود الدولة إلى إقليم دولة أخرى[٢]

ج- ضبط الرسائل ومراقبة الاتصالات الإلكترونية

القوانين الإجرائية تجيز ضبط الرسائل ومراقبة المحادثات الهاتفية وفقا لقواعد وشروط معينة وسائر المراسلات الإلكترونية المستخدمة[٣] .

د- البريد الإلكتروني:

يقصد بالبريد الإلكتروني استخدام شبكات الانترنت من أجل نقل الرسائل بدلا من الطرق التقليدية، وباعتبار أن استعماله سهل أضحى من أكثر وسائل الانترنت استعمالا في الوقت الحالي ، وأهم مسائل تتعلق بالبريد الإلكتروني هو وجوب المحافظة على سريته، وهو ما أدى إلى اصطناع برامج تشفير خاصة به، حيث لا يمكن الاطلاع على رسائل الأشخاص إلاَ لمن يعرف الشيفرة ، ولقد ساعد ذلك على ظهور التوقيع الإلكتروني في تيسير عملية التراسل عبر البريد الإلكتروني[٤] .

---

(١) – عفيفي كامل عفيفي : مرجع سابق، ص٣٧٤ .

(٢) – عفيفي كامل عفيفي : مرجع سابق، ص٣٧٥ .

(٣) – فايز محمد راجح غلاب: مرجع سابق، ص٣٥١ .

(٤) – علي محمود علي حموده : مرجع سابق، ص٣٣.

هـ- بالنسبة للبرامج التطبيقية ونظم التشغيل

وفي هذه الحالة يمكن ضبط أدلة الجريمة إذا كان محلها سرقة الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه بصورة غير مشروعة أو إتلافه بوسائل تقليدية، ولكن الأمر يزداد صعوبة في حال استخدام وسائل فنية في إتلاف البرنامج كالفيروسات مثلاً، فقد يؤدي الضبط إلى عزل النظام الإلكتروني بالكامل عن دائرته لمدة زمنية طويلة وهو ما يسبب حتماً أضراراً بالجهة مستخدمة النظام، وهذه النتيجة المتوقعة من عملية الضبط ستؤدي حتما إلى امتناع مستخدمي الأنظمة الإلكترونية من التعاون الكامل والفعال مع سلطة التحقيق، الأمر الذي يخلق اشكالية كبيرة تواجه إجراءات الضبطية القضائية [١] .

و- بالنسبة للبيانات الرقمية

في هذه الحالة يصطدم المحقق الجنائي بعوامل عدة تحول دون ضبطه للبيانات التي تعد دليلاً على ارتكاب الجريمة، وتكمن هذه العوامل في عدم وجود دليل مرئي يمكن فهمه بالقراءة، بالإضافة إلى عدم وجود آثار مادية يمكن على أساسها الاستدلال على وجود دليل على ارتكاب الجريمة [٢] .

رابعاً : التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي

فقد أجازت بعض التشريعات التنصت والمراقبة الإلكترونية، منها التشريع الفرنسي والذي أجاز على اعتراض الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات، وكما أجاز التشريع الهولندي لقاضي التحقيق أن يأمر بالتنصت على شبكات اتصالات الحاسب الآلي إذا كان الهدف منها ضبط الجرائم الخطيرة، وكذا إمكانية مراقبة التلكس والفاكس ونقل البيانات[٣]

وكذا التشريع الألماني بالمادة ٢٠٣ -٣ عقوبات سنة١٩٧٤ " أو وسائط تخزين البيانات من حيث الحماية الجنائية في مواجهة خطر المراقبة غير المصرح بها "، وقد حذف

---

(١) - سعيد عبد اللطيف حسن: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت: الجرائم الواقعة في جرائم تكنولوجيا المعلومات ، دار النهضة ،١٩٩٩ م ، ص ٤٢ .

(٢) - محمد حماد الهيتي: التكنولوجيا الحديثة والقانون الجنائي، عمان، دار الثقافة للنشر والتوزيع،٢٠٠٤م ، ص٢٣٩.

(٣) - علي محمود علي حموده: مرجع سابق، ص٣٤ ، ٣٥ .

القانون الثاني لمكافحة الجريمة الاقتصادية الصادر عام ١٩٨٦ عبارة " وسائل التخزين من المادة المذكورة "، واستحدث ماده جديدة تعاقب " كل من حصل بغير تصريح سواء لنفسه أو لغيره، على بيانات غير معده أو مخصصه له، ومحمية بوجه خاص ضد الوصول غير المأذون به " أما إذا كانت هذه الأجهزة أو الأنظمة غير تابعه لهيئة البريد، كالبريد الإلكتروني لشركه خاصة، أو بشخص في منزله، فضبط ما يتم إرساله أو استقباله غيرها يخضع للقاعدة العامة لضبط المنقولات وتسرى عليه القيود الخاصة بضبط الأوراق[١].

خامساً: تحريز الأشياء محل الضبط:

إن الهدف من إجراء التحريز هو تنظيم العمل للمحافظة على الدليل من التلف والحفاظ على سلامته، وتقضي القواعد العامة المنصوص عليها في إجراء التحريز للأشياء محل الضبط في الوقائع الجنائية في التشريع الإجرائي المصري بأن يتم على النحو التالي[٢]:

لقد وضعت النظم الأنجلو أمريكية قواعد لضبط وتحريز الأدلة الرقمية هي :ـ

أـ الحصول على بصمة للبيانات الرقمية محل الضبط:

ينبغي على القائمين بالضبط في الوقائع الرقمية توثيق البيانات الرقمية التي يتم التحصيل عليها من إجراء التفتيش حتى لا يطعن عليها أمام القضاء بالتلاعب بها أو تعديلها أو تحريفها، ويستخدم في عملية التوثيق والتحريز أدوات تقنية ، لأخذ بصمه للملفات في مسرح الجريمة للبيانات الرقمية محل الضبط، ويعد اجراء أخذ بصمه رقمية للملفات إثبات

---

(1) MoHENS CHLAGER (MOnfred) " Computer Crim and other crimes Against information Technology in Germany " R.I.D.P.1993.P.283.

(٢)) تنص المادة ٥٣ في الفقرة الاولى على انه "لمأموري الضبط القضائي أن يضعوا الأختام على الأماكن التي بها آثار أو أشياء تفيد في كشف الحقيقة ولهم أن يقيموا حراساً عليها. ويجب عليهم إخطار النيابة العامة بذلك في الحال، وعلى النيابة إذا ما رأت ضرورة ذلك الإجراء أن ترفع الأمر إلى القاضي الجزئي لإقراره".

تنص المادة ٥٥ من قانون الإجراءات الجنائية على أنه " لمأموري الضبط القضائي أن يضبطوا الأوراق والأسلحة وكل ما يحتمل أن يكون قد استعمل في ارتكاب الجريمة أو نتج عن ارتكابها أو ما وقعت عليها الجريمة، وكل ما يفيد في كشف الحقيقة. وتعرض هذه الأشياء على المتهم، ويطلب منه إبداء ملاحظاته عليها ويعمل بذلك محضر يوقع عليها من المتهم، أو يذكر فيه امتناعه عن التوقيع."

