وزارة التعليم العالي والبحث العلمي
جامعة الدكتور مولاي الطاهر
كلية الحقوق والعلوم السياسية

بعنوان:

الإثبات الجزائي في الجرائم الإلكترونية بأدلة رقمية

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر في الحقوق
تخصص:قانون جنائي وعلوم جنائية

من إعداد الطالبة:
عواد منال حنان

تحت إشراف الدكتور:
عياشي بوزيان

أعضاء لجنة المناقشة

الدكتور: عياشي بوزيان ..... مشرفا مقررا

الدكتور: عثماني عبد الرحمان ..... رئيسا

الأستاذ:شيخ قويدر..... عضوامناقشا

الأستاذ:مرزوق محمد.....عضوامناقشا

السنة الجامعية

2019 – 2018

بسم الله الرحمن الرحيم
١٤٢٠
اللهم صل وسلم على محمد وآل محمد

شكر و عرفان

مصداق لقوله تعالى:

﴿وَإِذْ تَأَذَّنَ رَبُّكُمْ لَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ وَلَئِنْ كَفَرْتُمْ إِنَّ عَذَابِي لَشَدِيدٌ﴾

نحمد الله بمنه وكرمه علينا و توفيقه لنا بإتمام هذا البحث المتواضع الذي هو بين أيديكم.

و إقتداء بسنة نبينا محمد ﴿من لم يشكر الناس لم يشكر الله﴾

نتقدم بالشكر الجزيل إلى الدكتور المشرف " **عياشي بوزيان**"

على نصائحهم وإرشاداتهم المنهجية والعلمية التي

لم يبخلا بها علينا طوال إنجاز هذا البحث، كما نتوجه بالشكر إلى كل من قدم لنا يد العون من قريب أو بعيد.

وفي الأخير نتقدم بشكرنا الواسع لأوليائنا وأساتذتنا الكرام

وزملائنا الذين وقفوا على نجاحنا طيلة تواجدنا بالجامعة

إهداء

أهدي هذا العمل المتواضع:

إلى التي جعل الله الجنة تحت أقدامها، وريحانة حياتي، وبهجتها التي غمرتني بعطفها وحنانها، وأنارت لي درب حياتي، وكلما جارت على الأيام بكيت في حضنها، وكانت لي عونا، الصدر الرحب الحنون، والقلب العطوف، **أمي العزيزة الغالية**

إلى جدي وجدتي حفظهم الله وأطال لي في عمرهم.

وأهدي هذا العمل إلىإخوتي الأعزاء

"**سعيدة**"، "**هناء**"، "**سناء**"

"**أسامة**"، "**وسيم**"، "**رفيق**"

إلى الدكتور المحترم " **عياشي بوزيان**"

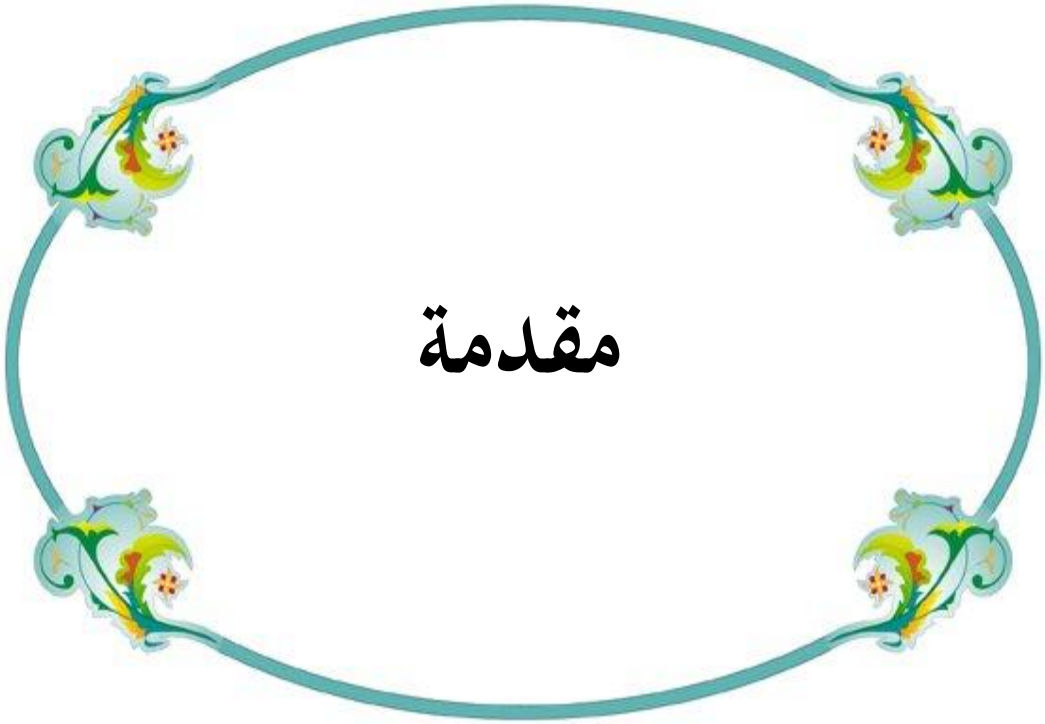
إلى"**خلف عبد الله**"

إلى كل الأساتذة وعمال الإدارة بالجامعة

عواد منال حنان

قائمة المختصرات

ج.ر:	الجريدة الرسمية
ق.ع.ج :.....	قانون العقوبات الجزائري
ق.إ.ج.ج :.....	قانون الإجراءات الجزائية
ق.م.ج:	قانون المدني الجزائري
ج:	الجزء
ط:	الطبعة
ب.ط :.....	بدون طبعة



مقدمة

مقدمة:

إن التطور المتسارع الذي شهدته نواحي الحياة في جميع المجالات، حيث استفاد محترفواالإجرام من هذا التطور فلم تعد الجريمة ترتكب بشكل تقليدي بل أصبحت تستدعي إلى استعمال الحاسب الآلي ونظم المعلومات كأداة في إحداث الجريمة والمتمثلةأساسا في ظهور جرائم مستحدثة لم تكن معهودة من قبل، التي أطلق عليها مصطلح الجرائم المعلوماتية.

ولمكافحة هذه الجريمة أصبح من لازم إيجاد وسائل حديثة وجديدة لاكتشاف المجرم، كما حاولت أجهزة البحث والتحقيق الاستعانة بالوسائل العلمية الحديثة في إثبات الجريمة لفك الخيوط المتشابكة للواقعة الإجراميةوذلك لسبب عجز إجراءات التحقيق التقليدية في مواكبة تطور الجرائم لإثبات وقوعها وهذا ما استدعى على جهات التحقيق استعمال نوع جديد من الأدلة الجنائية في مجال الإثبات الجنائي تعرف بالأدلة الجنائية الرقمية.

