الـمــقـدمــة:

مع بداية أنتشار شبكة الإنترنت لم يكن هناك قلق تجاه الجرائم التي يمكن أن ترتكب على الشبكة، وذلك نظرا لمحدودية استخدامها حيث كانت قاصرة على البحث العلمي فقط ، علاوة على كونها مقصورة على فئة معينة من المستخدمين والباحثين والعلماء وطلبة الجامعة لاكن مع بزوغ فجر الثورة المعلوماتية وتوسع استخدام شبكات الإنترنت وبدء استخدمها في المعاملات ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة ازدادت مع الوقت وتعددت صورها واشكالها، وهذه الجرائم يطلق عليها الجرائم المعلوماتية ، أي تلك الأعمال والأفعال المجرمة التي تتم عن طريق الإنترنت، وهي من أهم واخطر التحديات التي تواجه المعاملات الإلكترونية[١].

أولا: تعريف الجرائم المعلوماتية :

من خلال ما سبق يمكن تعريف الجريمة المعلوماتية بأنها نشاط غير مشروع موجه للنسخ او التغير او حذف او الوصول إلى المعلومات المخزنة داخل الحاسوب والتي تحول عن طريقه[٢] ، وتعرف كذلك بأنها نشاط جنائي يمثل اعتداء على برامج الحاسوب[٣].

تعتبر جرائم نظم المعلومات ظاهرة مستحدثة في مجال الجريمة ، يبذل بشأن مكافحتها جهود دولية وإقليمية لما لها من تأثير كبير على المصلحة الاجتماعية والاقتصادية والسياسية في أي دولة ، وهذا الامر يقتضي البحث في سبل حماية نظم المعلومات، ولاسيما ان هذي التكنولوجيا قد ربطت العالم برابط واحد من خلال شبكة المعلومات الدولية ، ومن ثم يكون الفعل المشروع الذي لا يجرم في دولة بشكل سلبي على الحماية المقررة من قبل الدول الأخرى [٤].

---

[١] خالد ممدوح أبراهيم: م س ص ٥.

[٢] محمد حماد مرهج الهيتي :" جرائم الحاسوب ماهيتها وموضوعها واهم صورها دراسة تحليلية " كلية الحقوق، جامعه الانبار ، دار المناهج للنشر والطباعة ط أولى س ط ٢٠٠٦ ص ٨٤.

[٣] "أعمال المؤتمر الدولي الرابع عشر الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري "، طرابلس الفترة من ٢٤-٢٥-٢٠١٧ ص ٤.

[٤] أيمن عبد الله فكري:" جرائم نظم المعلومات دراسة مقارنة" دار الجامعة الجديدة للنشر ، ط، س ط ، ٢٠١٧ ص ٩.

تظم الجريمة المعلوماتية اشكالا متعددة ومتنوعة يصعب حصرها وقد طرا عليها تطورا ملحوظا في اساليبها تشمل صناعة ونشر الفيروسات، ولاختراعات، وانتحال الشخصية، والمضايقة ، والملاحقة، التشهير وتشوية السمعة صناعة ونشر الإباحية ، وجرائم النصب والاحتيال وغيرها من الأفعال الاجرامية حيث ان هذه الأنماط لا تعد هي الاشكال الوحيدة للجريمة عبر الانترنت، ذلك بسبب تقدم وسائل الاتصالات والمعلومات وانتشار استعمال الكمبيوتر وسهولة استخدام الانترنت الامر الذي أدى الى ظهور نوع جديد من الجرائم أصبحت معه نصوص قانون العقوبات ولإجراءات الجنائية التقليدية عاجزة عن مواجهتها او التصدي لها [٥].

تتمثل اركان الجريمة المعلوماتية مثل الجريمة العادية في الركن الشرعي أي على تجريم الفعل المرتكب من قانون العقوبات اليمني "لا جريمة ولا عقوبة الا بنص" والركن المادي المتمثل في السلوك الاجرامي والنتيجة والعلاقة السببية بينهما، والركن المعنوي للجريمة المعلوماتية الذي يتكون من عنصرين هما العلم والإرادة[٦].

تختلف الجريمة الالكترونية عن الجريمة التقليدية من حيث خصائصها ، فالجريمة الالكترونية لم تظهر الا في عصر الحاسوب، كون هذه الجريمة حديثة ومتطورة فأن لها خصائص منفردة تتميز بها عن غيرها من الجرائم التقليدية[٧] ومن اهم هذه الخصائص ما يلي:

١. يتطلب لارتكابها وجود جهاز الكتروني ومعرفة بتقنية المعلومات.
٢. موضوع الاعتداء هو من معطيات الجهاز الالكتروني.
٣. الجريمة الالكترونية عابرة للحدود.
٤. الجريمة الالكترونية صعبة الاكتشاف والاثبات[٨].
٥. سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول اليه.
٦. نقص الخبرة لدى الأجهزة الأمنية والقضائية وعدم كفاية القوانين السارية[٩].

---

[٥] خالد ممدوح إبراهيم : م س ص ٦.
[٦] "أعمال المؤتمر الدولي الرابع عشر" م س ص ٥.
[٧] يوسف خليل العفيفي: "الجرائم الالكترونية في المشاريع الفلسطيني دراسة مقارنة " مذكره للحصول في القانون الدولي من كلية الشريعة والقانون بالجامعة الاسلامية بغزة العام الجامعي ٢٠١٣ ص .
[٨] نفس: م س ص٢٢.

ثالثا: أهمية البحث:

تتجلى أهمية موضوع الجرائم المعلوماتية في حداثته وانتشار الجرائم المعلوماتية في الوقت الراهن ، كما انه يعتبر من الموضوعات الي اثارت جدلا فقهيا لدى فقهاء القانون الجنائي، إضافة الى تعلق هذا الموضوع بالوسائل الحديثة حيث انه كلما تطورت الوسائل الالكترونية كلما تطور اسلوب ارتكاب هذا النوع من الجرائم ، وهذا ما شكل عائق امام القائمين بأثبات الجرائم المعلوماتية حيث ان قواعد البحث والتحقيق واسس الاثبات الجنائي في القوانين التقليدية لا تكفي بل يحتاج هذا النوع من الجرائم الى استحداث تشريعات جديدة تتلائم مع طبيعته الفنية ، تكمن أيضا أهمية الموضوع في ان العلم قد أحدث الكثير من وسائل الاثبات من بينها الدليل الرقمي الذي يطرح مسألة تقديره امام القاضي الجنائي وتأثيره في اثبات الجرائم المعلوماتية خصوصا مع تضاؤل دور القاضي الجنائي امام طبيعة هذه الجرائم لكونها تحتاج دائما الى خبير معلوماتي باعتبارها مسائل فنية بحتة.

ثالثا: اهداف البحث:

١. تحديد طرق الوصول إلى ادلة الاثبات الجنائية في الجرائم المعلوماتية وكيفية استخلاصها.
٢. تقديم رؤية خاصة بشأن التحقيق الجنائي في هذي الجرائم حيث ان مسرح الجريمة الرقمي هو مسرح افتراضي غير مرئي.
٣. بيان الصعوبات التي تواجه عملية التحقيق الجنائي.
٤. التعريف بالدليل الرقمي وتحديد ماهيته حيث يعتبر من اهم ادلة الاثبات في الجرائم المعلوماتية.

---

[٩] صغير يوسف:" الجريمة المرتكبة عبر الانترنت " مذكرة للحصول على شهادة الماجستير الدولي في جامعة مولد معمري – تيزي وزو الجزائر لسنة ٢٠١٣ ص ١٨-١٩.

رابعا : منهج البحث:

سيتم اتباع الأسلوب العلمي المنهجي القائم على الوصف والتحليل الذي يقوم على وصف هذه الظاهرة وتحليل هذه المواد التي تناولتها ، لابد من الدراسة تهتم بسبل كشف وضبط ادلة الاثبات الجنائية في الجرائم المعلوماتية من الناحية الفنية والقانونية وعلى وجه التحديد بالدليل الرقمي من خلال تعريفة وتباين تقسيماته وخصائصه وانواعه وامثلته مع توضيح محل الدليل الرقمي وتعدد مراحلة ومدى قبوله امام القضاء الجزائي.

خامسا: إشكالية البحث:

باعتبار ان صعوبة كشف وضبط الدليل الرقمي المستخلص من الجرائم المعلوماتية وما يصاحب الحصول علية من خطوات معقدة واتساع مسرح هذه الجريمة الذي يتخطى غالبا حدود الدولة الواحدة وعدم ملاءمة القوانين والأنظمة أحيانا لبعض القضايا المطروحة في هذا المجال ، نظرا لما قد يثيره قبول الدليل الرقمي من مشكلات في الاثبات كدليل جنائي .

ذلك ان مستودع هذي الأدلة هو الوسائل الالكترونية التي يمكن التلاعب فيها وتغيرها عن الحقيقة التي يجب ان تعبر عنها ومن خلال هذي الدراسة نسع للإجابة عن التساؤلات الاتية:

هل تكفي القواعد الإجرائية المقررة لأثبات الجرائم التقليدية لكي تسري الجرائم المعلوماتية؟

كيف يتم استخلاص الدليل الرقمي ماهي الصعوبات والمعوقات التي تواجه جهات البحث والتحري في استخلاص الدليل الرقمي؟

حتى نتمكن من معالجة الإشكالية المطروحة قمنا بتقسيم الخطة الى مبحثين وهي كالاتي:

المبحث الأول: سنتناول طرق الحصول على ادلة البحث الجنائي في الجرائم المعلوماتية والذي ادرجناه في مطلبين :

- المطلب الأول: المعاينة والتفتيش.
- والمطلب الثاني: الضبط والخبرة القضائية.

المبحث الثاني: سنتناول استنباط الدليل الرقمي وادرجناه في مطلبين:

- المطلب الأول: مفهوم الدليل الرقمي ومشروعية.
- والمطلب الثاني : مشاكل الاثبات بالدليل الرقمي.