على أن الدليل المستخلص من أعمال التفتيش والضبط التي تتم لاحقا في المعامل أو في مسرح الجريمة لم يجرى تعديل لبياناتها.[١]

فيمكن أخذ بصمة للملفات من خلال مولدات التقدير الكمي للملف Cyclical Redundancy Checksum CRC ويعد هذا الأمر مهماً للغاية للمحقق بالحاسب الجنائي لضمان صلاحية النسخة المعدة من البيانات الأصلية لإجراء الاختبارات عليها عن طريق قياسها بواسطة CRC، وهذه العملية تجرى عندما يتم نقل البيانات بين الحواسب، فيتم تقدير البيانات المنقولة، فإذا كانت البيانات التي تم انتقالها، كانت مختلفة في تقديرها فان حاسب المستقبل سوف يطلب إعادة نقل البيانات مرة أخري، وتستخدم هذه الوسيلة أيضًا مع البيانات التي يتم تخزينها بشكل مضغوط، وهذا الأمر له أهمية خاصة في القضايا الجنائية في حالة الطعن في صحة الأدلة الرقمية.[٢]

ويعد MD5 Hash من أبرز أدوات التقدير الكمي للبيانات للتعامل مع عدد كبير من الملفات الموجودة على الحاسب، والجدير بالذكر أن هناك رقماً تقييمياً واحداً فقط هو المتاح لكل منها، ولقد ثار الجدال بين أعضاء الادعاء في الولايات المتحدة الأمريكية بشأن ظهور التقنيات المعقدة ذلك يقود نسبياً إلى ملفين مختلفين لرقم تقييمي واحد، ولكن الخبراء أكدوا بإجراء الحسابات والتجارب البالغة الصعوبة لأن يكون لملفين الرقم التقييمي نفسه.[٣]

بـ نسخ البيانات الرقمية محل الضبط:

تعد عملية النسخ لها أهمية بالغة حيث يتم على أساسها بناء عمليات التفتيش لاستخراج الأدلة والاعتراف بها لدى القضاء، فيجب أن تتم عملية النسخ وفقاً لطريقة Bit Stream Back-up وهي التي يتم بمقتضاها إجراء عملية النسخ لكامل القرص الصلب على مستوى البت Bit وهي اصغر وحدة لقياس كم البيانات الرقمية، وينبغي إعداد أكثر من نسخة وفقاً للطريقة السابقة بحيث تظل دائماً هناك نسخة لم يطالها إجراءات الفحص التي تتم بمعرفة

(1) Bruce Middletion: cyber crime investigator field guid,Op-Cit, P3
(2) http://en,wikipedia.org/wiki/ Cyclical_ Redundancy_ Checks
(3) http://en,wikipedia.org/wiki/md5

الخبراء سواء في مسرح الجريمة أو في معمل الحاسب الجنائي، حتى يتم المحافظة على الأدلة في حالة فساد النسخة التي يتم العمل من خلالها في الفحص:[1]

(1) Bruce Middletion: cyber crime investigator field guid, Op-Cit, P5.

المبحث الثاني
الخبرة القضائية في الجرائم الإلكترونية

أولاً: التعريف:

تعرف الخبرة بأنها إبداء رأى فني من شخص مختص فنياً في شأن واقعة ذات أهمية في الدعوى الجنائية،[١] و يري البعض أنها الاستشارة الفنية التي يستعين بها القاضي في مجال الإثبات لمساعدته في تقدير المسائل التي يحتاج تقديرها إلى معرفة فنية أو إدارية عملية لا تتوافر لدي عضو السلطة القضائية المختص بحكم عمله وثقافته.[٢]

وتعرف الخبرة أيضاً بأنها إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان استخلاص الدليل الرقمي منه، أو هي الاستشارة الفنية التي يستعين بها المحقق أو القاضي في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى مساعدة فنية أو إدارية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته[٣] .

ثانياً: أهمية الاستعانة بالخبراء

الخبير هو كل شخص تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة[٤]، وتكمن أهمية الخبرة في أنها تنير الطريق للقاضي الذي يهتدي به لتحقيق العدالة . سيما في المجال الجنائي[٥] .

وهناك ضرورة لاعتبار الخبرة الفنية في الجرائم الإلكترونية دليلاً مادياً فهي وسيلة علمية في مواجهة الجرائم الإلكترونية في ضوء طبيعة هذه الجريمة التي تعتمد على نبضات إلكترونية تتم من خلال التلاعب بقواعد البيانات في المنظمات، وذلك بالإضافة أو الحذف

---

(١) -محمود نجيب حسني: الاختصاص والإثبات، في المواد الجنائية، مرجع سابق، ص١٢٢ .

(٢) -أبو العلا علي أبو العلا : الإثبات الجنائي، دراسة تحليلية لموطن القوة والضعف في الدليل الجنائي، دار النهضة العربية ، ص٩٤

(٣) - مأمون محمد سلامة : الإجراءات الجنائية في التشريع المصري. القاهرة، دار النهضة العربية ، ٢٠٠١م ، ص ٦٤٥.

(٤) - عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري: مرجع سابق، ص ٢٤ .

(٥) - الشربيني الخطيب: مغني المحتاج إلى معرفة معاني ألفاظ المنهاج بيروت، دار العلم للملايين ١٤٢٥هـ المجلد الرابع ، ص٤٨٨ .

أو التعديل وإخراج مخرج أو وثيقة إلكترونية مزورة بصورة صحيحة مستغلاً مهاراته في الدخول على النظام والقيام بالجرائم الإلكترونية والتلاعب الذي يصعب كشفه بالطرق التقليدية، مما يحتم الاستعانة بأساليب علمية وخبرات فنية ذات فاعلية في إثبات الجريمة الإلكترونية والعمل على تطويرها والاستفادة من فاعليتها في إثبات هذه الجرائم. ومن خلال ذلك يمكن توضيح الأدوات العلمية لضبط إثبات الجريمة على أنها أدوات تقوم بضبط الجريمة كغالبية برامج الحماية، وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وأدوات التنصت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات وأدوات الضبط الأخرى، ويمكن استخدام الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين للمواقع [١].

ثالثاً : أنواع الخبرة في المجال الإلكترونية

١ـ الخبرة الفردية

تعتبر الخبرة الفردية من أهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والانترنت فالمؤسسات الكبرى المتخصصة في هذا المجال تعمل جاهدة على الاستعانة بأشخاص ثبتت كفاءتهم في مجال الحاسب الآلي والانترنت، فهناك من الدول تقوم بمحاولة التعرف على القراصنة الذين تحولوا مع مرور الزمن إلى رموز وطنية من جراء تحركاتهم عبر الشبكة الإلكترونية[٢] .