وتكمن أهمية موضوع الإثبات الجزائي في الجرائم المعلوماتية بالأدلة الرقمية في أنها تعد الجريمة المعلوماتية من الجرائم المستحدثة وبالتالي لا يمكن الاعتماد على الإجراءات التقليدية فأصبح من الضروري استحداث وسائل وإجراءات تحقيق حديثة تواكب هذا التطور الحاصل في مجال الإجرام.

وتكمن أيضا في أن العلم قد أحدث الكثير من الوسائل الإثبات من بينها الدليل الرقمي والذي يطرح مسألة تقديره أمام القضاء الجنائي أثيره في إثبات الجرائم المعلوماتية خصوصا مع تضاؤل دور القاضي الجنائي أمام طبيعة هذه الجرائم لكونها تحتاج إلى خبير معلوماتي باعتبارها مسائل فنية بحتة.

وأنها تعالج نوعا جديدا من الأدلة الجنائية من الناحيتين الفنية والقانونية، ومن جهة أخرى تعالج الإشكاليات الإجرائية التي أثارها.

ومن أهم الأسباب التي دفعتني لاختيار هذا الموضوع الإثبات الجزائي في الجرائم المعلوماتية بأدلة رقمية، هو من المواضيع المستحدثة ورغبة مني في إثراء الدراسات الجامعية النظرية، وذلك بسبب ندرة

الأبحاث والدراسات المتعلقة بالأدلة الجنائية الرقمية وتقديرها أمام القضاء، والقواعد الإجرائية الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ولقد تطرقت عدة دراسات سابقة إلى الإثبات الجزائي في الجرائم المعلوماتية بأدلة رقمية ومن بين هذه الدراسات:

- طاهري عبد المطلب بعنوان الإثبات الجنائي بالأدلة الرقمية، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، جامعة المسيلة سنة 2015/2014.
- دراسة خالد عياد الحلبي، بعنوان إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت الصادرة عن دار الثقافة للنشر والتوزيع بالأردن سنة 2011.
- دراسة عبد الناصر محمد محمود فرغلي ومحمد عبيد، سيف سعيد المسماري بعنوان الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة (والصادرة عن جامعة نايف العربية للعلوم الأمنية بالسعودية في سنة 2007.

وانطلاقا مما سبق ذكره نهدف من خلال هذا الموضوع إلى إزالة الغموض عن الأدلة الجنائية الرقمية، وذلك من خلال مفهوم عام لها من خلال التعريف بها وإبراز خصائصها وإعفاء أنواعها مع ذكره أمثلة عنها لتوضيح أكثر، وزيادة على ذلك معرفة تقديرها أمام القضاء ومدى تأثيرها على الاقتناع الشخصي للقاضي الجنائي.

وعليه تكون إشكالية بحثنا على النحو التالي: كيف ساهمت الأدلة الرقمية في إثبات الجريمة؟

وللإجابة على إشكالية البحث اعتمدنا على المنهج الوصفي بالتطرق إلى مواصفات الجريمة الإلكترونية والدليل الرقمي التي يتميزون بها، إضافة إلى منهج تحليلي لنعرض على مدى تأثير الدليل الرقمي على القناعة الشخصية للقاضي الجزائي.

وللإجابة على هذا التساؤل اتجهنا تقسيم خطة بحثنا إلى مقدمة وفصلين رئيسيان وخاتمة.

الفصل الأول سوف يخصص للجريمة المعلوماتية والتحقيق فيها من خلال مبحثين نستعرض ضمن المبحث الأول ماهية الجرائم المعلوماتية ونقود المبحث الثاني منه التحقيق في الجرائم المعلوماتية.

في حين نتناول في الفصل الثاني من هذه الدراسة القيمة القانونية للدليل الرقمي وتقديره أمام القضاء من خلال مبحثين نتطرق على أولهما إلى ماهية الدليل الرقمي أما المبحث الثاني حجية الدليل الرقمي وتقديره أمام القضاء.

وعليه سندرس موضوع الإثبات الجزائي في الجرائم المعلوماتية بأدلة رقمية كما يلي:

الفصل الأول: للجريمة المعلوماتية والتحقيق فيها.

الفصل الثاني: القيمة القانونية للدليل الرقمي وتقديره أمام القضاء.

الفصل الأول

الفصل الأول: الجريمة الإلكترونية وإجراءات التحقيق فيها.

لقد شهدت البشرية تطورا و اتساعا بالغا في نطاق استخدام تقنية المعلومات مما خلف ظهور الجريمة الإلكترونية و قد قطع استخدام الحياة أشواطابعيدة في اختراع أساليب علمية لارتكاب جرائمهم دون أن يتركوا أي أثر ورائهم يدل على إدانتهم و الآن أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفنين والمهتمين بالأمن المعلومات ونظرا لطبيعة هذه الجرائم فإنها تجعل المعلومات المتحصل عليها لها طبيعة من نوع خاص وأنها معلومات مستحدثة من القيم وهذا ما يضفي عليها الطابع الفني و العلمي مما يصعب الوصول إليها و إثبات توافرها.

لقد مرت الجريمة المعلوماتية بعدة مراحل تماشيا مع تطور التقنية واستخدامها ففي المرحلة الأولى مع الستينيات إلى السبعينيات بظهور استخدام الحاسوب واتصال بشبكة الأنترنت كانت هناك بعض أساليب ناشئة عن سوء استغلال تقنية المعلومات فناقشت في شكل مقالات صحفية طرحت تساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أو ظاهرة إجرامية مستجدة؟ وه ل هذه الجرائم بمعنى الأخلاقي أم القانوني؟ فأدرجت على أساس أنها ذات سلوك أخلاقي دون النطاق القانوني ومع انطلاق الدراسات كيفت في السبعينات على أنّها ظاهرة إجرامية أمّا المرحلة الثانية تبدأ في الثمانينات حيث ظهر نوع جديد من الجرائم اختراق النظم أين شاع مصطلح (الهاكرز) ومع تزايد خطورة هذه الممارسات أصبح من الضروري تجريم هذا السلوك الذي أصبح يستهدف التجسس والاستيلاء على البيانات الاقتصادية و السياسية و الاجتماعية و حتى العسكرية و مرحلة أخيرة تبدأ في التسعينيات شهدت هذه الحقبة تطور هائل في مجال الجرائم التقنية و هذا راجع لفعل شبكة الأنترنت التي سهلت عمليات دخول و اقتحام أنظمة المعلومات و ظهرت بسببها أنماط جديدة من الجرائم.