المبحث الأول: طرق الحصول على ادلة الأثبات الجنائي في الجرائم المعلوماتية:

تعد الجريمة المعلوماتية كغيرها من الجرائم لها أركانها وعناصرها، وتسير بها الدعوى في الجرائم التقليدية[١٠] ، تهدف إجراءات التحقيق في هذه الجرائم الى جمع وفحص الأدلة الالكترونية القائمة على وقوع الجريمة ونسبتها الى فاعلها ، وتتمثل هذه الإجراءات كما بينها القانون من المعاينة والتفتيش والخبرة القضائية والضبط وسماع الشهود ومراقبة المحادثات وتسجيلها والاستجواب والمواجهة والاعتراف الا ان بعض هذه الاجراءات لها دور ضئيل في عملية اكتشاف تكنولوجيا المعلومات ،فالشهادة مثلا لا يمكن تصور ورودها على السلوك المكون للجريمة المعلوماتية، كون هذه الأخيرة تقتضي التلاعب في البيانات والبرامج فهي غير مشاهدة من قبل الغير حتى يمكن ان يشهد بها امام القضاء شهادة مباشرة[١١]، ومن خلال ما سبق سوف تقتصر كليتينا على إجراءات التحقيق التي تتنسب مع هذا النوع من الجرائم وذلك من خلال مطلبين الأول سوف نتناول فيه المعاينة والتفتيش والثاني الضبط والخبرة القضائية .

المطلب الأول: المعاينة والتفتيش:

تعد المعاينة والتفتيش من بين الإجراءات التي تباشرها سلطات التحقيق والتي تؤدي للوصول للدليل المستمد من الواقعة الاجرامية، عن طريق التفتيش عن الحقيقة من حيث ثبوت التهمه ونسبتها الي المتهم من عدمه وسوف نتحدث في هذا المطلب عن المعاينة والتفتيش.

أولا: المعاينة: يقصد بالمعاينة مشاهدة واثبات الأثار المادية التي خلفها ارتكاب الجريمة ، بهدف المحافظة عليها خوفا من اتلافها او محوها او تعديلها[١٢] ، والمعاينة

---

[١٠] معمش زهية ونسميه:" الاثبات الجنائي في الجرائم المعلوماتية " أطروحة للحصول على درجة الماجستير ، جامعة عبد الرحمن ميرة ، السنة الجامعية ٢٠١٢ /٢٠١٣ ص ٥.

[١١] نفس: م س ص ٦.

[١٢] علي عدنان الفيل :"اجراءات التحري وجمع الادلة والتحقيق الابتدائي في الجريمة المعلوماتية " المكتب الجامعي الحديث ، سنة ٢٠١٢ ص ٣٢.

اجراء من إجراءات التحقيق وتتم بالانتقال الى محل الواقعة الاجرامية كقاعدة إجرائية مقررة في هذا الشأن الا انه في إطار جرائم الانترنت فأن الانتقال يعد من الموضوعات الجديدة ،وذلك لان مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي وانما يجب ان تكون بالضرورة عبر العالم الافتراض[١٣] حتى تصبح للمعاينة فائدة في كشف الحقيقة في الجرائم المعلوماتية لابد من مراعاة عدة قواعد اهمها:

١. وجود خريطة توضح الموقع الذي ستتم معاينته وعدد الأجهزة والخزائن والملفات الموجودة فيه.
٢. تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة او برامج.
٣. تأمين عدم انقطاع التيار الكهربائي ، لان معاينة الأجهزة وما بها من شبكات وأنظمة تشغيل لا جدوى منها في عدم وجود التيار الكهربائي .
٤. اعداد فرق متخصصة وهي فريق التفتيش العملي فريق التأمين والقبض ، وفريق تحرير الأدلة وفريق لأخذ الافادات.
٥. التحفظ على النظام ونسخ بياناته[١٤].
٦. اخذ صور لواجهة وخلفية وجوانب الأداة والكوابل المرتبطة مع الأداة وعدم نقل أي مادة معلوماتية من مسرح الجريمة قبل اجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسوب من أي مجالات لقوى مغناطيسية ممكن ان تتسبب بمحو البيانات المسجلة[١٥].
٧. قصر مباشرة المعاينة على فئة معينة من الباحثين والمحققين الذي تتوفر لديهم الكفاءة العلمية والخبرة الفنية في مجال الحاسوب والشبكات ونظام المعلومات[١٦].

[١٣] عمر محمد ابو بكر بن يونس:" الجرائم الناشئة عن استخدام الانترنت "ط الأولى في القاهرة ،س ٢٠٠٤ ص ٨٩٥.
[١٤] نداء فايز المصري :" خصوصية الجرائم المعلوماتية "أطروحة مقدمة للحصول على الماجستير ، فلسطين ، س ٢٠١٧ ص ٥٧.
[١٥] نداء فايز المصري : م س ص ٥٧.
[١٦] على عدنان الفيل : م س، ص ٥٧.

السلطات المختصة لمعاينة الجرائم المعلوماتية:

بما ان إجراءات التحقيق ومنها المعاينة تطال حقوق وحريات الافراد الخاصة فقد حرص المشرع في قانون الإجراءات الجزائية اليمني على ايلائها الى الجهة القضائية وهي النيابة العامة وهذا ما أشار اليه في المادة (١٣٠) من قانون الإجراءات الجزائية اليمني بقولها:" وله استدعاء الخبراء لأجراء المعاينة ويحرر محضرا بالمعاينة يكون صورة كاملة ومطابقه لشي محل المعاينة [١٧].."

وأكدت أيضا المادة (٢٠٧) من القانون أعلاه حيث نصت على انه:" للنيابة العامة ان تطلب من طبيب او شخص له خبرة فنية في أي مجال ابداء الرأي في أي مسألة متعلقة بالتحقيق.."

لسلطة التحقيق الاستعانة بالخبراء لأجراء المعاينة وتقديم الإيضاحات في أي مسألة من المسائل المتعلقة بالجرائم المعلوماتية التي تخرج عن نطاق اختصاصها[١٨].

وللنيابة العامة سلطة تقديرية في تقدير راي الخبير ،فلها ان تأخذ به ولها ان ترفضه مع تحديد أسباب الرفض ، او طلب تقرير إضافي من الخبير ذاته او من خبير اخر، اذا احتوى التقرير الأول على أوجه نقص، كما يجوز طلب تقرير من خبير اخر في حالة وجود شك في صحة التقرير الأول[١٩] .

يشترط لصحة المعاينة توفر عدة شروط من أهمها ما يلي:

١. السيطرة على المناطق المحيطة بمسرح الجريمة.
٢. تحديد أجهزة الحاسوب الموجودة في مكان الاغارة لتحديد موقعها بأسرع فرصة ممكنة وفي حالة وجود شبكات اتصالات يجب البحث عن خادم الملف لتعطيل حركة الاتصالات[٢٠].

---

[١٧] نديم محمد الترزي :" سلطات النيابة العامة في الجرائم المعلوماتية " مجلة الاندلس ، العدد ١٣، المجلد١٥، أبريل ،س ٢٠١٧ ص ٣٥١.
[١٨] نفس: م س، ص٣١٦.
[١٩] نديم محمد حسن الترزي: م س ص ٣١٧.
[٢٠] علي عدنان الفيل: م س ص ٣١٧.

٣. الدقة والعناية في معاينة مسرح الجريمة والتحفظ علية وتدوين معاينة ويكون كتابيا ورسميا وتصويريا [٢١].

ثانيا: التفتيش:

قد يتطلب التحقيق تفتيش شخص المتهم او منزلة او غيرة لضبط الأشياء المتعلقة بالجريمة، والتفتيش كأجراء من إجراءات التحقيق الابتدائي هو في الأصل من اختصاص سلطة التحقيق المتمثلة في قاضي التحقيق والنيابة العامة لاختلاف التشريعات ، الا انه يخول استثناء لرجال الضبطية القضائية في حالات محددة قانونا[٢٢].

وقد اجمع الفقه القانوني على ان التفتيش بأنه عبارة عن اجراء من إجراءات التحقيق التي تهدف الى البحث عن ادلة مادية لجناية او جنحه تحقق وقوعها في محل يتمتع بحرمة المسكن او الشخص وذلك بهدف اثبات ارتكابها او نسبتها الى المتهم وفقا لإجراءات قانونيه محدده[٢٣].

خصائص التفتيش:

١. أنه إجراء من إجراءات التحقيق.
٢. أنه يهدف للبحث عن ادلة مادية.
٣. أن تكون الأدلة ناشئة عن جناية او جنحة تحقق وقوعها.
٤. أن يقع التفتيش على محل يتمتع بحرمة المسكن او الشخص.
٥. ان يتم التفتيش وفقا للإجراءات القانونية المقررة [٢٤].

---

[٢١] معمش زهية ونسميه غانم : م س ص ١٠.
[٢٢] براهيمي جمال :"التحقيق في الجرائم الإلكترونية "أطروحة مقدمة للحصول على الدكتورة جامعة مولد معمري – تيزي وزو س٢٠١٨ ص ٣٨.
[٢٣] علي عدنان الفيل : م س ص ٣٨.
[٢٤] نداء فايز المصري : م س ص ٦٦.

محل التفتيش الإلكتروني:

يقصد بمحل التفتيش الإلكتروني المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سريته وخصوصية والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة كالمسكن او الرسائل ، لان المستودع في الجرائم الإلكترونية هو الحاسوب الذي يقوم في تركيبه على مكونات مادية كوحدات المعالجة المركزية ، ووحدات الادخال والاخراج والتخزين كما أن له شبكات اتصال بعيدة سلكية ولاسلكية متواجدة على المستوى المحلي والدولي فأن الامر يتطلب منا البحث في مدى قابلية جميع هذه المكونات للتفتيش[٢٥].

أولا: تفتيش المكونات المادية للحاسوب:

لا يختلف اثنان ان الولوج الى المكونات المادية للحاسوب بحثا عن شيء متصل بالجريمة المعلوماتية واقعة يفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش بمعنى ان حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، فاذا كانت موجوده في مكان خاص كمسكن المتهم او احد ملحقاته كان لها حكمه فلا يجوز تفتيشها قانونا الا في الحالات المقررة في التشريعات المختلفة مع مراعات التميز بين ما اذا كانت مكونات الحاسوب المراد تفتيشها منعزلة عن غيرها من الحواسيب الأخرى او انها متصلة بحاسوب الكتروني اخر غير منزل المتهم اما لو وجد شخص يحمل مكونات الحاسب الالكترونية المادية او كان مسيطر عليها او حائز لها في مكان ما من الأماكن العامة فأن تفتيشها لا يكون الا في الحالات التي لا يجوز فيها التفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[٢٦].

---

[٢٥] معمش زهية ونسميه غانم : م س ص ٢٠ .
[٢٦] علي عدنان الفيل : م س ص ٤١.

