جامعة ابن خلدون– تيارت
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر
في الحقوق
التخصص: قانون جنائي
بعنوان:

الأدلة الرقمية في إثبات الجريمة الإلكترونية

إعداد الطالبة:
* هروال أية نور الهدى

تحت إشراف:
* أ/د. هروال نبيلة هبة

لجنة المناقشة		
د.عيسى علي	أستاذ محاضر (أ)	رئيسا
أ/دة. هروال هبة نبيلة	أستاذة التعليم العالي	مشرفةومقررا
د.بردال سمير	أستاذ مساعد (أ)	عضوا مناقشا
دة. بطاهر آمال	أستاذة محاضرة (أ)	عضوا مدعوا

السّنة الجامعيّة

1441 ـ 1442هـ /2020- 2021م

بسم الله الرحمن الرحيم

كلمة شكر

﴿وَأَمَّا بِنِعْمَةِ رَبِّكَ فَحَدِّثْ ﴾

بسم الله الرحمن الرحيم و الصلاة و السلام على أشرف المرسلين و على آله و صحبه إلى يوم الدين شكر إلى الرحمن الرحيم الذي وفقني في إتمام هذا العمل المتواضع ووهبني الصبر الجميل و الحمد للوهاب رب العالمين.

أشكر جزيل الشكر الأستاذة المحترمة الأستاذة الدكتورة "هروال نبيلة هبة" التي كانت لي خير سند و لم بتخل عليّ بالمعلومات و التوجيهات التي تدعم بحثي كما لا أنسى لها دعمه المعنوي في تحفيزي في إنجاز هذا العمل أطال الله في عمرها

كما أتقدم بالشكر إلى الأساتذة أعضاء اللجنة الذين وافقوا على مناقشة هذه المذكرة و إلى كل من قدم لي يد العون من قريب أو بعيد.

إهداء

بسم الله الرحمن الرحيم و الصلاة و السلام على اشرف المرسلين و على آله وصحبه إلى يوم أهدي هذا العمل إلى من هو في الدنيا سند و حبه خالد إلى الأبد إلى تاج الزمرد

إلى أبي العزيز رزقه الله الصحة والعافية وطول العمر

إلى من باركها القدير إلى من حملتني تسعة أشهر إلى من تدمع عيناي كلما ذكر اسمها

إلى من تعجز الكلمات عن وصفها و الجنة تحت أقدامها إلى من لا أنسى طول حياتي فضلها علي إلى أمي الغالية أطال الله في عمرها.

إلى من هم جزء من حياتي و بهم تكتمل سعادتي إخوتي: فتيحة– سولاف– محمد

و إلى كل من نساهم قلمي و لم ينساهم قلبي.

قائمة المختصرات

المختصر	المعنى
ق إ ج	قانون الإجراءات الجزائية
ج ر ج ج	الجريدة الرسمية للجمهورية الجزائرية
ص	صفحة
ط	طبعة
د ط	دون طبعة
د ت	دون تاريخ
د د ن	دون دار نشر
مج	مجلد
ج	جزء
د د ن	دون دار نشر
ف	فقرة
ع	عدد
P	Page

مقدمة

مقدمة:

أحدث التطور التكنولوجي تغييرا جذريا في حياة الأفراد والمجتمعات وترك تأثيراته في كل تفاصيلها، فلم يسلم أي مجال من مجالات الحياة من هذا التأثير، سواء كان ذلك بطريقة إيجابية أو سلبية، ولكن الجريمة ظاهرة من الظواهر الاجتماعية الملازمة للمجتمعات، فإنها لم تكن بمنأى عن هذا التأثير، بحيث أصبح المجرمين يرتكبون جرائمهم بوسائل تكنولوجية حديثة، وهو ما أدى إلى ظهور نوع جديد من الجرائم يخرج عن النطاق المادي الملموس الذي تقع فيه الجرائم التقليدية، وانتقل إلى النطاق الغير المادي سمته التكنولوجيا والمعلومات، فظهرت جرائم تدور وقائعها في العالم الافتراضي لا ترى بالعين المجردة، ولا وجود فيه للدم ولا للكسر ولا يترك الجناة وراءهم آثار مادية بالمعنى المتعارف عليه في مسرح الجريمة، فهذا التأثير الذي أضفاه التطور العلمي على الجريمة من حيث استخدام الوسائل التكنولوجية الحديثة في ارتكابها للجريمة، والصفات والخصائص التي يتميز بها مرتكبوها من جهة،[1] وما نجم عن ذلك من الصعوبات في عملية اكتشاف واثبات هذا النوع من الجرائم دفع إلى التفكير في البحث عن وسائل وطرق إثبات هذا النوع من الجرائم الحديثة التي تواكب هذا الطور الذي عرفته الجرائم المستحدثة، ومن بينها الجريمة المعلوماتية والتي أصبحت في الوقت الحاضر خطرا يهدد مصالح الأفراد والدول في جميع المجالات.

وبالتالي جريمة الأمس ليست كجريمة اليوم، فهذا التطور في تكنولوجيا المعلومات كما كان له أثر ايجابي، كان له آخر سلبي من خلال بروز الجرائم الإلكترونية في الميدان، مما استوجب توفير الحماية القانونية، وإيجاد نظام عقابي لمرتكبي جرائم الحاسوب وشبكة المعلومات التي رافقت نشوء ونمو وتطور نظم الحاسوب والشبكات، وثورة تقنية المعلومات لما تنطوي عليه من مخاطر عديدة

[1]-يتوقع **دون باكر** وهو من المتخصصين في الجريمة المعلوماتية، إذ يأتي اليوم الذي تصبح فيه الجريمة المؤتمنة، حيث يستطيع الفرد تحميل البرنامج الذي يريده من الانترنت أو يشتريه من موقع من مواقعه دون ذكر اسم المجرم أو عنوانه أو أية تفاصيل عنه.

وخسائر كبيرة تلحق بالمؤسسات والأفراد باعتبارها تستهدف الاعتداء على البيانات والمعلومات التي تمس الحياة الخاصة للأفراد.

ولمكافحة الجريمة الإلكترونية أصبح من الضروري إيجاد وسائل جديدة تختلف جذريا عن ما يتم استعماله في مكافحة الجريمة العادية، وذلك بسبب عجز إجراءات التحقيق التقليدية في مجريات نسق تطور هذه الجريمة، بالإضافة إلى عجز الأدلة الجنائية المادية في إثبات وقوعها، وهو ما توجب على جهات التحقيق الاعتماد على نوع جديد من الأدلة الجنائية في مجال الإثبات الجنائي تعرف بالأدلة الجنائية الرقمية.

إن موضوع الأدلة الرقمية من المواضيع التي هي في تطور مستمر، ويظهر صدق هذه الملاحظة سواء تعلقت بالدليل بنفسه أو بوسائل الوصول إلى الدليل، وعلى هذا الأساس تكمن في أنها تعالج أهمية الموضوع نوعا جديدا من الأدلة الجنائية من الناحيتين اللغوية والقانونية، تعريف الدليل الرقمي من الناحية اللغوية والاصطلاحية والقانونية، والفرق بينه وبين الدليل التقليدي ومن جهة أخرى خصائصه.

أسباب اختيار الموضوع:

الدليل الرقمي ودوره في إثبات الجريمة الإلكترونية هي رغبة منا في إثراء الدراسات الجامعية النظرية، وذلك بسبب ندرة الأبحاث والدراسات المتعلقة بتحديد الإطار المفاهيمي للأدلة الرقمية، بحيث أن هذه الأدلة يتم دراستها بشكل علمي وقانوني معمق في الجزائر، وإنما تم التطرق إليها في مؤلفات عامة بشكل مقتضب دون أن يتم الإحاطة بها.

أهداف الدراسة:

نهدف من خلال هذه الدراسة إلى إزالة الغموض عن الأدلة الجنائية الرقمية، وذلك بوضع مفهوم عام له منة خلال تعريفه وإبراز خصائصه وأنواعه، وسب كشفه وضبطه من الجانبين اللغوي

والقانوني، زيادة على ذلك معرفة مدى فاعلية الأدلة الجنائية القيمة في إثبات الجريمة الإلكترونية وتأثير ذلك على الاقتناع الشخصي للقاضي الجنائي في التشريعين.

وعليه تكون الإشكالية المطروحة كالتالي:

-ماهي الأدلة الرقمية التي تستخدم في إثبات الجريمة الإلكترونية؟

الصعوبات:

لا يفوتنا القول أنه واجهتنا صعوبات جمة في اختيار موضوع البحث في حد ذاته، كون أن هذا الموضوع 'الدليل الرقمي في إثبات الجريمة الإلكترونية' حديث لم يسبق بحثه بوضوح وتعمق، ولو أن هناك مراجع ومقالات تناولت هذا الموضوع، إلا أنها لم تعالجه من كل جوانبه أو أدرجته بشكل سطحي، إضافة إلى أن الجرائم محل الدراسة ترتبط بالحاسب الآلي بما يتطلب الإلمام بمكوناته، وبنظام المعالجة الآلية للمعلومات والشبكات الإلكترونية، وكما يحتاج الأمر إلى دراية باللغة والمصطلحات التقنية والفنية، وهذا ما يتطلب جهد كبير ناهيك عن الجهد القانوني.

المنهج المتبع:

وللإجابة على هذه الإشكالية اعتمدنا المنهج التحليلي والمقارن من خلال المزج بينهما، حيث استخدمنا المنهج التحليلي في عرض الآراء الفقهية وتحليل النصوص القانونية، كما استخدمنا أيضا المنهج المقارن في بعض الجزئيات التي تتطلب المقارنة، وذلك بين موقف التشريع اللاتيني من الأدلة الجنائية الرقمية، بالإضافة إلى الاستئناس في بعض الأحيان لموقف التشريعات الأخرى مثل التشريع الإنجليزي والأمريكي.

ولمعالجة هذا الموضوع والتصدي للإشكالية المطروحة ارتأينا تقسيم البحث إلى فصلين:

الفصل الأول جاء بعنوان 'الإطار المفاهيمي للأدلة الرقمية '، فتناولنا في المبحث الأول تعريف

الدليل الرقمي والفرق بينه وبين الدليل التقليدي وخصائص الدليل الرقمي وأنواعه، أما في المبحث الثاني فتناولنا إجراءات جمعه.

والفصل الثاني الذي جاء بعنوان "حجية الدليل الرقمي في التشريعات المقارنة وأمام القاضي الجنائي" تناولنا في المبحث الأول حجية الدليل الرقمي في التشريعات المقارنة والتشريعات الأجنبية والتشريعات العربية، وفي المبحث الثاني حجية الدليل الرقمي أمام القاضي الجنائي، وفي الختام انتهينا إلى توضيح النتائج والتوصيات التي تم التوصل إليها.

الفصل الأول

الإطار المفاهيمي للدليل الرقمي

تمهيد:

مما لا شك فيه أن الثورة العلمية بمجال نظم المعلومات والتكنولوجيا أثرت على نوعية الجرائم وتطورها بانتقالها من أرض الواقع لساحات شبكات الاتصال، فقد أثرت على أدوات وآليات الإثبات الجنائي خاصة وأن طرق الاثبات التقليدية لا يمكنها الوقوف في مواجهة هذا النوع من الجرائم المستحدثة والقائمة على التكنولوجيا بشكل كبير، وعلى هذا الأساس فقد ظهر نوع مستحدث من وسائل الإثبات يمكن الاعتماد عليها في اثبات الجرائم الإلكترونية ونسبة الجريمة إلى مرتكبها، وهو الليل الإلكتروني أو الدليل الرقمي أو غيرها من المسميات المستحدثة، ونحن في دراستنا نجد أن استخدام لفظ الدليل الإلكتروني (Electric évidence) كما جاء اللفظ في نصوص القانون الدولي، وتحديدا نص المادة الرابعة عشر من اتفاقية بودابست 2001[1]، وعدة قوانين محلية أخرى، مثل المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسب بهدف الوصول إلى الدليل الإلكتروني في التحقيق الجنائي لسنة 1994.

وللدليل الإلكتروني ذاتية خاصة تميزه عن غيره من الأدلة التقليدية، تلك الذاتية اكتسبها الدليل الإلكتروني من خصائصه المميزة عن الأدلة المعتادة، والتي ارتبطت به بحكم البيئة الرقمية التي ينشأ فيها.

وعلى أساس ما سبق ظهر لنا أن الدليل الإلكتروني كفرة تتسع كثيرا عن النظرة المعتادة للدليل التقليدي، ولذا تطرقنا في هذا الفصل على اعتماد التأصيل المفاهيمي للدليل الرقمي.[2] ومن ثمة فقد قسمناه إلى مبحثين، تناول رصد تعريف الدليل الرقمي وخصائصه في **المبحث الأول**، ونتطرق إلى أنواع الدليل الرقمي والفرق بينه وبين الدليل التقليدي في **المبحث الثاني**.

---

[1]–التقرير التفسيري لاتفاقية الجريمة الإلكترونية، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 185، بودابست في 23 نوفمبر/ تشرين الثاني، 2001م.

[2]–عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفيدرالي الأمريكي للتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية للنشر والتوزيع، القاهرة،2008، ص 04.

المبحث الأول: مفهوم الدليل الرقمي.

نظرا للطبيعة الخاصة للجرائم المتصلة بالتكنولوجيا الحديثة سواء الجرائم الإلكترونية أو الجرائم المستحدثة (التقليدية والمعتمدة على التكنولوجيا) فإثباتها بالأدلة التقليدية مثل الكتابة والشهادة وغيرها يكاد يكون مستحيلا، فلا يجوز أن يقول شخص أنه رأى آخر يخترق موقعا مثلا على حاسوبه، فتلك الجرائم تحتاج لنوعية خاصة من الأدلة تستخدم فيها الطبيعة التقنية الناجمة عن أجهزة الحاسوب، والتي تمثل في الأدلة الإلكترونية، وبمعنى آخر تقوم عملية الإثبات الجنائي لجرائم التكنولوجيا أو الجرائم الإلكترونية على الدليل الرقمي، إذ يعد الوسيلة الوحيدة لإثبات تلك الجرائم، وهو محور بحثنا.

المطلب الأول: تعريف الدليل الرقمي والفرق بينه وبين الدليل الجنائي التقليدي.

سنعرض في هذا المطلب الدليل في اللغة، الدليل الإلكتروني اصطلاحا، الدليل في الفقه الشرعي، الدليل الإلكتروني في الفقه القانوني.

الفرع الأول: تعريف الدليل الرقمي.

سوف نتطرق في هذا الفرع إلى تعريف الدليل الرقمي في اللغة (أولا)، واصطلاحا (ثانيا)

أولا: تعريف الدليل الرقمي لغة.

الدليل في اللغة مأخوذ من دل يدل دلالة[1]، وقد دل على الطريق يدله دلالة ودلالة ودلولة والفتح أعلى، يدل دلا ودلالة فاندل، ودللته فاندل، واندلت بالألف لغة، وأدلة على الطريق: دله عليه[2] وهو ما يستدل به، والدليل هو الدال، ويقال: دله على الطريق أي أرشده، والاسم الدال

[1]-الصحاح للجوهري (دلل)، 1698/4، لسان العرب لابن منظور (دلل)، 248/11.

[2]-أحمد رضا، معجم متن اللغة، (دل)، 443/2.

مع تشديد اللام فلانا أي يثق به، فالدليل في اللغة هو المرشد وما به الارشاد والجمع أدلة ومفرده دليل[1]، وقال الجرجاني: "الدليل هو ما يلزم من العلم به العلم بشيء آخر"[2].

ويطلق الدليل في اللغة على عدة معان منها:

المعنى الأول: يطلق الدليل ويراد به: المرشد جاء في لسان العرب (الإرشاد: الهداية والدلالة)، وفيه كذلك (...في أسماء الله الحسنى الرشيد: وهو الذي أرشد الخلق إلى مصالحهم أي هداهم ودلهم عليها، فعيل بمعنى مفعل).

وأرشده: (أي: هداه ودله).

وفي لسان العرب أيضا: (ودله على الشيء يدله دلا ودلالة فاتدل: سدده إليه) وفيه أيضا: الدليل والدليلي: الذي يدلك.

المعنى الثاني: ويطلق الدليل ويراد به، ما به الإرشاد، وهو العلامة المنصوبة من الأحجار وغيرها لتعريف الطريق.

وجاء في لسان العرب: الدليل ما يستدل به، وفي الصحاح للجوهري الدليل: ما يستدل[3].

ثانيا: الدليل الإلكتروني اصطلاحا.

وهو ما يلزم من العلم به شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة[4].

---

[1]-الفيروز آبادي، القاموس المحيط، حرف الدال، ج1، ص 180.

[2]-عبد القاهر الجرجاني، كتاب التعريفات، ص 76.

[3]-عبد الرحمن بن محمد بن عبد الله العجلان، الدليل عن الأصوليين (حقيقته وتقسيماته)، رسالة مقدمة لنيل درجة الماجستير، جامعة الغمام محمد بن سعود الإسلامية، 1415هـ، ص 20.

[4]-د. أحمد أبو القاسم، الدليل الجنائي ودوره في إثبات جرائم الحدود والقصاص، بحث منشور بالمركز العربي للدراسات الأمنية والتدريب، الرياض، 1991، ص 174.

الإلكتروني: ويقصد بكلمة الإلكترونية (Electronique)الجسيمات السالبة الشحنة والمتناهية الصغر تنبعث من المهبط بتأثير اصطدام أيونات الغاز الموجبة به.

الموجات الكهرومغناطيسية: هي صورة تنشر فيها أنواع الطاقة في الفراغ على شكل مجالين مترددين أحدهما كهربائي والآخر مجال مغناطيسي في مستويين متعامدين على بعضهما وعمودين على اتجاه انتشار الموجات[1].

من المفاهيم اللغوية السابقة، يظهر لنا أن الموجات الإلكترونية عبارة عن مجموعة من الدوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة، ولا تدرك بالحواس البشرية الطبيعية، وتنتقل عبر الأجواء بتفاعل علمي محدد، تتواجد بمحل الاستقبال مثل الهاتف أو الحاسب الآلي وغيرهما من الأجهزة الإلكترونية والرقمية الحديثة، بشكل جعل بعض رجال القانون يعرفون الدليل الإلكتروني بأنه :"الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة[2] .

وكلمة الدليل عموما لدى فقهاء القانون تتمثل في البرهان أو الحجة التي تظهر صحة واقعة ما أو تنفيها، وقيل في معناه أنه الوسيلة التي تمكن القاضي من التوصل للحقيقة المنشودة فيما يعرض أمامه من وقائع محددة بغرض إعمال القانون عليها، وعرفه البعض بأنه: "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها".

وقيل أيضا أن الدليل هو: "الواقعة التي يستمد منها القاضي البرهان على اثبات قناعته بالحكم الذي ينتهي إليه"[3].

---

[1]-حسن مصطفى، مقال منشور على الإنترنت متاح على الرابط التالي:
-www.sudanradio.inf/php/ub.353/showthread.ph2p=1548langi=2.

[2]-أحمد بن عبد الله الرشودي، حجية الوسائل الإلكترونية في الإثبات الجنائي (دراسة تأصيلية مقارنة تطبيقية)، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه فلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2008، ص 250.

[3]-د. مأمون سلامة، الإجراءات الجزائية في التشريع المصري، دار النهضة العربية، ط1، القاهرة، 1981، ص418.

والناظر لتعريفات الدليل السابقة يجد أن استخدام مصطلح الواقعة للدلالة على الدليل غير دقيق، فالواقعة هي الجريمة نفسها لا الدليل، وأما الوسيلة فتطلق على ما يتوصل به وهو عمل الدليل.

ويعرف الدليل الجنائي عموما على أنه: "معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية ووسائل فنية ومادية أو قولية ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة أو فعل أو شيء أو شخص له علاقة بالجريمة أو جاني أو مجني عليه"[1].

ثالثا: الدليل الإلكتروني قانونا.

لقد عرفت بعض التشريعات الدليل الإلكتروني والتي سنذكرها كالآتي:

01-التشريع الأمريكي:

بالنسبة للولايات المتحدة الأمريكية، قد تناولت بعض قوانينها مسألة قبول الدليل الجنائي الرقمي، ومثال ذلك ما نص عليه قانون الحاسب الآلي الصادر في سنة 1984 في ولاية أيوا، وتشترط محاكم الولايات المتحدة الأمريكية لقبول الأدلة الرقمية بصفة عامة أن يكون جهاز الحاسب الآلي يؤدي وظائفه بصورة سليمة، وعليه يقوم القضاء بتحديد مصداقية الدليل عن طريق إخضاعه لاختيار "داور بورت" والذي هو عبارة عن اختيار قانوني لتقرير صلاحية الدليل العلمي وصلته بالواقعة الإجرامية.

02-التشريع المصري:

اتخذ التشريع المصري نهج التشريعات اللاتينية ويعتمد هذا النظام على وسائل الإثبات التي يتقيد القاضي الجنائي بها، فتركت حرية الإثبات لأطراف الخصومة أن يقدموا كل ما هو مناسب لاقتناع القاضي الذي يبني في الإثبات عقيدته من أي دليل مطروح أمامه، ويتضح من خلال ذلك

[1]-سالم بن حامد بن علي البلوي، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض،2099، ص 42.