٢ـ المؤسسات التعليمية

ويمكن مواجهة الجريمة الإلكترونية عن طريق المؤسسات التعليمية والتي تهدف بدورها إلى تطوير العلم والقضاء على المشكلات التي تواجه الإنسانية، حيث يتم تدعيمها مادياً ومعنوياً حتى تكون أفضل سبيل للمواجهة، وأنشأت العديد من المؤسسات التعليمية

---

(١) – محمد علي العريان: الجرائم المعلوماتية ،دار الجامعة الجديدة للنشر، الإسكندرية ، ٢٠٠٤م، ص٤٤ – ٤٥.

(٢) – عمر محمد أبو بكر بن يونس، مرجع سابق، ص١٠٣٥.

منها دراسات الكمبيوتر في جامعة ستانفورد ومعهد التكنولوجيا في ماساشوستس والذي وفَر خبراء على درجة عالية من التفوق[١] .

وآخر نشاط مؤسسي في هذا الإطار هو الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية **FBI** أطلق عليه المعمل الإقليمي الشرعي للحاسوب، وأصبح مقر خبرة عامة متعددة النواحي القضائية هدفه مكافحة التصعيد الخطير في الجرائم الإلكترونية من خلال التصنيف والتحليل للدليل الرقمي، وأهم دور يقوم به هذا المعمل هو التقاء العديد من منظمات الضبط القضائي من أجل التعاون فيما بينها[٢] .

رابعاً : مجالات الخبرة في الجرائم الإلكترونية:

أفرز التطور الهائل في مجال تكنولوجيا المعلومات على العديد من الأنشطة المستحدثة، منها العمليات المصرفية الإلكترونية، والإدارة الإلكترونية والتجارة الإلكترونية، وهو ما أدى إلى تنوع الجرائم التي تقع على هذه العمليات وفقا لنوع الوسائل الإلكترونية المستخدمة في ارتكابها، من بين هذه الجرائم: -الغش أثناء نقل البيانات أو بثها ، التلاعب في البيانات أو في البرامج سواء الأساسية منها أو برامج التطبيقات[٣] .

الأدوات الفنية للنظم الإلكترونية التي يمكن أن تستخدم في ارتكاب الجرائم، وأهمها ما يلي:

عنوان برتوكول الانترنت IP والبريد الإلكتروني وبرامج المحادثة ، ويقصد بعنوان الانترنت المسؤول عن تراسل كم من البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها ويشبه عنوان البريد العادي حيث يسمح للشبكات بنقل الرسالة وهو يوجد بكل جهاز إلكتروني مرتبط بالأنترنت ويتكون من أربعة أجزاء وهي المنطقة الجغرافية، مزود الخدمة، الحاسبات الآلية المرتبطة، والرابع يقوم بتعيين الحاسب الآلي الذي تم الاتصال به[٤] .

---

(١) - خالد ممدوح إبراهيم : فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص٢٩٩ .

(٢) - عمر محمد أبو بكر بن يونس : مرجع سابق، ص١٠٣٧ ، ١٠٣٨ .

(٣) - علي محمود علي حموده : مرجع سابق، ص٣٠.

(٤) -خالد ممدوح إبراهيم : فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص٣٠٤ .

وتقتصر مهمة الخبير على التحقيق في الدعوى وإبداء رأيه في المسائل الفنية التي يصعب على القاضي استنتاجها دون المسائل القانونية[١] .

ويقوم الخبير بتقديم تقريراً موقعاً منه لما توصل إليه من نتائج من بداية إجرائه للخبرة، وغالباً ما يرفق معه الملاحق الإيضاحية سواء كانت مصورة أو مسجلة وغيرها، ويقدم الملف إلى جهة التحقيق أو جهة الحكم[٢].

وعملية حفظ الأدلة الرقمية تتطلب من الخبير التقني حفظ الأدلة من الخبير أن يقوم باستخدام البرمجيات للقيام بحفظ الأدلة الرقمية كما أنه ملزم أن يقوم بعرض الأدلة على المحكمة أو جهات التحقيق[٣].

وتتطلب طبيعة الجريمة الإلكترونية أساليب غير تقليدية في التحقيق لاكتشاف الدليل الرقمي ودعمه من قبل الفنيين المختصين، وذلك يستدعي اتخاذ إجراءات سريعة؛ لأن الدليل الرقمي غير مادي، ويمكن التخلص من أية أدلة أو أثار من قبل مرتكبي الجرائم الإلكترونية، كما تختلف أساليب تلقي البلاغ وإجراء المعاينة والقيام بالتحريات والتفتيش والاستجواب عنها في الجرائم التقليدية نظراً لطبيعة الجرائم الإلكترونية وخصائصها[٤] .

خامساً : مراحل جمع الأدلة الرقمية

إن عملية تجميع الأدلة الرقمية الجنائية في الجرائم الإلكترونية أو الرقمية، تعد من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، لذا كان لزاماً أن يتم اللجوء إلى خبير قضائي معلوماتي، متخصص، لاشتقاق الدليل العلمي الفني الجنائي ، ويرى بعض

---

(١) – محمد حسين منصور : الإثبات التقليدي والإلكتروني ، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م ، ص٢٥٤ .

(٢) – عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري : مرجع سابق، ص ٣٥ ، ٣٦ .

(٣) – عمر محمد أبو بكر بن يونس : مرجع سابق، ص١٠٤٣ ، ١٠٤٤ .

(٤) – عبد الله بن سعود السراني : فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني. رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم المنية، ٢٠٠٩م ،ص ٦٥.

المتخصصين أن عملية تجميع الأدلة الرقمية في الجرائم الرقمية التي تتم عبر الإنترنت تتم عبر ثلاثة مراحل[١]:

المرحلة الأولى:

تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة حيث تتبع الحاسبات الخوادم التي دخل المجرم منها ومحاولة إيجاد أي أثر له.

المرحلة الثانية:

مرحلة المراقبة فهناك فرضية بأن المجرم لابد أن يعود أو يحوم حول مسرح جريمته، وتتعدد طرق مراقبة هذه الحواسيب، ويمكن توضيح هذه الطرق كما يلي:

١ - استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع استخدام أجزاء توضع في الحاسب الآلي لمراقبته.

٢- استخدام كاميرات مراقبة لشاشة الحاسب الآلي معدة للاستخدام التجاري، وأبسط الطرق لمراقبة الحاسب هي الدخول لمكان وجوده وزرع فيروس كمبيوتر أو دودة من نوع الفيروسات.

٣- وهناك وسيلة أخرى وهي حصان طروادة وهذه الوسيلة لها ميزة أنها تستطيع مراقبة أكثر من جهاز واحد.

المرحلة الثالثة:

ضبط الأجهزة المشتبه فيها وفحصها فحصاً فنياً وشرعياً، حيث يبدأ عمل الخبير المعلوماتي في فحص النظام الحاسوبي المشتبه فيه بمكوناته المادية ومكوناته البرمجية، سعياً لاشتقاق الدليل الرقمي لتقديمه لجهة التحقيق أو الحكم، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه، ولتقرير إدانة المتهم، أو تأكيد براءته، ويتم ذلك وفق القواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة المعلوماتية، مع مراعاة القواعد القانونية لمبدأ المشروعية.