ثانيا: تفتيش المكونات المنطقية للحاسوب:

يرى جانب من الفقه بأنه غير ممكن اخضاع المكونات المنطقية للحاسوب لقواعد التفتيش التقليدية ، لان هذه القواعد وضعت في وقت لم تكن نظم المعالجة الالية الحواسيب موجوده وتطبيقاتها غير معروفه ، بالتالي فطبيعة هذه المكونات تتطلب احداث قواعد تفتيش جديدة خاصة بها ، او على الأقل تعديل قواعد التفتيش المألوفة بشكل يجعلها تلائم احكامها مع متطلبات هذه التقنية الجديدة، ويبدو ان غالبية تشريعات الدول المتقدمة تميل الى هذا الاتجاه[٢٧].

ثالثا: تفتيش شبكات الحاسوب:

قد يكون حاسب المتهم متصل بغيرة من الحواسيب عبر شبكة الالكترونية وهنا يجب التميز بين ما اذا كان حاسوب المتهم متصلا بأخر داخل إقليم الدولة ، او كان متصلا بحاسوب يقع في نطاق إقليم دولة أخرى.

حالة وجود جهاز متصل بجهاز المتهم داخل الدولة:

تكمن المسألة في هذه الحالة في تجاوز الاختصاص المكاني للسلطة المختصة بالتفتيش ، كما انه يعتبر بمثابة عدوان على حقوق الافراد وحرياتهم وذلك عند قيام سلطة التحقيق بتفتيش جهاز له علاقة بجهاز المتهم داخل الدولة. قد اجازات بعض التشريعات للأشخاص القائمين على التفتيش امتداد هذا الأخير على سجلات البيانات المتصلة في النهاية أي انه يمكن امتداد الحق في تفتيش المساكن الى نظم المعلومات الموجودة في موقع اخر حيثما يهدف الى اظهار الحقيقة دون وجود اصدار اذن مسبق من قاضي التحقيق[٢٨].

---

[٢٧] براهيمي جمال : م س ص ١٨.

[٢٨] معمش زهية ونسميه غانم: م س ص ٢٤.

حالة وجود جهاز متصل بجهاز المتهم خارج الدولة:

تعد هذه المسألة من المشكلات التي تواجه اجراء التحقيق بخصوص مسألة التفتيش ، ذلك لما توصلت الية الدول من خلال برمجيات يمكنها القيام بأجراء التفتيش الذي لا يستند الى مبرر قانوني من جهة، وباعتباره اعتداء على خصوصيات الافراد وأجهزة حواسبهم من جهة أخرى[٢٩].

رابعا: شروط تفتيش نظم الحاسوب الالكتروني:

يمكن تقسيم شروط تفتيش نظم الحاسبة الالكترونية الى نوعين موضوعية والأخرى شكلية.

أولا: الشروط الموضوعية لتفتيش الحاسب الالكتروني يمكن حصر هذه الشروط فيما يلي:

وجود سبب التفتيش:

كقاعدة عامة فأن سبب التفتيش باعتباره من إجراءات التحقيق هو وقوع جريمة او اتهام شخص او عدة اشخاص بارتكابه او المساهمة فيها مع توفر امارات او قرائن قوية على وجود أشياء تفيد في كشف الحقيقة لدى المشتبه فيه او غيره تأسيسا على ما سبق وتطبيقا على الجرائم المعلوماتية وحتى يكون التفتيش فيها مشروعا فلا بد من تحقق الاتي:

وقوع جريمة معلوماتية:

اتهام شخص او أكثر بارتكاب هذه الجريمة المعلوماتية او المساهمة في ارتكابها.

توفر امارات قوية او قرائن على وجود ادلة معلوماتية في أحد الأجهزة الالكترونية او الشبكات تفيد في كشف الحقيقة [٣٠].

---

[٢٩] عمر محمد ابو بكر بن يونس: م س ص ١٣١، ١٣٢.

[٣٠] براهيمي جمال: م س ص ٢٤.

محل التفتيش الخاص بنظم الحاسبة الالكترونية هي كل مكونات الحاسوب سواء كانت مادية او معنوية او شبكات الاتصال الخاصة بها بالإضافة الى الأشخاص الذين يستخدمون الحاسوب محل التفتيش [٣١].

خامسا: الشروط الشكلية لتفتيش نظم الحاسوب الالكتروني:

الى جانب الشروط الموضوعية لتفتيش نظم الحاسوب هناك شروط أخرى ذو طابع شكلي يجب مراعاتها والاخذ بها اثناء القيام بالتفتيش وتتمثل فيما يلي:

١. ضرورة حضور بعض الأشخاص عند اجراء التفتيش لنظم الحاسوب اشتراط قانون أ. ج. ي في المادة (١٣٤) منه ضرورة حضور شخص او اشخاص اثناء التفتيش فقد نصت هذه المادة على انه" يحصل التفتيش بحضور المتهم او من ينيبه وبحضور شاهدين من اقاربه او جيرانه ولا يجوز ان يكون الشاهدين من رجال التحقيق".
٢. تحرير محضر بإجراء التفتيش حيث اوجبت المادة (١٥٠) ا. ج. ي ضرورة إعداد محضر بإجراءات التفتيش بقولها" يجب على عضو النيابة القائم بالتفتيش تحرير محضر بالإجراءات وما اسفرت عنه وما تم ضبطه من أشياء[٣٢] "
٣. تحديد ميعاد التفتيش يعد ميعاد التفتيش أحد اهم الضمانات الشكلية بحيث لا يجوز اجراء هـ خارج الأوقات المحددة قانونا ، لم يحدد قانون أ. ج. ي ميعاد اجراء لتفتيش في الجرائم المعلوماتية وانما حدد موعد لتفتيش المساكن حيث نصت المادة (١٤٤/ أ) منه على انه تفتيش المساكن يجب ان يكون بعد شروق الشمس وقبل غروبها الا في حالات الجريمة المشهودة او مطاردة شخص هارب من العدالة[٣٣]"

---

[٣١] علي عدنان الفيل : م س ص ٩٤، ٥٠ .
[٣٢] نديم محمد حسن لترزي : م س ص ٣٣٠.
[٣٣] راجح محمد راجح غلاب :" الجرائم المعلوماتية في القانون الجزائري واليمني "أطروحة مقدمة للحصول على الدكتورة فرع القانون الجنائي كلية الحقوق جامعة الجزائر س ٢٠١١ _ ٢٠١٢ ص ٣٢٨.

المطلب الثاني: الضبط القضائية والخبرة:

يلعب الضبط والخبرة دورا هاما في مجال الإثبات الجنائي للأدلة المعلوماتية خاصة في ضل تزايد تطور التكنولوجيا، وبعد انتهاء المحقق الجنائي من اجراء التفتيش يقوم بضبط الأشياء التي يراها ضرورية ، ومن ثم يأتي دور الخبير بالبحث عن الحقيقة بناء على الأشياء المضبوطة، ثم يقدم الدليل المستنبط للقاضي الذي يمكن ان يبني حكمه بناء علية[٣٤]، هذا ما سوف نعالجه من خلال الاتي:.

أولا: الضبط في الجرائم المعلوماتية:

ويعرف الضبط بأنه حق لجهة الإدارة في فرض قيود تحد بها من الحقوق والحريات التي يتمتع بها الافراد بقصد حماية النظام العام ، اذ انه سلطة تمنح بقصد تتبع الجرائم والتوصل الى مرتكبها[٣٥].

مدى صلاحية ضبط الأدلة في الجرائم المعلوماتية:

هناك صعوبة في اعتبار ان مكونات الحاسب الالي من الأشياء التي يمكن ضبطها وبالخصوص ضبط الشبكة الالكترونية والمكونات المعنوية وفيما يلي نلقي الضوء على مدى قابلية المكونات المادية والمعنوية لان تكون محلا للضبط [٣٦].

ثانيا: ضبط المكونات المادية للحاسب الالي:

الأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في اثبات جرائم الحاسوب ونسبتها الى المتهم هي:

الورق ويعتبر من الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة وينقسم الورق الى أربع انواع:

---

[٣٤] معمش زهية ونسميه غانم: م س ص ٢٦.
[٣٥] عمر محمد ابو بكر بن يونس : م س ص ٨٩٠.
[٣٦] معمش زهية ونسميه غانم: م س ص ٢٧.

١. أوراق تحضيرية يتم اعدادها بخط اليد كمسودة او تصور للعملية التي يتم برمجتها.
٢. أوراق تالفة تتم طباعتها للتأكد ومن ثم القائها في سلة المهملات.
٣. أوراق اصلية تتم طباعتها والاحتفاظ بها كمرجع او لأغراض تنفيذ الجريمة.
٤. أوراق أساسية وقانونية محفوظه في الملفات العادية او دفاتر الحاسبات وتكون لها علاقة بالجريمة خاصه عند تلقيها او تزوير بيانتها لتنفيذ جريمة الحاسوب الالكتروني [٣٧].

جهاز الحاسوب وملحقاته ، وجود جهاز الحاسوب مهم للقول بأن هناك جريمة ولأجهزة الحاسوب اشكال واحجام والوان مختلفة وخبير الحاسوب يستطيع ان يتعرف على الحاسوب ومواصفاتها بسرعة فائقة، كما يستطيع تميزه عن الأجهزة الالكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحريز[٣٨].

الحاسبة الالكترونية، لوحة المفاتيح ، والشاشة ، اصبح من السهل التعرف على جهاز الحاسب الشخصي الذي اصبح مألوفا اليوم فهو يتكون من وحدت المعالجة المركزية ولوحة المفاتيح والشاشة ومع التطور السريع نجد إضافات جديدة مثل المودم والسماعات والسيرفر ونجد ان اشكالها تتغير باستمرار لذلك من الضروري اطلاع العاملين في مجال التحقيق على مختلف اشكال الحاسوب فور ظهورها[٣٩] .

أقراص الليزر ومن اهم مميزات هذه الأقراص هي انها ذات سعة كبيرة في التخزين، حيث تمتاز بسعة التخزين للمعلومات والبيانات مما يكسبها أهمية تفوق بقية الأقراص الأخرى[٤٠].

الشرائط الممغنطة وتستخدم للحفظ الاحتياطي وقد تكون في مكان بعيد أمن كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوفيق الحكومية الأمنة.

---

[٣٧] بخي فاطمة الزهراء: "إجراءات التحقيق في الجريمة الإلكترونية" مذكرة للحصول على الماجستير السنة الجامعية ٢٠١٤ ص ٨٠.
[٣٨] علي عدنان الفيل : م س ص ٥٥.
[٣٩] نفس: م س ص ٥٦.
[٤٠] محمد حماد مرهج الهيتي: م س ص ٤٠.