بأن القاضي يقوم بتقدير كل دليل مطروح أمامه لأن مبدأ الحرية والاقتناع لدى القاضي هي تقدير الأدلة.

03-التشريع الجزائري:

المشرع الجزائري أخذ بالنظام الحر من خلال استقراء نص المادة 212 قانون الإجراءات الجزائية وكذا نص المادة 307 منه،[1] وبالرجوع إلى نص المادة 212 قانون الإجراءات الجزائية أجاز فيها المشرع الإثبات الجنائي بأي طريق من طرق الإثبات وضع القاضي حرية في تقدير الدليل بناء على اقتناعه الشخصي.

الفرع الثاني: الفرق بين الدليل الرقمي وبين الدليل التقليدي.

لمعرفة الفرق بين الدليل الرقمي والدليل التقليدي لابد من التطرق إلى أوجه التشابه، وأوجه الاختلاف بين كلا الدليلين، وهذا ما سنوضحه من خلال الآتي:

أ-أوجه التشابه:

-كلاهما دليل إثبات يعتد به في المجال الجنائي ويساعد على إثبات الجريمة.

-كلاهما يستخلص من الجريمة.

-كلاهما يهدف إلى إثبات الحقيقة القضائية الحقة.

[1] - الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية، العدد 48، المؤرخة في 10 جوان 1966، المعدل بالأمر رقم 15-02 المؤرخ في 23 جويلية 2015 المتضمن قانون الإجراءات الجزائية، ج ر ج ج ، العدد 40، المؤرخة في 23 جويلية 2015.

ب- أوجه الاختلاف:

1- من حيث التعريف:

الأدلة التقليدي:

هي الأدلة التي يتقيد بها القاضي، وتكون كأصل عام مقبولة في كافة المواد (قانون تجاري، قانون بحري، قانون الأحوال الشخصية...) تتمثل في: الكتابة، الإقرار، القرائن، اليمين الحاسمة، فالقاضي ليست له سلطة تقديرية بشأنها في حال توافر شروطها.

الدليل الرقمي:

دليل مستخلص من أجهزة الحاسوب الآلي وملحقاته أو شبكة الانترنت أو أي جهاز آخر له خاصية معالجة أو تخزين المعلومات، وهو عبارة عن مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة بمكن الاعتماد عليها في مرحلة التحقيق.

2-من حيث الإجراءات:

-الأدلة التقليدي:

وضع المشرع إجراءات للوصول إلى الغاية المنشودة والتي تتمثل في: المعاينة، الخبرة، الضبط، التفتيش.

الدليل الرقمي:

وسائل إجرائية حديثة تستخدم في جمع الأدلة الجنائية الرقمية، فهي إجراءات تستعمل أثناء تنفذ طرق التحقيق الثابتة والمحددة.

تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها:

-حفظ المعطيات

-التسرب واعتراض المراسلات الإلكترونية.

-المراقبة الإلكترونية.

3-من حيث الأنواع:

الدليل التقليدي:

يتمثل في: الدليل الكتابي، المحررات، المحاضر، الاعتراف، الشهادة، القرائن.

الدليل الرقمي:

صناعة الفيروسات ونشرها. سرقة أجهزة أو مكونات أو معلومات وما في حكمها، الغش أو التغيير في المواصفات والخصائص تقنية المعلومات.

04-من حيث القانون المطبق:

الدليل التقليدي:

قانون الإجراءات الجزائية.

الدليل الرقمي:

قانون الإجراءات الجزائية والقوانين الخاصة، مثلا القانون 09-04 .

05-من حيث الطبيعة:

الدليل التقليدي:

جهاز الشرطة، الضبطية القضائية، شرطة عادية.

الأقطاب المتخصصة تنظر في مدى قبول هذا الدليل

الدليل الرقمي:

ضبطية قضائية مختصة في مكافحة هذه الجرائم، وتعدد هذه التسميات بين شرطة الأنترنت أو الشرطة الإلكترونية. تعتمد على تخصص رجال القضاء في الإلكترونيات.

المطلب الثاني: خصائص الدليل الرقمي وأنواعه.

إن البينة الرقمية التي يعيش فيها الدليل الإلكتروني بينة مطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكون دليلا للإدانة أو البراءة، وقد يعكس هذا العالم الرقمي على طبيعة هذا الدليل مما يجعله يتصف بعدة خصائص ميزته عن الدليل الجنائي التقليدي وهي كالآتي:

الفرع الأول: خصائص الدليل الرقمي.

يتميز الدليل الرقمي بجملة من الخصائص تميزه عن غيره من الأدلة والتي نوردها كالآتي:

أولا: الدليل الجنائي الرقمي دليل علمي وتقني.

يتكون هذا الدليل من البيانات والمعلومات ذات أدلة جنائية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بالأجهزة والمعدات، وأدوات الحسابات الآلية، واستخدام نظم برامجية حاسوبية، وهو يحتاج إلى مجال تقني يتعامل معه، وهذا لا يعني أنه كدليل يحتاج إلى البيئة التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الجنائي الرقمي، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة الكاملة وفقا لقاعدة في القانون المقارن 'إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة'، إذا كان الدليل العلمي له منطقه الذي لا يجب أن يخرج عليه، إذ يستبعد تعارضه مع القواعد العلمية السليمة، فإن الدليل الجنائي الرقمي له ذات الطبيعة، فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه[1].

فهو مستوحى من البيئة التي يعيش فيها وهي البيئة الرقمية والتقنية وتتمثل هذه الأخيرة في إطار الجرائم الإلكترونية في العالم الافتراضي، وهذا العالم يتمثل في كل من أجهزة الحاسوب

[1]– عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، 2006، ص 969.

الآلي... والشبكات بمختلف أنواعها، الأدلة الرقمية ليست مثل الدليل العادي، فلا تنتج التقنية..به اكتشاف القائل أو اعترافا مكتوبا أو بصمة أصبع...، وإنما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل منة مكان لآخر عبر شبكات الاتصال متعدية حدود الزمان والمكان.

ثانيا: الدليل الرقمي يصعب التخلص منه وقابل للفصل.

وتعد من أهم خصائص الدليل الإلكتروني بل أنه يمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة الرقمية [1]، حيث يمكن التخلص بكب سهولة من الأوراق والأشرطة المسجلة إذا حملت في ذاتها إقرار بارتكاب الشخص لجرائم، وذلك بتمزيقها وحرقها، كما يمكن أيضا التخلص من بصمات الأصابع بمسحها من موضعها، بالإضافة غلى أنه في بعض الدول الغربية يمكن التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة، هذا الأمر بالنسبة للأدلة التقليدية، أما بالنسبة للأدلة الرقمية فإن الحال غير ذلك، حيث يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها مما يؤدي إلى صعوبة الخلاص منها، لأن هناك العديد من البرامج الحاسوبية وظيفتها استعادة البيانات التي تم حذفها أو إلغائها مثلO Sorescue Bosc.v4.05 RecoverLost Data[2]سواء تم هذا الإلغاء بالأمر (Delete) أو عن طريق إعادة تهيئة أو تشكيل للقرص الصلب (Hard Disk) باستخدام الأمر (Format)، سواء كانت هذه البيانات صورا أو رسومات أو كتابات أو غيرها، كل ذلك يشكل صعوبة اخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة، طالما علم رجال

[1]-يتشابه الدليل الإلكتروني مع الدليل العلمي أو ما يطلق عليه DNA ولذلك لاتخاذها في خصوصية صعوبة التخلص منها من ناحية، ومن ناحية أخرى يمكن إحداث تعديل في تكوينها.

[2]-لمزيد من التفصيل حول هذه البرامج أنظر الموقع التالي:
Htt://Edu.arabsgate.com/shouthread.php ?t=502020.

البحث والتحقيق الجنائي بوقوع الجريمة، بال إن نشاط الجاني لمحو الدليل يشكل كدليل أيضا، نسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا كدليل[1].

حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة الأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الادلة الأخرى (التقليدية)، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق نسخ طبق الأصل من الدليل[2].

ومثل هذا الأمر لاحظه المشرع البلجيكي فقام بتعديل قانون التحقيق الجنائي Code d'instruction criminelle. بمقتضى القانون المؤرخ في 28 نوفمبر 2000، حيث تم إضافة المادة (bis29) التي سمحت بضبط الأدلة الرقمية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية[3].

-يمتاز الدليل الالكتروني بالسعة التخزينية العالية، فآلة الفيديو الرقمية، يمكنها تخزين مئات الصور، وسك صغير يمكنه تخزين مكتبة صغيرة...إلخ[4].

-الدليل الإلكتروني يرصد معلومات عن الجاني ويحللها في ذات الوقت، حيث يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

---

[1]- ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، مج5، المنعقد في: 10، 12 مايو 2003، ص 2240.

[2]-عبد الناصر محمد محمود فرغلين د. عبيد سيف سعيد المسماري، ورقة بحثية مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية وللطب الشرعي، 'الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية'، دراسة تطبيقية مقارنة، الرياض، المنعقد في الفترة: 02، 1148/11/04هـ الموافق لـ: 12، 2007/11/14.

[3]- عمر محمد أبو بكر بن يونس، مرجع سابق، ص 970.

[4]- ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، وعبد الله عبد العزيز، مرجع سابق، ص 2241.

الفرع الثاني: أنواع الدليل.

إن التعريف بالدليل الرقمي يحتم علينا تحديد أنواعه وأشكاله حتى يتسنى فهم الهيأة التي يتخذها للحكم على قيمته القانونية فيما بع، ولذا سنتناول أولا أنواع ثم نحدد الأشكال التي يبدو عليها هذا الدليل وذلك على النحو التالي:

أولا: أنواع الدليل الإلكتروني: يمكن تقسيم الدليل الرقمي إلى نوعين رئيسيين:

أ- أدلة أعدت لتكوين وسيلة الإثبات.

هذا النوع من الأدلة الرقمية يمكن إجمالها فيما يلي:

1-اسجلات التي يتم انتشارها بواسطة الآلة تلقائيا، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي[1].

2-السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة ويتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

ب- أدلة لم تعد لتوكين وسيلة الإثبات.

وهذا النوع من الأدلة الإلكترونية نشأ دون إرادة شخص، أي أنها أثر يتركه الجاني دون أن يكون راغبا في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وفيما يمكن تسميته أيضا بالآثار المعلوماتية الرقمية[2]، وهي تتجسد في الآثار التي يرتكبها مستخدم الشبكة بسب تسجيل

[1]-خالد ممدوح إبراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على الانترنت، ص2. نقلا عن الموقع الإلكتروني: http://www-f-law.net اطلع عليه بتاريخ: 2016/04/22، على الساعة: 14:30.

[2]-ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر الأعمال المصرفية والإلكترونية، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة التجارة والصناعة دبي، في الفترة من10، 2003/05/12، مج5، ص 2237.

الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال آلة أو شبكة المعلومات العالمية[1].

والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تجري عبر الانترنت والمراسلات الصادرة عن الشخص أو التي يتلقاها كلها يمكن ضبطها بواسطة تقنية خاصة بذلك[2] وتبدو أهمية التميز بين هذين النوعين فيما يلي:

1-النوع الثاني من الأدلة الإلكترونية هو الأكثر أهمية من النوع الأول لكونه يعد أصلا ليكون أثر لمن صدر عنه، ولذا فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.

2-يتميز النوع الأول من الأدلة الإلكترونية بسهولة الحصول عليه لكونه قد أعد أصلا لأن يكون دليلا على الواقعة التي يتضمنها، في حين يكون الحصول على النوع الثاني من الأدلة باتباع تقنية خاصة لا تخلو من صعوبة وتعقيد.

3-لأن النوع الأول قد أعد كوسيلة إثبات لبعض الوقائع فإنه عادة ما يعمد إلى حفظه للاحتجاج به لاحقا وهو ما يقلل من إمكانية فقدانه، وعلى عكس النوع الثاني حيث لم يعد ليحفظ ما يجعله عرضة للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز مثلا.

---

[1]- ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز ، المرجع السابق، ص 2237.

[2]-حيث يتم الاعتماد في ضبط هذا النوع من الأدلة على ما يعرف بـ: بروتكول p والذي يمكن من ضبط تحركات مستخدم الشبكة تحدي الجهاز الذي يمكن من ضبط تحركات مستخدم الشبكة تحدي الجهاز الذي يستعمله من خلال بيانات الجهاز عند مزود الخدمة، راجع في ذلك: عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والانترنت، دراسة معمقة في جرائم الحاسب الآلي والانترنت، مصر، بهجات للطباعة والتجليد، 2009، ص 63، 64.

وهذا النظام لا يحدد شخصية مرتكب الجريمة، وإنما يحدد الجهاز الذي استعملت منه، ويرى البعض أن ذلك يصلح كقرينة لاعتبار صاحب الجهاز مرتكب للجريمة إلى أن يثبت العكس، راجع د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت، مصر، دار الكتب الوطنية، 2006، ص 108-109.

ثانيا: أشكال الدليل الإلكتروني: يتخذ الدليل الإلكتروني ثلاثة أشكال رئيسية هي الصورة الرقمية، التسجيلات، النصوص المكتوبة، وسنتناول هذه الأشكال على النحو التالي:

أ-الصورة الرقمية: هي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقديم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تتمثل في التكنولوجيا البديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطورا ولكنها ليست بالصورة الأفضل من الصور التقليدية[1].

ب-التسجيلات الصوتية: وفي التسجيلات التي يتم ضبط تخزينها بواسطة الآلة الرقمية وتشمل المحادثات الصوتية على الانترنت والهاتف...إلخ.

ج-النصوص المكتوبة: وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية، ومنها الرسائل عبر البريد الإلكتروني، والهاتف المحمول، البيانات المسجلة بأجهزة الحاسب الآلي...إلخ.

[1]-ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005، ص 09-10، وتجدر الإشارة إلى أن الفارق بين النوعين هو فارق تقني يتعلق بالأسلوب الذي تعمل به كلا الآليتين.

المبحث الثاني: إجراءات جمع الدليل الرقمي وحجيته في الإثبات الجنائي أمام القضاء الجنائي.

في إطار البحث عن سياسة ناجحة لمكافحة الجرائم المستحدثة ومنها الجريمة المعلوماتية والتغلب على تحدياتها قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006والذي تم من خلاله موائمة وتكييف بعض نصوصه مع خصوصية هذه الجرائم، بالإضافة إلى إصداره للقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، [1] الذي تضمن نصوصا إجرائية مستحدثة تتوافق مع الطبيعة التقنية للجريمة المعلوماتية واستحداث هيئة خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

إن تكييف الإجراءات التقليدية مع خصوصية الجريمة المعلوماتية، واستحداث أساليب خاصة بالبحث والتحري من أجل مواجهة الجريمة الإلكترونية يعد من الآليات التي اعتمدتها العديد من التشريعات المقارنة وأوصت بها الإتفاقية الأوروبية لمكافحة المجرم الإلكتروني "اتفاقية بودابست" وهو نفس المنهج الذي اعتمده المشرع الجزائري أيضا والذي تبلور من خلال تعديل بعض النصوص القائمة لاسيما قانون الإجراءات الجزائية، وسن تشريع خاص بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال.

كما أنه تم إسناد سلطة النظر والفصل في هذه القضايا لجهات قضائية متخصصة، وهذا الذي سنتناوله في هذا الفصل والذي قسمناه كالآتي:

المطلب الأول: إجراءات الجمع بين الأحكام التقليدية والأحكام الإجرائية.

المطلب الثاني: مدى حجية الدليل الرقمي في إثبات الجريمة.

[1] – القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من جرائم الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 غشت 2009، ج ر ج ج، العدد47.

المطلب الأول: إجراءات الجمع بين الأحكام التقليدية والأحكام الإجرائية.

إن خصوصية الجريمة الإلكترونية وذاتية الدليل الإلكتروني سيقودان دون شك إلى تغيير كبير غن لم يكن كليا في مفاهيم سائدة حول إجراءات الحصول على هذا الدليل، وذلك نتيجة لضالة دور بعض الإجراءات التقليدية في بيئة التكنولوجيا المعلوماتية كالمعاينة أو الشهادة مثلا، وبالتالي يقودنا إلى إتباع نوع مستحدث من إجراءات تتلائم وطبيعة هذه البيئة.

وعلى هذا الأساس سنتناول في هذا المبحث الإجراءات التقليدية لجمع الدليل الإلكتروني في **الفرع الأول**، ثم نتطرق إلى الإجراءات الحديثة لجمع هذا الدليل في **الفرع الثاني**.

الفرع الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني.

نضم المشرع كيفية استنباط الدليل عن طريق إجراءات يتم من خلالها الوصل إلى الغاية المنشودة، وأهم هذه الإجراءات كما بينها القانون هي المعاينة، والخبرة، والضبط، والتفتيش التي تستخدم بصفة عامة لجمع الدليل في الجرائم التقليدية والمستحدثة. وهذا ما سنتطرق إليه بنوع من التفصيل من خلال الآتي.

أولا: المعاينة.

يقصد بالمعاينة: "فحص شيء، أو شخص له علاقة بالجريمة" [1]، وكما تعرف أيضا: "أنها عبارة عن رؤية وإثبات الآثار المادية التي خلّفها مرتكب الجريمة، بهدف المحافظة عليها خوفا من إتلافها وفقدانها"[2]

[1] – علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية، الموصل، 2012، ص32.

[2] – بوعناد فاطمة الزهراء، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة الدراسية للقانون، العدد 01، جامعة الجيلالي اليابس، سيدي بلعباس، 2013، ص 67.

وعرّفها جانب من الفقه بأنها: "عبارة عن رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته، وضبط كل ما يلزم لكشف الحقيقة"[1]

والمعاينة في علم التحقيق الجنائي هي عبارة عن مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له، سواء بالكتابة أو بالرسم التخطيطي أو بالتصوير لإثبات حالته بالكيفية التي تركها الجاني.[2]

من خلال هذه التعاريف نجد أن المعاينة تعتبر أهم إجراء من إجراءات التحقيق عن كيفية ارتكاب الجرائم، وكما تقدم للمحقق صورة حقيقية عن مكان وقوع الجريمة، تختلف المعاينة في قانون الإجراءات الجزائية عن المدني، بحيث أن المعاينة إجراء يتولى قيامها كل من الخبير والمحضر القضائي.

بالإضافة إلى نص المادة 146 من قانون الإجراءات المدنية والإدارية [3] التي تنص على: «**يجوز للقاضي من تلقاء نفسه أو بطلب من الخصوم القيام بإجراء معاينات أو تقديرات أو إعادة تمثيل الواقع التي يراها ضرورية مع الانتقال إلى عين المكان إذا اقتضى الأمر ذلك**»

أما المادة 79 من قانون الإجراءات الجزائية [4] تنص على: «**يجوز لقاضي التحقيق الانتقال إلى مكان وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في موافقته**»

---

[1] – بوعناد فاطمة الزهراء، المرجع السابق، ص 67.

[2] – طاهيري عبد المطلب، المرجع السابق، ص35.

[3] – القانون رقم 08-09 المؤرخ في 18 صفر عام 1429هـ الموافق لـ 25 فبراير 2008، يتضمن قانون الإجراءات المدنية والإدارية، الصادر في 02 مارس 2008، ج ر ج ج، العدد 11، الصادرة في 03 مارس 2008.

[4] – الأمر رقم 66-155 المؤرخ في 18 صفر عام 1436هـ الموافق لـ 08 يونيو 1996، يتضمن قانون الإجراءات الجزائية المعدل والمتمم، ج ر ج ج، العدد 48، الصادرة في 11يونيو1966، المعدل والمتمم بالقانون رقم 17-07 المؤرخ في 27مارس2017، ج ر ج ج، العدد 48، الصادرة في 29 مارس 2017.

من خلال هذه المادة نلاحظ أن المعاينة في الإجراءات الجزائية يتولى القيام بها النيابة العامة وقضاة التحقيق.

والمعاينة في الأصل يتم الانتقال إلى محل الجريمة، أما فيما يخص جرائم الانترنت والجرائم الإلكترونية يتم عن طريق العالم الافتراضي، بحيث يستطيع المحقق القيام بالمعاينة من المحكمة من خلال الحاسب الآلي، أو من مقر مزود بالخدمة ويعتبر أفضل مكان للقيام بالمعاينة، وكما يجب على المكلف بالقيام بالمعاينة أن يعجل في إجرائها، وذلك تفاديا لفقدان الأدلة، [1] وللمعاينة أهمية كبيرة تتمثل في أمرين:

الأول: يتمثل في جمع الأدلة عن الجريمة.

الثاني: يتمثل في وقوف المحقق أمام مسرح الجريمة للتحقيق عن كيفية وقوع الجريمة، لذلك يعتبر المعاينة الدليل المباشر الذي يطمئن إليه المحقق باعتبارها تؤدي للوصول إلى الحقيقة.

إلا أنه رغم أهميتها في الجرائم التقليدية فهي تملك نفس الأهمية في مجال الحصول على الدليل الرقمي، وذلك لأن الجرائم الإلكترونية غالبا ما ترتب أثارها، أما الدليل الرقمي فهو دليل غير مرئي، وكذلك سهولة إزالة الدليل وذلك لتعديله أو محوه.