---

(١) - محمد أمين البشري : التحقيق في جرائم الحاسب الآلي مؤتمر القانون والحاسب الآلي والانترنت المنعقد في الفترة من : (١ -٣) مايو ٢٠٠٠ م ، الإمارات العربية المتحدة، العين، كلية الشريعة والقانون، ص ٢٤٣.

الخاتمة

النتائج

- هناك مجموعة شروط يجب توافرها لقبول مخرجات الوسائل الإلكترونية كأدلة إثبات في المواد الجنائية، فيجب أن تكون الأدلة يقينية، ويتعين مناقشتها تطبيقاً لمبدأ شفوية المرافعة، ومتحصلة من وسائل الكترونية مشروعة.

وتتسم الجرائم الالكترونية بسهولة إخفائها ودقة وسرعة محو آثرها ، ويتم إثبات الجريمة الإلكترونية بالدليل الرقمي ؛ وهو دليل غير مادي.

تساعد الخبرة الفنية في إثبات الجريمة الإلكترونية، لذا فقد اهتمت القوانين المختلفة بأهمية الاستعانة بالخبراء .

ويوجد اختلاف ملموس في الأدلة لكل من الجرائم التقليدية والجرائم الإلكترونية فالجرائم التقليدية يكون الدليل ظاهراً للعيان ومحسوساً ويمكن كشف، أما الأدلة في الجرائم الإلكترونية ليست بالصورة المذكورة في الجرائم التقليدية.

وتمس الجرائم الإلكترونية بالاقتصاد الوطني والدولي، كما أنها تمس منظومة الأخلاق في المجتمع.

وتأخذ الجرائم الإلكترونية صوراً متعددة، وكل صورة من هذه الصور تثير مشكلات موضوعية وإجرائية.

فاكتشاف الجريمة الإلكترونية وإثباتها أمر يحيط به كثير من الصعاب مما يستلزم الكثير من الجهد والخبرة الفنية .

تعانى الجرائم الإلكترونية بشكل كبير من مشكلة عدم الإبلاغ ، حيث يرتفع الفارق بين الحجم الحقيقي للجريمة وبين ما هو مسجل بالإحصائيات، ويرجع ذلك إلى عدة عوامل أولها يتعلق بالجريمة ذاتها، ثانيها عوامل تتعلق بالمجنى عليهم.

وهناك صعوبات بشأن اكتشاف الجريمة الإلكترونية ، لعدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية كما يمكن ارتكاب هذه الجريمة في دول متعددة.

وتعتبر صعوبة ظهور الدليل المادي من أهم المعوقات التي تواجه إثبات الجريمة الإلكترونية ، حيث تتم الجريمة في وقت قياسي قد يكون جزءاً من الثانية، وهذا يعد من أهم المعوقات التي تواجه إثبات الجريمة الإلكترونية .

قد تكون الجريمة الالكترونية جريمة إلكترونية مستقلة. وقد تكون جريمة تقليدية ، وذلك في ظل ارتباط الناس بالتقنيات الحديثة ، وأهمها الحاسبات الآلية والهواتف الذكية ، وشبكة الإنترنت .

التوصيات

يجب تطوير أساليب التحقيق وإجراءاته بصورة تتلاءم مع خصوصيته ، ولتحقيق ذلك يجب تدريب الكوادر التي تباشر التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية .

ولهذا يجب تدريب مأموري الضبط القضائي على الجرائم الإلكترونية فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة، وكذلك فيما يتعلق بطرق الكشف عنها ، وكيفيه فحصها فنيا والتحفظ عليها، وهذا يتطلب تنمية استعدادهم الخاص وتكوين مهارات فنية تكون على درجة من المعرفة الفنية تتناسب بحجم المتغيرات والتطورات المتلاحقة في مجال الجرائم الإلكترونية مع تطوير أساليب البحث عن الأدلة[1].

ضرورة التحفظ على الأجهزة المشتبه بها في ارتكاب الجريمة الإلكترونية وكذلك تقنيات الاتصال المرتبطة بها التي يشك المحقق في استخدامها في اركان الجريمة الإلكترونية لكي لا يقوم الجاني بتدميرها أو إتلافها .

ضرورة الاهتمام بتطوير دور الخبرة الفنية، لما لها من دور فعال في إثبات الجريمة الإلكترونية، حتى تساعد في سهولة إثبات الجريمة الإلكترونية .

ضرورة إنشاء قاعدة بيانات للجرائم المعلوماتية من حيث أساليبها وأنواعها للرجوع إليها عند اللزوم.

ضرورة التعاون المشترك من قبل سلطات التحقيق مع مزودي خدمة الاتصال وهذا يساعد عملية البحث والتحري عن الجرائم الالكترونية.

أهمية التنسيق المستمر بين الجهات القضائية والأمنية من جهة، والجهات ذات العلاقة بالتكنولوجيا من جهة أخرى لمسايرة ما يستجد في هذا المجال.

ضرورة التعاون الدولي فيما يتعلق بجرائم المعلوماتية من أجل التوفيق بين تبادل المعلومات، وتسليم المجرمين، ومكافحة الجريمة المعلوماتية.

---

(١) – سعيد عبداللطيف حسن : مرجع سابق ، ص١٢٩ .

وضرورة إيجاد الوسائل المناسبة للتعاون الدولي فيما يتعلق بالجرائم الإلكترونية من أجل التوفيق بين التشريعات الخاصة بهذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، وتسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة الإلكترونية .

ضرورة نشر الوعي بين الأشخاص سواء طبيعيين أو معنويين بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات الإلكترونية.

الوقاية من إشكاليات الجرائم الإلكترونية خير من العلاج[1]، **لذلك** من الأفضل لمستخدمي الوسائل الإلكترونية بمختلف أشكالها وصورها أن يحصنوا أجهزتهم وبياناتهم ضد هذه الجرائم وأقترح عدة طرق في ذلك ومنها:

أولا: منع المطاردة في الإنترنت: ويقصد بذلك الامتناع عن كشف المعلومات الشخصية للغرباء مثل رقم الهوية، رقم الضمان الاجتماعي، رقم الحساب البنكي، ورقمه السري.

ثانيا يجب على المستخدم أن يتجنب إرسال أي صور خاصة لا سيما للغرباء لتجنب استخدام هذه الصورة في عمليات الاحتيال أو الابتزاز .

ثالثاً: تحميل واستخدام أحدث البرامج المضادة للفيروسات وتحديثها باستمرار تحسباً للهجمات الفيروسية.

رابعا: الاحتفاظ بنسخ احتياطية للبيانات الموجودة في جهاز المستخدم في وحدات تخزين خارجية، حيث تحفظه من فقدان هذه البيانات نتيجة التعرض لهجوم إلكتروني.