وحدات الإخراج وهي الوحدات التي تمكن من خلالها تحويل المعلومات غير المقروءة وغير المرئية الى معلومات مقروءة ومرئية.

المودم وهي الوسيلة التي تمكن اجهزت الحاسوب من الاتصال مع بعضها البغض عبر خطوط الهاتف وقد تطور المودم الى أجهزة الفاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها [٤١].

ووحدة المعالجة المركزية : وتعتبر بمثابة العقل المفكر والمسيطر على عمل باقي الوحدات المكونة لجهاز الحاسوب وتقوم بمعالجة البيانات حسب التعليمات الواردة في البرامج حيث يتم فيها جميع العمليات الحسابية والمنطقية وتتكون بدورها من وحدة التحكم والسيطرة [٤٢].

ثالثا: ضبط المكونات المعنوية للحاسوب:

تكمن المشكلة في الأشياء المعنوية للحاسوب التي تتضمن البرامج والبيانات، ويثور التساؤل الى مدى صلاحيتها كمحل للضبط، حيث ان بعض الفقهاء يتجه الى اعتبارها لا تصلح كمحل للضبط وهذا ما ذهب الية الفقه الألماني [٤٣]، اما البعض الاخر يرى بأنه لا مانع من ضبط البيانات الالكترونية مستندين الى ان الغاية من التفتيش هو ضبط الأدلة المادية المفيدة في كشف الحقيقة ، بالتالي يمتد هذا المفهوم ليشمل البيانات الالكترونية بمختلف اشكالها[٤٤]، ويأخذ المشرع اليمني بمبدأ جواز التفتيش وضبط لأنظمة الحاسوب .

غير ان المسألة الصعبة تكمن في الخلاف حول مدى خضوع المكونات غير المادية للضبط وفقا للنصوص التقليدية وكذلك في إجراءات ضبطها سواء تعلق الامر ببرامج الحاسوب أو بياناته[٤٥].

---

[٤١] علي عدنان الفيل : م س ص ٥٦ – ٥٧.
[٤٢] بخي فاطمة الزهراء: م س ص٨١.
[٤٣] معمش زهية ونسميه غانم: م س ص ٢٨.
[٤٤] بخي فاطمة الزهراء: م س ص ٨٣ .
[٤٥] فايز محمد راجح غلاب: م س ص ٣٤٤.

بيانات الحاسوب: بالنسبة لضبط البيانات التي تعد دليلا على ارتكاب الجريمة، هناك صعوبات كثيرة منها عدم وجود دليل مرئي يمكن لرجال الضبط القضائي فهمه عن طريق القراءة وعدم وجود اثار مادية يمكن من خلالها الاستدلال على ادلة في ارتكاب الجريمة وتظهر في شكل واضح في جرائم الاختلاس والتزوير[٤٦].

برامج الحاسوب: ان الامر يتعلق بكيفية ضبط الأدلة في حالة استخدام الوسائل الفنية في نسخ او اتلاف البرامج كالفيروسات مع قلة خبرة وتدريب رجال الضبط وسلطات التحقيق في جمع الأدلة في مجال فني وتقني وهذا من الناحية الأولى، من الناحية الثانية يتمثل في قيام عملية ضبط الوسائل التقنية بواسطة الأنظمة والشبكات المعلوماتية، حيث يؤدي الضبط الى عزل النظام المعلوماتي بالكامل عن دائرته لفترة زمنية ممكن ان تطول او تقصر والذي يسبب خسائر او اضرار مستخدمة النظام[٤٧].

رابعا: الخبرة القضائية:

منذُ بدء الجرائم ذات الصلة بالحاسوب تستعين الشرطة وسلطات التحقيق او المحكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسبة الالكترونية، ذلك بغرض كشف الغموض في الجريمة وتجميع الأدلة والتحفظ عليها او مساعدة المحقق في اجلاء جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[٤٨].

تظهر أهمية الخبرة في مجال الجريمة المعلوماتية لتعلقها الوثيق بالحاسوب وشبكات الاتصال المرتبطة بالخصوصيات الفنية والعلمية الدقيقة ، مع التطور السريع لها يصعب على المختصين مواكبتها واستيعابها بالإضافة الى انه لا يوجد خبير يستطيع التعامل مع جميع الجرائم المعلوماتية نظرا للتعدد النماط هذا النوع من الجرائم[٤٩].

---

[٤٦] معمش زهية ونسميه غانم : م س ص ٢٩.
[٤٧] معمش زهية ونسميه غانم: م س ص ٢٩.
[٤٨] علي عدنان الفيل : م س ص ٢٦.
[٤٩] معمش زهية ونسميه غانم: م س ص ٣٥.

تعريف الخبرة والخبير:

هي الوسيلة لتحديد التفسير الفني للأدلة او الدلائل بالاستعانة بالمعلومات فهي في الحقيقة ليست دليل مستقل عن الدليل القولي او الدليل المادي، انما هيا تقيم فني لهذا الدليل والعنصر المميز للخبرة عن غيرها من الإجراءات الاثبات كالمعاينة والشهادة والتفتيش .

اما الخبير فهو كل شخص له الالمام باي علم او فن سواء كان اسمة مقيد في جدول الخبراء على مستوى المحاكم أولا[٥٠].

تعين الخبير المعلوماتي:

ان من اهم الصعوبات التي تواجهه الخبرة هي الحصول على الخبير المناسب للاستعانة به باعتبار ان الخبرة في مجال المعلومات لا تعتمد على الشروط التقليدية الخاصة في تعين الخبير بل يتطلب الامر شروط تتلاءم مع التطورات ، فيحتاج الشخص لكي يكون خبير قضائي في مجال الجريمة المعلوماتية بشكل خاص ان يتمتع بشروط خاصة، حيث يجب ان يكون مؤهل مهنيا وحاصل على شهادات ودراسات عليا في فرع التخصص ، وان يخضع للتدريب العملي والقانوني مع استمراريته التدريب، فيتطلب من الخبير ان يكون ملما بالجوانب الفنية والتقنية[٥١] ومنها ما يلي:

١. طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم والتركيز والتوزيع عمل المعالجة الالية وتحديد أماكن التخزين والوسائل المستخدمة لذلك.
٢. المعرفة بتركيب الحاسب وصناعته وطرازه ونوع نظام تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به.
٣. المواضيع المحتمل للأدلة الاثبات والشكل او الهيئة التي تكون عليها.
٤. الكيفية التي يمكن عند الاقتضاء عزل النظام المعلوماتي دون تلف الأدلة او تدميرها.

---

[٥٠] بخي فاطمة الزهراء: م س ص ٨٨.
[٥١] معمش زهية ونسميه غانم : م س ص ٣٥.

٥. الكيفية التي تجسد الأدلة في صورة مادية ينقلها أذا أمكن الى اوعية ورقية يتاح للقاضي مطالعتها وفهمها [٥٢].

ومن التشريعات الحديثة التي نظمت اعمال الخبرة في مجال الجرائم الالكترونية القانون البلجيكي الصادر في23_11_2000 فقد نصت الماه (٨٨) من القانون المذكور على انه يجوز للقاضي التحقيق ، والشرطة القضائية ان يستعين بخبير ليقدم وبطريقة مفهومة المعلومات الازمة عن كيفية تشغيل النظام وكيفية الدخول فيه، او الدخول للبيانات المخزونة فيها او المعالجة المنقولة بواسطة ويعطي القانون كذلك لسلطات التحقيق ان تطلب من الخبير تشغيل النظام او البحث فيه او عمل نسخة من البيانات المطلوبة للتحقيق ، او سحب البيانات المخزونة او المحولة، على ان يتم ذلك بالطريقة التي تريدها جهات التحقيق[٥٣].

دور الخبير التقني في حفظ الأدلة الالكترونية:

يتطلب لحفظ الأدلة داخل جهاز الحاسوب معرفة دقيقة لصحة البيانات الواردة في الحاسب الالي وهذا ما يستلزم من الخبير التقني ضرورة الكشف بداية على نطاق محتوى صحة حركة الحاسوب من وجود شك في صحت الأدلة المستفادة خاصة حالة وجود خلل او عطل مثل الفيروس[٥٤].

على الخبير المعلوماتي في سبيل تحري الحقيقة استخدام الأساليب كافة مالم تكن تلك الأساليب غير مشروعه، وليس للمحكمة ان ترفض تلك الأساليب الا اذا كان رفضها مسبب ومعلل وهناك اسلوبان لعمل الخبير التقني :

الأول: القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كما هو الشأن في التهديد او النصب او جرائم النسخ وبث صور فاضحة بقصد الدعاية لتحريض على ارتكاب جرائم الدعارة والرقيق وغيرها ، ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية اعدادها البرمجي ونسبتها الى مسارها الذي اعدت فيه وتحديد

---

[٥٢] معمش زهية ونسيمة غانم : م س ص ٣٦.
[٥٣] علي عدنان الفيل : م س ص ٣٠.
[٥٤] معمش زهية ونسيمة غانم: م س ص ٤٢.

عناصر حركتها وكيف تم التوصل الى معرفتها ومن ثم التوصل في النهاية الى معرفة جهاز الحاسوب الذي صدر عن هذه المواقع[٥٥].

ثانيا: القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها ، جريمة في ذاته، وانما تؤدي حال تتبع موضوعها الى قيام الفرد بارتكاب جرائم ، كما هو الحال في المواقع التي تساعد الغير للتعرف على جرعات المخدرات والمؤثرات العقلية، وكيفية زراعة المخدرات بعيدا عن اعين الغير، وكيفية اعداد القنابل وتخزينها وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها ، ويتم في إطار تصنيف المواقع المذكورة استخدام برمجيات متطورة مهمتها الكشف عن مثل هذه المواقع باستمرار ومعرفة الجديد فيها[٥٦].

ثالثا: مدى كفاية النصوص التقليدية في معالجة المسائل المتعلقة بالخبرة المعلوماتية.