وكما انه هناك حالات إستثنائية لا يلزم أن يكون المعاينة فيها مثلا جريمة السب العلني تقع بالقول فقط.

01- كيفية إجراء المعاينة في مسرح الجريمة.

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة، لأن هذا الأخير حجر الزاوية في التحقيق الجنائي، ومكمن الآثار والأدلة المادية، وينبغي التعامل في هذا الإطار مع مسرح الجريمة الإلكترونية على أنه مسرحان هما:

[1] – حسن محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة دكتوراه في الحقوق، جامعة عين شمس، 2000، ص 154.

-مسرح تقليدي: ويقع خارج بيئة الحاسوب والأنترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، قد يترك فيها الجاني آثار عدة، كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

-مسرح افتراضي: ويقع داخل البيئة الإلكترونية، ويتكون من البنايات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله.

وإذا كانت عملية الانتقال إلى المسرح التقليدي يتم بطريقة مادية، فالأمر يختلف بالنسبة إلى المسرح الافتراضي، حيث يستطيع عضو سلطة التحقيق أو مأمور الضبط القضائي أن يقوم بهذه المعاينة، وهو جالس في مكتبته من خلال الحاسوب موضوع في المحكمة، كما يمكنه أن يلجأ إلى بعث الخبرة القضائية أو إلى الخبرة الاستشارية أو إلى مقهى الأنترنت، ويمكنه اللجوء أيضا إلى مقر مزود الأنترنت الذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة.[1]

ونتيجة الاختلاف مسرح الجريمة الإلكترونية عن غيره من الجرائم لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، لذلك ينبغي تعامل خاص معه، ويكون ذلك من خلال إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية أبرزها ما يلي:

1-توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة المتوقع مداهمتها وشبكات الاتصال الخاصة بها.

2- إعداد خريطة للموقع الذي يتم الإغارة عليه، وإعداد خطة للهجوم على ذلك المكان، وتكون موضحة بالرسومات.

[1] - عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، مصر، 2004، ص 23.

3-إعداد فريق التفتيش من المتخصصين، على أن يكون هذا الفريق مرفقا بالأمر القضائي اللازم للقيام بالتفتيش، لأن أغلب الجرائم الإلكترونية تكون داخل أمكنة لها خصوصياتها.[1]

4-الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل، مثل برنامج معالجة الملفات، وبرنامج النسخ، وبرنامج (encase) الذي ينتج صورا مطابقة من القرص الصلب، ويستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفيدرالية الأمريكية ويسميها الخبراء حقيقة الأدلة الرقمية.

تأمين التيار الكهربائي من الانقطاع المفاجئ، لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء علق جهاز الكمبيوتر، وبالتالي فقدان كافة العمليات التي كان يتم تشغيلها واتصالات الشبكة والأنظمة الثابتة.

02- إجراءات المعاينة التي يتم أمام مسرح الجريمة للعالم الافتراضي.

-القيام بتصوير جهاز الحاسب الآلي، وكل ما يتصل به من أجهزة ظرفية ومحتويات الذي بواسطته ارتكبت الجرائم.

- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص التي يخففها ولوج النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في الحوار.

- الاستعانة بأهل الخبرة عند الضرورة. ويسميها الخبراء "حقيقة الأدلة الرقمية".

[1] - محمد الأمين البشيري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط 1، 2004، ص 59.

-تأمين التيار الكهربائي من الانقطاع المفاجئ، لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء غلق جهاز الكمبيوتر، وبالتالي فقدان كافة العمليات التي كان يتم تشغيلها واتصالات الشبكة والأنظمة الثابتة.[1]

03- إجراءات المعاينة التي يتم أمام مسرح الجريمة للعالم الافتراضي.

-القيام بتصوير جهاز الحاسب الآلي، وكل ما يتصل به من أجهزة ظرفية ومحتوياته الذي بواسطته ارتكابه الجرائم.[2]

- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص التي يخففها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في الحوار.[3]

-الاستعانة بأهل الخبرة عند الضرورة.

[1] – قد لا يكون فقدان هذا الدليل أمرا هاما عند التعامل مع أجهزة الكمبيوتر الشخصية (personal computer) حيث يمكن تخزين المعلومات في الذاكرة العشوائية (Ram Slack) أو الذاكرة الظاهرة (virital merrory) في شكل ملفات (swap and page files).ينظر: ممدوح عبد المطلب، البحث والتحقيق الجنائي الرقمي، المرجع السابق، ص115.

[2] – هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية 'دراسة مقارنة'، مكتبة الآلات الحديثة، أسيوط، 1994، ص60.

[3] – سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الأنترنت)، دار النهضة العربية، مصر، 2007، ص 290. وينظر: عبد الفتاح بيومي حجازي، المبادئ الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، الإسكندرية، ط1، 2006، ص104.

ثانيا: الخبرة.

الخبرة القضائية هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية عملية خاصة، [1] إذن فالخبرة وسيلة لتحديد التفسير الفني للأدلة للاستعانة بالمعلومات العلمية، فهي في تحقيقها ليست دليلا مستقلا وإنها في تقييم فني لهذا الدليل،[2]وعليه ما أهمية الخبرة في مجال استخلاص الأدلة الرقمية؟

01- أهمية الخبرة في الكشف وتحليل الدليل الجنائي الرقمي.

الخبير هو شخص مختص فنيا في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ويستطيع من خلال ما لديه من معلومات وخبرة إبداء الرأي من أمر من الأمور المتعلقة بالقضية التي تحتاج إلى خبرة فنية خاصة، [3]وإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر ضروري، فالاستعانة به في مجال الجريمة المعلوماتية أكثر من الضروري، [4] وذلك بسبب أن عملية استخلاص الأدلة الجنائية الرقمية يتطلب مهارة ودراية كبيرة في مجال الحاسب الآلي، ولهذا كان لزاما أن يتم اللجوء إلى خبير فني ومتخصص.[5]

ونظرا لطبيعة عمل الخبير في هذا المجال، اهتم المشرع الجزائري مثل المشروع الفرنسي في تنظيم أعمال الخبرة وكيفية اللجوء إليها وذلك من خلال المواد من 143 إلى المادة 156 من قانون الإجراءات الجزائية الجزائري، بحيث نصت المادة 143 من نفس القانون: «**أنه لجهات**

---

[1] – فاطمة زهرة بوعنان، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد 01، الجزائر، 2013، ص 68.

[2] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 29.

[3] – خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، ط1، 2009، ص 85.

[4] – نعيم سعداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص 53.

[5] – ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية –دراسة تأصيلية تطبيقية– رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، كلية الدراسات العليا، السعودية، 2012، ص 156.

التحقيق أو الحكم عندما تعرض لها مسألة ذات الطابع الفني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها»

ومن جهة أخرى نص المشرع الجزائري من خلال نص المادة 05 في فقرتها الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنه: «**يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية لعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تضمنتها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها**»

وعليه يمكن القول أنه دائما هناك حاجة ماسة إلى خبير أو فني من أجل القيام بالعديد من المهام التقنية مثل الكشف عن الدلالة الجنائية الرقمية وتحليلها، أو إصلاح الدليل وإعادة تجميعه من المكونات المادية للحاسب الآلي، أو التأكد من أن الدليل لم يتم العبث به.[1]

02- الضوابط التي تحكم عمل الخبير في مجال الجريمة المعلوماتية.

مما لاشك فيه عند قيام الخبير بمزاولة مهامه، يجب أن تتوفر مجموعة من الضوابط القانونية والفنية، فإن الضوابط القانونية هي أن يتم اختياره من قائمة الخبراء المعدة سلفا، وهو ما نص عليه المادة 144 من قانون الإجراءات الجزائية، بحيث يختار الخبراء من الجدول لذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة، واستثناء يجوز للجهات القضائية بصفة استثنائية أن يختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول، ويجب على الخبير أيضا أن يكون قد أدى اليمين القانونية وذلك لكي لا يترتب على عمله البطلان، وهو ما نصت عليه المادة 145 من نفس القانون وذلك بأن: «**يحلف الخبير المقيد لأول مرة بالجدول الخاص**

[1] - خالد ممدوح إبراهيم، المرجع السابق، ص 302.

بالمجلس القضائي يمينا أمام ذلك المجلس»،[1] وبعد ذلك يقوم الخبير بمزاولة مهامه المحددة له، وبعد انتهائه من عمله يعد تقريرا كتابيا مفصلا لما توصل إليه من نتائج، ويوعد خلال المدة المحددة له في الأمر أو الحكم بالندب، وأما الضوابط الفنية فيجب على الخبير أن يكون ملما بكل ما يتعلق بالحاسب الآلي وملحقاته،[2]بالإضافة إلى وجوب تمكينه وفهمه البيئة التي يعمل فيها، والقدرة على أداء المهام الموكلة له دون أن يترتب على ذلك ضررا للدليل الجنائي الرقمي المراد استخلاصه.[3]

ثالثا: التفتيش وضبط الأدلة الرقمية.

يعتبر التفتيش من أهم إجراءات التحقيق التي تفيد في الكشف عن الحقيقة، لأنه غالبا ما يسفر عن الأدلة المادية التي تؤيد نسبة الجريمة إلى المتهم، فيعرف التفتيش بصفة عامة بأنه: "البحث في مكنون سر الأفراد على دليل الجريمة المرتكبة، أو هو البحث عن الدليل..." [4] وعرف أيضا بأنه: "البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سند من القانون" [5]، وبالنسبة للفقه الفرنسي فقد عرفه بأنه: "البحث الدقيق لكل عناصر الأدلة التي يمكن استخدامها في الدعوى الجزائية والتي تجري على مسكن المتهم" [6]، إذن يتضح أن التفتيش ما هو إلا وسيلة إجرائية تستهدف ضبط الأشياء المادية التي تتعلق بالجريمة، وتفيد في كشف حقيقتها، إلا أن ذلك يتنافر مع الطبيعة غير المادية للدليل الجنائي

[1] – إبراهيم بلعليان، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر،2012، ص 304.

[2] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 303.

[3] – المرجع نفسه، ص 331.

[4] – عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، دار هومة، الجزائر، ط 4، 2013، ص266.

[5] – خالد ممدوح إبراهيم، المرجع السابق، ص 182.

[6] – Merk et veter traite de droit, paris, 1967, p758.

الرقمي،[1] وهو ما يجعلنا نطرح السؤالين التاليين: ما مدى قابلية أنظمة الحاسب الآلي وشبكاته للتفتيش؟ وكيف يتم ضبط الأدلة الجنائية الرقمية؟

01- مدى خضوع أنظمة الحاسب الآلي للتفتيش.

يقصد بالتفتيش عن الأدلة الجنائية الرقمية إجراء يسمح بجمع الأدلة المخزنة او المسجلة بشكل إلكتروني، أو هو التفتيش عن معطيات الحاسب الآلي غير المادية والمخزنة في الجهاز أو المخزنة في الأقراص،[2] وبناء على ذلك يمكن القول بأن التفتيش أنظمة الحاسب الآلي يكون بأحد الصورتين:

الصورة الأولى: [3] تتمثل في هذه الصورة في تفتيش المكونات المادية لجهاز الحاسب الآلي، والمكونات المادية عبارة عن مجموعة من الوحدات المتصلة ببعضها البعض بشكل يجعلها تعمل كنظام متكامل، [4] وهي: وحدات الإدخال مثل الفأرة ولوحة المفاتيح، ووحدات الإخراج مثل شاشة الحاسب الآلي والطابعة وأخيرا وحدة الذاكرة.[5]

وبناء على هذه الصورة فلا توجد أي صعوبة عند المعاينة قائمين على التفتيش لمسرح الجريمة الواقعة على المكونات المادية لجهاز الحاسب الآلي، مع مفهوم التفتيش التقليدي، لأنه يمثل في ذاته بحثا عن الأدلة المادية، وكل ما يتطلبه إجراء التفتيش في هذه الحالة هو أن يتم وفقا للقواعد القانونية التي تحكم التفتيش.[6]

---

[1] – علي حسن محمد طوايلية، التفتيش الجنائي على نظم الحاسوب والأنترنت 'دراسة مقارنة'، عالم الكتب الحديث، الأردن، 2004، ص12.

[2] – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الاردن، ط 1، 2011، ص 87.

[3] – بكري يوسف بكري، التفتيش عن المعلومات في الوسائل التقنية الحديثة، دار الفكر الجامعي، مصر، ط1، 2011، ص 67.

[4] – خالد عياد الحلبي، المرجع السابق، ص 158.

[5] – علي حسن محمد طويلية، المرجع السابق، ص 19.

[6] – بكري يوسف بكري، المرجع السابق، ص 68.

الصورة الثانية: تتمثل في تفتيش المكونات المعنوية لجهاز الحاسب الآلي، والمكونات المعنوية عبارة عن مجموعة البرامج والأساليب المتعلقة بتشغيل وحدة معالجة البيانات. [1] وتنقسم إلى كيانات أساسية تضم البرامج الضرورية التي يتم تشغيل واستخدام جهاز الحاسب الآلي، وكيانات تطبيقية تضم برامج تمكن للمستخدم أن ينفذ بواسطته عملا معينا.[2]

وبناء على الصورة الثانية، فقد آثار غلافا فقهيا حول إمكانية تفتيش المكونات المعنوية للحاسب الآلي، إذ رأى جانب من الفقه أنه متى كانت الغاية من التفتيش ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يمتد حتى يشمل جميع المعلومات والبيانات الرقمية بمختلف أشكالها،[3] وبسبب ذلك أن القوانين الإجرائية عندما تنص على الإصدار إذن بضبط أي شيء، فإن ذلك يجب تفسيره بحيث يشمل جميع المعلومات والبيانات المادية أو المعنوية،[4] ومن جهة جهة أخرى ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب الآلي غير مسموحة (المعنوية)، لذلك فإنه يقترح لمواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الحاسب الآلي لابد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بياناته.[5]

وعليه يتضح موقف المشرع الجزائري من خلال القانون رقم 09-04 المتعلقة بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إذ ينص صراحة على تفتيش انظمة الحاسب الآلي، وذلك بموجب نص المادة 05 منه، بحيث يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش

[1] – علي حسن محمد طويلية، المرجع السابق، ص 24.
[2] – المرجع نفسه، ص24.
[3] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 378.
[4] – خالد ممدوح إبراهيم، المرجع السابق، ص 197.
[5] – المرجع نفسه، ص 197.

ولو عن بعد إلى المنظومة المعلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، وكذا منظومة تخزين المعلوماتية.

وإلى جانب المشرع الجزائري، نص أيضا المشرع الفرنسي على تفتيش أنظمة الحاسب الآلي من خلال المادة 94 من قانون الإجراءات الجزائية، إذ أنه نصت على: «**يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها إلى أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة**» وتجدر الإشارة أن هذه المادة قد جرى تعديلها بموجب المادة 42 من القانون رقم 545-204 المؤرخ في 2004/06/21 المتعلق بالثقة مع الاقتصاد الرقمي، والذي أضاف لنص المادة عبارة "المعطيات المعلوماتية".[1]

02- مدى خضوع شبكات الحاسب الآلي للتفتيش.

مما لاشك فيه أن طبيعة التقنية الرقمية قد زادت من الصعوبات التي تواجه القائمين على التفتيش والضبط في الجرائم المعلوماتية، فالبيانات التي تحتوي على أدلة قد توزع عبر شبكات الحاسب الآلي في أماكن قد تكون على مسافات بعيدة عن الموقع المادي، الذي يتم فيه التفتيش، كما قد يكون الموقع الفعلي للبيانات والمعلومات ضمن الاختصاص القضائي لدولة أخرى، وهو ما يعقد ويصعب من عملية التفتيش وضبط الأدلة الجنائية الرقمية، [2] وعلى هذا الأساس نميز بين احتمالين اثنين في تفتيش شبكات الحاسب الآلي:

[1] – نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013، ص 106.

[2] – أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الامنية والتدريب، العدد 58، المجلد 29، أكاديمية نايف العربية للعلوم الأمنية، السعودية، دت، ص 91.

الاحتمال الأول: أن يكوون الحاسب الآلي للمشتبه فيه أو المتهم متصلا بحاسب آلي آخر أو نهاية طرفيه موجودة في مكان آخر داخل الدولة.

وبناء على هذا الاحتمال الذي يشكل عائقا أمام السلطات القائمة على التفتيش وضبط الأدلة الجنائية الرقمية، عمدت بعض التشريعات الإجرائية إلى حل هذه المشكلة من خلال نصها على إجازة تفتيش أنظمة الحاسب الآلي، وتسجيل كل البيانات اللازمة كأدلة غثبات لإدانة المتهم أمام المحكمة.[1]

وهو نفس المسار الذي اتخذه المشرع الجزائري، إذ نص في الفقرة الثانية من المادة 05 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة او جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وإلى جانب المشرع الجزائري، نجد المشرع الفرنسي قد حسم هذه المسألة أيضا بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون 03-239 الصادر في 2003/03/18، والذي أجاز له من خلال نص المادة 17 لضباط الشرطة القضائية أو تحت مسؤوليتهم أعوان الشرطة القضائية بتمديد نطاق التفتيش إلى أي جهاز آخر إذا كانت معلومات مخزنة يتم الدخول إليها من الحاسب الآلي الأصلي محل التفتيش.[2]

[1] - نعيم سعيداني، المرجع السابق، ص 149.

[2] - المرجع نفسه، ص150.

الاحتمال الثاني: اتصال الحاسب الآلي للمشتبه فيه أو المتهم بحاسب آلي آخر أو نهاية طرفيه موجودة في مكان آخر خارج الدولة.

وهو أن يقوم مرتكب الجريمة المعلوماتية بتخزين بياناتهم في أنظمة معلوماتية خارج إقليم الدولة بهدف عرقلة سلطات التحقيق في جميع الأدلة، [1] لذا ولحل هذه المسألة يرى جانب من الفقه أن تفتيش أنظمة الحاسب الآلي العابر للحدود لابد أن يتم في إطار الاتفاقيات تعاون ثنائية أو دولية تجيز هذا الامتداد، وبالتالي لا يجوز القيام بذلك التفتيش العابر للحدود في ظل غياب تلك الاتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى.[2]

ولمواجهة هذا الاحتمال نجد أن المشرع الجزائري قد أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج الإقليم الوطني، وهو ما نصت عليه الفقرة الثالثة من المادة 05 من القانون 09-04 السابق الذكر، بحيث إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأمنية المتخصصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل، والملاحظ على هذه الفقرة أنها مأخوذة حرفيا من نص الفقرة الثانية من المادة 57 من قانون الإجراءات الجزائية الفرنسي.

03- مدى صلاحية ضبط الدليل الجنائي الرقمي.

يترتب على التفتيش سوء الحق في ضبط الأشياء التي تفيد في الكشف عن الجريمة المرتكبة،[3] وذلك بوضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل لكشف عن الحقيقة

[1] - عبد الفتاح بيومي حجازي، المرجع السابق، ص382.

[2] - خالد ممدوح إبراهيم، المرجع السابق، ص 205.

[3] - بكري يوسف بكري، المرجع السابق، ص 128.

وعن مرتكب الجريمة، [1] وفي هذا الصدد لا تثير عملية الضبط أي صعوبة إذا ما تعلق بضبط المكونات المادية للحاسب الآلي، بل يقع الإشكال في مدى صلاحية المكونات المعنوية للضبط، لهذا فقد انقسم الفقه في هذا الأمر إلى اتجاهين:

-الاتجاه الأول: يرى أصحاب هذا الاتجاه أنه لا يمكن تصور إجرام الضبط على الكيانات المعنوية وذلك لانتفاء الكيان المادي عنها، بالإضافة إلى أن البيانات والمعلومات لا تعتبر من قبيل الأشياء المادية، وبالتالي لا يقع الضبط عليها، ولتجاوز هذا الإشكال اقترحوا ان يتدخل المشرع ويوسع من دائرة الأشياء التي يمكن أن يرد عليها الضبط، لتشمل جميع البيانات والمعلومات الرقمية بكافة أنواعها.

-الاتجاه الثاني: يرى أنصار هذا الاتجاه أنه لا يوجد ما يمنع من أن يرد الضبط على البيانات والمعلومات الرقمية، وذلك أن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، وبالتالي يمتد هذا المفهوم ليشمل جميع البيانات الرقمية بمختلف أشكالها، [2] وقد تدخل المشرع الجزائري لحل هذا الإشكال، وذلك ما نص عليه في المادة 06 من القانون 09-04 بحيث أنه:« **عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية** »، وإلى جانب المشرع الجزائري نجد أن المشرع الفرنسي قد تدخل أيضا بموجب تعديله لقانون الإجراءات الجزائية من خلال القانون رقم 239-2003 أين استحدث الفقرة الثالثة من المادة 57، والتي

[1] - خالد عباد الحلبي، المرجع السابق، ص 168.

[2] - المرجع نفسه، ص 146.