خامساً: الامتناع عن إرسال رقم بطاقة الائتمان الخاصة على أي موقع غير مضمون لحمايتها.

سادساً: ينبغي على أصحاب المواقع مراقبة مواقعهم باستمرار والتحقق من أي مخالفات، وتثبيت برامج تكشف الحركات غير الطبيعية والمشبوهة.

" في النهاية آخر دعوانا أن الحمد لله رب العالمين "

---

(١) – عبدالله دغش العجمي: مرجع سابق ، ص ١١٨ .

قائمة المراجع

أولاً : مراجع باللغة العربية

الكتب

- إبراهيم حامد مرسي طنطاوي: سلطات مأمور الضبط الجنائي. دار النهضة العربية ، ١٩٩٧م .
- أبو العلا علي أبو العلا : الإثبات الجنائي، دراسة تحليلية لموطن القوة والضعف في الدليل الجنائي، دار النهضة العربية .
- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، القاهرة، دار النهضة العربية ، سنة٢٠٠٠م .
- أحمد عوض بلال: الآثم الجنائي، القاهرة، دار النهضة العربية، سنة٢٠٠٣م .
- إدوارد غالي الدهبي : مجموعة بحوث قانونية، المسئولية الجنائية للأشخاص الاعتباريين، الطبعة الأولى، دار النهضة العربية، ١٩٧٨م .
- جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالأنترنت ، دار النهضة ، ٢٠٠١م .
- خالد عياد الحلبي : إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط ١ ، دار الثقافة للنشر والو توزيع، عمان، الأردن ، ٢٠١١م .
- خالد ممدوح على إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي الإسكندرية ، ٢٠١٠م .
- زين الدين بلال أمين: جرائم نظم المعالجة الآلية للبيانات، ط ١ . الإسكندرية: دار الفكر الجامعي، ٢٠٠٨م .
- سليمان احمد محمد فضل : المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الإنترنت، دار النهضة للنشر .
- سعيد عبد اللطيف حسن: إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت: الجرائم الواقعة في جرائم تكنولوجيا المعلومات ، دار النهضة ،١٩٩٩ م .
- سمير حجازي : التهديدات الإجرامية للتجارة الالكترونية دبي ، مركز البحوث والدراسات بإدارة شرطة دبي ١٩٩٩م .

- عادل سقف الحيط : جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية دراسة قانونية مقارنة، ط١ ، عمان ، دار الثقافة للنشر والتوزيع ، ٢٠١١م .
- عادل يوسف عبد النبي الشكري: الجريمة المعلوماتية وأزمة الشرعية الجزائية ، كلية القانون، جامعة الكوفة، ٢٠٠٨ م .
- عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت دراسة متعمقة في جرائم الحاسب الآلي والانترنت ، دار الكتب القانونية ، مصر ، ٢٠٠٥م .
- عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، ط١، الإسكندرية ، دار الفكر الجامعي ،٢٠٠٧م .
- عبد الله بن سعود السراني : فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني. رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم المنية، ٢٠٠٩م .
- عبد الله بن عبد العزيز اليوسف : الظواهر الإجرامية المستحدثة وسبل مواجهتها الرياض جامعة نايف العربية للعلوم الأمنية، ١٩٩٩م .
- عبدالله حسين على محمود: "سرقة المعلومات المخزنة على الحاسب الآلي ، دار النهضة العربية ، ٢٠٠٤م .
- عبدالله دغش العجمي : المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة ، رسالة ماجستير ، جامعة الشرق الأوسط ، ٢٠١٤م .
- عفيفي كامل عفيفي: جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط٢ منشورات الحلبي الحقوقية، بيروت- لبنان، ٢٠٠٧م .
- على ذكى العرابي: "المبادئ الأساسية للتحقيقات والإجراءات الجنائية"، مطبعة لجنة التأليف والترجمة والنشر، القاهرة، ١٩٤٥م .
- عمر السعيد رمضان : مبادئ قانون الإجراءات الجنائية القاهرة، دار النهضة العربية، المجلد الأول،١٩٩٠م .
- فتوح الشاذلي : عفيفي كامل عفيفي : جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. بيروت، منشورات الحلبي الحقوقية،٢٠٠٣م .

- كامل السعيد: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات دراسات جنائية معمقة في القانون والفقه والقضاء المقارن، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٢م .
- محمد ابراهيم زيد : تنظيم الاجراءات الجزائية في التشريعات العريقة جـ٢،الرياض،المركز العربي للدراسات الامنيه،سنة١٩٩٠م .
- محمد حسين منصور : الإثبات التقليدي والإلكتروني ، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م .
- محمد حماد الهيتي: التكنولوجيا الحديثة والقانون الجنائي، عمان، دار الثقافة للنشر والتوزيع،٢٠٠٤م .
- محمد دباس الحميد ، ماركو إبراهيم ونينو: حماية أنظمة المعلومات عمان، دار الحامد للنشر والتوزيع .
- محمد ذكى أبو عامر: الإجراءات الجنائية ، منشأة المعارف ، الاسكندرية، ١٩٩٤ م .

- محمد سامي الشواء: ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، القاهرة.

- محمد علي العريان : الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر ، الإسكندرية ، ٢٠٠٤م .
- حمد موسى مصطفى : دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، ٢٠٠٥م .
- محمود عبد الله حسين : سرقة المعلومات المخزنة في الحاسب الألي القاهرة، دار النهض العربية، الطبعة الثانية ، ٢٠٠٢م .

- محمود نجيب حسني: شرح قانون الإجراءات الجنائية القاهرة، دار النهضة العربية، الطبعة الثانية،١٩٨٨م .
- مصطفى سليمان أبكر: جرائم الحاسوب وأساليب مواجهتها مجلة الأمن والحياة، العدد ٢١٠، ١٤٢٠هـ السنة١٩ .

- مدني عبد الرحمن تاج الدين : أصول التحقيق الجنائي وتطبيقاتها في المملكة العربية السعودية، الرياض، معهد الإدارة العامة، ٢٠٠٤م .

- مصطفى محمد موسى: أساليب إجرامية للتقنية الرقمية: ماهيتها مكافحتها، القاهرة، دار النهضة العربية ، ٢٠٠٣م .

- ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، ط ١ ، دار الكتب القانونية، مصر،٢٠٠٦م .

- معن احمد الحياري : الركن المادي للجريمة، ط١ . لبنان : منشورات الحلبي ٢٠١٠م .

- ناصر محمد البقمي : مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، أبو ظبي ، مركز الإمارات للدراسات والبحوث الاستراتيجية ، ٢٠٠٨م . جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، ط ١ : السعودية: مطابع الحميضي ٢٠٠٩م-١٤٣٠ هـ .

- نبيلة هبه هروال : الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، ط . د دار الفكر الجامعي الإسكندرية .