باعتبار ان القاضي قد يستخدم خبير استشاري بشكل غير رسمي في المجال الرقمي، ذلك قد يشكل صعوبة ويعيق إجراءات التحقيق وكثر من ذلك قد تكون وجها من أوجه البطلان ،كون ان بعض القوانين تخول للمتهم دون سلطة التحقيق او الاتهام الاستعانة بخبير استشاري، لأنه قد لا يجد القاضي خبير في مجال تكنولوجيا المعلومات ضمن قائمة جدول الخبراء ، هذا ما يستدعي من المشرع التدخل من خلال تضمين نصوص قانونية تسمح بالاستعانة بالخبرة الاستشارية من طرف جهات التحقيق والاتهام في المجال المعلوماتي دون التقيد بالخبراء الجدول المعتمدين[٥٧]،ولقد نظم قانون الإجراءات الجزائية اليمني نصوص خاصة بالحكام المتعلقة بالخبرة بالنسبة للجريمة التقليدية من المادة 216الى المادة 270، رغم عدم تضمين نصوص خاصة تتعلق بالخبرة الرقمية ونقص الخبرة في مجال التكنولوجيا المعلوماتية الا انه هناك إمكانية تطبيق الاحكام المتعلقة بالخبرة في الجرائم الناشئة عن الحاسوب، فبات الامر على القاضي على ان يكون ملما بالأمور الفنية، باعتباره يشرف ويراقب اعمال الخبرة ، كما ان يحدد المواضيع التي تتطلب

---

[٥٥] نداء نائل المصري : م س ص ٦٠.

[٥٦] عمر محمد ابو بكر بن يونس: م س ص ١٠٤٣.

[٥٧] نفس : م س ص ٨٩٢.

الاستعانة بالخبرة ، غير ان هذا الامر غير متوفر في الدول النامية ، وبالتالي تدريب كوادر أجهزة الضبط والقضاة في مجال الخبرة الرقمية تكان ان تكون ضرورة لا غنى عنها.

وعلية في الأخير يمكن القول ان الجرائم المعلوماتية هي جرائم ذو طبيعة خاصة فإجراءات التحقيق فيها لاتزال محل خلاف فقهي وقضائي ، وغياب الخبير المعلوماتي المختص في المجال الرقمي وغيرها من إجراءات التحقيق باعتبار ان الدليل المراد استنباطه يكون خفيا غير مرئي وفقدان الدليل لأثاره سواء بالتلاعب او التغير او الحذف ، لذا فأن متابعة إجراءات التحقيق في مجال الجريمة المعلوماتية تحتاج الى الامن المعلوماتي ولرجال الضبط القضائي المتمكنون في الأمور الفنية والتي لا يتسنى تحقيقها الا عن طريق التدريب والتأهيل في المجال التقني المعلوماتي[٥٨]، وكل هذه الأمور لا تؤدي الى الكشف عن الحقيقة الا بالحصول على الدليل الالكتروني الرقمي ، الذي يقوم علية الاثبات الجنائي في الجريمة المعلوماتية للوصول الى الحقيقة وبالتالي من المهم جدا التعرض الى الدليل الرقمي والذي سنتحدث عنه في المبحث الثاني.

المبحث الثاني: استنباط الدليل الرقمي:

بما ان الجرائم المعلوماتية جرائم غير تقليديه فانه من شأن ذلك ان تكون الأدلة وطرق استخلاصها ايضا طرق غير تقليديه [٥٩].

نظرا للطبيعة الخاصة للجريمة المعلوماتية والوسائل الخاصة المستعملة في ارتكابها فلاشك ان هناك صعوبة في الحصول على ادله معلوماتية ، وذلك نظرا لسهولة محو الأدلة وأتلافها بزمن قصير ويعتبر الدليل المعلوماتي بأنه ذلك الدليل المستمد من وسائط ترتبط بتقنية المعلومات ،وكلها تدور حول استخدامات الحاسوب وتطبيقاته

[٥٨] معمش زهية ونسميه غانم : م س ص ٤٤.
[٥٩] محمد حامد مهرج الهيتي:" جرائم الحاسوب- وماهيتها - وموضوعها - أهم صورها دراسة تحليلية " دار المناهج للنشر والتوزيع ط اولى ص ٢٣١ .

وشبكه الانترنت وغيرها من التقنيات الحديثة وفي هذا المبحث سنتناول مطلبين الاول مفهوم الدليل الرقمي ومشروعيته والثاني مشاكل الاثبات بالدليل الرقمي[٦٠].

المطلب الأول: مفهوم الدليل الرقمي ومشروعيته:

باعتبار ان الدليل الرقمي ذو اهمية بالغة في مجال الاثبات الجنائي للجرائم المعلوماتية فأنه يجب التعرض اليه بتحديد مفهومه من خلال تعريفه وتقسيماته وخصائصه وأنواعه وامثلة عنه وذلك كما يلي:

اولاَ: تعريف الدليل الرقمي:

يعرف الدليل الرقمي بأنه عباره عن معلومات مخزنة في الأجهزة ذات الأنظمة الالكترونية على شبكات الاتصال ، ويتم جمعها وتحليلها باستخدام برمجيات وتطبيقات خاصة بهدف اثبات وقوع الجريمة ونسبتها الى المتهم او نفيه عنة[٦١].

كما عرف الدليل الرقمي ايضا بأنه "الدليل الذي يجد له اساسا في العالم الافتراضي ويقود الى الجريمة "فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات والذي بدوره يؤدي الى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الانترنت [٦٢].

هناك من يعرفه بأنه معلومات يقبلها العقل والمنطق ويعتمدها العلم يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقتها وشبكات الاتصال، ويمكن استخدامها في أي مرحله من مراحل التحقيق او المحاكمة لإثبات حقيقة فعل او شخص له علاقة بارتكاب الجريمة [٦٣].

ثانيا: تقسيمات الدليل الرقمي:

للدليل الرقمي أشكال مختلفة وقد قسمها البعض الى الأقسام الاساسية التالية:

---

[٦٠] نداء نائل فايز المصري : م س ص ٧٨.

[٦١] سلامة محمد المنصوري :" تطبيق مبدأ الأقناع القضائي على الدليل الإلكتروني "أطروحة مقدمة للحصول على درجة الماجستير في القانون ، العام جامعة الامارات العربية المتحدة ٢- ١٢- ٢٠١٨ ص ٢٠.

[٦٢] عمر محمد أبو بكر بن يونس: م س ص ٩٦٩.

[٦٣] سعيداني نعيم: م س ص ١٢١.

١. ادله رقميه خاصة بالشبكة الدولية للمعلومات الانترنت.
٢. ادله رقمية خاصة بأجهزة الحاسوب وشبكاتها.
٣. ادله خاصة ببروتوكولات تبادل ونقل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
٤. ادله خاصة بالشبكة العالمية للمعلومات [٦٤].

وبتالي هذا التقسيم يتطابق مع تقسيم الجريمة عبر الحاسوب وقد قررت وزارة العدل الامريكية لسنة 2002 ان الدليل الرقمي يمكن تقسيمه كالتالي:

١. السجلات المحفوظة في الحاسوب وتشمل الوثائق والملفات المكتوبة والمحفوظة كالبريد الالكتروني والملفات المعالجة والكلمات مثل winword ورسائل غرف المحادثات عبر الانترنت.
٢. السجلات التي تم انشائها و اعدادها بواسطة الحاسوب ، وهي تعد مخرجات الحاسوب والتي لم يشارك الاشخاص فيها مثل سجلات الهاتف وتوفير أجهزة الحاسوب.
٣. السجلات التي تم حفظ جزء منها بالإدخال وجزء تم انشاؤه عن طريق الحاسوب ومنها اوراق العمل المالية التي تحتوي على مدخلات تم تلقيها مباشرة الى برامج اوراق العمل، بعد ذلك يتم معالجتها من خلال البرنامج بأجراء العمليات الحسابية عليها تلقائيا مثل اكسل[٦٥].

ثالثا: خصائص الدليل الرقمي:

يتميز الدليل الرقمي عن بعدة خصائص تميزه عن الدليل التقليدي نتناول اهمها على النحو الاتي:

١. الدليل الرقمي دليل علمي:

الدليل الرقمي هو دليل يحتاج الى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فأن ما ينطبق على الدليل العلمي ينطق على الدليل

[٦٤] سلامة محمد المنصوري: م س ص ٢٤.
[٦٥] معمش زهية ونسميه غانم: م س ص ٤٨.

الرقمي الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن هي قاعدة ان القانون مسعاه العدالة اما العلمي فمسعاه الحقيقة .

واذا كان الدليل العلمي له منطقته الذي يجب الا يخرج عليها من حيث انه يجب عدم تعارضه مع القاعدة العلمية السليمة ، فأن الدليل الرقمي له ذات الطبيعة اذ يجب الا يخرج الدليل العلمي عما توصل اليه العلم الرقمي والا فقد معناه [٦٦].

٢. الدليل الرقمي صعب التخلص منه:

ان القاعدة التي تسري على كافة ما يتعلق بهيكلة التكنولوجيا ،هي انه كلما حدث اتصل بتكنولوجيا المعلومات بمعنى ادخال البيانات الى ذلك العالم فأن الصعب التخلص منها ولو كان ذلك باستخدام افضل ادوات الإلغاء ،فمحاولة التخلص من الدليل الرقمي باستخدام خصائص التخلص من الملفات في الحاسوب لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة لا اذا تتوفر برمجيات ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافه الملفات التي تم الغاؤها او ازالتها من الحاسوب ، ويمكن اعتبار هذه الخاصية ميزه يتمتع بها الدليل الرقمي عن غيره من الادلة التقليدية[٦٧].

٣. الدليل الرقمي دليل متنوع ومتطور:

ان الدليل الرقمي يشمل جميع انواع البيانات الرقمية التي يمكن تداولها الكترونيا وتعني هذه الخاصية بأنه على الرغم من ان تكوين الدليل الرقمي يعتمد على لغة الحوسبة والرقمنة ، الا انه يتخذ اشكالا مختلفة كأن يكون في شكل بيانات غير مقروءة كما هو الحال في المراقبة عبر الشبكات وقد يكون عبارة عن بيانات مقروءة كالوثيقة المعدة بنظام المعالجة الالية بالإضافة الى ذلك يمكن ان يكون عبارة عن صوره ثابتة او متحركة او مخزنه في البريد الالكتروني وبهذا نستنتج ان الدليل

[٦٦] خالد ممدوح إبراهيم : م س ص ١٨٠ .
[٦٧] سعيداني نعيم : م س ص ١٢٤.

الرقمي يشمل أنواع متعددة من البيانات الرقمية والتي تصلح بأن تكون دليل ادانة او براءة [٦٨].

4. الطبيعة التقنية والفنية ، وكيفية معنوية للأدلة الجنائية الالكترونية لا تدرك بالحواس العادية يتطلب ادراكها الاستعانة بأجهزة ومعدات ونظام الحاسوب.