نصت أيضا على نسخ جميع المعلومات والبيانات الرقمية الناتجة عن التفتيش على دعامات التخزين الإلكترونية وتحريزها.[1]

وزيادة على ذلك، وإذا كان الدليل الجنائي الرقمي يخضع إلى قواعد تحريز الأدلة الجنائية، إلا أنه وبالنظر إلى الطبيعة التقنية والفنية التي يختص بها، فإن عملية ضبطه تستوجب بعض الإجراءات الخاصة لحمايته والحفاظ عليه من العبث والتلف، وهو ما نص عليه المشرع الجزائري من خلال نص المادة 06 في فقرتها الثانية من القانون رقم 09-04 أنه: «**يجب في كل الاحوال على السلطة القائمة على التفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية** »، ومن بين هذه الإجراءات ضبط الدعائم الأصلية دون نسخها، عدم تعريض الأقراص والأنشطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة، وأيضا عدم الضغط عليها بوضع أشياء ثقيلة.

الفرع الثاني: الإجراءات الحديثة لجمع الدليل الإلكتروني

يقصد بالوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية، تلك الإجراءات التي تستعمل أثناء تنفيذ طرق التحقيق الثابتة والمحددة والأساليب الصغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، ومنه فالوسائل الإجرائية عبارة عن أساليب محددة قانونا تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها، وذلك استخدام تقنيات وبرامج الكترونية مختلفة، تماشيا مع إرادة المشرع في مكافحة الجرائم المعلوماتية، أو حتى الجرائم التقليدية التي تتطلب استخدام هذه الوسائل.

[1] – نعيم سعيداني، المرجع السابق، ص 160.

أولا: حفظ المعطيات

ألزم المشرع الجزائري مقدمي الخدمات بحفظ المعطيات، وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف، ووضعها في ترتيب معين، في حين اتخاذ الإجراءات القانونية المحتملة أخرى كالتفتيش وغيره، وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة، وهي المعطيات المتعلقة بحركة السير (معطيات المرور)،وهي كما عرفتها المادة الثانية من القانون رقم: 09-04 تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الاتصالات توضح مصدر الاتصال، الوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم مدة الاتصال ونوع الخدمة، وقد حصر المشرع الجزائري معطيات المرور التي ألزم بحفظها في المادة 11 من القانون رقم09-04 ويتضمن:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الظرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال.
- معطيات متعلقة بالخدمات التكميلية المطلوبة أو مستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه، الاتصال وكذا عناوين المواقع المطلع عليها، وبما أن حفظ المعطيات إجراء وقتي، واحتراما للحق في خصوصيته، فإن المشرع الجزائري فرض على مزودي الخدمات يغيرون مصدر لجهات التحقيق وللحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها، وفي نفس الوقت ملزمين بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها.[1]

[1]- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012، ص ص 60-61.

ثانيا: التسرب واعتراض المراسلات الالكترونية

01-التسرب:

استحدث المشرع الجزائري في مجال مكافحة الجرائم الماسة بأنظمة الحاسب الآلي عدة إجراءات، وذلك بسبب عجز الأساليب التقليدية، ومن بينها إدراج المشرع لعملية التسرب بموجب القانون رقم: 06-22 المؤرخ في سنة 2006، المتضمن قانون الإجراءات الجزائية ، حيث نص الفصل الخامس منه تحت عنوان «**في التسرب**» المواد من 65مكرر 11 إلى المادة 65 مكرر 18، إذ نتناول من خلالها مفهوم هذه العملية وشروط إجرائها والحماية الجنائية للقائم بعملية التسرب.

-تعريف التسرب: قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك، وهذا ما نصت عليه المادة 65 مكرر 12 من قانون الإجراءات الجزائية، ومثاله في الجريمة الالكترونية اشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال، أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث الفيروسات، فيتخذ المتسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكرز لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم[1].

-شروط صحة التسرب:

-صدور إذن من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار وكيل الجمهورية.

-أن يكون الإذن مكتوبا ومسببا.

-يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة.

[1]- بوعناد فاطمة الزهرة، المرجع السابق، ص ص 69-70.

تحدد مدة عملية التسرب التي لا يمكن أن تتجاوز 04 أشهر، غير أنه يمكن أن تجدد، حيث تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على أنه: «... **يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن حسب الحالة بمباشرة عملية التسرب**»[1].

02- اعتراض المراسلات الإلكترونية

يقصد بهذا الإجراء مراقبة الاتصالات الالكترونية أثناء بثها، وليس الحصول على الاتصالات الالكترونية مخزنة، وقد استحدث المشرع الجزائري هذا الإجراء من خلال القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، حيث حدد الحالات التي يجب فيها اللجوء إلى المراقبة الالكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو في حالة توفير معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو مؤسسات الدولة أو في إطار تنفيذ طلبات مساعدة قضائية ، وهذا طبقا للمادة 04 من القانون رقم: 09-04 ، ويترتب على المراقبة السرية للاتصالات عموما، ومن ضمنها الاتصالات الالكترونية في الغالب تسجيل محتوى تلك الاتصالات وتخزينها على الوسائط المادية القابلة للنقل، بغية استخدامها فيما بعد لإثبات الجريمة الواقعة، وتختلف نوعية التسجيل هنا حسب ما إذا كانت المحادثة الالكترونية المراقبة عبارة عن اتصال صوتي مرئي، ففي الأول يكون التسجيل صوتي فقط، في حين أنه يكون الثاني تسجيل صوتي مرئي، كما تجدر الإشارة إلى أن المراقبة السرية للاتصالات الالكترونية ، ومن ضمنها المحادثات الهاتفية ، لا يمكن اعتبارها نوع من أنواع التفتيش، لأن المراقبة الالكترونية ترد على البيانات الالكترونية المتحركة(الاتصالات الالكترونية حال إجرائها)، دون التي انتهت وخزنت، في حين التفتيش يرد

[1]- بوعناد فاطمة الزهرة، المرجع السابق، ص 70.

فقط على البيانات الالكترونية الساكنة أو المخزنة(الاتصالات التي تمت وخزنت)، وتكون عملية المراقبة في جميع الحالات بإذن مكتوب من السلطة القضائية المختصة طبقا للمادة 04 من القانون رقم09-04 التي تنص على أنه: « **لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه، إلا بإذن مكتوب من السلطة القضائية المختصة...**».

المطلب الثاني: طرق الحصول عليه.

حتى يمكن تحديد مشكلات قبول الوسائط الإلكترونية في الإثبات، فإن دراسة الجانب القانوني لا ينبغي أن تنفصل عن التطور التكنولوجي كدليل وتقدير قوته في الإثبات يعتمدان على توافر شرائط أساسية في ذلك المحرر.

والتحقيق والتحري في الجرائم الإلكترونية ينطوي على المشكلات والتحديات الإدارية القانونية تتصل إبتداءا بمعوقات ومتطلبات عمليات ملاحقة الجناة، فإن تحققت مكانة الملاحقة أصبحت الإدانة صعبة لسهولة أتلاف الأدلة الإلكترونية من قبل الجناة أو صعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم.

الفرع الأول: مصادر الحصول على الدليل الإلكتروني.

إن الحصول على الدليل الإلكتروني يكمن في الطريقة التي ارتكبت بها الجريمة، وتنحصر تلك الأدلة في المتهم المشتبه به والمجني عليه ومقدم خدمة الانترنت، وهذه الأدلة على سبيل المثال وليس الحصر، غذ أنن التطور العلمي والفقهي قد يستقر على أنواع جدية من هذه الأدلة.[1]

1-الكمبيوتر الخاص بالمتهم المشتبه فيه:

فحص جهاز كمبيوتر المتهم المشتبه فيه، وخاصة وحدة التخزين الدائمة القرص الصلب (Hard disk) والوحدات الفرعية الملحقة وتشمل على القرص المرن وأقراص الليزر أو أي وحدة

[1]-د.ممدوح عبد الحميد، جرائم الكمبيوتر عن الانترنت، إصدارات مكتبة الحقوق الشارقة، الإمارات، 2000، ص 29.

تخزين أخرى من الممكن استعمالها مثل جهاز (flash memery)، كل تلك الأجهزة يمكن فحصها وبيان الطريقة التي قام بها المتهم في ارتكاب جرائمه.

2-جهاز كمبيوتر المجني عليه:

مما لاشك فيه أن المجني عليه هو المصدر الكاشف والنتيجة التي يترتب عليها ما قام به المشتبه فيه من جرائم، والمجني عليه قد يكون شخص طبيعي أو مؤسسة خاصة أو عامة أو مؤسسة مالية أو هيئة حكومية وغيرها، وبالتالي فغن فحص مثل تلك الأجهزة يمكن المحقق من معرفة الدخول وتتبع مصدر المشتبه فيه.

3-مقدم خدمة الانترنت: internet server provider.

يمكن الاستعانة أيضا في كشف الأدلة الإلكترونية بعدة جهات أخرى: مثال مقدم خدمة الانترنت مثل شركة ياهو yahoo أو جوجل google أو sms، فإن مثل تلك الشركات بمنتفعيها وهنا يمكن اللجوء غليهم للتعرف على هوية المجرم المشتبه فيه، وكذا البريد الإلكتروني على شبكة الانترنت، وذلك حيث أن عن طريق البريد الإلكتروني يمكن التعرف على البيانات الشخصية، ومنه نستطيع تحديد هوية المشتبه فيه عن طريق صندوق الرسائل الواردة إليه والمرسلة منه ومن ثم يتم تحددي مكانه وموقعه وذلك من أرشيف الجم وعات البريدية.

الفرع الثاني: البرامج المستخدمة في جمع الأدلة الإلكترونية.[1]

عادة ما توجد الأدلة الرقمية في مخرجات الطابعة والتقارير والرسوم في أجهزة الكمبيوتر وملحقاتها في الأقراص المرنة والصلبة وأنشطة تخزين المعلومات في أجهزة مودم والبرامج وأجهزة التصوير ومواقع الويب والبريد الإلكتروني، ولذلك تستخدم عن طريق أو أدوات تساهم في جمع الأدلة الرقمية منها.

[1]-حسن طاهر دواد، جرائم نظام المعلومات، الإصدار رقم 244 لأكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000، ص 288.

1-برنامج إذن التنفيذ computer scorch warrant program:

هو برنامج قاعدة البيانات، يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة، وتسجيل البيانات منها، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحددي مكان الدليل أو تحددي ظروف ضبط هذا الدليل.

2-قرص بدء تشغيل الكمبيوتر bootable deskette:

وهو قرص يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل فيه محميا بكلمة مرور، ويجب أن يكون القرص مزودا ببرنامج مضاعفة المساحة double space، فربما كان المتهم قد استخدم البرنامج لمضاعفة مساحة القرص الصلب.

3-برنامج معالجة الملفاتx tree pro gold :

وهو برنامج يمكن المحقق العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقديم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضغوطة، أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن من البحث عن الكلمات الصعبة أو أسماء ملفا أو غيرها.

4-برامج النسخ مثل lap Link:

هو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالتهم ونقلها إلى قرص آخر سواء على التوازي parallèle port أو على التوالي serial port، وهو برنامج مقيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

5-برامج كشف الدسك مثل AMA disk new disk:

ويمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان: نسخة عادية خاصة بالأفراد، ونسخة خاصة بالشرطة.[1]

6-برامج الاتصالات la ntastic:

هو يستطيع ربط جهاز حاسب المتهم لنقل المعلومات وحفظها ف جهز نسخ المعلومات ثم إلى القرص الصلب، هذه هي أهم الطرق العامة لجمع الأدلة الرقمية، والتي يجب أن يقوم بها.

الفرع الثالث: الأجهزة والأنظمة الواجب فحصها للحصول على الدليل الإلكتروني.

للحصول على الدليل الإلكتروني هناك أنظمة وأجهزة يجب فحصها للحصول على الدليل الإلكتروني، فإن الأمر يتطلب أولا فحص نظام اتصال الانترنت وثانيا فحص مركبات الحاسوب، وفيما يلي بيان لذلك:[2]

أ-فحص نظام الاتصال بالانترنت:

يقصد بنظم الاتصال بالانترنت بالمفهوم الإجرائي مدى إمكانية اقتناع محكمة الموضوع بالإجراءات المتبعة حال استخدام وسيلة الاتصال بالانترنت، ومن أهم المسائل المثارة في صدد فحص نظام الاتصال بالانترنت سعيا وراء إقامة الدليل على الإدانة في مسألة مدى إمكانية تحديد مكان الجريمة أو جهاز الحاسب الآلي الذي انطلق منه النشاط المادي للجريمة، ومثل هذا الأمر وإن كان لا يقود تحديدا إلى الشخص مرتكب الجريمة أو جهاز الحاسب الآلي الذي انطلق منه النشاط المادي للجريمة، ومثل هذا الأمر ، وإن كان لا يقود تحديدا إلى الشخص مرتكب الجريمة، استنادا إلى الدليل التقليدي فيما بعد أن الأمر لا يقف عند هذا الحد، وغنما يمتد إلى ضرورة التطرق إلى نقص الحقيقة في أماكن أخرى مثلما هو الحال في فحص كلما يتعلق بنظم اتصال

[1]-حسين بن سعيد بن يوسف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، ص419.

[2]- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص997.

الانترنت، كالشبكات المحلية والعالمية والبيانات وحركة الاستيراد والنظام الأمني المحاط بالانترنت ونظام الاتصالات القائم وحركته وامتداداته وبرمجيات الانترنت وحركة الإنزال والتحميل والنظام المعلوماتي المحمل على الانترنت ودرجة استيعابه...إلخ هذه كلها يلزم فحصها للتوصل إلى دليل رقمي يفيد في الكشف عن الحقيقة، فلا يقف الأمر عند مجرد إبراز العجز عن التقصي والبحث والتفتيش هذا فقد يمكن من خلال استطلاع أي من هذه الوسائل القيام برصد دليل رقمي ما.

ذلك أن الدليل الرقمي على الرغم من اتساع قاعدته إلا أنه يمكن أن يكون متواجد في صيغة كما لا يمكن توقعها، فمثلا نجد أن التفتيش والتقصي في الحاسوب الشخصي سعيا وراء البحث عن ملف ما، يرتبط بارتكاب جريمة موضوع هذا التقصي والبحث من قبل الخبير قد لا يؤدي إلى وجودها يقيد في إثبات الجريمة، كما لو كان مرتكب الجريمة قد قام بوضع نسخة من هذا الملف في خادم البريد الإلكتروني عبر الانترنت والخاص بهذا الشخص، حيث يمكنه أن يطاله من أي مكان وفي أي وقت.

هذا ويتم فحص نظام الاتصال بالانترنت بحسب المناطق التي يتكون منها، وهذا التقييم هو تقييم مادي مستمد من تفصيل الانترنت التقني، وهو تفصيل على أية حال لا يرتبط بضرورة تسلسله، وإنما يمكن القيام باتخاذ هذا أو ذلك الإجراء دون أن يكون مرتبطا بهذا التسلسل.

1-مسار الانترنت: تعني عبارة مسار الانترنت Routing الحركة التراسلية للنشاط الممارس من خلال الانترنت، فالكمبيوتر بمجرد أن يتعرف على المسار يقوم تلقائيا باختيار البروتوكول التراسلي le protocole transmission الذي من خلاله يقوم باستدعاء البيانات، وهي الحركة التي أشار إليها علماء الانترنت على أنها تتشابه مع شبكة العنكبوت من حيث عدم انتظام شكل المسار الاتصالي والتواصلي عبرها، لذلك يطلق عليها الشبكة العنكبوتية، ويستخدم في تتبع حركة مسار الانترنت نظام الفحص الإلكتروني Electronic trail الذي يطلق عليه البصمات

المعاصرة، أو علم البصمات twenty ferst century وهو منهج متبع في تتبع الحركة العكسية لمسار الانترنت، ولقد تم تطبيقه على أكثر من جريمة، مثل تتبع مرتكب فيروس ميلسا Melissa virus وكذلك في التوصل إلى الشخص الذي ابتكر موقع خدمات بلومبرج لأخبار المال الاحتيالي لكي يرفع أسعار الأسهم بطريقة الخداع...إلخ.[1]

ويتنازع مع إمكانية تحديد مسار الانترنت من عدمه رأيان، فيذهب الرأي إلى أنه لا يمكن تحديد مسار ارتكاب الجريمة،[2] وتكمن وجاهة هذا الرأي في أن شبكة الانترنت ذات طبيعة مرنة بحيث أنه حتى وإن أمكن مستقبلا تحديد مسار الإنترنت ذات طبيعة مرنة، بحيث انه حتى وإن أمكن مستقبلا تحديد مسار الانترنت، فإن ما يتم الحصول عليه في هذا الإطار، إنما هو دليل رقمي يحتاج إلى تكملته بأدلة إثبات أخرى، فيم لو اقتصر الأمر على هذا الدليل فإن الأمر يظل في حومة الشك، ذلك أن ما يتم الوصل إليه في الحقيقة من خلال الدليل الرقمي، وإنما هو عنوان رقمي فقط IP adress وهذا لا يكفي في نسبة العمل الإجرامي أو غير المشروع إلى صاحب أو مالك الحاسوب أو عنوان الاسم المذكور، إذ من الممكن ألا يكون هو مرتكب الجريمة حقا، كما لو كان الكمبيوتر[3] خاصته مسروقا أو مؤجرا (في مقهى انترنت) أو أن يكون عنوانه الرقمي IP مسروقا أو مختلسا أن يكون أحد مستخدمه احتيالا، وكذلك أن يكون له أي تأثير في الإدانة إذ تبين أن المتهم لا يعرف عن الانترنت أو عن الحاسوب أي شيء، فمثل هذه الأمور تجعل من

[1]-حسين بن سعيد بن يوسف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص521.

[2]-Vincent grymbaunv le droit de reproduction a l'heure de la societé de l'information, A propos de la direction, 2001/ 29/CE de certains aspects du droit d'auteur et des droits voisins dans la societé de l'information, OP.cit, P02.

[3]-Fourth amendment and the internet, hearing before the subcommittee on the constitution of the commentte on the judiciary bouse of representatives one hundred sisch congress second session april 6 2000, Serial no, 135, Op.cit, forth amendment and the internet, hearing before the subcomnuelted on the constitution of the committee the judiciary house of representatives one hundred sisch.

الصعوبة بمكان إمكانية الاعتماد على مسار حركة الانترنت للتوصل إلى المتهم، وإنما يحتاج الأمر هنا على الدليل المادي، [1] ومثابرة من جهات الاستدلال والتحقيق لكي يتوافر لها دليل مادي كالاعتراف أو شهادة أو خبرة أو قرائن...إلخ.[2]

2-فحص النظام الأمني للشبكات:[3]

إن جهاز الحاسب الآلي المنفرد الغير متصل بأي نوع من أنواع الشبكات Stand alone computer لا يكون عرضة للاختراق المعلوماتي إطلاقا، وإنما كل ما يمكن أن يتوافر لو إختراق مادي، بحيث يتصل مرتكب الجريمة بالكمبيوتر المنفرد اتصالا مباشرا، وهذا يجعل عملية الحصول على الدليل التقني سريعة، بحيث تتجه الشبهات إلى حائز الجهاز الفعلي وكذلك كل من قام باستخدامه على نحو آخر.[4]

أما أجهزة الحاسب الآلي المرتبطة بالنظام التواصلي عبر الشبكات، وكنتيجة له، تقدمه من نشاط معلوماتي متشابك العنكبوت فإنها تكون أكثر عرضة لاستخدامها في ارتكاب الجرائم واحتوائها على الأدلة الرقمية، خاصة الشبكات غير المحصلة بالتشفير، حيث أنها تكون أكثر عرضة للاختراق،[5] وبالتالي فإن فحصها يتطلب وقتا أطول للحصول على دليل رقمي هنا، قي حين تشكل الشبكات المحصلة للتشفير ذات صعوبة أقل في تحصيل الدليل لكون الاختراق يبدو واضحا من خلال الكشف الدوري عليها، فيتبين مداه من خلال فحص حركة الدخول هنا.

---

[1] -Fourth amendment and the internet , Op.cit, "the creator of the melissa vivy and the individual who created a fraudulent bo blooglerg news service website in oder to artificially drive up the stock puce of pair cain, a telecommunication", compary based in california.

[2] -جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت.

[3] -عمر محمد أو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، مرجع سابق، ص105.

[4] -د. عمر محمد أبو بكر بن يونس، الإثبات الجنائي عبر الانترنت، ص16.

[5] -حسين بن سعيد بن سيف الغامدي، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص424.