وفي هذا الفصل سوف نتناول تعريف الجريمة المعلوماتية وخصائصها وأث ر طبيعتها على الإثبات الجزائي ثم سنعرض تعريف الدليل الإلكتروني وأهم خصائصه وتقسيماته وإجراءات جمعه.

المبحث الأول: مفهوم الجريمة الإلكترونية:

تعد الجريمة المعلوماتية جريمة حديثة نسبيا وهذا نظرا لارتباطها بتكنولوجيا واستخدام تقنيات علمية وجديدةومتطورة لارتكابها،ونظرا لحداثتها فهناك اتجاهات مختلفة في تعريفها كما أنها تتميز بسمات تفصلها عن غيرها من الجرائم الأخرى،وتتمتع بطبيعة خاصة لها أثر بالغ في إثبات الجزائي واختصاص قضائي فقد يصعب حصرها وتعدادها نظرا لازديادها وتنوع أساليبها فهي تتحدى الأجهزة الأمنية والقضائية حيث يصعب تحديد زمان ومكانالجريمة.

المطلب الأول: تعريف الجريمة الإلكترونية:

لقد أطلق على ظاهرة الجرائم المتعلقة بالحاسوب والأنترنت عدة مصطلحات دون أن يتم الاتفاق على مصطلح واحد للدلالة على هذا النوع من الجرائم الحديثة، و قد ساير هذا التباين تطور تقني، و نمو الظاهرة الإجرامية بالموازاة، فبدأ بمصطلح جرائم الحاسوب و الجريمة المرتبطة بالكمبيوترثم جرائم التقنية العالية إلى جرائم الكمبيوتر و الأنترنت، أو بعدها جرائم الهاكرز أو الاختراقات وأخيرا،السيبركرايم، و جرائم العالم الافتراضي، بالإضافة لمصطلحات أخرى تبعد قليلا عن التقنية مثل جرائم الياقات البيضاء ولاختيار المصطلح المناسب يجب مطابقة البعدين التقني والقانوني من جهة و الاستناد إلى المصطلح الأشمل الذي يعبر عن الأفعال المراد تجريمها.[1]

1: جرائم الأنترنت، منتديات ستار تايمز، لوحظ يوم 2018/10/29 على الساعة 23:14
www.startimes.com

الفرع الأول: التعريف القانوني.

تبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطياتمعتبرا أن النظام المعلوماتي في حد ذاته ما يحتوي من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية لمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توفر أو عدم توفر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث.

حيث أنه عرف من خلال نص المادة 02 من القانون رقم 04/09 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصالومكافحتها.[1]

مسميا إياه: المنظومة المعلوماتية و" هي أي نظام منفصلا ومجموعة من الأنظمة المتصلة مع بعضها البعض أو مرتبطة، يقوم واحد منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين"[2]

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 15/04 المؤرخ في العاشر نوفمبر 2004 المتمم للأمر رقم 165/66 المتضمن قانون العقوبات والذي ورد في القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 08 مواد من المادة 394 مكرر والمادة 394 مكرر07.[3]

1: القانون رقم 04/09 المؤرخ في 14 شعبان 1430- 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتعلقة بالتكنولوجيا الإعلام والاتصال ومكافحتها ج.ر عدد 47 صادرة بتاريخ 2009/06/16، ص5.

2: نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة2016،2015، ص 2-3.

3: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة

اشترط المشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات.[1]

كما تعرف بأنها: "مجموعة الأفعال أو الأنشطة المعاقب عليها قانونيا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية"، وتعرف كذلك على أنها: "نشا ط جنائي يمثل الاعتداء على برامج الحاسب الآلي.[2]

كما أن هناك من عرفها بأنها: "جريمة التي يتم ارتكابها إن قام شخص ما باستخدام معرفته بالحاسب بعمل غير قانوني.[3]

وبأنها:"الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".[4]

هي ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها.

هي "أي عمل غير قانوني يستخدم فيه الحاسب كأداة أو موضوع الجريمة".

جميع أفعال المخالفة للقانون والشريعةوالتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الأنترنت.[1]

الجديدة، ب ط، كلية الحقوق، جامعة الإسكندرية، 2006، ص 27.

1: نشناش منية، المرجع السابق، ص 04.

2: عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006، ص ص 01، 02.

3: محمد عادل ريان، جرائم الحاسب الآلي وأمن البيانات بدون دار النشر، بدون طبعة، بيروت،2002، ص 03.

4: فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، ب ط، كلية الحقوق، جامعة الإسكندرية، 2016، ص 37.

أنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الإلكترونية للبيانات أو نقل هذه البيانات ".

أو أنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الإلكتروني أو التي تحول من طريقه"

أو هي "أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات"[2]

الفرع الثاني: التعريف الفقهي.

عرفها الفقه المصري فيرى بأنها تنشأ عن استخدام غير مشروع لتقنية المعلوماتية هدف إلى الاعتداء على الأموال و الأشياء المعنوية و هناك فريق آخر يرى أن الجريمة المعلوماتية هي: "عم ل أو امتناع يأتيه إضرار بمكونات الحاسب، و شبكات الاتصال الخاصة به، التي يحميها قانون العقوبات و يفرض له عقابا" ،كما عرفها آخرون لأنها: " كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على التقنية المعلوماتية أية كان غرض الجاني.[3]

يعرف تاديمان« Tiedeman » جريمة الحاسب الإلكتروني بأنها :"كل أشكال السلوك الغير مشروع، الذي يرتكب باستخدام الحاسب الآلي، وللفقيه تاديمان « Tiedeman »تعريف آخر لجريمة الحاسب الإلكتروني بأنها: "كل جريمة ضد المال مرتبطة بالمعالجة الإلكترونية للبيانات" و هو تعريف يختلف عن التعريف السابق، و يلاحظ أنه في ظل التباين حول المصطلحات الدالة على الجريمة و حول تعريفها يتوقع أن يبين لدى المؤلف الواحد عدة تعريفات.[4]

1: عبد الفتاح مراد، شرح جرائم الكمبيوتر والأنترنت، بدون دار النشر، بدون طبعة، ص40.

2: فهد عبد الله العبيد العازمي، المرجع السابق، ص39.

3: محمد عادل الريان، مرجع سابق، ص18.

4: فهد عبد الله العبيد العازمي، مرجع سابق، ص41.