5. كما ان المعلومة الرقمية غير ثابتة اذ يمكنها ان تظهر على شكل حركي يصعب بذلك ايجادها وهي سهلة النسخ فالموسوعة العالمية هي صوره يمكن نسخها في دقيقة تقريبا بواسطة usb.

6. كما ان طرق نسخ الدليل الرقمي من اجهزة الكمبيوتر تقلل من مخاطر اتلاف الدليل الاصلي.

7. تمتاز بعض الادلة الرقمية بسعة تخزينية عالية، بحيث يمكن لقرص صغير تخزين مكتبة كاملة كما يمكن لآلة فيديو رقمية تخزين مئات الصور [٦٩].

رابعا: الشروط الواجب توفرها في الدليل الإلكتروني:

لقبول الادلة الالكترونية كأساس تشيد علية الحقيقة في الدعوى الجنائية سوى أكان الحكم الصادر فيها بالإدانة ام بالبراءة فأنه يلزم ان تتوفر فيه الشروط الاتية:

١. يجب ان تكون هذي الادلة يقينية:

وهذا يستوجب ان تقترب نحو الحقيقة الواقعية قدر المستطاع وان تبتعد عن الظنون والتخمينات، يترتب على ذلك ان كافة مخرجات الوسائل الالكترونية من مخرجات ورقيه او الكترونية او اقراص مغناطيسية او مصغرات فيلميه تخضع لتقدير القاضي الجنائي ، ويجب ان يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال [٧٠].

٢. ان يكون الدليل الالكتروني ذي علاقة بموضوع الجريمة المعلوماتية:

---

[٦٨] الهام بوالطمين: " الاثبات الجنائي ، في مجال الجرائم الإلكترونية " لنيل شهاده الماجستير، جامعة العربي بن مهدي السنة الجامعية ٢٠١٧- ٢٠١٨ ص ٣٣- ٣٤.

[٦٩] غرباوي نادية : م س ص ٤٢- ٤٩ .

[٧٠] د. خالد ممدوح إبراهيم : م س ص ١٨٧ .

وهذا الشرط يشار اليه في قانون الاثبات الفيدرالي الامريكي بمبدأ العلاقة الكاشفة، حيث يتطلب القانون الامريكي ضرورة ان يكون هناك علاقة من نوع ما بين الدليل وبين الواقعة وذلك وفقا للمادة(401) وهي المادة التي تعرف الدليل الكاشف بأنه الدليل الذي يملك بذاته غاية محددة ممثلة في قدرته على ابراز حقائق يمكنها التأثير في اتجاه الدعوى الى الحد الذي يمكن ان يحدث تطويرا فيه بحيث لا يمكن حدوث هذا التطور بدونه[٧١].

٣. ان تكون هذه الاله قد تم الحصول عليها بطريقة شرعيه:

اي ان يتم الحصول عليها وفقا للقواعد والضوابط العامة ،التي يفرضها القانون وفي إطار مشروعية الأدلة الالكترونية نجد ان قانون الاجراءات الجنائية الفرنسي رغم انه لم يتضمن اي نصوص تتعلق بمبدأ الامانة والنزاهة في البحث عن الحقيقة إلا ان الفقه والقضاء اقر بهذا المبدأ في مجال التنقيب في جرائم الحاسوب والانترنت وكان يستخدم اعضاء الضابطة العدلية طرقا معلوماتية في اعمال التنصت على المحادثات الهاتفية، ويشير رأي الفقه الفرنسي الى استخدام الوسائل العلمية الحديثة للكشف عن الحقيقة، ولاسيما الادلة المتحصلة من الحاسوب والانترنت تحت التحفظ ،وهو الحصول على هذي الادلة بطريقه نزيهة وشرعية[٧٢].

خامسا: مصادر الحصول على الدليل الرقمي:

ان الحصول على الدليل الرقمي تكمن في الطريقة التي ارتكبت بها الجريمة وتنحصر تلك الادلة في المتهم المشتبه به والمجني عليه ومقدم خدمة الانترنت وهذي الادلة على سبيل المثال وليس الحصر اذ ان التطور العلمي والتقني قد يسفر عن انواع جديدة من هذي الأدلة:

أ- الكمبيوتر الخاص بالمتهم المشتبه فيه:

[٧١] د. عمر محمد أبو بكر بن يونس: م س ص ٩٩٢ .
[٧٢] معمش زهية نسميه: م س ص ٨٠- ٨١ .

فحص جهاز كمبيوتر المتهم المشتبه فيه وخاصة وحدة التخزين الدائمة القرص الصلب والوحدات الفرعية الملحقة وتشمل على القرص المرن وأقراص الليزر او أي وحدة تخزين اخرى من الممكن استعمالها، كل تلك الاجهزة يمكن فحصها وبيان الطريقة التي قام بها المتهم في ارتكاب الجريمة.

ب- جهاز كمبيوتر المجني علية:

مما لا شك فيه ان المجني عليه هي المصدر الكاشف والنتيجة التي يترتب عليها ما قام به المشتبه فيه من جرائم ،والمجني عليه قد يكون شخص طبيعي او مؤسسة خاصة او عامة او مؤسسة مالية او هيئه حكومية وغيرها وبالتالي فأن فحص مثل تلك الأجهزة يمكن المحقق من معرفة الدفوع وتتبع مصدر المشتبه فيه[٧٣].

ت- مقدم خدمة الانترنت:

يمكن الاستعانة ايضا في كشف الادلة الالكترونية بعدة جهات اخرى مثل مقدم خدمة الانترنت مثل شركة ياهو او جوجل، فأن مثل تلك الشركات يتم تسجيل البيانات الخاصة بمنتفعيها ومن ثم يمكن اللجوء أليهم لتتعرف على هويت المجرم المشتبه فيه وكذا البريد الالكتروني على شبكة الانترنت، وذلك حيث انه عن طريق البريد الالكتروني يمكن التعرف على البيانات الشخصية ومنها نستطيع تحديد هوية المشتبه فيه عن طريق صندوق الرسائل الواردة اليه المرسلة منه ومن ثم تحديد مكانه وموقعه وذلك من ارشيف المجموعات البريدية[٧٤].

سادسا: مشروعية الدليل الالكتروني:

لا يتم اصدار حكم الادانة لمجرد وجود ادله تثبت وقوع الجريمة ، بل يجب ان تكون لها قيمه قانونيه بمعنى خضوعها للقواعد المقررة للإثبات الجنائي .

[٧٣] خالد ممدوح إبراهيم: م س ص ٢٠١-٢٠٢.
[٧٤] خالد ممدوح إبراهيم: م س ص ٢٠٢ .

بالإضافة الى ذلك فأن القانون يفرض على القاضي بأن يلتزم بعدم قبول أي دليل يكون الحصول علية او البحث عنه بطريقه غير مشروعه وهي المسألة التي تقع على عاتق القاضي الجزائي بعد عملية التنقيب وقبل اخضاعه لتقديره وهذا من اجل حماية حقوق الافراد وحريتهم وهو الامر الذي قادنا الى دراسة مشروعيته الدليل الالكتروني ومشروعية الحصول على الدليل الالكتروني[٧٥].

يقصد بمشروعيه وجود الدليل ان يكون الدليل معترف به، بمعنى ان يكون القانون يجيز للقاضي الاستناد اليه لتكوين عقيدته للحكم بالإدانة، ويمكن القول ان النظم القانونية تخلف في مواقفها من الادلة التي تقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه، وهناك اتجاهان رئيسيان الاول نظام الادلة القانونية والثاني نظام الاثبات الحر[٧٦].

اولا: نظام الادلة القانونية:

وفيه يقوم المشرع بتحديد سالفا وبشكل حصري الادلة التي يجوز للقاضي قبولها ولاستعانة بها في الاثبات وكذا تحديد القوة الاستدلالية لكل دليل بناء على قناعته بها، في حين لا يكون للقاضي الجزائي في هذا النظام أي دور في تقدير الادلة او البحث عنها، وإنما يقتصر دوره على فحص الدليل لتأكد من مدى مشروعيته وتوفره على الشروط التي حددها القانون[٧٧].

ثانيا: نظام الاثبات الحر:

وهو نظام يسود فيه مبدأ حرية الاثبات اذ لا يحدد فيه المشرع طرق معينه للإثبات ولا حجيتها امام القضاء ، انما يترك ذلك للقاضي الجزائي الذي يكون له دور ايجابي للبحث عن الادلة المناسبة وتقدير قيمتها الثبوتية حسب اقتناعه بها فلا يلزمه القانون بالاستناد الى ادله معينه لتكوين قناعته فله ان يبني هذه القناعة على أي دليل يقدم في الدعوى وان لم يكن منصوصا عليه، بل ان المشرع في مثل هذا

[٧٥] الهام بوالطمين : م س ص ٧٣ .
[٧٦] طارق محمد الجملي: "الدليل الرقمي في مجال الاثبات الجنائي " مجلة الحقوق المجلد ١٢ ،العدد ١، ص ٥٠ .
[٧٧] براهيمي جمال : م س ص ١٣٨.

النظام لا يختص بالنص على ادلة الاثبات، فكل الادلة تتساوى قيمتها في نظر المشرع والقاضي هو الذي يختار من بين ما يطرح عليه من ادلة ما يراه مفيدا للوصول الى الحقيقة وهو في ذلك يتمتع بمطلق الحرية في قبول الدليل او طرحه جانبا اذا لم يطمئن اليه دون ان يكون مطالب بتسبيب اقتناعه[٧٨].

مشروعيه الحصول على الدليل الالكتروني:

يقصد بمشروعية التحصيل ان تتم عملية البحث عن دليل الإدانة وتقديمه للقضاء من طرف القائمين بالتحقيق وفقا للقواعد والإجراءات التي رسمها القانون لذلك فمشروعيه الدليل اذ تتطلب صدقه في مضمونة ، وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعه تدل على الامانة والنزاهة [٧٩].

ولكن مشروعية جمع الدليل الالكتروني مرتبطة بالقواعد القانونية المكتوبة فاذا ما خالفتها عدت بأنها باطله وبالتالي بطلان الدليل المستمد منها لأنه ما بني على باطل يكون باطل تصلح بأنها تكون ادله تبنى عليها الادانة في المواد الجزائية[٨٠].