3-نظام فحص بروتكول الانترنت:

يعد هذا البروتكول الطابع المميز لاستخدام الانترنت، فأي شخص يحصل على بروتكول الانترنت يمكنه الولوج إليها ليكون عضوا كاملا فيها، يباشر الحركة خلالها ويحصل على خدماتها. وعملية البحث في قواعد البيانات لدى مسجلي بروتكول الانترنت ليست بالمهمة الصعبة، غذ يمكن لأي كان القيام بتحديد حائز هذا أو ذلك البروتكول عن طريق البحث في قاعدة بيانات who is الخاصة بالمسجلين Rregestrars فمثلا كان موقع المؤسسة Network Solutions في موقعها www.networksolutions.com يحتوي على عناوين المؤسسات الأمريكية، تمنح هذه المؤسسة عبر موقعها المذكور نظام استطلاعي لقاعدة البيانات who is فيها، كذلك يمكن استخدام برمجيات متعددة ومتوافرة عبر الانترنت تقوم برصد بروتوكولات الانترنت.[1]

4-فحص الخادم أو الملقم: ويتضمن فحص نظام الاتصال بالانترنت لزوم فحص الخادم أو الملقم، وهو حاسوب ضخم مهمته تحقيق حركة الاتصال بالمواقع والصفحات التي يتم استضافتها على هيئة رقمية فيه،[2] لذلك نجد ان الخادم يطلق عليه lieu de stokage des données numérées ومن الخوادم ما يكون مهمته ليس تحقيق اتصال موع المواقع والصفحات، وإنما فقط نظام تخزين البريد الإلكتروني...إلخ، وبحيث يعمل هذا الخادم على ربط أعضاء الانترنت بغرض التداول والحديث المتواصل فيبرر عضو الانترنت كما لو كان يستضيف من يتحدث معه.

[1]-Eoghan casey computer et internet crime FAQ-Avialable online in feb 2001 at http://www.foreusic science.com/gov computer, htmp.

[2]-Tgi paris, 17 ch, correc, 28/02/1999, note: maitre stephane lilti P.3 desponible enlegna a now, 1999.http://www.legalis; netljnet ecommentaire lelti, 28/01.htm.

ب–فحص مكونات الكمبيوتر:

الحاسب الآلي في ذاته يقوم في تركيبه على أمرين هما القطع الصلبة hardware والقطع المرنة أو البرمجيات software، هناك عنصر ثالث يتوزع بين البرمجيات والقطع الصلبة وهو عنصر المعلوماتية informatique.

لو نظرنا إلى متطلبات المحاكمة العادلة نجد أنها تستلزم أن يكون الفحص ماديا، ومعنويا لارتباط القائم في شكل طبيعي بين مكونات الحاسوب ككل، وذلك ضمانة لازمة حتى تتوافر للمتهم ضمانات المحاكمة الكاملة التي صارعت الإنسانية مراحل طويلة مسيرتها للحصول عليها.

هذا وتعتمد عملية الفحص هنا على الحاسب الآلي، سواء بالفحص الذاتي للجهاز، وهو قيام جهاز الكمبيوتر ذاته بفحص مكوناته وتقديم تقرير كامل بذلك إلى طالب الفحص، ومثل هذه الحالة يجب أن لا يقوم بها الهواة أو المستخدمون العاديون، حيث يتطلب مثل هذه الحالة قدرات تقنية عالية.

وقد يتم الفحص عن طريق الاستعانة بجهاز آخر أو أجهزة تقنية عالية متخصصة في بحث جزيئة أو جزيئات عبر جهاز الحاسب الآلي، فمثلا قصف نظام معلوماتي في نظم كمبيوتر تشغيل الخبرات المدني وأجهزة كمبيوتر المستشفيات أو بورصة المعلومات Nasdaq ومؤسسات الخدمة المدنية وما تجريه من بيانات اسمية، وكذلك تداول الملفات التي تحوي معلومات خطرة مثل الفيروسات وتبادل صور الدعارة، ودعارة الأطفال على الخصوص، يمكن من خلال تلك التقنيات القيام برصدها، وحيث أمكن لمؤسسات كبيرة مثل actic telecom actic technology في بريطانيا القيام بإعداد برمجيات راصدة لمثل هذه الحالات.

أ-فحص القرص الصلب:

يعد القرص الصلب المحتوى الذي يضم في داخله مجموع البيانات الرقمية ذات الطابع الثنائي، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي (0-1) الذي يتكون منه تفصيل البيانات المذكورة، ويشير العلماء إلى إمكانية القيام بفحص كلي أو جزئي للقرص الصلب.

والفحص الجزئي للقرص الصلب the moleculaire of hard disk يؤدي إلى التعرف على محتوى البيانات الثانية الرقم، والتي يؤدي التعامل معها إلى الكشف على القيمة الاسترادادية للبيانات المخزنة فيه سواء كانت محتويات مكتوبة أو صور أو أصوات، وكذلك ما تم حذفه delete من بيانات وبرمجيات وبرامج وعملية الإلغاء أو الحذف بطبيعة الحال تحتاج إلى برمجية خاصة للقيام بها، فليس الأمر مرتبط بقطعة صلبة وإنما برمجيات أيضا.[1]

والمثال التقليدي المستخدم هنا هو حالة البحث في ملفات النسخ الإضافية التي يحتويها نظام التشغيل مثل الوافذ ومثل ملفات temp و internet temporary وهذه الأخيرة ملفات تأخذ نسخا احتياطية من كل صفحة يتم الولوج إليها عبر الانترنت، كذلك توجد في نم التشغيل ملفات خاصة بالإنزال dowload file مهمتها استقبال الملفات التي يتم تحميلها على جهاز الحاسب الآلي من خارجه عبر الانترنت، فهذه الملفات جميعها مركزها القرص بطبيعة الحال حتى في ظل رصد أماكن أخرى تحتوي برمجيات مثل المعالج processor الذي يتم تصنيعه processor برمجته في ظل ظروف خاصة بحيث يمكنه القيام بدوره في الحاسب الآلي.

[1]-عمر محمد أبو بكر بن يونس، مرجع سابق، ص 10-11.

ب–فحص البرمجيات:[1]

وهنا نستطيع أن نميز بين الفحص الداخلي للبرمجيات وحالة الفحص الداخلي، والذي يتم من خلال بحث البناء المنطقي للبرمجة بما يوحي بأن هناك مجهودا جديدا في إعداده للعمل Setup حين إنزاله في جهاز الحاسب الآلي installation وذلك من الأمور التي يدركها الخبراء من حيث استلزام الربط الصحيح في البرمجية ذاتها، بحيث يلزم المبرمج تتبع الخطوات المنطقية التي تعبر عن جهده التجديدي سيما، وأن الخبراء على دراية بكيفية البرمجة والخيارات المتعددة وأكثر ما يتم العمل في إططار الفحص الداخلي هو في البحث عن مصدر الملفات الموجودة في هذا الإطار، غذ أنن النسخ عبر الانترنت لا يعد مشابها في هذا الشأن مع القيام بنسخ المؤلف باستخدام برمجيات معالجة الكلمات word processing ثم عبر العالم الافتراضي في حين أن النسخ الثاني تم استخدامه مصنف متداول في العالم المادي.

وإذا كانت الوسيلة التي تم بها النسخ ليست ذات أهمية في هذا الإطار إلا أنها على أية حال تفيد في ترتيب كيفية حدوث الجريمة، وقد يقود مثل هذا الأمر إلى التوصل إلى جرائم أخرى، كما لو كان هناك صور داعرة في الحاسوب، فإن الكشف عما إذا كانت جذورها عبر الانترنت أم في الواقع المادي من خلال مسح صور فوتوغرافية، يمكن أن يقود إلى مروجيها في العالم المادي أو القبض على شبكات الدعارة والرقيق الأبيض أو دعارة الأطفال...إلخ أو أن يتم التعرف على الكيفية التي تم بها إعداد مثل هذه الصور كما هو الشأن في استخدام برمجيات الرسومات لوضع رأس امرأة أو قناة على جسد عار (تزييف الصور) بما يمثل مشكلة أو أخرى لصاحبة الرأس، إذ يمكن التوصل إلى الحقيقة دائما باستخدام برمجيات معقدة نوعا ما (كونها لا تزال حديثة فقط).

[1]–عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص1013.

ج-فحص النظام المعلوماتي:[1]

يعني فحص النظام المعلوماتي وضبط كافة ما يحتوي جهاز الحاسب الآلي من معلومات يمكن إستردادها عبره، تكون مخزنة في ملفات files على أية شاكلة يمكن أن تكون عليها الحركة الاسترادادية ما دام موضوعها يشكل جريمة، ويلزم هنا التطرق إلى فكرة محتوى المعلوماتي للحاسوب حتى يمكن فهم الكيفية التي يلزم لأن يتم فيها عملية فحص النظام المعلوماتي.

إن النظام المعلوماتي للحاسب الآلي لا يحتوي على المعلومات كما هو المعتقد السائد لدى الكثيرين، وإنما المحتوى المعلوماتي عادة ما يتكون من بيانات ثنائية الهيئة الرقمية، يتم إيداعها في الحاسب الآلي، وهذا الإيداع يأخذ شكل تخزين stockage، وهذه البيانات يقوم الحاسوب بمعالجتها على هيئة معلومة محددة، حين يتم استدعاؤها من قبل الغير أو أي مستخدم للحاسوب، وما دام لم يتم استدعاء معلومة محددة فإن بياناتها تظل في حالة تخزين في الحاسوب، وذلك على درجة كبيرة من الأهمية إذا تأملنا فكرة أن ما يوجد من معلومات في الحاسوب، إنما يتكون حال قيام الغير باستدعاء أيا منها تحديدا، ومن ثم يجب بداية أن يتم تحديد معلومة المراد استدعائها من البيانات المختلفة المخزنة في الحاسوب لكي تظهر لنا بعد.[2]

فحص نظام ذاكرة التخزين caching:

يعد نظام ذاكرة التخزين stokage من مزايا نظم تشغيل الحاسوب تحديدا، وكلما كان نظام التشغيل متطورا كان نظام ذاكرة التخزين أكثر دقة، وإذا كنا قد تعرضنا لنظام التخزين بشكل مستقل عن النظام البرمجي، فإن ذلك عائد على خطورة هذا النظام، حيث انه يشكل أحد المقدمات الكبرى إلى فحص نظام الحاسوب ومركباتها.

[1]- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص23.

[2]-حسين بن سعيد بن سيف الغافري، مرجع سابق، ص 43.

ويمكن تعريف نظام ذاكرة التخزين بأنه قدرة الحاسوب الآلية على الاحتفاظ في ذاكرته كاملة مما اطلع عليه عضو الانترنت أثناء إبحاره عبر العالم الافتراضي.

فحص الطابعة:

يمكن رصد الحركة الخارجية سعيا وراء الدليل التقني بفحص الطابعات، سيما الحديثة منها، غذ تتضمن الطابعات الحديثة ميزة التخزين منطقيا لمجموع الصفحات التي تم استخراجها من الحاسوب، حتى في الحالة التي يكون هذا الملف قد تم إلغاؤه من أوامر عبر جهاز الحاسب الآلي، منها أمر الطباعة، بطباعة ما قامت في فترة زمنية سابقة بطباعته hard copy print التي تفيد في الكشف عن الحقيقة.

والجدير بالملاحظة في هذه البرمجية أنها تتضمن حيزا لكي يوضع فيه تاريخ اليوم المراد تقصي قيام طابعة بعمل ما فيه، حيث أنها تعمل على استرجاع النظام التاريخي history المتطور في متصفح المستكشف explorer من miciosoft حيث أنها لا تعمل على متصفح أقدم أو أي متصفح آخر.

فمثل هذه البرمجيات تساعد في معرفة ما إذا كان الشخص قد قام بطباعة صفحات تتضمن صور خليعة من الانترنت، وتاريخ قيامه بذلك وساعته، بدقة غريبة، كذلك في الجرائم الأخرى من ذات النوعية، ويمكن مثلا التعرف على عدة نسخ التي تمت في موضوع العدوان على حقوق المؤلف، كما يمكن أيضا معرفة تاريخ وساعة القيام، والمدد المختلفة التي يتم فيها ارتكاب هذه الأفعال.[1]

[1]-عمر محمد أبو بكر بن يونس، مرجع سابق، ص 1018.

و-فحص لوحة المفاتيح:

يمكن أن تكون لوحة المفاتيح keyboard محلا لفحص خبراء تكنولوجيا المعلومات في المعامل الجنائي، حيث أن لوحة المفاتيح الحديثة كثيرا ما يتم استخدامها كملقم أو خادم وهي من قبل الهجرة، وفي هذه الحالة يكون التعامل معها كأداة أو وسيلة مساعدة في ارتكاب الجريمة، ومن ثم يمكن اعتبار الدليل يساعد في إبراز حقيقة الواقعة الإجرامية. [1]

الفرع الرابع: الحصول على الدليل الرقمي من بروتوكولات الانترنت ECP/IP:

تلعب إشكالية البحث والمتمثلة في كيفية تقديم دليل بروتوكولات الانترنت ECP/IP كدليل له حجية قضائية، حيث تلعب ECP/IP دورا رئيسيا في اختيار وتحديد المنهج الذي سيتم إتباعه، وبناء على ذلك سوف يكون البحث مقسما إلى الموضوعات التالية والتعرف على البروتوكول ECP/IP وجمع وتوثيق وحفظ الدليل المستخرج من البروتوكول ECP/IP.

1-بروتوكول التحكم بالعقل/بروتوكول الانترنت ECP/IP:

ECP/IP transmission control protocol (ECP), internet protocol (IP)

وهي عائلة البروتوكولات والاتصالات بين عدة أجهزة من كمبيوتر صورت أساسا لنقل البيانات بين أنظمة (UNIX)، ثم أصبح المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الانترنت بواسطة الاتصال الهاتفي والمجموعة منها تسمى Stack tch/ip.

وبروتوكول ECP/IP[2] يضم في الواقع بروتوكولين مستقلين في شبكة الانترنت، هما بروتوكول transport control protocol-ECP وبروتوكول internet protocol IP[3].

---

[1]-حسين بن سعيد بن يوسف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص434.

[2]-هلال عبد الإله أحمد ، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية،1997، ص 11.

[3]-ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول ECP/IP في بحث وتحقيق الجرائم على الكمبيوتر، بحث منشور على شبكة الانترنت على موقع الدليل الإلكتروني للقانون العربي بتاريخ2006/08/17.

يعملان معا بشكل متزامن ويركز البروتوكولان معا ECP/IP على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Packet) بين مختلف الاتصالات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها.

الفصل الثاني

حجية الدليل الرقمي في التشريعات المقارنة وأمام القاضي الجنائي.

تمهيد:

إن مرحلة الحكم هي المرحلة الحاسمة في الدعوى الجنائية، ذلك أن غاية الدعوى الوصول إلى حكم حاسم لها، حائز قوى إنهاءها، ولهذا فإن الحكم يمثل أهم إجراءات هذه الدعوى لأنه يمثل غايتها، وعملة تقدير الدليل تشكل جوهر هذا الحكم، حيث لا يمكن الوصول إليه وإدراكه ما لم يمارس القاضي سلطة تقديرية على الأدلة محل الوقائع، وفي مجال الجريمة الإلكترونية يكون الدليل الإلكتروني هو الأوفر، سيما إذا اعتبرنا الحكم هو الكلمة النهائية للقضاء، وهو غاية التنظيم القضائي برمته، وسلامة هذا الحكم يتوقف بدرجة كبيرة على سلامة تقدير الأدلة.

والدليل الإلكتروني شأنه شأن باقي الأدلة الأخرى يخضع لنفس القواعد المقررة لباقي الأدلة، سواء كانت هذه القواعد تتعلق بسلطة القاضي الجنائي في قبول الدليل الإلكتروني، او تتعلق بسلطته في تقدير هذا النوع من الدليل، ذلك أن القاضي لا يقدر إلا الدليل المقبول، ولا يكون مقبولا إلا بعد التيقن من مراعاة الدليل لقاعدة مشروعية والتي لا يمكن من دونها أن يترتب عن الدليل الإلكتروني آثار قانونية.

وبالنظر إلى الطبيعة الخاصة التي يتميز بها الدليل الرقمي، وما قد يصاحب الحصول عليه من خطوات معقدة، فإن قبوله في الإثبات قد يثير العديد من المشكلات، حيث أن مستودع هذه الأدلة هو الوسائل الإلكترونية، ولذا التلاعب فيها وتغيير الحقيقة أمر وارد، وهذا ما يجعلنا نتساءل: كيف نضمن مصداقية الدليل الإلكتروني وأنها بالفعل تعبر عن الحقيقة التي تهدف إليها الدعوى الجنائية؟ وعلى ذلك ستكون الإجابة على هذا الإشكال من خلال تعرضنا بالدراسة إلى سلطة القاضي الجنائي في قبول الدليل الرقمي في الأنظمة الأجنبية والأنظمة العربية، وذلك من خلال المبحث الأول، أما المبحث الثاني فنتطرق فيه إلى سلطة القاضي الجنائي في تقدير الدليل الرقمي.

المبحث الأول: حجية الدليل الرقمي في التشريعات المقارنة.

يعد قبول الدليل الخطوة الإجرائية الأولية التي يمارسها القاضي اتجاه الدليل الجنائي بصفة عامة، والدليل الرقمي بصفة خاصة، وذلك قبل البدء في تقديره، للتأكد من مدى صلاحيته، وملائمته لتحقيق ما قدم من أجله، وقبول القاضي الجنائي للدليل الرقمي في الإثبات لابد وأن يستند على أساس، وهذا الأخير يختلف من نظام إلى آخر، سواء كان نظام لاتيني، أو نظام أنجلوسكسوني، ويهدف القاضي الجنائي في هذه المرحلة إلى التيقن من مدى مراعاة الدليل الجنائي أساسا لقاعدة المشروعية، والتي لا يمكن بدونها أن يترتب على الدليل آثار قانونية، بل يثير إهمالها أو مخالفة ما تستلزمه من شروط آثار قانونية أخرى، تكمن أساسا في بطلانه وبطلان كل ما يترتب عليه من إجراءات.

المطلب الأول: حجية الدليل الرقمي في التشريعات الأجنبية.

لم تورد التشريعات المنتمية إلى العائلة ذات الأصل الأجنبي مثل فرنسا وغيرها من الدول المتأثرة بها كالجزائر ومصر، نصوصا خاصة فيما يتعلق بقبول الدليل الإلكتروني، وذلك على أساس أن هذه الدول تستند لمبدأ حرية الإثبات في المسائل الجنائية، هذا المبدأ الذي يمثل لب نظام الإثبات الحر،[1] حيث أصبح هذا النظام الأخير القانون العام في الإجراءات الجزائية في التشريعات اللاتينية، بمقتضاه يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، وتتمثل خصائص هذا النظام في عدم تحديد الأدلة، بمعنى أن الخصوم لهم الحرية في الالتجاء إلى أي دليل يمكنهم من إثبات ادعائهم، كما أن هذا النظام يخول القاضي سلطة تقديم الادلة دون أن يفرض

[1] – يطلق عليه البعض نظام الأدلة الأدبية، أما البعض الآخر فيطلق عليه نظام الأدلة الإقناعية، أو نظام الاقتناع الشخصي أو الذاتي système de l'intime conviction de juge ، وهناك من يسميه بحرية القاضي الجنائي في الاستسلام لنداء ضميره، لمزيد من التفصيل حول هذا النظام. ينظر: أحمد فتحي سرور، أصول الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1969، ص 343. وينظر كذلك: مفيدة سويدان، نظرية الاقتناع الذاتي للقاضي الجنائي، أطروحة دكتوراه في القانون، كلية الحقوق، جامعة القاهرة، 1985، ص 109.

عليه قيد أو شرط، فالقاضي حر في أن يستعين بكل طرق الإثبات للبحث عن الحقيقة، وهو حر في وزن وتقدير كل دليل، وفي التنسيق بين الأدلة التي تتمثل في الحكم بالإدانة أو البراءة.
ونتيجة لذلك، فإنه يحظر على المشرع إضفاء قوة معينة لأي دليل من شأنه أن يقيد سلطة القاضي في تكوين قناعته، أو يسبغ على بعها البعض شكا أو عدم ثقة كي يستبعدها القاضي من تقديره الحر.[1]

ونتيجة لذلك فإنه تخطر على المشرع إضفاء قوة معينة لأي دليل من شأنه أن يقيد سلطة القاضي في تكوين قناعته، أو يسبغ على بعضها شكا أو عدم ثقة كي يستبعدها القاضي.
وانطلاقا مما سبق ذكره يتضح لنا مبدئيا أنه يجوز للقاضي الجنائي الإسناد إلى الدليل الإلكتروني لإثبات الفعل الجنائي في سائر الجرائم، والجرائم الإلكترونية على وجه الخصوص، وهو ما سوف نبينه بالتفصيل التالي، من خلال دراسة أساس قبول هذا النوع المستحدث من الدليل في التشريعات ذات الأصل اللاتيني أولا، ثم نبين أهم النتائج المترتبة على الأخذ بهذا الأساس ثانيا.

الفرع الأول: حجية الدليل الرقمي في التشريعات اللاتينية.

أولا: التشريع الفرنسي:

وفي فرنسا صدر قانون 5 يناير 1988 بشأن جرائم الغش المعلوماتي المرتكبة ضد نظم المعلوماتية، وتضمن هذا القانون عدة مواد منها نص المادة 2/462 والتي تجرم الدخول أو البقاء الغير مشروع في كل أو جزء من نظام المعالجة الآلية للبيانات.

وقد جاء نص المادة 2/462 على أن كل شخص قام بالدخول أو البقاء بطريقة كلية أو جزئية في داخل نظام معالجة المعلومات، سيعاقب بالحبس الذي لا يقل عن شهرين وغرامة لا تزيد عن خمسين ألف فرنك، أو بإحدى هاتين العقوبتين، وإذا نتج عن الدخول أو البقاء الغير المشروع

[1] – فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق، جامعة بغداد، 1992، ص 60.