عرفها كل من « A Hard Castle R. Toll » بأنها:"تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسب" أو بمعنى آخر هي:"التي يكون للحاسب فيها دورا إيجابيا أكثر سلبية"[1]

و عرفها الدكتور "ديفيد تومبسون" «David Thompson»بأنها:" أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلهامعرفة بتقنية الحاسوب"ويعرفها الفقيه "ستين سكيوليبرغ" « StinSchiolber »بأنها:" أي فعل غير مشروع تكون المعرفة بتقنية المعلومات الأساسية لمرتكبه والتحقيق فيه و ملاحقته قضائيا".[2]

وعرفها « Asolary »تحت هذا النمط بأنها:"أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه".

ويعرفها آخرون بأنها:"أي عمل ليس له في القانون أو العرف جزاء ويضر بالأشخاص والأموالويوجه ضد التقنية المتقدمة لنظم المعلومات."[3]

وقد عرف خبراء متخصصون في بلجيكا الجريمة المعلوماتية في معرض ردهم على منظمة التعاونالاقتصادي والتنمية«OECD»بأنها:"كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية."[4]

وضمن التعريفات التي تعتمد أكثر من معيار، يعرف جانب من فقه الجريمة المعلوماتية وفق معايير قانونية صرفة، أولها تحديد محل الجريمة، و ثانيها وسيلة ارتكابها و هو في كلا المعيارين (الحاسب الآلي) لما يلعبه من الضحية ودور الوسيلة حسب الفعل المرتكب حيث يعرفه الأستاذ

1: أحمد خليفة الملط، مرجع سابق، ص 85.

2: علي حسن الطوالبة، مرجع سابق، ص 49.

3: أحمد خليفة الملط، مرجع سابق، ص 86.

4: هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، بدون طبعة،1992، ص 35.

« Thomas J.Smedinghoff » في مؤلفه (المرشد القانوني لتطوير وحماية وتسويق البرمجيات) أنها:"أي ضرب من النشاط الموجه ضد استخدام نظام الحاسوب" و هذا تعبير"النشاط موجه ضد"ينسحب على الكيانات المادية إضافة إلى الكيانات المنطقية و كذلك تعريف الأستاذ « Bolgna ,J.RobertLindquist Jacq »:"جريمة يستخدم الحاسوب كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسها ضحيتها" والجرائم المعلوماتية لدى الفقه جرائم ضد الأموال ويستخدم أساس لهذا التعريف معيارين أولها الوسيلة.[1]

أما المعيار الثاني وهو تحقيق الربح والمستمد من معيار محل الجريمة المتمثل بالمال لدى هذا الجانب من الفقه.

وحديثا تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا لجرائم الحاسب الآلي وشبكاته، حيث عرف الجريمة المعلوماتية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام وتشمل تلك الجرائم من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية.[2]

المطلب الثاني: خصائص الجريمة الإلكترونية.

تتميز الجريمة الإلكترونية بجملة من الخصائص والسمات التي تميزها عن غيرها من الجرائم التقليدية الأخرى وهذا راجع إلى ارتباطها بجهاز الحاسوب وشبكة الأنترنت فهي ذات صبغة تقنية علمية.

1: إبراهيمي سهام، الجريمة المعلوماتية، مذكرة تخرج لنيل الشهادة المدرسة العليا للقضاة، الدفعة الخامسة عشر، 2007/2004، ص 03.

2: عقد هذا المؤتمر في فينا في الفترة ما بين (10- 17) أفريل 2000 مشار إليه لدى أحمد المناعسة، جرائم الحاسب الآلي والأنترنت (دراسة مقارنة)، ط1، دار وائل للنشر والتوزيع، عمان،2001، ص 78.

الفرع الأول: أسلوب ارتكاب الجريمة المعلوماتية:

ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو حال في جريمة السرقة .... فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها ((soft crime لا تحتاج إلى العنف والإيذاء، بل كما لا تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال الغير مشروعة.[1]

تتطلب من مرتكبيها إلماما كافيا في تشغيل الحاسوب، وفهم نظمه وآلية عمل الشبكات، كما أنها لا تحتاج إلى مجهود عضلي مثل السرقة أو الاغتصاب وغيرها، فهي جرائم ناعمة، تعتمد بشكل كبير على القدرة الذهنية والتفكير العلمي القائم على المعرفة بتقنيات الحاسوب والأنترنت.[2]

تقع الجريمة في بيئة المعالجة الآلية للبيانات، حيث يستلزم لقيامها التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتية بغرض معالجتها إلكترونيا بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة، والتي يتوافر فيها إمكانية تصحيحها أو تعديلها محوها أو تخزينها أو استرجاعها وطباعتهاوهذه العمليات وثيقة الصلة بارتكاب الجرائم، ولابد من فهم الجاني لها أثناء ارتكابها في حالات التزوير والتقليد.[3]

1: نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر، ط1، عمان، 2008، ص57 ،58.

2: على حسن الطوالبة، المرجع السابق، ص20.

3: أحمد الخليفة الملط، المرجع السابق، ص93.

الفرع الثاني: خصوصية مجرمي المعلوماتية:

المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة عن المجرم الذي يقترف الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة عامة فإن الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة ما يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الأنترنت.[1]

الجامع بين محترفي الجرائم الإلكترونية، تمتعهم بقدرة عالية من الذكاء، وإلمام جيد بالتقنية العالية واكتسابهم معارف علمية وعملية،وانتمائهم إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية، وهذه السمات تتشابه مع سمات مجرمي ذوي الياقات البيضاء، أما فيما يتعلق بكفاءة مجرمي الحاسوب، فإن الدراسات القليلة المتوفرة، تشير إلى تمتعهم بكفاءة عالية، إلى درجة اعتبارهم مستخدمين مثاليين من قبل الجهات العاملين لديها، وممن يوسمون بالنشاط الواسع والإنتاجيةالفاعلة.[2]

فعلى سبيل المثال فإن الجرائم الإلكترونية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية وتقنية عالية من قبل مرتكبها، كذلك فإن البواعث على ارتكاب المجرم المعلوماتي لهذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.[3]

1: نهلة عبد القادر المومني، المرجع السابق، ص 59.

2: على حسن الطوالبة، المرجع السابق، ص 66.

3: المويشير، تركي عبد الرحمن (2009)، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، الرياض، رسالة ماجستير، جامعة نايف الأمنية ص 35.

الفرع الثالث: الجريمة الإلكترونية عابرة الحدود.