- هلالي عبد اللاه أحمد : تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، الطبعة الأولى، سنة ١٩٩٧م.

- **رسائل دكتوراة**

- أحمد ضياء الدين محمد خليل: مشروعية الدليل في المواد الجنائية ، رسالة دكتوراة ، جامعة عين شمس ، ١٩٨٢م .

- عمر محمد أبو بكر بن يونس: عمر محمد أبو بكر بن يونس : الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٤ م .

- **رسائل ماجستير**

- ثنيان ناصر آل ثنيان : إثبات الجريمة الإلكترونية ، رسالة ماجستير مقدمة كلية الدراسات العليا قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، عام ١٤٣٣هـ - ٢٠١٢م .

- سيدي محمد لبشير: دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية-، رسالة ماجستير في العلوم الشرطية تخصص التحقيق و البحث الجنائي، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية، الرياض، ، ٢٠١٠م .

• صالح بن سعد المقبل : بناء نموذج لمهارات التحقيق الاستدلالي في جرائم الابتزاز الالكتروني. ، رسالة ماجستير منشورة ، جامعة نايف العربية للعلوم الأمنية الرياض السعودية ٢٠١٥م .

- قارة أمال : الجريمة المعلوماتية، رسالة لنيل الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، بن عكنون ، ٢٠٠٢م .

• محمد بن نصير السرحاني: مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت ، رسالة ماجستير ، مقدمة بجامعة نايف العربية للعلوم الأمنية ، كلية الدراسات العليا ، قسم العلوم الشرطية ، سنة ١٤٢٥هـ ، ٢٠٠٤م .

• يوسف صغير: الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير منشورة ، جامعة مولود معمري- كلية تيزي وزو ، الجزائر ، ٢٠١٣ م .

• **مجلات ومؤتمرات**

• أحمد عبد الحكيم عبد الرحمن شهاب : شروط قبول الأدلة الالكترونية أمام القضاء الجنائي الفلسطيني ، مجلة العلوم السياسية والقانون-العدد ٧٠ فبراير٢٠١٨ المجلد ٢ ، تصدر عن المركز الديمقراطي العربي ألمانيا- برلين .

• إسماعيل عبد النبي شاهين: أمن المعلومات في الانترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من (١ - ٢) مايو ٢٠٠٠، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون ٢٠٠٠م .

• الأزرق عبد الله: مؤتمر البيئة المعلوماتية الأمنة الرياض جمعية المكتبات والمعلومات السعودية، ،٢٠١٠م .

• جودة حسين محمد جهاد: المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية، دراسة مقارنة، مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة من ١ - ٢ مايو ٢٠٠٠م، بدولة الإمارات العربية المتحدة، كلية الشريعة والقانون .

• عبد الناصر محمد محمود فرغلي : محمد عبيد سيف سعيد المسماري: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف العربية للعلوم الأمنية، الرياض، ،٢٠٠٧م .

- علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسوب. مجلة الحقوق للبحوث القانونية الاقتصادية، مصر . العدد الأول ١٩٩٢م .
- علي محمود حمودة :الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث منشور ضمن أبحاث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية مركز البحوث والدراسات أكاديمية شرطة دبي محور القانون الجنائي في الفترة من ٢٦ – ٢٨ أبريل ٢٠٠٣م .
- محمد الأمين البشري : التحقيق في جرائم الحاسب والإنترنت. المجلة العربية للدراسات العربية والتدريب العدد ٣٠ ، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ٢٠٠١م .
- محمد عبيد سيف سعيد المسماري والخبير ،عبد الناصر محمد محمود فرغلي: "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة"، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، ١٢-١٤/ ١١/ ٢٠٠٧ م .
- _ محمد محيى الدين عوض، مشكلات السياسة الجنائية المعاصرة فى جرائم نظم المعلومات (الكمبيوتر)، قسم الجرائم الواقعة في مجال تكنولوجيا المعلومات، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، من ٢٥ :٢٨ أكتوبر سنة ١٩٩٣م .
- مصعب القطانة : الإجراءات الجزائية الخاصة في الجرائم المعلوماتية ، بحث ص ٧ ، مقدم في عبدالله دغش العجمي : المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة ، رسالة ماجستير ، جامعة الشرق الأوسط ، ٢٠١٤م .
- هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، سنة ١٩٩٢م الجوانب الإجرامية للجوانب المعلوماتية مجلة الأمن والقانون، العدد الثاني، شرطة دبي ، ١٩٩٤م .

معاجم وقواميس

- الشربيني الخطيب: مغني المحتاج إلى معرفة معاني ألفاظ المنهاج بيروت، دار العلم للملايين ١٤٢٥هـ المجلد الرابع .

ثانياً : مراجع باللغة الأجنبية

- Albert J. Marcella Robert s. Greenfield, Cyber forensics a Field Manual for collecting, Examining, and preserving evidence of Computer crime, CRC Press, USA, 2001
- Andrea Campbell. Making Crime Pay: The Writer's Guide to Criminal Law. 2002.
- Bruce Middleton, cybercrime investigation field guid, Op-Cit .
- David Johnston&Sunny Handa, Cyber Law – second edition, Stoddart Publishing, New York, U.S.A., 1997
- Eoghan Casy: Digital Evidence forensics Science computer and the internet computer crime, Academic Press, USA, 2003.
- Henry,J.F, "Testimony befor permanent Subcommmittee On Governmental Affairs, The United States Senate, Ninety Ninth congress, 1984.
- Jody R. and Westby. Project Chair & Editor, international Guide to Combating Cybercrime, defending liberty pursuing Justice, USA,2003
- Marjie T. and Britz, PHD: computer Forensics and Cyper crime an introduction, pearson prentice Hall, USA,2003.
- Mohens Chlager (MOnfred) " Computer Crim and other crimes Against information Technology in Germany " R.I.D.P.1993.
- Urich sieber, the international handbook on computer crime, UK, 1986, John Wiley & Sons Ltd .

References:

alkutub

• 'iibrahim hamid mursi tantawi: sulutat mamur aldabt aljanayiy. dar alnahdat alearabiat , 1997m .

• 'abu aleula eali 'abu aleala : al'iithbat aljanayiyu, dirasat tahliliat limawtin alquat walduef fi aldalil aljanayiy, dar alnahdat alearabia .

• 'ahmad husam tah tamamu, aljarayim alnaashiat ean aistikhdam alhasib alaly, alqahirata, dar alnahdat alearabiat , sunati2000m .

• 'ahmad eawad bilali: alatham aljanayiy, alqahirata, dar alnahdat alearabiati, sanatu2003m .

• 'iidward ghali aldahbi : majmueat buhuth qanuniatin, almasyuwliat aljinayiyat lil'ashkhas aliaetibariiyna, altabeat al'uwlaa, dar alnahdat alearabiati, 1978m .

• jamil eabd albaqi alsaghir: aljawanib al'iijrayiyat liljarayim almutaealiqat bial'antirnit , dar alnahdat , 2001m .