محو أو تعديل في المعطيات المخزنة في النظام، تكون العقوبة الحبس لمدة تتراوح ما بين شهرين إلى سنتين والغرامة تتراوح ما بين عشرة آلاف جنيه إلى مائة ألف فرنك.

وبعد تعدل هذه المادة في عام 1994 بالمادة رقم 1/323، عدلت العقوبة إلى الحبس سنة ومائة ألف فرنك فرنسي تغريم، وفي حالة إذا نتج عن هذا الدخول غير المشروع محو أو تعديل في المعلومات الموجودة بالنظام، تكون العقوبة الحبس سنتين ومائتين ألف فرنك فرنسي غرامة.

وقد أجاز المشرع الفرنسي بموجب المادة 1/323، وبغرض حماية نظم المعلومات، مساءلة الأشخاص الاعتبارية عن الجرائم المذكورة سالفا، في ضوء الأحكام العامة لمساءلة الأشخاص الاعتبارية الواردة بالمادة 2/121 من قانون العقوبات.

ويرى البعض [1] أنه بالرغم من أن هذا النص يمثل خروجا على القواعد العامة، بحيث يعاقب على الأعمال التحضيرية للجريمة التي تسبق البدء في التنفيذ المادي لها، فإنه يمكن على القواعد الخاصة بنص خاص ذلك على أساس رغبة المشرع الفرنسي في تقرير نوع من الحماية الوقائية لنظم المعلومات من مخاطر الاعتداء لمثل هذه الجرائم.

ويرى البعض [2] أن المادة 1/323 تعالج جريمتين مختلفتين من ناحية الركن المادي، ذلك لأن المشرع يفرق ما بين الدخول من ناحية والبقاء مكن ناحية أخرى داخل نظام المعالجة الآلية للبيانات.

ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام، وبالتالي يجوز الدخول إلى النظام بأية وسيلة، مثل الدخول عن طريق كلمة السر الحقيقية عندما يكون الجاني غير مخول له استخدامها أو استخدام برامج أو شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص آخر، أو الدخول

[1] –د.علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت،/ والذي عقد خلال الفترة 2000، كلية الشريعة والقانون، جامعة الإمارات.

[2] –أحمد حسام طه تمام، الجرائم الناشئة عن استخدم الحاسب الآلي، ص262.

من خلال شخص مسموح له بالدخول سواء تم ذلك عن طريق شبكات الاتصال التليفونية أو محطات طرفية terminal سواء محلية أو عالمية.[1]

ثانيا: موقف التشريع البلجيكي.[2]

من بين التشريعات الحديثة التي أشارت إلى الجرائم الاعتداء على نظم المعالجة الآلية للمعطيات، التشريع الجنائي البلجيكي، بعد تعديله بالقانون الصادر بتاريخ 2000/11/28.[3]

حيث أضيف إلى قانون العقوبات البلجيكي فصل جديد هو الفصل التاسع المكرر، وقد تضمن هذا الفصل مادة جديدة هي المادة 6مكرر، التي تضمنت في قرتها الأولى مسألة الدخول أو البقاء غير المصرح بها في النظام الإلكتروني.

ونشير إلى أن القانون البلجيكي الصادر بتاريخ 2000/11/28 بشأن الإجرام المعلوماتي[4]، تضمن مجموعة من التعديلات تخص قانون العقوبات، وقانون الإجراءات الجنائية، والجدير بالذكر أن ما يهمنا في هذا القانون ارتباطا بموضوع هذا الفصل هو المادة 6 التي تطرقت لحماية نظم المعالجة الآلية للمعطيات لكل صور الاعتداء سواء بالاختراق أو محو أو تعديل البيانات الموجودة داخل النظام الإلكتروني[5]، بحيث نصت المادة 6 على أن يضاف إلى الكتاب الثاني[6] من قانون العقوبات البلجيكي عنوان تاسع مكرر تحت عنوان: 'الخروقات ضد سرية النظم

[1]–د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه حقوق، جامعة عين شمس، ص101.

[2]-Alain benoussan , internet aspects juridiques, 2 édition hermes, Paris, 1998, P110.

[3]–أمين أعزان، المرجع السابق، ص 102.

[4]-Lois belge du 28 novembre 2000 relative à la criminalité informatique.

[5]-Christophe meunier, la loi du 28 novembre 2000 relative a la criminalité informatique ou lz droit penal et la procedure penal à 1ere numerique, revue de droit penal et de criminology, juillet, aout 2001, P 620.

[6]–أمين أعزان، المرجع السابق، ص 103.

المعلوماتية والمعطيات المخزنة أو المعالجة أو المرسلة عبر هذه النظم'، وتتضمن المادة 6 من القانون الجديد مادتين هما المادة 550 مكرر، والمادة 550 مكرر3.

وقد نصت المادة 550 مكرر على مايلي: "كل من دخل نظام معلوماتي مع العلم أنه غير مرخص له بذلك، يعاقب بالحبس من ثلاثة أشهر إلى سنة وبالغرامة، أو إحدى هاتين العقوبتين فقط، إذا ارتكبت الجريمة المنصوص عليها في البند الأول بنية الاحتيال تكون العقوبة من ستة أشهر إلى سنتين".

كل من يتجاوز المسموح به في الدخول إلى النظام المعلوماتي بنية الاحتيال أو إلحاق الضرر، ويعاقب بالحبس من ستة أشهر إلى سنتين وبالغرامة من 26 فرنك إلى 25000فرنك أو إحدى العقوبتين فقط.

الفرع الثاني: حجية الدليل الرقمي في التشريعات الانجلوسكسونية.

أولا: النظام الإنجليزي.

تقتضي القاعدة الأساسية في نظام القانون العام، أنه متى كان الدليل منتجا في الإثبات فهو مقبول أيا كانت طريقة تحصيله أي حتى ولو كان ذلك بطريق غير مشروع.

فنجد مثلا قضية (v.ouien) قام رجل الشرطة بتفتيش المستأنف بصورة غير قانونية، وعثر على كمية من سمك السالمون في جيبه، فتم قبولها كدليل في قضية الصيد بدون ترخيص، وقال في ذلك القاضي (mollor) أن عدم قبول الأدلة بسبب الحصول عليها بطريقة غير مشروعة، يمثل عائقا خطيرا لغدارة العدالة الجنائية، وبعد ذلك ظهر اتجاه آخر للقضاء يخفف من

صرامة وحدة مبدأ قبول أيا كانت طريقة تحصيلة [1] ولكن سرعان ما تم الرجوع إلى تكريس مبدأ الإطلاق في عدم استبعاد الدليل غير المشروع، والسير ف اتجاه نظرية الضبط الجرمي.[2]

ولما صدر قانون الشرطة والإثبات الجنائي في سنة 1984، والذي بدأ العمل به منذ سنة 1986، تضمن أحكاما تقيد استبعاد الأدلة غير المشروعة، حيث خصص ثلاث مواد لهذه الأحكام هي: المادة 76، المادة 78، وكذا المادة 2/82.

فنظمت المادة 76 قواعد استبعاد الاعتراف الذي يتم إما باستعمال وسيلة قصرية ضد المتهم،[3] أو أنه غير حقيقي أولا يعتمد عليه،[4] أي قبل أو حصل من غير شخص غير متهم3.

أما المادة 78 فهي تنظم السلطة التقديرية للقضاة في استبعاد الدليل، حيث يجوز للمحكمة أن تفرض السماح بقبول الأدلة التي قدمها الادعاء، إذ ظهر للمحكمة من خلال تقدير كافة الظروف بما فيها الظروف التي يتم تحصيل الدليل فيها، وأن قبول الأدلة يمكن أن يحدث تأثير على نزاهة الإجراءات إلى حد أن المحكمة تقضي بعدم قبولها.

ولكن هذه المادة جاءت خالية من أي معايير تسهل إعمالها، وكيف تعرف أن الإجراءات غير عادلة أو غير نزيهة، ولذلك أوجد بعض الفقهاء معايير يمك استلهامها أثناء تطبيق أحكام المادة 18 تتمثل في ثلاثة مبادئ، أولها مبدأ حسن النية (good faith)، وثانيها مبدأ الحماية(protecture principale) يدور حول فكرة حماية المتهمين وآخرها المخالفة الجوهرية (signifecant breath) لنصوص قانون الشرطة الجنائي العام 1984.

---

[1]-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، شهادة الماجستير، كلية الحقوق، جامعة الإسكندرية، دار الجامعة الجديدة، 2010، ص56.

[2]-عمار عوض عدس، التحريات إجراء من إجراءات البحث عن الحقيقة، دار النهضة العربية، القاهرة، 2007، ص 394.

[3]-هلالي عبد الله أحمد، حجية المخرجات الإلكترونية في المواد الجنائية، دار النهضة العربية، القاهرة، 2003، ص88.

[4]-أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، ط2، 2006، ص44.

وتطبيقا لذلك رفض القاضي في إحدى القضايا قبول التسجيلات على أساس أنها تمت من خلال اشتراك، حيث قام البوليس بتركيب جهاز التصنت على خط تلفون إحدى الشاكيات بناء على مواقفها، حيث افتعلت هذه الأخيرة عدة مكالمات تلفونية مع الشخص المشبوه، وقد تم تسجيل تلك المكالمات التي تضمنت موضوعات تدين المتهم.

ثانيا: النظام الأمريكي.

بالنسبة للولايات المتحدة الأمريكية قد تناولت بعض القوانين مسألة قبول الأدلة الجنائية الرقمية، ومن ذلك على سبيل المثال ما نص عليه قانون الحاسب الآلي الصاد في سنة 1984 في ولاية آيوا، وذلك لأن الأدلة الناتجة عن الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرنامج والبيانات المخزنة فيه، وأيضا ما احتوى عليه قانون الإثبات الصادر في سنة 1983 في ولاية كاليفورنيا، وذلك بأن النسخ المستخرجة من البيانات التي يحتويها جهاز الحاسب الآلي تكون مقبولة بوصفها أفضل وأنسب الأدلة المتاحة لإثبات هذه البيانات.[1]

وتشترط المحاكم في الولايات المتحدة الأمريكية لقبول الأدلة الجنائية الرقمية بصفة عامة أن يكون جهاز الحاسب الآلي يؤدي وظائفه بصورة سليمة، [2] وأيضا يكون هناك ارتباط بين الواقعة والأشخاص المشتبه فيهم، بالإضافة إلى أن يكون محل ثقة ومعتمد كشرط لقبوله.[3]

وعليه يقوم القضاء بتحديد درجة مصداقية وفاعلية هذا الدليل عن طريق إخضاعه لاختبار (داوبورت) والذي هو عبارة عن اختيار قانوني لتقرير صلاحية الدليل العلمي وصلته

[1] – علي حسن محمد طوالبية، التفتيش الجنائي على نظم الحاسوب والأنترنت (دراسة مقارنة)، عالم الكتب الحديث، الأردن، ط1، 2004، ص 59.

[2] – أحمد عبد الله هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة) في بحوث مؤتمر القانون والكمبيوتر والأنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، 2004، ص 429.

[3] – ممدوح عبد المطلب، المرجع السابق، ص 130.

بالواقعة الإجرامية، ونشأ هذا الاعتبار بموجب قرار المحكمة العليا في الولايات المتحدة الأمريكية، والتي أصدرته في قضية "داوبورت" ضد "ميريل دو للصناعات الدوائية" في سنة 1993.[1]

وبناء على هذا الاختيار تنحصر مسؤولية القاضي أثناء الجلسة في تحديد سلامة المنهجية المتبعة والطرق الفنية المتخذة في استخلاص الادلة الجنائية الرقمية، [2] وذلك من خلال استخدام أربعة معايير أساسية، يتمثل المعيار الأول (التجربة والاختيار) في التحقق من أنه سبق وأن تجربة الطريقة المتبعة في استخلاص الدليل الجنائي الرقمي والحصول على نفس النتائج عند المقاربة، وأما المعيار الثاني "نسبة الخطأ" يتمثل في التحقق من إمكانية وجود نسبة خطأ محتملة ترافق استخدام طريقة الاستخلاص والتحليل، وبالنسبة للمعيار الثالث (النشر)، فهو يتعلق بنشر الطريقة المتبعة في استخلاص الدليل ومراجعتها من قبل المختصين في هذا المجال، وأخيرا يتمثل المعيار الرابع (القبول) بقبول طريقة الاستخلاص من قبل المختصين المنتسبين للمجموعات العلمية والمتخصصة في وضع أنسب الوسائل والأساليب الواجب استخدامها في استخلاص الأدلة الرقمية.[3]

وتجدر الإشارة إلى أنه قبل ظهور اختيار (داوبورت) كانت محاكم الولايات المتحدة الأمريكية تبنت اختيار "فراي" في تقرير صلاحية الدليل العلمي بصفة عامة، والذي صدر بموجب قرار المحكمة العليا للولايات المتحدة الأمريكية في سنة 1923 وكان اختبار "فراي" مقتصرا فقط على معيارين وهما التجربة والاختيار بالإضافة إلى معيار القبول، [4] إلا أنه قد بينت عجزه في مواجهة أنواع جديدة من الأدلة العلمية والتي من بينها الأدلة الجنائية الرقمية، مما تحتم على الخبراء والمختصين في إيجاد معايير أخرى تتماشى مع تطور الأدلة الجنائية.[5]

---

[1] - Steve Bunting and wiliam wei, op cit, p500-501.

[2] - ممدوح عبد المطلب، المرجع السابق، ص 130.

[3] - المرجع نفسه، ص 130.

[4] - linda volonino and reynaldo aza anaza aldia, op cit, p 83.

[5] - ibid, p83.

لذا في حال عدم توفر هذه الشروط التي قررها القانون، يقوم القاضي باستبعاد الدليل الجنائي الرقمي مباشرة، بسبب أن دور القاضي في هذا النظام سلبي يقتصر فقط على مراعاة توافر الشروط القانونية المتطلبة في الدليل الجنائي التي حددها المشرع.

المطلب الثاني: حجية الدليل الرقمي في التشريعات العربية.

سوف نتناول في هذا الفرع مدى حجية الدليل الرقمي في التشريعات العربية من خلال التطرق إلى حجيته في مصر بصفة عامة، وفي التشريع الجزائري بصفة خاصة.

الفرع الأول: حجية الدليل الرقمي بصفة عامة مصر.

اتخذ التشريع المصري نهج التشريعات اللاتينية المتمثلة في القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الإيطالي والاسباني، وقوانين أمريكا اللاتينية.[1]

ويعتمد هذا النظام على نظم الإثبات التي يتقيد بها القاضي الجنائي، بل ترك حرية الاثبات لأطراف الخصومة في أن يقدموا ما يرون أنه مناسب لاقتناع القاضي الذي يبني الإثبات عقيدته من أي دليل يطرح أمامه، ولو وله أن يقدر القيمة الاقناعية لكل منهما حسبما تتكشف لوجدانه، حيث لا سلطان عليه في ذلك إلا ضميره.

ويتضح من خلال ذلك أن القاضي له مطلق الحرية في أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة والكشف عنها ما دام انه كانت هذه الطرق مشروعة.

ويقوم بتقدير كل دليل مطروح أمامه، لأن مبدأ الحرية ولاقتناع لدى القاضي هي تقدير الأدلة القائم، وله أن يستمدها من أي مصدر يطمئن إليه، دون أن يملي عليه المشرع حجية معينة أو يلزمه بإتباع وسائل محددة للكشف عن الحقيقة كقاعدة عامة.

[1]-أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، د.د.ن، 2005، ص91.

ويبين القاضي الأدلة التي اعتمد عليها وكانت مصدرا لاقتناعه، وإذا كان تقديره لا يخضع لرقابة النقض، ليس لها أن تراقبه في تقديره، إلا أن لها أن تراقب صحة الأسباب التي استدل بها على هذا الاقتناع.[1]

ولعل من أهم ما يبرر هذا المبدأ الذي خوله القانون للقاضي الجنائي هو ظهور أدلة علمية مثل الأدلة المستمدة من الطب الشرعي والتحاليل، وتحقيق الشخصية ومضاهاة الخطوط، ويلاحظ أن هذه الأمور لا تقبل أي قيود بشأنها عند تعويل القاضي عليها لتكوين عقيدته.

ولما كانت الوقائع الجنائية يمكن تحديدها مسبقا كما في القانون المدني لأنها ليس مما يحرر بها العقود، أن يمكن الحصول من الجاني على اعتراف مكتوب بها، فإن يتميز به موضوعية وحياد وكفاءة في اقتناع القاضي الجنائي.

ويعد من أوضح النماذج لتلك القضية التي نظرت أمام محكمة امن الدولة العليا والمتهم فيها أحد الأشخاص بالتخابر مع دولة إسرائيل، وقد تم تأجيل القضية لحين إحضار الديسكات ووحدات التخزين الداخلية بالحاسب الآلي الخاص بالمتهم لتفريغ محتوياتها، ولاشك أنه يعتبر دليلا هاما في القضية، تعترف به المحكمة، وقد يكون أساسا في تكوين عقيدة القاضي في حكمه.

الفرع الثاني: حجية الدليل الرقمي بصفة خاصة الجزائر.

المشرع الجزائري قد أخذ بنظام الإثبات الحر شأنه شأن المشرع الفرنسي، فمن خلال استقراء نصوص قانون الإجراءات الجزائية، نلاحظ مدى تكريسه لمبدأ الاقتناع الشخصي للقاضي، حيث نص المادة 212 منه على: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات، ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص...".

[1]-هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، ط1، 1997.

كما نصت المادة 307 أيضا على هذا المبدأ بقولها: "إن القانون لا يطلب من القضاة أن يقدموا على حساب عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقديراتهم أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبير، ون يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها، ولم يضع لها القانون السؤال الذي يتضمن كل نطاق".

ولكن استثناءا في بعض الجرائم المحددة حصرا في المادة 212 من قانون الإجراءات الجزائية، بعدم جواز إثبات بعض الجرائم بأي طرق من طرق الإثبات، وهو ما يعني الأخذ بنظام الإثبات المقيد(القانوني).

على العموم، وبالرجوع إلى موقف المشرع الجزائري من الأدلة الجنائية الرقمية، وانطلاقا من نص المادة 212 من قانون الإجراءات الجزائية، والتي أجاز فيها المشرع إثبات الجرائم بأي طريق من طرق الإثبات، وضع القاضي الحرية في تقدير الدليل بناء على اقتناعه الشخصي، يمكن القول أن المشرع سلك ما سلكه المشرع الفرنسي من خلال اعتبار الدليل الرقمي، [1] مثل باقي الأدلة الجنائية الأخرى، وإن السلطة التقديرية التي يتمتع بها القاضي تمتد لتشمل جميع الأدلة الجنائية بما فيها الأدلة الرقمية أيضا، هي لا تثير أشكالا بالنسبة للمشرع الجزائري مادام يعتنق حرية الإثبات، والقاضي مطالب فقط باحترام القواعد العامة المتعلقة بقبول الأدلة الجنائية أمام القضاء التي تأخذ شكل محاضر على إثر القيام بإجراء التفتيش، أو اعتراض المراسلات مثلا، أو تأخذ أيضا شكل تقدير خبرة فنية بمناسبة معاينة أو فحص، وتحليل الأدلة الجنائية الرقمية الناتجة عن أجهزة الحاسب الآلي وملحقاته.

[1]–بوزيد أغليس، تلازم مبدأ الإثبات الحر بالاقتناع الذاتي للقاضي الجزائي، دراسة تحليلية مقارنة بين القانون الجزائري والقانون المصري وبعض القوانين العربية، دار الهدى للنشر والتوزيع، عين مليلة، الجزائر، 2010، ص 110.

المبحث الثاني: حجية الدليل الرقمي أمام القاضي الجنائي.

يعتبر مبدأ حرية الاقتناع الشخصي للقاضي الجزائي من أهم عناصر الإثبات في الدعوى الجنائية، فالقاضي حر بأن يأخذ الأدلة التي يراها مناسبة للكشف عن الحقيقة ولو أن يحتوي بنفسه صدق الأدلة الجنائية، وله الحق في أن يستمد اقتناعه وعقيدته من أي مصدر يطمئن إليه، وحرية الاقتناع هي حرية خاصة بالقاضي من خلالها يحمل سلطة تقديرية ويبسطها على الأدلة الجنائية.

فبالرغم من أن النيابة العامة عليها أن تقيم الدليل على الإدانة والمتهم عليه أن يبقي هذا الدليل، إلا أن الالتزام القاضي بإدراك الحقيقة الواقعة أما المادية استجابة لمقتضيات التجريم جعلت له دورا إيجابيا يدرك بمقتضاه الحقيقة وتختلف عن دور القاضي المدني الذي يقتصر على الموازنة بين الأدلة التي يقدمها الأطراف دون البحث عن الحجج الأخرى من تلقاء نفسه.

المطلب الأول: ماهية اقتناع القاضي الجزائي بالدليل الرقمي.