إن تعبير الجرائم العابرة للدول أو جرائم غير وطنية هي تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعرف بالحدود الجغرافية للدول كجرائم تبييض الأموال والمخدرات، وغيرها.[1]

اعتبار جرائم التقنية جرائم عابرة للدول يظهر الحاجة الملحة للتعاون الدولي في مجال مكافحة هذه الجرائم وضبط فاعليها، وتجدر الإشارة هنا غلى جهود الإنتربول في هذا المجال، من خلال ضبط الارتباط المنتشرين في كافة الدول عبر العالم، والمكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكل نقطة انطلاق لمكافحة وتصدي لهذه الجرائم.

هذه الجرائم لا تعرف الحدود بين الدول والقارات حيث أن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغا من المال لأي مكان في العالم مضيفا له صفر أو بعض الأصفار لحسابه الخاص بل يستطيع أي شخص أن يعرف كلمة السر لأي شبكة في العالم ويتصل بها ويغير ما بها عن معلومات.[2]

جرائم عابرة للقارات، بحيث يمكنها أن ترتكب في دولة وأثرها في يكون في دولة أخرى، لهذا فهي لا تعرف بالحدود الجغرافية للدول وهذا الأمر يتطلب ضرورة التعاون الدولي لمواجهة هذا النوع المستحدث من الجرائم بالجرائم العابرة للحدود والأخرى، كالمخدرات وتجارة الرقيق وغيرها، وتجدر الإشارة إلى أن هذه الجرائم الأخيرة يمكن ارتكابها عبر الحاسوب والأنترنت.[3]

1: أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، عمان 2014،ص95.

2: أحمد الخليفة الملط، المرجع السابق، ص 94.

3: علي حسن الطوابلة، المرجع السابق، ص 59.

ومن خلال هذه الخاصية الدولية يثار إشكال حول الاختصاص القضائي في محاكمة المجني عليه بمعنى آخر ماهي الدولة المختصة بمحاكمة الجاني؟ هل هي الدولة التي يرتكب على إقليمها النشاط الإجرامي أم التي يوجد فيها المجني عليه.[1]

الفرع الرابع: صعوبة اكتشافها وإثباتها

تمتاز الجرائم المعلوماتية بصعوبة اكتشافها والإثباتوذلك نظرا لعدم ترك الجاني آثار تدل نظرا لعدم ترك الجاني آثار تدل إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام، هي رموز دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة وغالبا ما يتم معاقبة المجرمين وذلك لعدم وجود أدلة قائمة في حقه.[2]

فالجريمة المعلوماتية لا تترك آثارا ملموسة وذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلك مادية يمكن فحصها لأنها تقع على البيئة الافتراضية، يتم فيها نقل المعلومات وتناولها بواسطة نبضات إلكترونية غير مرئية.[3]

وصعوبة اكتشافها وإثباتها راجع لعدة أسباب منها وسيلة التنفيذ التي تتسم في غالب الأحيان بالطابع التقني الذي يصفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها لأنها تتطلب إلماما خاصة بتقنيات الكمبيوتر ونظم المعلومات.[4]

1: سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، 2013/2012 ص 32.

2: معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير والعلوم الجنائية، 2011- 2012، ص 24.

3: سعيد نعيم، المرجع السابق، ص 34.

4: سعيد نعيم، المرجع نفسه، ص 34.

ويصعب في الجرائم المعلوماتية العثور على الدليل المادي للجريمة وذلك راجع إلى استخدام الجاني وسيلة فنية وتقنية معقدة في الكثير من الأحيان، وهذا السلوك المادي في ارتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به.[1]

إثبات تلك الجرائم يحيط به الكثير من الصعوبات التي تتمثل في اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا، فلا يوجد جثث لقتلى أو آثار لدماء وإذا اكتشفت الجريمة فلا يكون ذلك إلا بمحض الصدفة والدليل على ذلك أنه لم يكتشف منها إلا نسبة 01 فقطوالذي تم الإبلاغ عنه للسلطات المختصة لا يتعدى 15 من النسبة السابقة.[2]

المطلب الثالث: أثر الطبيعة القانونية الخاصة بالجريمة الإلكترونية على الإثبات الجزائي.

تطرقت فيما سبق إلى خصائص الجريمة المعلوماتية بأنها تمتاز ببعض الخصائص تميزها عن غيرها من الجرائم التقليدية كما أن لها طبيعة قانونية خاصة تأثير كبير من ناحية إثبات الجزائي ومن الضروري قبل أن أتعرض للطبيعة القانونية للجريمة الإلكترونية أن أبين بإيجاز الطبيعة القانونية للمعلومات.

الفرع الأول: الطبيعة القانونية للمعلومات:

هنا يثار التساؤل بخصوص القيمة القانونية فهل يمكن اعتبارها قيمة قابلة للاستئثار ومن ثم يمكن أن تكون حيث الحصول عليها محل الاعتداء؟

للإجابة على هذا التساؤل اتجه الفقه إلى اتجاهين:

1: هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، ط1، 1994 ص 82.
2: أحمد خليفة الملط، المرجع السابق ص94

أ) المعلومات لها طبيعة من نوع خاص:

يرى الفقه التقليدي أن المعلومة طبيعة خاصة مستوحيا ذلك من تطبيق المنهج التقليدي بشأنها والذي بموجبه يضفي وصف القيمة على الأشياء المادية، ويركز على هذا المبدأ على بديهية مسلم بها أن الأشياء التي توصف بالقيم هي تلك الأشياء القابلة للاستحواذ، ومؤديذلك، أ ن الأشياء التي يمكن الاستئثار بها هي الذي تكون لها قيمة، بالنظر للمعلومات كبيعة معنوية فإنه من غير المقبول أن تكون قابلة للاستئثار وفقا لهذا المنهج. إلا عن طريق حق الملكية الأدبية أو ذهنية أو الصناعية.[1]

ب) المعلومات مجموعة مستحدثة من القيم:

إن المعلومات ماهي إلا مجموعة مستحدثة من القيم ويرجع الفضل في ذلك للأستاذين catala– vivantإلى قابلية المعلومة للاستحواذ كقيمة واستقلالا عن دعامتها المادية على سند من قول أن المعلومة تقوم وفقا لسعر السوق متى كانت غير محظورة تجاريا و أنها تنتج بصرف النظر عن دعامتها المادية عن عمل قدمها و أنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك الذي يملكه و هي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما.[2]

1: أحمد خليفة الملط، المرجع السابق، ص 104.

2: أشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة للنشر، بدون طبعة، الإسكندرية، 2015 ص96.