• khalid eayaad alhalabi : 'iijra'at altahariy waltahqiq fi jarayim alhasub walaintirnti, t 1 , dar althaqafat lilnashr walw tawzie, eaman, al'urduni , 2011m .

• khalid mamduh ealaa 'iibrahim: fanu altahqiq aljinayiyi fi aljarayim al'iilikturuniati, dar alfikr aljamieii al'iiskandariat , 2010m .

• zayn aldiyn bilal 'amin: jarayim nazam almuealajat alaliat lilbayanati, t 1. al'iiskandiriatu: dar alfikr aljamieii, 2008m .

• sulayman aihmad muhamad fadl : almuajahat altashrieiat wal'amniat liljarayim alnaashiat ean aistikhdam shabakat almaelumat alduwaliat al'iintirnti, dar alnahdat lilnashr .

• saeid eabd allatif hasan: 'iithbat jarayim alkumbiutar waljarayim almurtakabat eabr alantirnti: aljarayim alwaqieat fi jarayim tiknulujia almaelumat , dar alnahdat ,1999 m .

• smir hijazi : altahdidat al'iijramiat liltijarat alalkitruniat dubay , markaz albuhuth waldirasat bi'iidarat shurtat dubay 1999m .

• eadil saqf alhayt : jarayim aldhami walqadh waltahqir almurtakabat eabr alwasayit alalkutruniat dirasat qanuniat muqaranati, ta1 , eamaan , dar althaqafat lilnashr waltawzie , 2011m .

• eadil yusif eabd alnabii alshukri: aljarimat almaelumatiat wa'azmat alshareiat aljazayiyat , kuliyat alqanuni, jamieat alkufati, 2008 m .

• eabd alfataah biumi hijazi: aldalil aljinayiyi waltazwir fi jarayim alkumbiutir walantirnit dirasat mutaeamiqat fi jarayim alhasib alali walantirnit , dar alkutub alqanuniat , misr , 2005m .
• eabd alfataah biumi hijazi: mabadi al'iijra'at aljinayiyat fi jarayim alkumbuyutir walantirnit , ta1, al'iiskandariat , dar alfikr aljamieii ,2007m .
• eabd allah bin sueud alsaraaniu : faeiliat al'asalib almustakhdamat fi 'iithbat jarimat altazwir alalkitruni. risalat majistir, alriyad, jamieat nayif alearabiat lileulum almaniati, 2009m .
• eabd allah bin eabd aleaziz alyusif : alzawahir al'iijramiat almustahdathat wasubul muajahatiha alriyad jamieat nayif alearabiat lileulum al'amniati, 1999m .
• eabdallah husayn ealaa mahmud: "sariqat almaelumat almukhazanat ealaa alhasib alali , dar alnahdat alearabiat , 2004m .
• eabdallah dughsh aleajami : almushkilat aleamaliat walqanuniat liljarayim al'iiliktruniat dirasat muqaranat , risalat majistir , jamieat alsharq al'awsat , 2014m .
• efifi kamil eafifi: jarayim alkumbiutar, wahuquq almualif walmusanafat alfaniyat wadawr alshurtat walqanuni, dirasat muqaranati, ta2 manshurat alhalabii alhuquqiati, bayrut- lubnan, 2007m .
• ealaa dhakaa alearabi: "almabadi al'asasiat liltahqiqat wal'iijra'at aljinayiyati", matbaeat lajnat altaalif waltarjamat walnashri, alqahirati, 1945m .
• eumar alsaeid ramadan : mabadi qanun al'iijra'at aljinayiyat alqahirati, dar alnahdat alearabiati, almujalad al'uwli,1990m .
• futuh alshaadhli : eafifi kamil eafifi : jarayim alkumbuyutar wahuquq almualif walmusanafat alfaniyat wadawr alshurtat walqanuni. bayrut, manshurat alhalabii alhuquqiati,2003m .
• kamil alsaeid: jarayim alkumbiutar waljarayim al'ukhraa fi majal tiknulujia almaelumat dirasat jinayiyat mueamaqat fi alqanun walfiqh walqada' almuqarani, dar althaqafat lilnashr waltawziei, eaman, 2002m .
• muhamad abrahim zayd : tanzim alajira'at aljazayiyat fi altashrieat aleariqat ji2,alrryad,almarkaz alearabiu lildirasat alamnihi,sinat1990m .
• muhamad husayn mansur : al'iithbat altaqlidiu wal'iiliktruniu , dar alfikr aljamieii, al'iiskandariati, ,2006m .

• muhamad hamaad alhiti: altiknulujya alhadithat walqanun aljanayiyi, eaman, dar althaqafat lilnashr waltawziei,2004m .
• muhamad dabaas alhumid , marku 'iibrahim waninu: himayat 'anzimat almaelumat eaman, dar alhamid lilnashr waltawzie .
• muhamad dhakaa 'abu eamir: al'iijra'at aljinayiyat , munsha'at almaearif , alaiskandiriati, 1994 m . - muhamad sami alshawa': , thawrat almaelumat waineikasatuha ealaa qanun aleuqubat , dar alnahdat alearabiat , alqahiratu.
• muhamad eali aleuryan : aljarayim almaelumatiat , dar aljamieat aljadidat lilnashr , al'iiskandariat , 2004m .
• hamd musaa mustafaa : dalil altahariy eabr shabakat al'iintirnti, dar alkutub alqanuniati, masr, 2005m .
• mahmud eabd allah husayn : sariqat almaelumat almukhzanat fi alhasib al'alii alqahirati, dar alnahd alearabiati, altabeat althaaniat , 2002m . - mahmud najib hasni: sharh qanun al'iijra'at aljinayiyat alqahirati, dar alnahdat alearabiati, altabeat althaaniatu,1988m .
• mistafaa sulayman 'abakr: jarayim alhasub wa'asalib muajahatiha majalat al'amn walhayati, aleadad 210, 1420h alsanatu19 .
• midani eabd alrahman taj aldiyn : 'usul altahqiq aljinayiyi watatbiqatuha fi almamlakat alearabiat alsaeudiati, alrayad, maehad al'iidarat aleamati, 2004m . - mistafaa muhamad musaa: 'asalib 'iijramiat liltiqniat alraqamiati: mahiatuha mukafahataha, alqahirata, dar alnahdat alearabiat , 2003m .
• mamduh eabd alhamid eabd almutalab: albahth waltahqiq aljinayiyu alraqamiu fi jarayim alkumbuyutir walantirnti, t 1 , dar alkutub alqanuniati, masr,2006m .
• maean aihmad alhayaari : alrukn almadiyu liljarimati, ta1. lubnan : manshurat alhalabi 2010m .
• nasir muhamad albaqami : mukafahat aljarayim almaelumatiat watatbiqatuha fi dual majlis altaeawun lidual alkhalij alearabiati, 'abu zabi , markaz al'iimarat lildirasat walbuhuth alastiratijiat , 2008m . jarayim almaelumatiat wamukafahatiha fi almamlakat alearabiat alsaeudiati, t 1: alsaeudiati: matabie alhumaydi 2009m-1430 hu .
• nabilat habah hirwal : aljawanib al'iijrayiyat lijarayim alaintirnit fi marhalat jame alastidlalati, t . d dar alfukar aljaamieii al'iiskandaria .