إن الأدلة الرقمية سواء تلك المتواجدة على هيئة ورقة يتم إنتاجها عن طريق الطابعات أو الراسم، أو كانت شكل مخرجات رقمية كالأشرطة، الأقراص الممغنطة أو الضوئية وأسطوانات الفيديو، أو المصغرات الفيلمية وغيرها من الأشكال التقليدية، وإما تكون مخرجات مرئية يتم عرضها على شاشة الحاسوب تخضع جميعها لنظام الأدلة المعنوية الذي تأخذ به أغلب التشريعات المقارنة حديثا والذي تقوم على مبدأ الاقتناع الشخصي للقاضي الجنائي.

الفرع الأول: تعريف الاقتناع الشخصي للقاضي الجزائي.

هو الإيمان العميق والركون إلى صحة الوقائع التي يقدمها الأطراف المتنازعة والتي اعتمدها القاضي وتنتج عنها آثار عميقة في نفسية القاضي الجزائي، تتركه يصدر حكمه عن قناعة وحرية وإحساس كبير بإصابته في حكمه.[1]

ولقد أشار المشرع الجزائري إلى هذه المسألة بنصه على مبدأ الاقتناع القضائي الجزائي في المادة 307 من قانون الإجراءات الجزائية الجزائري، والتي هي مستوحاة من المادة 353 من قانون الإجراءات الجزائية الفرنسي.[2]

كما تطرق المشرع الجزائري إلى مبدأ الاقتناع القضائي في نص المادة 212 من قانون الإجراءات الجزائية الجزائري على: «**يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال الشخصية التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص**»، ويطبق المبدأ العام جهات الحكم القضائية.[3]

ثانيا: أساس مبدأ الاقتناع القضائي.

تناولت أغلب التشريعات المقارنة موضوع الاقتناع الشخصي للقاضي الجزائي وجسدته في قوانينها الإجرائية، كما تم الأخذ في أحكام محاكمها، ويتم تناول أهم الأنظمة القانونية وأهم الأحكام القضائية التي طبقت المبدأ دون أن نبين موقف كل من التشريع والقضاء الجزائري في هذا الصدد، يتم دراسة الأساس القانوني لمبدأ الاقتناع، ثم الأساس القضائي لمبدأ الاقتناع القضائي.

---

[1] – سامي جلال حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2004، ص 280.

[2] – هلال أمينة، الإثبات الجنائي بالدليل الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015/2014، ص66.

[3] – بن فريدة محمد، الإثبات الجنائي للجرائم المعلوماتية بالادلة الرقمية، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر، 2015، ص 193.

أ-الأساس القانوني لمبدأ الاقتناع القضائي:

حرصت الكثير من التشريعات على جعل مبدأ الاقتناع القضائي عنوانا للإثبات الجزائي، حيث يستند إليها القاضي في حكمه، فقد أقر المشرع الجزائري ذلك في قانون الإجراءات الجزائية على مبدأ الاقتناع الشخصي للقاضي الجزائي وجسده بنصوص واضحة، وهذا ما أوردته المادة 307 من قانون الإجراءات الجزائية الجزائري: «يتلو الرئيس قبل مغادرة قاعة الجنايات التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة... »

كما أوردته المادة 212/ف1 من نفس القانون الذي يتضمن توجيه القسم من الرئيس إلى الحل فين فيما يخص إجراءات انعقاد محكمة الجنايات.

ومن بين التشريعات التي أخذت بهذا المبدأ نجد القانون الفرنسي الذي يقر على مبدأ الاقتناع الشخصي للقاضي الجزائي لأول مرة وذلك ما جسدته في المادة 343 من قانون الإجراءات الجزائية،[1] في شأن التعليمات التي تلقى على محكمة الجنايات حتى الغي هذا الأخير بموجب القانون، إلا أن مضمون المادة السالفة الذكر أعاد القانون الجديد التأكيد عليها في نص المادة 353 من قانون الإجراءات الجزائية.

وتقر المادة 304 من قانون الإجراءات الجزائية الفرنسي على أنه: «**على المحلفين أن يحلفوا يمينا بأن يحكموا بالعدل لأدلة الاتهام وسائل الدفاع على ضمائرهم واقتناعهم الداخلي مع النزاهة التي يتمتع بها الإنسان الحر المستقيم** » وأيضا كما خول المشرع لرئيس محكمة الجنايات سلطة تفويضية بمقتضاها يمكنه أن يتخذ كافة الإجراءات التي تعتقد أنها مفيدة للكشف عن الحقيقة، حيث لا يقدم عليه سوى ضميره وشرفه حسب نص المادة 310 من قانون الإجراءات الجزائية الفرنسي.

[1] – محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 427.

كما نصت المادة 427/ف1 من قانون الإجراءات الجزائية الفرنسي فيما عدا الحالات التي ينص فيها القانون على خلاف ذلك تثب الجرائم بكل وسائل الإثبات ويقضي القاضي بمقتضى اقتناعه الشخصي.

أما التشريعات العربية أخذت بهذا المبدأ فقد تناول القانون المصري مسألة الاقتناع في المواد 291/ف1-300-302/ف1 من قانون الإجراءات الجزائية المصري.

وتنص المادة 302/ف1 قانون الإجراءات الجزائية المصري بحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حرياته.[1]

ونستخلص مما سبق أن أغلب التشريعات المعاصرة تأخذ بمبدأ الاقتناع القضائي مع اختلاف في الصياغة بين التشريعات اللاتينية والتشريعات الأنجلو أمريكية، ولكن العبرة ليس النص بل هو التعبير في جانبه العلمي الذي يقره القاضي في حكمه خاضعا بذلك لضميره دون تقييده بأي قيد، عدا القيود والضوابط التي وضعها القانون.

حيث يُخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ومن ثم النهي على الحكم المطعون فيه بحر القانون غير سديد مما يستوجب رفضه، ولما كان الثابت في قضية الحال أن الحكم الصادر من محكمة الجنايات بالبراءة كان بأغلبية الأصوات، وأن الأسئلة قد طرحت بصفة قانونية، وأن الأجوبة المعطاة كانت حسب الاقتناع الشخصي للقضاة الذي لا يخضع لرقابة المحكمة العليا ومتى كان كذلك استوجب رفض الطعن.[2]

وجاء بذات المبدأ في قرار آخر ما يلي: "من المقرر قانونا أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك ومن ثم فإن القضاة بما

[1] – بن فريدة محمد، المرجع السابق، ص 310.

[2] – قرار المحكمة العليا الجزائرية، الصادر بتاريخ 1987/06/30، الملف رقم 5097، المجلة القضائية، العدد الثالث لسنة 1991، ص 199.

يخالف هذا المبدأ يعد خرقا للقانون، ولما كان الثابت في قضية الحال أن قضاة الاستئناف ناقشوا أدلة الإثبات وأوجه دفاع المتهم واقتنعوا بعدم صحة دفاعه فيما يخص النكران للتهمة المنسوبة إليه علما أن الجريمة لم تكن من الجرائم التي ينص فيها القانون على إثباتها بنص خاص يكونوا قد طبقوا القانون تطبيقا سليما، ومتى كان الأمر كذلك استوجب رخص الطعن"[1]

وكما جاء في قرار آخر أنه: يمكن للقاضي تأسيس اقتناعه على أية حجة حصلت مناقشتها حضوريا أمامه.[2]

كما "لا يمكن لقضاة الموضوع أن يؤسسوا قرارهم إلا على الأدلة المقدمة لهم أثناء المرافعات والتي تم مناقشتها حضوريا"[3]

ولم يكن القضاء الجزائري الوحيد الذي انتهج هذا المبدأ، حيث نجد من بين هذه التشريعات القضاء الفرنسي بإدراجه هذا الأخير لمبدأ الاقتناع القضائي الذي يشمل قبول الدليل وتقديره وفقا لحرية القاضي الجزائي في تكوين اقتناعه، وذلك ما جاء به في المادة 427 من قانون الإجراءات الجزائية الفرنسي.[4]

أما القضاء المصري فقد أكدت محكمة النقض المصرية في العديد من أحكامها على حرية القاضي الجنائي في تكوين اقتناعه من أي دليل برامج إليه ما لم يفرض عليه القانون الأخذ بدليل معين.[5]

---

[1] – قرار المحكمة العليا الصادر بتاريخ 1991/01/29، الملف رقم 70690، المجلة القضائية، العدد الثالث لسنة 1991، ص 199.

[2] – مجموعة قرارات الغرفة الجزائية، 09جويلية 1990، المجلة القضائية، 1993، ص 153.

[3] – ر. غ.ج .م 28-03-1989 ملف 647-56، المجلة القضائية 1993-3، ص 291.

[4] – بن فريدة محمد، المرجع السابق، ص 313.

[5] – نقض جلسة 1939/03/06 مجموعة القواعد القانونية 31 رقم 62، ص 328. وكذا ورد في الطعن رقم 29020 جلسة 1998/02/08 لسنة 59 ق رقم 28، ص 193.

ونستخلص مما سبق من أحكام محاكم النقض في مختلف الأنظمة القضائية أن الاتجاه القضائي في عملية الإثبات يقوم أساسا على مبدأ الاقتناع الشخصي للقاضي الجزائي، وللقاضي السلطة التقديرية في الأخذ بالدليل بغض النظر سواء كان هذا الأخير رقميا أو دليلا ماديا دون تفاضل في الأدلة، فالعبرة في النهاية تعود إلى قناعته الشخصية.

الفرع الثاني: ممارسة القاضي الجزائي لمبدأ الاقتناع الشخصي بالدليل الرقمي.

إن ممارسة القاضي الجنائي لمبدأ الاقتناع الشخصي فيما يخص الدليل الرقمي، تتجسد هذه المظاهر في الممارسة من جهة، ثم تطبيقات هذه الممارسة فيما يخص الدليل من جهة أخرى، وعليه تجدر الإشارة إلى أن القاضي الجزائي في أغلب التشريعات القضائية لاسيما تشريعات الدول اللاتينية لم يتناول مسألة الدليل الرقمي كمسألة مستقلة في الإثبات، وإنما يخضعها للمبادئ العامة في الإثبات، فمثلها مثل أي دليل آخر، فالأدلة الرقمية ليست استثناء من الأدلة الأخرى فهي تخضع للقواعد العامة وعلى ما استقرت عليه الأحكام القضائية وعليه سيتم تناول هذه الجزئية كالتالي.

أولا: مظاهر ممارسة القاضي الجنائي لمبدأ الاقتناع بالنسبة للدليل الرقمي:

أوضحت محكمة النقض المصرية مظاهره لمبدأ الاقتناع القضائي في حكمها الصادر في 1939/04/12، كما نصت عليها المادة 302 من قانون الإجراءات الجزائية المصرية سالفة الذكر، وهو أيضا ما قضت به محكمة التمييز الكويتية في أحد أحكامها حيث تقضي بأن القاضي الجزائي يعتمد على تكوين قناعته الشخصية اعتمادا منه على الأدلة التي تعرض عليه وتتسع سلطته التقديرية لأخذ أو رفض أي دليل أو قرينة يرتاح إليها.[1]

[1] – محكمة التمييز الكويتية، 1976/06/30، المجلة القضائية العربية، الأمانة العربية لمجلس وزراء العدل العرب، العدد الأول، السنة الأولى، نيسان 1984، ص ص326-327.

أ-سلطة القاضي الجنائي في تقدير الأدلة الرقمية بذاتها:

يظهر من أحكام محاكم النقض أن للقاضي الجنائي أن يستبعد الدليل ويطرحه إن لم يطمئن إليه وأن يأخذ به كاملا أو يأخذ بالجزء الذي يطمئن إليه ويقتنع بصحته، [1] وهو الأمر الذي ينطبق على الأدلة الرقمية سواء أكانت في بيئتها الرقمية إما على شكل مخرجات طباعة أو اتخذت شكل صور أو مقاطع فيديو.

01-حرية القاضي الجنائي في استبعاد الأدلة:

للقاضي الجنائي أن يستبعد في مجال تقديره الدليل ما لم يطمئن إليه عندما يمارس سلطته في الدعوى موضوعيا، [2] ويعود عدم اطمئنان القاضي لقيمة الدليل الذي يطرحه تكمن في ضعف الدليل المستبعد في الدلالة على الحقيقة التي يسعى الحكم في جعلها عنوانا له بذلك القضاء، أو لأن هناك أدلة أقوى منه في الإثبات وكافية في تكوين قناعة المحكمة، كما قضت به محكمة تمييز دبي. [3]

02-حرية القاضي الجنائي في الأخذ بالدليل:

هذه الحرية لها صور عديدة فالقاضي يأخذ بمبدأ الاقتناع القضائي فيما يتعلق بالدليل، فللقاضي أن يأخذ به كاملا أو يأخذ بجزء منه دون الجزء الآخر، وأن يأخذ به المتهم دون شريكه،

[1] – شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 85.

[2] – جباري عبد الحميد، دراسة قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر، 2012، ص122..

[3] – محكمة تمييز دبي: وزن أقوال الشهود وتقديرها من حق محكمة الموضوع المنزلة التي تراه وتقر التقرير الذي تطمئن إليه وللمحكمة أنتعود على ما قاله شهود الإثبات وتعترض عما قاله شهود النفي فقضاؤها بالإدانة استناد إلى ادلة الثبوت يفيد دلالة أنها طرحت شهادتهم ولم ترد الأخذ بها.

وأن يأخذ بالدليل في حالة تعدد التهم دون التهم الأخرى،[1] وهذا كما قضت عليه محكمة دبي في قرارها.[2]

ب–سلطة القاضي الجنائي في تقدير الأدلة الرقمية من حيث مصدرها:

إن سيادة مبدأ الاقتناع القضائي في مجال الإثبات الجنائي، منحت للقاضي الجزائي الحرية في تقدير الأدلة، بغض النظر عن المصدر الذي استمدت منه المهم أن يكون مشروعا، [3] دون النظر عن أي مرحلة من مراحل الدعوى تحصل على هذا الأخير، كما له أن يعتد بمحاضر جميع الاستدلالات التي يحررها ضباط الشرطة المختصون وله أيضا سلطة عدم الاعتداد بها، [4] كما له أن يرفض تقرير خبرة أجريت في مرحلة التحقيقات بتعيين من قاضي التحقيق، إذن فالقاضي يقدر الدليل بحسب اقتناعه لا حسب الدليل ذاته، على أنه وجب عليه تسبيب الحكم إثر رفضه لهذا النوع من المحاضر أو التقارير كي لا يتعسف القاضي في استعمال حقه.[5]

المطلب الثاني: الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي.

إن الأصل العام أن القاضي الجنائي حر في تقدير الأدلة المطروحة عليه في الدعوى عملا بمبدأ الاقتناع الشخصي، فهو غير ملزم بإصدار حكم الإدانة أو البراءة لتوافر دليل معين طالما أنه لم يقتنع به، وهذا الأمر وضعت له ضوابط حيث لا تعطي لهذا القاضي الجنائي مطلق الحرية التي يتمتع بها لغاية يراها المشرع ضرورية.[6]

---

[1] – محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011، ص 45.

[2] – محكمة تمييز دبي: أنه من المقرر للمحكمة أن تأخذ بأقوال الشاهد في مرحلة من مراحل التحقيق والمحاكمة، فلها أن تأخذ بأقواله في محضر الجلسة وإن خالفت قولا آخر أثناء تحقيقات النيابة العامة.

[3] – شيماء عبد الغني، المرجع السابق، ص 94.

[4] – المرجع نفسه، ص 95.

[5] – محمد علي العريان، المرجع السابق، ص 52.

[6] – بهلولي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، رسالة ماجستير، كلية الحقوق، جامعة الحاج لخضر، الجزائر، 2011، ص 189.

وعلى ذلك فإن دراستنا للضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي سنتطرق فيها في البدء إلى الضوابط التي تتعلق بمصدر الاقتناع أولا، ثم نتكلم عن الضوابط المتعلقة بالاقتناع في حد ذاته ثانيا.

الفرع الأول: الضوابط المتعلقة بمصدر الاقتناع.

إن الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي، والتي تتعلق بهذا الأخير تكون هي الضوابط المستقاة في حد ذاته وتتمثل في:

1-مشروعية الدليل الرقمي:

هذا الضابط مكمل لقيد مشروعية الدليل الرقمي، فعلى القاضي أن يستمد اقتناعه من أدلة مقبولة ومشروعة، [1] فإن مسألة قبول هذا الدليل الرقمي، ويستبعد في المقابل جميع الأدلة الإلكترونية غير المقبولة، لأنه من غير المعقول أن تكون عنصرا من عناصر اقتناعه وتقديره.[2]

فمشروعية ومقبولية الدليل الرقمي تعد ضمانا للحرية الفردية وللعدالة، وأيضا تجبر القائمين على جمع وتحصيل الأدلة المتعلقة بالإدانة أن يقوموا بعملهم على أكمل وجه، وذلك حتى لا يتم هدر أهم مبدأ وهي قرينة البراءة، ولهذا فعلى القاضي الجنائي أن يستمد اقتناعه الذاتي في مجال الإثبات المتعلق بالجرائم الإلكترونية، من دليل رقمي مشروع ومقبول.[3]

[1] - بهلولي مراد، المرجع السابق، ص 190.

[2] - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010، ص 51.

[3] - المرجع نفسه، ص 269.

2-ضرورة طرح الدليل ومناقشته في الجلسة:

يطرح الدليل الرقمي في الجلسة للمناقشة بصفة عامة يجب على القاضي أن يستمد اقتناعه من أدلة طرحت في الجلسة أو خضعت للمناقشة من طرف الخصوم الذين يتواجهون بهذه الأخيرة، واستناد القاضي لأدلة لم تعرض للمناقشة موجب للبطلان.[1]

فهذه القاعدة تعني أن القاضي لا يجوز أن يؤسس اقتناعه إلا على عناصر الإثبات التي طرحت في جلسات المحكمة، وخصصت لحرية منافسة أطراف الدعوى إعمالا لمبدأ المحاكمة الجزائية والمتمثلة في الشفوية بحسب المواد: 300-304-353 من قانون الإجراءات الجزائية الجزائري، ومبدأ العلنية بحسب المواد 285-342-355-399 من قانون الإجراءات الجزائية الجزائري، وكذا مبدأ المواجهة بحسب المادة 212/ف2 من نفس القانون وهذه المناقشة عليها أن تأخذ في عين الاعتبار ضرورة احترام حقوق الدفاع بإعطاء فرصة للمتهم للاستفسار حول كل وسيلة من وسائل الإثبات المقدمة أمام القاضي الجنائي هذا من جهة، ومن جهة ثانية يتعين توافر المناقشة الحضورية لأنها تعتبر مطلبا منطقيا وتنطوي على فحص شامل وجماعي لكل وسيلة إثبات، [2] وضابط وضعية الدليل الرقمي يقوم على عنصرين أساسيين، حيث يتمثل العنصر الأول في أن يكون الدليل الإلكتروني أصل في أوراق الدعوى.[3]

---

[1] - العربي شحط عبد القادر ونبيل صقر، الإثبات في المواد الجنائية، دار الهدى للطباعة والنشر والتوزيع، الجزائر، د س ن، ص 26.

[2] - ينظر: المواد 300-304-353-399-356-212/ف2 من الأمر 66-155 المتضمن قانون الإجراءات الجزائية المعدل والمتمم بموجب القانون رقم 17- 07 المؤرخ في 28 جمادى الثانية عام 1438هـ الموافق لـ 27 مارس 2017، ج ر ج ج، العدد 20، الصادرة في 28 مارس 2017.

[3] - باطني غنيمة، الجريمة الإلكترونية، أطروحة لنيل شهادة الدكتوراه، جامعة باجي مختار، عنابة،2015، ص 163.

الفرع الثاني: الضوابط المتعلقة بالاقتناع ذاته.

إن مبدأ الاقتناع القضائي الذي تبناه المشرع الجزائري كغيره من التشريعات، يتيح للقاضي الجنائي حرية كبيرة في تقدير عناصر الإثبات بما في ذلك الدليل الرقمي، والذي يعتبر من أهم النتائج التي تترتب عن هذا المبدأ والسبب في الأخذ بهذا الدليل المستحدث، لذلك فإن تقدير كفاية الدليل الإلكتروني أو عدم كفايته في إثبات الجريمة الإلكترونية ونسبتها إلى فاعلها، أمر تختص به محكمة الموضوع المعروض عليها هذا الأخير ولا تخضع في ذلك لرقابة المحكمة العليا التي يقتصر دورها على مراقبة المنطق القضائي لمحكمة الموضوع عن طريق مراقبتها صحة تسبيب الحكم.[1]

إن القاضي في تكوين اقتناعه وإن كان حرا في اختياره للأدلة التي يطمئن إليها، إلا أن هذا الأمر مشروط بأن يكون استنتاج القاضي حقيقة الواقعة وما كشف عنها من ادلة لا يخرج عن مقتضيات العقل والمنطق.[2]

وبهذا يكون القاضي قد توصل إلى اقتناع تام وتأكده بالحقيقة وذلك ما يعتبر يقين، ويتم التوصل إلى هذا الأخير عن طريق ما تستخلصه وسائل الإدراك المختلفة من خلال ما سبق وتقدم إليه من وقائع في الدعوى.[3]

وهذا يعني أنه في حالة إثبات القاضي الشك حول براءة أو إدانة المتهم لا يسعه إلا الحكم بالبراءة وذلك تقيدا بقاعدة الشك يفسر لصالح المتهم، وهو الأمر الذي حرص عليه المشرع الجزائري في آخر تعديل لقانون الإجراءات الجزائية لسنة 2017 في المادة الأولى منه التي جاءت كالتالي: «**أن يفسر الشك لصالح المتهم**»

[1] – باطلي غنيمة، المرجع السابق، ص 114.