الفرع الثاني: أثر الطبيعة الخاصة بالجريمة الإلكترونية على الإثبات الجزائي:

إن دراسة الجريمة الإلكترونية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوباتوهو القسم الخاص وهو ذلك الفرع الذي يدوس كل جريمة على حده متناولا كل عناصرها الأساسية والعقوبة المقررة لها، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة.[1]

إن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء كان في تجميعها أو تجهيزها أما في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة، كما قد ترتكب هذه الجرائم في مجال الكلمات أو معالجة النصوص وهذا النوع الأخير من الجرائم لا يعد أن يكون بطريقة أوتوماتيكية المستخدم من تحرير الوثائق والنصوص على الحاسب مع توفير إمكانيات التصحيح والمسحوالتخزينوالطباعة.[2]

فهذه العمليات كلها هي وثيقة الصلة بالجرائم محل البحث وعليه لابد للجاني من فهمها فضلا عن أن الجاني قد يتعامل مع مفرد ذات جديدة كالبرامج والمعطيات التي تشكل محل الاعتداء أو تستخدم وسيلة له.[3]

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة المعلومات على نقل وتبادل المعلومات ذات طابع شخصيا وعام في آن واحد مما يؤدي إلى الاعتداء على الخصوصية والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسبهم بالشبكة.[4]

1: محمد زكي أبو عامر وعلي عبد القادر القهوجي، قانون العقوبات القسم الخاص، دار النهضة العربية، ب ط، القاهرة، 1993، ص92.

2: أحمد السمدان، النظام القانوني لحماية البرامج الكمبيوتر، مجلة حقوقي، الكويت،1987، ص164.

3:جميل عبد الباقي، الجوانب الإجرامية للجرائم المتعلقة بالأنترنت، ب ط دار النهضة العربية، القاهرة،2001 ص92.

4: بعرة سعيدة، الجريمة الإلكترونية على التشريع الجزائري (دراسة مقارنة)، تخصص قانون جنائي، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة،2016/2015، ص .94

وبالتالي هذه الطبيعة خاصة بالأفعال المجرمة التي تدخل ضمن أحكام خدمات البريد أم التخابر الخاص أو يكون الهدف الأساسي للتحري عن نظام القانوني المناسب لطبيعة الجرائم المعلوماتية هو معرفة النصوص القانونية الوصفية التي يجب تطبيقها على الخدمات نشر المواقع والمعلومات فيها، ومن هذا النظام القانوني تتخذ المجال التي ترتكب فيه الجريمة المعلوماتية ومحل الاعتداء عليها تظهر لنا الطبيعة القانونية الخاصة بالجريمة.[1]

إن التطور المعلوماتي يفتح المجال لاقتناء وسائل الإلكترونية تمكن المتجاوزين لاستخدامها في ارتكاب جرائم مختلفة لأن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيما يتعلق بالمعالجة الآلية للبيانات وإدخال المعلومات ونقلهاومن ثم يتحتم ضمنه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارن عاجزة عن مواكبة التطور المعلوماتي أو بما يحيوه من فراغ تشريعي في هذا المجال.[2]

أما من حيث التكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة إذ لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، إن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات و صعوبة إيجاد دليل مادي يدين مرتكب الجريمة لأته من السهل على الجاني محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات و خاصةفي حالة تفتيش الشبكات أو عمليات اعتراض الاتصال قد تكون البيانات التي تجري البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على شبكة و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة.[3]

1: طوبي ميشال عيسى، التنظيم القانوني لشبكة الأنترنت، دار صادرة للمنشورات، بيروت، ط1، 2001، ص383.
2: مجلة جامعة بابل، العلوم الإنسانية، المجلد14، العدد6، 2007، ص11.
3: مجلة جامعة بابل، مرجع سابق، ص91.

ومن صعوبة ملاحقة مرتكبي الجرائم المعلوماتية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي يتحقق فيها السلوك الإجرامي أو جزء منه وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[1]

1: هلال عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ط1، 1997، ص22.

المبحث الثاني: التحقيق في الجريمة.

لقد كان لتزايد المستمر للجرائم المعلوماتية الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة، ونتيجة لهذا التحدي تتولى مهمة التحري من جرائم العالم الافتراضي وكشف النقاب عنها، وقد نظم المشرع كيفية استخلاص الدليل عن طريق إجراءات تتبع الوصول إلى هذه الغاية وهذا ما سيتم توضيحه فيمايلي:

المطلب الأول: الأجهزة المكلفة بالبحث والتحري في الجريمة المعلوماتية

حيث يتم إعطاء تعريف ومعنى واضح ودقيق للضبطية القضائية فلا بد من التطرق على تعريفها من ناحيتين تعريفها لغة (الفرع الأول)، ثم تعريفها اصطلاحا (الفرع الثاني).

الفرع الأول: التعريف اللغوي.

حسب ما يتماشى مع أصول اللغة فإن الضبطلغة يعني لزم الشيء هو حفظه [1]، وأصل كلمة بوليس نجدها مشتقة من الكلمة اللاتينية " Politia" والتي تعني كل تنظيم أو كل شكل حكومي ويقال ضبط الأمر بمعنى أنه حدد على وجه الدقة، كما يعني التدوين الكتابي المشتمل على أنه معالم واقعة يخشى لو ترك أمرها دون تسجيل لهل لتبددت معالمها زوال أثرها من ذاكرة من عاينها وشاهدها.

ومعنى الضبط يدخل في عنصر التدوين الكتابي الذي يسمى في لغة القانون " تحرير محضر" ولذا يقال إنّضبط واقعة يعني تحرير محضر لها.[2]

1: صيد خير الدين، مشروعية عمل الضبطية القضائية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمود خيضر، بسكرة، كلية الحقوق والعلوم السياسية، 2015/2014، ص 13.

2: ابن منظور جمال الدين، لسان العرب، دار الحياء التراث، لبنان، الجزء الثامن، ص33.

الفرع الثاني: التعريف الاصطلاحي.

أمّا اصطلاحا ومدلول الضبطية القضائية ينصرف إلى معنية:

المدلول الأول: موضوعي أو إجرائي يقصد به مجموع العمليات والاختصاصات والإجراءات التي يقوم بها رجال الضبط القضائي للبحث والتحري عن الجريمة ومرتكبيهاوجمع التحريات بشأنها أو بعبارة أخرى هي كل المهام المنوطة بأجهزة الضبط القضائي المحددة في المادة 12من (ق.إ.ج.ج) والتي تتمثل في: البحث والتحري عن الجرائم المقررة في (ق.ع) وجمع الأدلة عنها والبحث عن مرتكبها مادام لم يبدأ فيها تحقيق قضائي .[1]

أمّا إذا فتح التحقيق: فإن على الضابط تنفيذ تفويضات جهات التحقيق وتلبية طلباتهوفقا لنص المادة13 من (ق.ع).