المطلب الثاني: مشاكل الاثبات بالدليل الرقمي:

يقصد بمشكلات الدليل الرقمي، المشاكل الداخلية فيه والتي تتعلق به تحديدا من حيث تكوينه، كما يقصد به ايضا المشاكل الخارجية له والتي تتمثل في مدى الاعتراف به من قبل الجهات التي يجب ان تعترف به وتقبله أمامها، كجهات التحقيق والمحاكم مثلا لذلك فأن القول بوجود مشكلات الدليل الرقمي يمكن كعبارة ان تكون محل جدل او اختلاف بين الثقافات المختلفة[٨١].

اذ لا يترك المجرم المعلوماتي او الالكتروني في الكثير من الاحيان اثار تقودنا الية من اجل معاقبته، وهذا راجع لكون ان الجريمة مسرحها الشبكة العنكبوتية التي توصف بأنها عالم افتراضي، فكيف لعالم افتراضي ان يبقى على الاثر لحين اكتشافه

---

[٧٨] نفس: م س ص ١٤٠ .
[٧٩] براهيمي جمال : م س ص ١٤٤.
[٨٠] سعيداني نعيم : م س ص ٢٠١ .
[٨١] عمر أبو بكر بن يونس : م س ص ٩٨٤ .

فبدون أي شعور قد تتعرض لسرقه او تخترق المواضع دون ترك أي دليل مادي وفي هذا المطلب سنتطرق الي المشاكل التي تتعلق بالدليل المادي ومشاكل الاستدلال[٨٢].

اولا: مشاكل تتعلق بالدليل الرقمي:

١.عدم ظهور الدليل المادي:

كما اوضحنا سابقا ان الجريمة المعلوماتية تتم ببيئة لا علاقة لها بالورق والمحررات فعن طريق عمل بسيط يمكن تغير الكثير من المعلومات في وقت قصير فيصعب استخلاص الدليل المادي لهاذي الجريمة، لأنه في عالم غير واقعي ،فهناك الكثير من المواقع التي تحث على الارهاب والانتحار ولا يعرف حتى مالكها الحقيقي ،لذا فأنه لابد من وضع اجهزت مراقبه وبرامج من اجل تفادي اختراق القراصنة وتأهيل المحققين لتعامل مع المجرمين الذين يتمتعون بمؤهلات عالية فالدليل في الجريمة التقليدية مرئي على عكس الجريمة المعلوماتية التي تتم دون رؤية لدليل الادانة، حتى في حالة وجود الدليل فأنا للجاني طمسه او محوه، فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بالإبلاغ عنها ومن مبررات عدم ظهور الدليل المادي هو اننا نتعامل مع المعلومة وهذه المعلومة هي الوسيلة لاقتراف الجريمة التي كانت في الاصل فكره جسدت في قالب فني[٨٣].

٢.صعوبة تتعلق بإجراءات الحصول على دليل رقمي:

مما لاشك فيه ان هناك صعوبات تتمثل في اجراءات الحصول على الدليل الرقمي ، لان المجرمين الدين يرتكبون هذه الجرائم يتميزون بالذكاء ، فهم يضربون سياجا امنيا على افعالهم غير المشروعة حتى لا يطيلهم العقاب ويزيدون من صعوبات التفتيش باستخدامهم الكلمات السرية وشفرات الدخول بحيث لا تتمكن الجهات المختصة من الوصول الى البيانات المخزنة او المنقولة عبر شبكة الانترنت كما قد يلجا الى ادخال تعليمات خفيه بحيث يستحيل على غيرهم الاطلاع عليها[٨٤].

---

[٨٢] غرباوي نادية : م س ص ٥٣.
[٨٣] غرباوي نادية: م س ص ٥٤.
[٨٤] نداء نائل المصري : م س ص ٨٧ .

٣.سهولة اخفاء الدليل الرقمي:

في الجريمة العادية عادة يترك السارق المختلس او القاتل اثار مادية يمكن ان تستدل بها سلطات التحقيق من اجل ادانة المجرم، وبما ان الجريمة الالكترونية هي جريمة متخصصة فالمجرم المعلوماتي او الالكتروني له طبيعة خاصة ففي الكثير من الاحيان يمكنه محو ما قام به او مسح اثار الجريمة سواء عند نشر الفيروس او الاختلاس او الخرق الالي او التسلسل الى الموقع، ومن الاسباب التي تساهم في تعذر الحصول على اثار تقليديه تخلف الجريمة المعلوماتية ان الجاني نفسه يملك محو الادلة التي تدينه او تدميرها في زمن قصير جدا، وحتى لو تم ضبطه فقد ترجع هذه الجريمة الى خطاء في نظام الحاسب او الشبكة او الاجهزة[٨٥].

٤.صعوبة فهم الدليل الرقمي:

لاشك في ان طبيعة الدليل تنعكس عليه فالدليل الفني قد يكون مضمونه مسال فنيه لا يقوى على فهمها الا الخبير المتخصص ، بعكس الدليل القولي فأن الكثير ممن يتصلون به يسهل عليهم فهم مضمونه وادراك حقيقته ، واذا كان الدليل الناتج عن الجرائم التي تقع على العمليات الالكترونية قد يتحصل من عمليات فنيه معقده عن طريق التلاعب في نبضات وذبذبات الكترونيه وعمليات اخرى غير مرئية فأن الوصول اليها وفهم مضمونه قد يكون في غاية الصعوبة وتثار مشكلات عديدة في

الاثبات الجنائي ومثال ذلك ان اثبات التدليس الذي قد يقع على نظام المعالجة الالية للمعلومات يتطلب تمكين مأمور الضبط القضائي او سلطات التحقيق من جميع المعطيات الضرورية التي تساعد على اجراء التحريات والتحقق من صحتها لتأكد عما اذا كانت هناك جريمة وقعت ام لا، مثل هذا الامر يتطلب اعادة عرض كافة العمليات الالية التي تتم لأجل الكشف عن هذا التدليس وقد يستعصي هذا الامر على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة.

[٨٥] غرباوي نادية : م س ص ٥٧.

ثانيا: مشاكل الاستدلال:

كما ذكرنا سابقا فأن مشاكل اثبات الجرائم الالكترونية انها تترك أثر كما يصعب الاحتفاظ بأثار بحي تعتمد على التقنيات العالية حيث يصعب الاستدلال فيها ومع صعوبة اثباتها الا ان ما يزيد الوضع سوء هو عدم الابلاغ وايضا نقص الخبرة في هذا المجال [٨٦] .

١.عدم الابلاغ:

ان عدم الابلاغ من طرف الاشخاص الذين شاهدو المجرم عند قيامة بالجريمة هو ما يزيد في عدم اكتشاف الجريمة ومن اسبابه نجد:

عدم ابلاغ الشركات وخصوصا التجارية منها بعمليات الخرق التي يقوم بها المجرم المعلوماتي هذا الابلاغ يتسرب الى المجرم المعلوماتي وبالتالي تكشف الثغرات الامنية في النظام المعلوماتي ونقص الغطاء التشريعي لهاذي السلوكيات، قد يحدث ان يبلغ عن سلوكيات مشبوهة للمجرمين المعلوماتيين ولاكن في الكثير من الاحيان لا يمكن اكتشاف الشخص الذي قام بالسلوك الاجرامي مثلا جريمة نشر فيروس في الكثير من الاحيان لا يمكن اكتشاف الشخص الذي قام بنشره.

ومما يزيد من مشاكل عدم الابلاغ ما يلي:

أ- المعرفة المتأخرة من ان الجهاز اصيب بفيروس عن طريق الشبكة.
ب- تحويل الشبكة لساحه من المعارك بين الدول مما اصبحت المعاملات التجارية غنيمة سهله للاختراق.
ت- ضخامة الاضرار حيث ان الفيروس ليس مقيد برقعة جغرافية معينه[٨٧]

2. نقص الخبرة: ان صعوبة اكتشاف الجريمة بالدرجة الاولى مرده الى نقص خبرة المحققين مما يضعنا امام معادلة غير متكافأه طرفها اجهزت التحقيق بنقص خبرتها في مجال الكمبيوتر والانترنت الطرف الاخر قراصنة محتلون ومنحلون اخلاقيا

[٨٦] غرباوي نادية : م س ص ٥٧.
[٨٧] نفس : م س ص ٥٧.

يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية وقد وصل اسم النخبة اما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء ، ومن العوامل المساعدة في نقص الخبرة في الجرائم المعلوماتية :

أ- عدم تخصيص اموال من اجل التأهيل الجيد للمحققين وكذا حداثة. الجريمة وخصوصيتها التي لم يعتد عليها رجال الشرطة ، مما جعلهم قاصرين في مواجهتها .

ب- ضخامة المعلومات على الشبكة وانتشار اجهزت الكمبيوتر مما يصعب عملية التحقيق.

ت- الانترنت بيئة خصبة لسلوك الاجرامي.

ث- التطور السريع للتقنية الحديثة وعد وجود هيئات قضائية مختصة.

ج- وجود مواقع على الشبكة تسهل عملية ارسال البريد الالكتروني دون لحاجة الى ذكر البيانات ويمل الفقه الجنائي الى القول بضرورة تنمية الخبرة والمهارات لمتخصصين لوضع مناهج مدروسة للتدريب على التحقيق مع مراعاة خصوصية التطور التقني السريع دون اهمال التعاون الدولي في مثل هذه الحالات[٨٨]

[٨٨] غرباوي نادية : س ص٥٨ .

الـخـاتـمـة

نالت الجريمة المعلوماتية اهمية كبيرة لدى المشرعين، فهي موضوع العصر في القانون الدولي والاقليمي، حيث كان لهذا البحث اهمية كبيرة في تسليط الضوء على بعض الجرائم المعلوماتية وكذلك اجراءات التحقيق بشقيه ا لابتدائي والنهائي وقد اتضح لنا ان الجرائم الالكترونية تعد من الانماط الاجرامية الجديدة التي فجرتها حديثا ثورة تقنية المعلومات والاتصالات عن بعد والتي تتميز بخصائص مختلفة تماما عن الجرائم التقليدية، وانها من المستجدات التي لم تكن معروفه في القانون الجزائي من ثمة فأي محاولة للتعامل إجرائيا مع هذا النمط الاجرامي الجديد في إطار عملية البحث والتحقيق سوف يخلق اشكاليات اجرائية امام السلطات المكلفة بهذه العملية لذلك تعتبر هذه الدراسة بمثابة تقيم للنصوص القانونية التقليدية المطبقة على الجريمة المعلوماتية ذات الطبيعة الخاصة.