[2] – هلال أمينة، المرجع السابق، ص 112.

[3] – المرجع نفسه، ص 114.

وفي كل الحالات يجب تسبيب الحكم الذي يقوم به القاضي الجزائي من وقت سريان الدعوى إلى غاية صدور الحكم فيها، كما أن القاضي يثبت فهمه للواقع فهما كافيا، وتكفيه لكل الأدلة والقرائن الواردة وأنه قد قدرها تقديرا سليما وإضافة إلى أنه يثبت جدارته في تطبيق القانون تطبيقا سليبا.

ومدلول التسبيب في التشريع والقضاء الجزائري أن التشريع لم يضع مدلولا إلا أنه أشار إلى ضرورة بيان الأسباب الواقعية والقانونية، وأسباب الرد على الطلبات الهامة والدفوع الجوهرية، ولكن من ناحية أخرى نجد أن القضاء قد وضع الضوابط الصحيحة لتسبيب الأحكام والاستقرار على مدلول محدد للتسبيب لا يصح إلا به كما نراه في المادة 309 من قانون الإجراءات الجزائية نص على الحكم بالبراءة واستبعاده عن محكمة الجنايات.

الخاتمة

خاتمة:

يعد موضوع إثبات الجريمة الإلكترونية الأساس والعمود الفقري الذي تبنى على أساسه أية سياسية جنائية لمكافحة هذا النوع من الجرائم، لأنه بدون آليات إثبات واضحة ومحددة، فإن كل الإجراءات الأخرى تصبح بدون جدوى، ولا تحقق الغرض المرجو من هذه السياسة، وإن المختصين والعاملين في الميدان، لا يدركون جيدا مدى أهمية هذا الموضوع لإثبات الجريمة الإلكترونية، والحاجة الملحة إليه لما له م دور فعال في تسهيل عملهم والقيام بمهامهم في إطار من الوضوح والشرعية الإجرائية، لأن الإثبات والبحث عن الدليل هو حجر الزاوية والهدف الرئيسي لسلطات البحث والتحري للحصول على دليل مقبول ذو مصداقية، والذي لا يمكن تحقيقه إلا من خلال أدوات ووسائل علمية تكرس في النصوص القانونية للجوء إليها واستغلالها في اقتفاء آثار مرتكبي هذه الجرائم وسد المنافذ عليهم في الإفلات من العقاب.

حيث تبين من خلال دراستنا أن الاستخدام المتزايد لتكنولوجيا الإعلام والاتصال الذي أفرز الجريمة الإلكترونية، والتي تستهدف جميع مستخدمي ومستعملي هذه التكنولوجيا من أفراد ومؤسسات، هذا ما اكسبها طابعا خاصا من حيث وسائل ارتكابها ومن حيث مرتكبيها والبيئة التي تقع فيها.

لقد اتضح لنا أن الدليل الرقمي ومن خلال طبيعته الفنية يصلح لان يكون دليلا لإثبات الجريمة الإلكترونية، بالرغم من انه دليل غير مادي قد يسهل إخفاؤه وتدميره ومحو أثره، كما يسهل إثباته واسترجاعه في نفس الوقت، وكذا عملية إثباته تحتاج إلى الخبرة التقنية والفنية.

وبعد محاولة البحث عن مختلف الجوانب والمشكلات التي أثارها الدليل الرقمي، ينبغي علينا إبراز أهم النتائج:

*/الدليل الرقمي هو الوسيلة الرقمية الناتجة من تقنية المعلومات والتي يتم التنقيب عنها في العالم الافتراضي ومن شكليات الاتصال والأجهزة الإلكترونية.

*/بفضل التقدم العلمي والتكنولوجي، تم ظهور جرائم مستحدثة جديدة في مجال الجرائم المعلوماتية عديدة ومخاطرها كثيرة لطبيعة استخدام التقنية الرقمية في شتى الميادين.

*/تتميز الجرائم المعلوماتية بوقوعها في بيئة المعالجة الآلية للبيانات مما اكسبها صعوبة في الاكتشاف وبالتالي صعوبة في الإثبات.

*/الدليل الرقمي ذو طبيعة غير مرئية يصعب الحصول عليها، إلا أن التطور التقني أوجب برامج يمكن بواسطتها استرجاعه بالرغم من عملية محوه.

*/القصور الواضح في التشريع الجزائري حول طرق الحصول على الدليل الرقمي.

*/الدليل الرقمي لا يقتصر استخدامه فقط لإثبات الجريمة الإلكترونية، إنما يستخدم في إثبات الجرائم التقليدية.

*/إن الدليل الرقمي مثله مثل باقي الأدلة في إثبات الجريمة، فهو يخضع للسلطة التقديرية للقاضي الجنائي أي يخضع لقناعة القاضي.

بعد استعراضنا أهم النتائج يمكن الإشارة إلى مجموعة من الوصيات ينبغي الأخذ بها، وتتجلى في:

*/العمل على تحديث القواعد القانونية الإجرائية لكي تتماشى مع خاصية تطور الجريمة الإلكترونية ووسائل إتباعها، والاعتماد عليها حتى في إثبات الجريمة التقليدية.

*/الاهتمام بالخبرة العلمية لما لها من دور فعال في مجال الإثبات الجنائي، وذلك من خلال الاعتراف بقيمتها في الآليات دون إخراجها من دائرة السلطة التقديرية للقاضي.

*/تحقيق التعاون والتنسيق بين جهاز العدالة والشبكات المزودة لخدمة الاتصالات السلكية واللاسلكية وشبكة الانترنت، وذلك بتقديم جميع المعلومات التي تفيد في التحقيق.

*/العمل على تكوين القضاة والخبراء الفنيين وإرسالهم إلى دورات فنية متخصصة في مجال التعامل مع الأدلة الجنائية الرقمية.

*/إدراج موضوع الأدلة العلمية في المقررات الدراسية سواء في الجامعات أو في معاهد التكوين الخاصة بالقضاة والمحامين، لإزالة الغموض الذي يكتنف هذه الأدلة وحجيتها في الإثبات الجنائي.

وفي ختام هذا البحث لا يسعنا سوى القول إن أصبنا فمن الله، وذلك فضل الله يؤتيه من يشاء من عباده، والله ذو الفضل العظيم، وإن أخطأنا فمنا ونتحمل وحدنا عواقبه، وأسأل الله سبحانه وتعالى أن يديم علينا نعمة الإيمان والتوفيق.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: الإتفاقيات الدولية.

1-إتفاقية الجريمة الإلكترونية، مجلس أوروبا، سلسلة المعاهدات الأوروبية رقم 185، بودابست في 23 نوفمبر/ تشرين الثاني، 2001م.

ثانيا: النصوص التشريعية.

1-القانون رقم 08-09 المؤرخ في 18 صفر عام 1429هـ الموافق لـ 25 فبراير 2008، يتضمن قانون الإجراءات المدنية والإدارية، الصادر في 02 مارس 2008، ج ر ج ج، العدد 11، الصادرة في 03 مارس 2008.

2-الأمر رقم 66-155 المؤرخ في 18 صفر عام 1436هـ الموافق لـ 08 يونيو 1996، يتضمن قانون الإجراءات الجزائية المعدل والمتمم، ج ر ج ج، العدد 48، الصادرة في 11يونيو1966، المعدل والمتمم بالقانون رقم 17-07 المؤرخ في 27مارس2017، ج ر ج ج، العدد 48، الصادرة في 29 مارس 2017.

3- القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من جرائم الإعلام والاتصال ومكافحتها المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 غشت 2009، ج ر ج ج، العدد47.

ثانيا: الكتب.

1-إبراهيم بلعليان، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2012.

2-أحمد رضا، معجم متن اللغة، دار الكتب العلمية، بيروت، لبنان، 1992.

3-أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، ط2، 2006.

4-أحمد فتحي سرور، أصول الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1969.

5-أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، د.د.ن، 2005.

6-بكري يوسف بكري، التفتيش عن المعلومات في الوسائل التقنية الحديثة، دار الفكر الجامعي، مصر، ط1، 2011.

7-بوزيد أغليس، تلازم مبدأ الإثبات الحر بالاقتناع الذاتي للقاضي الجزائي، دراسة تحليلية مقارنة بين القانون الجزائري والقانون المصري وبعض القوانين العربية، دار الهدى للنشر والتوزيع، عين مليلة، الجزائر، 2010.

8-جباري عبد الحميد، دراسة قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الجزائر، 2012.

9-حسن طاهر دواد، جرائم نظام المعلومات، الإصدار رقم 244 لأكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000.

10-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الاردن، ط1، 2011.

11-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، مصر، ط 1، 2009.

12-سامي جلال حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2004.

13-سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الأنترنت)، دار النهضة العربية، مصر، 2007.

14-شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2007.

15-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، شهادة الماجستير، كلية الحقوق، جامعة الإسكندرية، دار الجامعة الجديدة، 2010.

16-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010.

17-عبد القاهر الجرجاني، كتاب التعريفات، دار العلم للملايين، مصر، د س ن.

18-عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، دار هومة، الجزائر، ط4، 2013.

19-العربي شحط عبد القادر ونبيل صقر، الإثبات في المواد الجنائية، دار الهدى للطباعة والنشر والتوزيع، الجزائر، د س ن.

20-علي حسن محمد طوالبية، التفتيش الجنائي على نظم الحاسوب والأنترنت (دراسة مقارنة)، عالم الكتب الحديث، الأردن، ط1، 2004.

21-عبد الفتاح بيومي حجازي، المبادئ الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، الإسكندرية، ط1، 2006.

22-علي حسن محمد طوايلية، التفتيش الجنائي على نظم الحاسوب والأنترنت 'دراسة مقارنة'، عالم الكتب الحديث، الأردن، 2004.

23-علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية، الموصل، 2012.

24-عمار عوض عدس، التحريات إجراء من إجراءات البحث عن الحقيقة، دار النهضة العربية، القاهرة، 2007.

25-عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرشد الفيدرالي الأمريكي للتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية، دار النهضة العربية للنشر والتوزيع، القاهرة، 2008.

26-محمد الأمين البشيري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط1، 2004.

27-محمد بن مكرم ابن منظور، لسان العرب دار صادر، بيروت، د س ن.

28-محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011.

29-محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي، ديوان المطبوعات الجامعية، الجزائر، 1999.

30-ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم عبر الكمبيوتر، مركز شرطة دبي، 2005.

31-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي في جرائم الكمبيوتر والانترنت، مصر، دار الكتب الوطنية، 2006.

32-مأمون سلامة، الإجراءات الجزائية في التشريع المصري، دار النهضة العربية، ط 1، القاهرة، 1981.

33-عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والانترنت، دراسة معمقة في جرائم الحاسب الآلي والانترنت، مصر، بهجات للطباعة والتجليد، 2009.

34-ممدوح عبد الحميد، جرائم الكمبيوتر عن الانترنت، إصدارات مكتبة الحقوق الشارقة، الإمارات، 2000.

35-هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية 'دراسة مقارنة'، مكتبة الآلات الحديثة، أسيوط، 1994.

36-هلال عبد الإله أحمد ، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، 1997.

37-الوفا محمد أبو الوفا، شرح قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة، ط 1، 2018.

38-هلالي عبد الله أحمد، حجية المخرجات الإلكترونية في المواد الجنائية، دار النهضة العربية، القاهرة، ط2، 2003.

ثالثا: الأطروحات والرسائل الجامعية:

1-أحمد بن عبد الله الرشودي، حجية الوسائل الإلكترونية في الإثبات الجنائي (دراسة تأصيلية مقارنة تطبيقية)، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه فلسفة في العلوم الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2008.

2-أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، رسالة دكتوراه حقوق، جامعة عين شمس.

3-باطني غنيمة، الجريمة الإلكترونية، أطروحة لنيل شهادة الدكتوراه، جامعة باجي مختار، عنابة، 2015.

4-بن فريدة محمد، الإثبات الجنائي للجرائم المعلوماتية بالادلة الرقمية، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر، 2015.

5-حسن محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة دكتوراه في الحقوق، جامعة عين شمس، 2000.

6-عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، 2006.

7-مفيدة سويدان، نظرية الاقتناع الذاتي للقاضي الجنائي، أطروحة دكتوراه في القانون، كلية الحقوق، جامعة القاهرة، 1985.

8-فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق، جامعة بغداد، 1992.

9-بهلولي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، رسالة ماجستير، كلية الحقوق، جامعة الحاج لخضر، الجزائر، 2011.

10-ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية –دراسة تأصيلية تطبيقية- رسالة ماجستير، جامعة نايف العربية للعلوم الامنية، كلية الدراسات العليا، السعودية، 2012.

11-سالم بن حامد بن علي البلوي، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

12-عبد الرحمن بن محمد بن عبد الله العجلان، الدليل عن الأصوليين (حقيقته وتقسيماته)، رسالة مقدمة لنيل درجة الماجستير، جامعة الإمام محمد بن سعود الإسلامية، 1415هـ.

13-نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012.

14-سالم بن حماد البلوي: التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة ماجستير في العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

15-هلال أمينة، الإثبات الجنائي بالدليل الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015/2014.

رابعا: المقالات والمجلات العلمية.

1-أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الامنية والتدريب، العدد 58، المجلد 29، أكاديمية نايف العربية للعلوم الأمنية، السعودية، دت.

2-بوعناد فاطمة الزهراء، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة الدراسية للقانون، العدد01، جامعة الجيلالي اليابس، سيدي بلعباس، 2013.

3-فاطمة زهرة بوعنان، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد01، الجزائر، 2013.

4- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار الإثبات الجنائي، بحث مقدم للمؤتمر العلمي الأول (حول الجوانب القانونية والأمنية للعمليات الإلكترونية)، انعقد المؤتمر بأكاديمية شرطة دبي، مركز البحوث والدراسات في دبي بتاريخ 26، 28 نيسان 2003، منشور بالعدد رقم01، 2003.

5-محكمة التمييز الكويتية، 1976/06/30، المجلة القضائية العربية، الأمانة العربية لمجلس وزراء العدل العرب، العدد الأول، السنة الأولى، نيسان 1984.

خامسا: المؤتمرات والأبحاث العلمية.

1-أحمد أبو القاسم، الدليل الجنائي ودوره في إثبات جرائم الحدود والقصاص، بحث منشور بالمركز العربي للدراسات الأمنية والتدريب، الرياض، 1991.

2-أحمد عبد الله هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة) في بحوث مؤتمر القانون والكمبيوتر والأنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، 2004.

3--عبد الناصر محمد محمود فرغلين د. عبيد سيف سعيد المسماري، ورقة بحثية مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية وللطب الشرعي، 'الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية'، دراسة تطبيقية مقارنة، الرياض، المنعقد في الفترة: 02، 1148/11/04هـ الموافق لـ: 12، 2007/11/14.

4-علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت،/ والذي عقد خلال الفترة 2000، كلية الشريعة والقانون، جامعة الإمارات.

5-ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (tcp-ip) في البحث وتحقيق الجرائم على الكمبيوتر، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، 26، 28 نيسان 2003، دبي.

6-ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول ECP/IP في بحث وتحقيق الجرائم على الكمبيوتر، بحث منشور على شبكة الانترنت على موقع الدليل الإلكتروني للقانون العربي بتاريخ 2006/08/17.

7-ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسم، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر الأعمال المصرفية والإلكترونية، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة التجارة والصناعة دبي، في الفترة من 10، 2003/05/12، مج5.

سادسا: الأحكام والقرارات القضائية.

1-قرار المحكمة العليا الجزائرية، الصادر بتاريخ 1987/06/30، الملف رقم 5097، المجلة القضائية، العدد الثالث لسنة 1991.

2-قرار المحكمة العليا الصادر بتاريخ 1991/01/29، الملف رقم 70690، المجلة القضائية، العدد الثالث لسنة 1991.

3-مجموعة قرارات الغرفة الجزائية، 09جويلية 1990، المجلة القضائية، 1993.

سابعا: المراجع باللغة الأجنبية.

1-Eaghamcasey, pigtailevidence and computer crime, London, academicpress, 2000.

2-Merk et veter traite de droit, paris, 1967..

3-Vincent grymbaunv le droit de reproduction a l'heure de la societé de l'information, A propos de la direction, 2001/ 29/CE de certains aspects du droit d'auteur et des droits voisins dans la societé de l'information .

4-Fourth amendment and the internet, hearing before the subcommittee on the constitution of the commentte on the judiciary bouse of representatives one hundred sisch congress second session april 6 2000, Serial no, 135.

5-Fourth amendment and the internet , Op.cit, "the creator of the melissa vivy and the individual who created a fraudulent bo blooglerg news service website in oder to artificially drive up the stock puce of pair cain, a telecommunication", compary based in california.

6-Eoghan casey computer et internet crime FAQ-Avialable online in feb 2001 at http://www.foreusic science.com/gov computer, htmp.

7-Tgi paris, 17 ch, correc, 28/02/1999, note: maitre stephane lilti P.3 desponible enlegna a now, 1999.http://www.legalis; netljnet ecommentaire lelti, 28/01.htm.

8-Alain benoussan , internet aspects juridiques, 2 édition hermes, Paris, 1998.

9-Lois belge du 28 novembre 2000 relative à la criminalité informatique.

10-Christophe meunier, la loi du 28 novembre 2000 relative a la criminalité informatique ou lz droit penal et la procedure penal à 1ere numerique, revue de droit penal et de criminology, juillet, aout 2001.

ثامنا: المواقع الإلكترونية.

1-www.sudanradio.inf/php/ub.353/showthread.ph2p=1548langi=2.

2-www.arablawinfo.com/reseauch search.asp ?va ;idate :articles et articald :133.

3-Htt://Edu.arabsgate.com/shouthread.php ?t=502020.

4-http://www-f-law.net

فهرس الموضوعات

فهرس الموضوعات

كلمة شكر .....

الإهداء .....

قائمة المختصرات .....

مقدمة ..... أ

الفصل الأول: الإطار المفاهيمي للدليل الرقمي

المبحث الأول: مفهوم الدليل الرقمي 07

المطلب الأول: تعريف الدليل الرقمي والفرق بينه وبين الدليل الجنائي التقليدي .. 07

الفرع الأول: تعريف الدليل الرقمي..... 07

الفرع الثاني: الفرق بين الدليل الرقمي وبين الدليل التقليدي..... 11

المطلب الثاني: خصائص الدليل الرقمي وأنواعه 14

الفرع الأول: خصائص الدليل الرقمي 14

الفرع الثاني: أنواع الدليل..... 17

المبحث الثاني: إجراءات جمع الدليل الرقمي وحجيته في الإثبات الجنائي أمام القضاء الجنائي

..... 20

المطلب الأول: إجراءات الجمع بين الأحكام التقليدية والأحكام الإجرائية..... 21

الفرع الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني..... 21

الفرع الثاني: الإجراءات الحديثة لجمع الدليل الإلكتروني..... 36

المطلب الثاني: طرق الحصول عليه..... 40

الفرع الأول: مصادر الحصول على الدليل الإلكتروني..... 40

الفرع الثاني: البرامج المستخدمة في جمع الأدلة الإلكترونية 41

الفرع الثالث: الأجهزة والأنظمة الواجب فحصها للحصول على الدليل الإلكتروني 43

الفرع الرابع: الحصول على الدليل الرقمي من بروتوكولات الانترنت ECP/IP .. 53

الفصل الثاني: حجية الدليل الرقمي في التشريعات المقارنة وأمام القاضي الجنائي

المبحث الأول: حجية الدليل الرقمي في التشريعات المقارنة 57

المطلب الأول: حجية الدليل الرقمي في التشريعات الأجنبية 57

الفرع الأول: حجية الدليل الرقمي في التشريعات اللاتينية..... 58

الفرع الثاني: حجية الدليل الرقمي في التشريعات الانجلوسكسونية 61

المطلب الثاني: حجية الدليل الرقمي في التشريعات العربية..... 65

الفرع الأول: حجية الدليل الرقمي بصفة عامة مصر 65

الفرع الثاني: حجية الدليل الرقمي بصفة خاصة الجزائر 66

المبحث الثاني: حجية الدليل الرقمي أمام القاضي الجنائي 68

المطلب الأول: ماهية اقتناع القاضي الجزائي بالدليل الرقمي 68

الفرع الأول: تعريف الاقتناع الشخصي للقاضي الجزائي..... 69

الفرع الثاني: ممارسة القاضي الجزائي لمبدأ الاقتناع الشخصي بالدليل الرقمي.... 73

المطلب الثاني: الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي 75

الفرع الأول: الضوابط المتعلقة بمصدر الاقتناع..... 76

الفرع الثاني: الضوابط المتعلقة بالاقتناع ذاته 78

خاتمة..... 81

قائمة المصادر و المراجع 85

فهرس الموضوعات.....95