المدلول الثاني: الضبط القضائي فينصرف إل الأجهزة المكلفة بتنفيذ المهام المشار إليها أعلاه، كالدرك الوطني، والأمن الوطني، وهو مفهوم شخصي يطلق على أعوان جهاز الضبط القضائي نفسه أي مجموعة أعضائه المكونين له.[2]

مزج الأستاذ شارل بارا في تعريفه لضباط الشرطة القضائية بين المعنين الموضوعي و الشخصي للضبط بقوله أنّ: ضباط الشرطة القضائية هم سلطات مهمتها معاينة الجرائم المقررة في (ق.ع) جمع الأدلة،والبحث عن مرتكبها من جهة أخرى تنفيذ تفويضات جهات التحقيق ...من وهو تعريف جاءت به المادة 14 من (ق.إ.ج.ج.الفرنسي) التي تقابلها المادة12 من (ق.إ.ج.ج.الجزائري)

1: الأمر 02/15 المؤرخ في 07 شوال 1436 الموافق لـ 23 يوليو 2015 المعدل والمتمم للأمر رقم 66/155 المتضمن ق.إ.ج.ج.

2: ابن منظور جمال الدين، المرجع السابق، ص 34.

تجدر الإشارة إلى أن المادة 12 السابقة قد تم تعديلها بموجب القانون 07/17 بحيث أصبحت مصاغة بالشكل التالي [1]: فيقوم بمهمة الشرطة القضائية القضاة والضباطوالأعوان والموظفون .

المطلب الثاني:الإجراءات التقليدية في جمع الأدلة الجنائية الرقمية.

لقد نظم المشرع كيفية استنباط الدليل الرقمي وذلك عن طريق إجراءات معينة نظمها في القانون تتبع للوصول إلى الغاية ومنها التفتيش، الضبط والمعاينة وهي تستعمل بصفة عامة لجمع الدليل.

الفرع الأول: التفتيش.

إجراءات من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة موضع التحقيق، وكل ما يفيد في كشف الحقيقة، إذ يمس حق المتهم في سرية حياته الخاصة، ويتمثل مجال هذه السرية إما في شخص المتهم أو في المكان الذي يعمل فيه أو يقيم فيه وذلك وفقا لإجراءات قانونية.[2]

ويمكن تعريف تفتيش نظام الحاسوب والأنترنت بأنه: البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد كشف الحقيقة ونسبتها إليه. [3]

كما يعرف على أنه: الاطلاع على محل منحة القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز حاسوب أو أنظمة أو الأنترنت. [4]

1: المادة 12 المعدلة بموجب القانون 07/17 المؤرخ في 29 مارس 2017 المعدل والمتمم لقانون.إ.ج.ج.

2: أمير فرح يوسف، القبض والتفتيش، الطبعة الأولى، مكتبة الوفاء القانونية، مصر،2013، ص 73.

3: علي حسن طوابلة، التفتيش الجنائي على نظم الحاسوب والأنترنت، الطبعة الأولى، عالم الكتب الحديثة للنشر والتوزيع، الأردن، 2004، ص12.

4: المرجع نفسه، ص 13.

حيث قررت المادة 81 من (ق.إ.ج.ج) أنه يجري التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة.

فالمشرع الجزائري كان واضحا في هذه المادة وأجاز التفتيش في مكونات وشبكات الحاسوب، حتى وإن كان فيه إطلاع على أمور شخصية، وهذا بغرض الوصول إلى الحقيقة المنشودة.

شروط التفتيش في البيئة الإلكتروني:

تضمنت معظم التشريعات الإجرائية على ضوابط لا بد من مراعاتها وهذا عند المساس بالحريات الشخصية بأحد الإجراءات كالتفتيش، إذ أنه يتوفر على مجموعة من الشروط الإجرائية، يمكن تصنيفها على شروط موضوعية وأخرى شكلية.

1 -الشروط الموضوعية:

أ – سبب التفتيش:

يعتبر عنصر السبب ضمانة قانونية لصحة ومشروعية إجراء التفتيش، يتحقق بوقوع جريمة، ما يتم بموجبها توجيه الاتهام إلى الشخص أو الأشخاص المراد تفتيشهم بناءا على أدلة وقرائن قوية تفيد تورطهم في هذه الجريمة، عملا بمبدأ الشرعية الجزائية للقاضي: "لا جريمة ولا عقوبة إلا بنص"[1]إذ بدون وقوع الجريمة، وتوجيه الاتهام إلى شخص أو أشخاص معينين وفقا لأدلة كافية، يكون التفتيش باطلا لانتفاء السبب الذي يبرره.

1: وهو ما أقرته محكمة النقض المصرية باعتبارها أن: " الإذن بالتفتيش لا يصح إصداره إلا لضبط جريمة واقعة بفعل وترجحت نسبتها إلى متهم معين وهناك من الدلائل ما يكفي في تصدي لحرمة مسكنه أو لحرمته الشخصية."، طعن نقض جنائي، جلسة 1967/10/16، مجموعة من أحكام النقض، س 18، رقم 165، ص 965، نقلا عن خالد ممدوح، إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، إسكندرية، 2009، ص 209.

وتطبيقا لما سبق فإن سبب التفتيش في الجرائم الإلكترونية لا يتحقق إلا بتحقق العناصر الثلاثة التالية:

وقوع جريمة إلكترونية تحمل وصف الجناية والجنحة:

اتفقت معظم تشريعات الدول على أنه لا يجوز لهيئات التحقيق مباشرة إجراءات التفتيش إلاّ بعد التأكد من الوقوع الفعلي للجريمة الإلكترونية نص عليها القانون في نصوص التجريم والعقاب، أي التفتيش في لا جريم ة محتملة الوقوع مستقبلا ولو أيقنت التحريات والدلائل الجدية أنها ستقع بالفعل بعد إجراء غير مشروع مآله البطلان.[1]

ولا يكفي وقوع الجريمة الإلكترونية للقول بمشروعية إجراء التفتيش طبقا لقواعد العامة، بل لابد أن تحمل هذه الجريمة بمنظور القانون وصف الجناية أو جنحة[2]، ويستثني من ذلك المخالفات بسبب ضعف خطورتها التي لا تستحق انتهاك حرمة الحياة الخاصة للأشخاص وسرية اتصالاتهم وحرمة منازلهم من أجلها.[3]

والجدير بالذكر أن مسالة وقوع الجريمة من عدمها تثير مشكلة كبيرة عندما يتعلق الأمر بالتفتيش في جرائم الحاسب الآلي و شبكات المعلومات، خاصة في الدول التي لم تسن حتى الأن قوانين تصنف فيها هذه الجرائم، و تحدد وصفها القانوني عناصر أو أركان كل جريمة وكذا

1:نشير إلى أن المشرع الجزائري خرج عن هذه القاعدة من خلال نص المادة 05 من القانون رقم 04/09 التي تجيز إمكانية اللجوء إلى تفتيش النظم المعلوماتية للوقاية من الجرائم أو في حالة توفر المعلومات للوقاية من الجرائم أو في حالة توفر معلومات احتمال وقوع جرائم معينة ذكرتها المادة 04 من نفس القانون.