اولا: الـنـتـائــج:

١. ان الجرائم المعلوماتية اصبحت تمثل اهمية كبيرة بالمجتمع وخصوصا بعد ظهور انماط جديدة منها، بالإضافة الى ان هناك انماط شائعة الى انها تتمتع بخصوصية ومن أبرزها جريمة الدخول الالكتروني وجريمة اتلاف البيانات الالكترونية وجريمة التزوير.
٢. تثير الجريمة المعلوماتية الكثير من الصعوبات في مجال الحصول على الادلة الجنائية فالمحقق اعتاد على كون محل الجريمة شيء مادي وملموس على عكس البيئة المعلوماتية ذات الطبيعة المعنوية التي يصعب معها تطبيق
٣. يتسم التحقيق بالجرائم المعلوماتية بصعوبة وتعقيد، وذلك لعدم المام رجال الشرطة والمحققين بمجالات الحاسب الالي والانترنت، وعدم تدريبهم على آليات الوصول الى الادلة المعلوماتية والحفاظ عليها من التلف والضياع.

٤. يوجد قصور في القواعد والتشريعات الإجرائية الواجب اتباعها في مرحلة التحقيق الابتدائي ومرحلة المحاكمة.
٥. المعاينة في الجريمة الإلكترونية اقل اهمية منها في الجرائم العادية، لقلة الأثار المادية بينما الخبرة تعتبر من اهم اجراءات التحقيق في الجرائم الالكترونية وهذا ما تستدعيه طبيعة هذه الجريمة كونها تعتمد بالدرجة الأولى على وسائل مستحدثة.
٦. الدليل الرقمي مجموعة من المجالات او النبضات الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر بشكل صور او تسجيلات صوتية او مرئية.
٧. يتميز الدليل الرقمي بصعوبة محوه او تحطيمه، ويمكن كشف محاولة الجاني محو هذا الدليل الرقمي لتتخذ بذاتها دليلا ضده.
٨. تتوقف مشروعية وجود الدليل الرقمي على طبيعة نظام الاثبات ما اذا كان نظام مقيدا ام حرا ويتبنى القانون اليمني نظاما مختلطا يأخذ بنظام الادلة القانونية ، مع اعطاء القاضي سلطة واسعة لتقدير القيمة الإقناعية للدليل.

ثانيا : التوصيات:

١. ضرورة النص صراحة على الأدلة الرقمية كأدلة اثبات في المجال الجنائي والاعتراف لها بحجية قاطعة باعتبارها استثناء على سلطة القاضي الجنائي في تقدير الدليل، مع امكانية النص على وسائل التأكد من سلامة الدليل الرقمي باعتبارها شرطا لقبول هذا الدليل.
٢. النص صراحة على جواز تفتيش الوسط الافتراضي وضبط محتوياته.
٣. تفعيل دور الجهات المختصة بمكافحة الجريمة المعلوماتية بحيث يتم تأهيل افرادها للتعامل مع النظام المعلوماتي بما يمكنهم من تفتيش الوسط الافتراضي وضبط محتوياته.
٤. ضرورة تشديد العقوبات والغرامات في حال ارتكاب أي من الجرائم المعلوماتية.

٥. ضرورة قيام المشرعين في الدول المختلفة بإصدار تشريعات خاصة بالجرائم المتعلقة بالحاسب الالي، وتطوير قواعد الاجراءات الجنائية وقواعد الاثبات وذلك لأنها ذات طبيعة خاصة.

٦. ضرورة تأهيل رجال الشرطة والمحققين تأهيلا يستطيع معه كل منهم التعامل مع هذا النوع من الجرائم.

٧. ضرورة تأهيل القضاة وتدريسهم حتى يستطيعوا التعامل مع الادلة الرقمية الناتجة عن الجريمة الالكترونية وبالتالي يصبح حكمهم أكثر عدالة.

٨. التطوير المستمر لأدوات التحليل كأدوات نسخ محتويات الاقراص وتخزين البيانات.

٩. ينبغي على كافة الدول وخاصة العربية وضع نظام مراقبة عبر شبكة الانترنت يسمح بتتبع الملفات المدخلة والمخرجة وتعقب الاختراقات غير المشروعة للأنظمة وتخزينها وملاحقة مرتكبيها.

١٠.ضرورة استحداث نصوص قانونية جديدة خاصة في قانون الإجراءات الجزائية، حتى تلائم في مجال الضبط والتحقيق لعدم ملائمة الاجراءات التقليدية في مواجهة هذه الجرائم اضافة الى تحديث الاساليب الاجرائية المتبعة في الجرائم المعلوماتية، دون ان تتعرض حقوق الافراد وحرياتهم للخطر عند الاثبات في مجالها.

١١. التوعية بشكل دائم عن مخاطر الجرائم المعلوماتية واساليب المجرمين في ارتكابها عن طريق وسائل الاعلام.

١٢. واخيرا تدريس مواد الانظمة المعلوماتية والجرائم التي قد تنشأ عنها في كلية الحقوق والشرطة والمعاهد القضائية.

الـمـراجــع

أولا: التشريعات:

قانون الإجراءات الجزائية اليمني رقم١٣ لسنه ١٩٩٤

ثانيا: قائمة المراجع العامة:

١. د. عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت (الاحكام الموضوعية والجوانب الإجرائية)الناشر دار النهضة العربية، القاهرة، الطبعة الاولى 2004.
٢. د. محمد حماد بن مرهج الهيتي، جرائم الحاسوب _ماهيتها _موضوعها واهم صورها والصعوبات التي تواجهها دراسة تحليله مقارنة، دار المناهج للنشر والتوزيع، الطبعة الأولى 2006.
٣. د. خالد ممدوح إبراهيم ،الجرائم المعلوماتية ،دار الفكر الجامعي ،الطبعة الأولى ،2009.
٤. ايمن عبد الله فكري ،جرائم نظم المعلومات ،دراسة مقارنة، دار الجامعة الجديدة للنشر 2007.

ثالثا: الرسائل والاطروحات الجامعية

١. براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتورة في العلوم تخصص القانون _جامعة مولد معمري _تيزي وزو_ تاريخ المناقشة 2018 .
٢. غرباوي نادية ،أساليب البحث والتحري في الجرائم المعلوماتية أطروحة مقدمة للحصول على الماجستير، جامعة اكلي محند _ البويرة كلية الحقوق والعلوم السياسية قسم القانون العام السنة الجامعية 2017.
٣. الهام بوالطمين ،الاثبات الجنائي في الجرائم الالكترونية مذكرة لنيل الماجستير ،جامعة العربي بن مهيدي _ا م البواقي كلية الحقوق والعلوم السياسية ،السنه الجامعية2018.

٤. بخي فاطمة الزهراء، الإجراءات التحقيق في الجرائم الالكترونية مذكرة للحصول على الماجستير في الحقوق تخصص قانون جنائي _كلية الحقوق والعلوم السياسية السنة الجامعية 2014.
٥. معمش زهية ونسميه غانم ، الاثبات الجنائي في الجرائم المعلوماتية مذكرة تخرج لنيل شهادة الماجستير ،قسم القانون الخاص ،جامعة عبد الرحمن ميرة _كلية الحقوق والعلوم السياسية السنة الجامعية 2013.
٦. نداء نائل فايز المصري ،خصوصية الجرائم المعلوماتية ،مذكرة للحصول على الماجستير ،جامعة النجاح الوطنية كلية الدراسات العلياء في نابلس فلسطين 2017.
٧. صغير يوسف، الجريمة المرتكبة عبر الانترنت ،مذكره للحصول على شهادة الماجستير تخصص القانون الدولي للأعمال ،جامعة مولد معمري _تيزي وزو _ تاريخ المناقشة2013 .
٨. سلامة محمد المنصوري ،تطبيق مبدأ الاقتناع القضائي على الدليل لنيل شهادة الماجستير الالكتروني ،جامعة الامارات العربية المتحدة كلية القانون ،قسم القانون العام 2018.
٩. علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجرائم المعلوماتية دراسة مقارنة، ماجستير كلية الحقوق ،جامعة الموصل ،دار الكتب والوثائق القومية 2012.
١٠. راجح محمد غلاب ، الجرائم المعلوماتية في القانون اليمني والجزائري أطروحة مقدمة للحصول على شهادة الدكتورة فرع القانون الجنائي كلية الحقوق جامعة الجزائر 2012 .
١١. يوسف خليل العفيفي، الجرائم الالكترونية في التشريع الفلسطيني، دراسة تحليلية مقارنة ،مذكرة لنيل شهادة الماجستير في القانون العام كلية الشريعة والقانون بالجامعة الإسلامية بغزة 2013.

١٢. سعيداني نعيم ،اليات البحث والتحري في الجريمة المعلوماتية في القانون الجزائري مذكرة لنيل شهادة الماجستير ،جامعة الحاج الخضر _باتنة_كلية الحقوق والعلوم السياسية ،السنة الجامعية 2013.

ثالثا: الدراسات

١. طارق محمد الجملي ، الدليل الرقمي في مجال الاثبات الجنائي مجلة الحقوق ، كلية الحقوق جامعة بنغازي ليبيا. المجلد 12، العدد 1

٢. نديم محمد حسن الترزي، سلطات النيابة العامة في الجرائم المعلوماتية (المعاينة والتفتيش) جامعة الاندلس المجلد 15 العدد 13

رابعا: المؤتمرات

١. اعمال المؤتمر الدولي الرابع عشر ،الجرائم الالكترونية وإجراءات مواجهتها الدكتور فضيلة عاقلي ،جامعة باتنة _الجزائر طرابلس _25_3_ 2016.

الفـــهـرس

المقدمة	١
التعريف بالبحث	١
أهمية البحث	٣
اهداف البحث	٣
منهج البحث	٤
إشكالية البحث	٤
المبحث الأول: طرق الحصول على ادلة الاثبات الجنائي في الجرائم المعلوماتية	٦
المطلب الأول: المعاينة والتفتيش	٦
السلطات المختصة لمعاينة الجرائم المعلوماتية	٨
خصائص التفتيش	٩
محل التفتيش	١٠
المطلب الثاني: الضبط والخبرة	١٤
ضبط المكونات المعنوية للحاسوب	١٦
تعريف الخبرة والخبير	١٨
المبحث الثاني: استنباط الدليل الرقمي	٢١
المطلب الأول: مفهوم الدليل الرقمي ومشروعية	٢٢
المطلب الثاني: مشاكل الاثبات بالدليل الرقمي	٢٩
الخاتمة	٣٤
النتائج	٣٤
التوصيات	٣٥
قائمة المراجع	٣٧
قائمة الرموز	

تم بحمد الله