• halali eabd allaah 'ahmad : taftish nuzam alhasib wadamanat almutaham almaelumati, altabeat al'uwlaa, sanatan 1997m.

rasayil dukturaa

• 'ahmad dia' aldiyn muhamad khalil: mashrueiat aldalil fi almawadi aljinayiyat , risalat dukturat , jamieat eayn shams , 1982m .

• eumar muhamad 'abu bakr bin yunus: eumar muhamad 'abu bakr bin yunis : aljarayim alnaashiat ean aistikhdam alaintirnti, risalat aldukturahi, kuliyat alhuquqi, jamieat eayn shams, 2004 m .

rasayil majistir

• thnyan nasir al thanyan : 'iithbat aljarimat al'iiliktruniat , risalat majistir muqadimat kuliyat aldirasat aleulya qism aleadalat aljinayiyat , jamieat nayif alearabiat lileulum al'amniat , eam 1433h - 2012m .

• sidi muhamad libashir: dawr aldalil alraqamii fi 'iithbat aljarayim almaelumatiati, dirasat tahliliat tatbiqiatun-, risalat majistir fi aleulum alshurtiat tukhasis altahqiq w albahth aljinayiy, kuliyat aldirasat alealia , jamieat naayif alearubiat lilealum al'amniti, alriyad, , 2010m .

• salih bin saed almuqbil : bina' namudhaj limaharat altahqiq alaistidlalii fi jarayim alaibtizaz alalkitruni. , risalat majistir manshurat , jamieat nayif alearabiat lileulum al'amniat alriyad alsaeudiat 2015m . - qarat 'amal : aljarimat almaelumatiatu, risalat linayl almajistir fi alqanun aljinayiyi waleulum aljinayiyati, kuliyat alhuquqi, jamieat aljazayar, bin eaknun , 2002m .

• muhamad bin nusayr alsarhani: maharat altahqiq aljinayiyu alfaniyu fi jarayim alhasub wal'iintirnit , risalat majistir , muqadimat bijamieat nayif alearabiat lileulum al'amniat , kuliyat aldirasat aleulya , qism aleulum alshurtiat , sanat 1425h , 2004m .

• yusif saghir: aljarimat almurtakibat eabr alaintirnit , risalat majistir manshurat , jamieat mawlud maemari- kuliyat tizi wuzu , aljazayir , 2013 m .

majalaat wamutamarat

• 'ahmad eabd alhakim eabd alrahman shihab : shurut qabul al'adilat alalkutruniat 'amam alqada' aljinayiyi alfilastinii , majalat aleulum alsiyasiat walqanunu-aleadad 70 fibrayir2018 almujalad 2 , tasadar ean almarkaz aldiymuqratii alearabii 'almania- barlin .

• 'iismaeil eabd alnabi shahin: 'amn almaelumat fi alaintirnit bayn alsharieat walqanuni, mutamar alqanun walkumbuyutir walaintirnit almuneaqad fi alfatrat min (1 - 2) mayu 2000, bidawlat al'iimarat alearabiat almutahidati, kuliyat alsharieat walqanun 2000m .
• al'azraq eabd allah: mutamar albiyat almaelumatiat al'uminat alriyad jameiat almaktabat walmaelumat alsueudiati, ,2010m .
• judat husayn muhamad jihad: almuajahat altashrieiat liljarimat almunazamat bial'asalib altaqniati, dirasat muqaranati, mutamar alqanun walkumbuyutir walaintirnit almuneaqad fi alfatrat min 1 - 2 mayu 2000m, bidawlat al'iimarat alearabiat almutahidati, kuliyat alsharieat walqanun .
• eabd alnaasir muhamad mahmud firghali : muhamad eubayd sayf saeid almismari: al'iithbat aljinayiyu bial'adilat alraqamiat min alnaahiatayn alqanuniat walfaniyati", dirasat tatbiqiat muqaranati, almutamar alearabii al'awal lieulum al'adilat aljinayiyat waltibi alshareii jamieat nayif alearabiat lileulum al'amniat, alrayad, ,2007m .
• eali eabd alqadir alqahwaji: alhimayat aljinayiyat libaramij alhasuba. majalat alhuquq lilbuhuth alqanuniat alaiqtisadiati, misr . aleadad al'awal 1992m .
• eali mahmud hamuwdat :al'adilat almutahasilat min alwasayil alalkitruniat fi 'iitar nazariat al'iithbat aljinayiyi, bahath manshur dimn 'abhath almutamar aleilmii al'awal hawl aljawanib alqanuniat wal'amniat lileamaliaat alalkitruniat markaz albuhuth waldirasat 'akadimiat shurtat dubay mihwar alqanun aljinayiyi fi alfatrat min 26 - 28 'abril 2003m .
• muhamad al'amin albashariu : altahqiq fi jarayim alhasib wal'iintirnti. almajalat alearabiat lildirasat alearabiat waltadrib aleadad 30 , alrayad, 'akadimiat nayif alearabiat lileulum al'amniati, 2001m .
• muhamad eubayd sayf saeid almismari walkhabir ,eabd alnaasir muhamad mahmud firighili: "al'iithbat aljinayiyi bial'adilat alraqamiat min alnaahiatayn alqanuniat walfaniyati, dirasat tatbiqiat muqaranati", almutamar alearabii al'awal lieulum al'adilat aljinayiyat waltibi alshareii, 12-14/11/ 2007 m .
• _ muhamad mahyaa aldiyn eawada, mushkilat alsiyasat aljinayiyat almueasirat faa jarayim nazam almaelumat (alkumbiutar), qism aljarayim alwaqieat fi majal tiknulujia

almaelumati, bahath muqadim lilmutamar alsaadis liljameiat almisriat lilqanun aljinayiy, alqahirat, min 25 :28 'uktubar sanat 1993m .

• maseab alqitaanat : al'iijra'at aljazayiyat alkhasat fi aljarayim almaelumatiat , bahth s 7 , muqadim fi eabdallah dughsh aleajami : almushkilat aleamaliat walqanuniat liljarayim al'iiliktruniat dirasat muqaranat , risalat majistir , jamieat alsharq al'awsat , 2014m .

• hisham muhamad farid rustum: qanun aleuqubat wamakhatir tiqniat almaelumati, sanatan 1992m aljawanib al'iijramiat liljawanib almaelumatiat majalat al'amn walqanunu, aleadad althaani, shurtat dubay , 1994m .

maeajim waqawamis

• alshirbini alkhatib: mughaniy almuhtaj 'iilaa maerifat maeani 'alfaz alminhaj bayrut, dar aleilm lilmalayin 1425hi almujalad alraabie .

فهـــــرس الموضوعـــــات