2:وهذا تصديقا للمادة ا66 من (ق.إ.ج.ج) التي تنص على أن: "التحقيق الابتدائي وجوبي في مواد الجنايات، أمّا في مواد الجنح فيكون اختياريا ما لم يكن ثمة نصوص خاصة"

3:نبيلة هبة هروال، الجوانب الإجرامية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، ب ط، الإسكندرية، 2013، ص 232.

العقوبات المقررة لها، مع العلم أن إجراء التفتيش لا يكون مشروعا إلاّ إذا بنيّ على سبب جدي يتمثل في وقوع فعلي للجريمة، و أن وقوع هذه الأخيرة من عدمه يتوقف أساسا على مدى تحقيق أركانها مجتمعة[1]فعلى سبيل المثال، مازالت العديد من الجرائم المتعلقة بنظم المعالجة الآلية و شبكة الأنترنت خارج نطاق التجريم في التشريع الجزائري من جرائم الاعتداء على المواقع الإلكترونية و حجبها و تدميرها، و كذا جرائم الاستغلال الجنسي للأطفال و غيرها من الجرائم الإباحية، و تبعا لذلك التفتيش قد يكون مصيره البطلان طالما لم يتركز على سبب مقبول قانونا، ناهيك عما تتطلبه الإجراءات التقنية في حالة النص على تلك الجرائم من نصوص تتناسب مع حداثتها.[2]

اتهام شخص أو أكثر بمساهمته في ارتكاب الجريمة الإلكترونية:

يشترط لقيام سبب التفتيش على جانب وقوع الجريمة الإلكترونية تحمل وصف الجناية أو جنحة، أن تتوفر في حق الشخص المراد تفتيشه أو تفتيش حاسبه أو مسكنه دلائل كافية توحي إلى الاعتقاد بانه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أصليا أو ثانويا، مما يستوجب اتهامه بها، ومن هنا كان عدم اكتشاف قاضي التحقيق لهوية المتهم في شكوى ضد مجهول سببا لحفظ ملف القضية وإصداره لأمر بأن لا وجه للمتابعة.[3]

وقد اجمع الفقه الجنائي على أن المقصود بالدلائل الكافية بصفة عامة هو: "الشبهات المستمدة من الواقع والقرائن التي تنبئ عن اقتراف الشخص جريمة من الجرائم."[4]

1:هلال عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ب ط، دار النهضة العربية، القاهرة، 1997، ص 121.

2:رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، ب ط، المكتب الجامعي الحديث، الإسكندرية، 2013، ص 69.

3:هذا ما نصت عليه المادة "163" من (ق.إ.ج.ج) : "إذا رأى قاضي التحقيق ... انه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة ما يزال مجهولا، إصدار أمر بأن لا وجه للمتابعة".

4:بوكرر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، ب ط،

أمّا في الجرائم الإلكترونية فيقصد بها " مجموعة من المظاهر أو الإمارات المعينة القائمة على العقل والمنطقوالخبرة الفنية والحرفية للمحقق والتي ترجع نسبة الجريمة الإلكترونية إلى شخص معين باعتباره فاعلا أصليا أو شريكا".

وعلى هذا الأساس فسبب التفتيش في البيئة الإلكترونية لا يتوقف على وقوع الجريمة من الجرائم الإلكترونية فقط، إنّما لابد أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معينين إما بصفتهم فاعلين أصلين أو شركاء.[1]

توافر إمارات قوية توحي وجود أدلة مادية تفيد في كشف الجريمة:

لا يكفي وقوع الجريمة من نوع جناية أو جنحة منصوص عليها في القانون، وتوجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في الجرائم الإلكترونية، إنّما ينبغي أن تتوافر كذلك لدى المحقق أدلة قوية وقرائن كافية على وجود لدى شخص المتهم أو في الموقع المراد تفتيشه أجهزة أو أدوات استعملت في الجريمة أو أشياء متحصل عليها، أو أية معلومات أو بيانات أو مستندات إلكترونية تفيد في استجلاء الحقيقة.[2]

بيروت، 2012، ص 407.

1:و هو ما يستشف من نص المادة 44 من (ق.إ.ج.ج) بنصها على أنه: "لا يجوز لضابط الشرطة القضائية الانتقال على مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش إلا..".

2:هذا ما أقرته محكمة النقض المصرية في حكمها الصادر في الطعن رقم 25380 جلسة 2002/01/20 عندما قضت بأن "كل ما يشترط لصحة التفتيش الذي تجريه النيابة أو تأذن بإجرائه في مسكن المتهم أو ما يتصل بشخصه، هو أن يكون رجل من الضبط القضائي قد علم من تحرياته و استدلالاته أن جريمة معينة قد وقعت من شخص معين أو يكون هناك من الدلائل الإمارات الكافية و الشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التفتيش لحريته أو لحرمة مسكنه في سبيل كشف اتصاله بتلك الجريمة" نقلا عن: أحمد بن زايد جوهر الحسن المهندي، تفتيش الحاسب الآلي و ضمانات المتهم، رسالة لنيل شهادة ماجستير، كلية الحقوق، جامعة القاهرة، 2009، ص 165.

ويتم الحصول على هذه القرائن والإمارات من خلال مختلف التحريات الجدية التي تجريها سلطات الضبط في مرحلة الاستدلال، بعد ما يتم إخضاعها لتقدير السلطة المختصة بإصدار الإذن بالتفتيش التي تتأكد من مدى توفر هذه القرائن لمصداقية كافية تبرر اللجوء إلى إجراء التفتيش.

و ينطبق على هذه الضمانة ما قبل في سابقتها بأنها لا تجدي في مجال الجرائم الإلكترونية،بخلاف ما هي عليه في الجرائم التقليدية، لأن التوصل إلى قرائن أو إمارات قوية كسبب لقيام التفتيش في الجريمة الإلكترونية ليس بالأمر الهين، نظرا للصعوبات الكثيرة و العقبات الجمّة التي تواجه سلطات التحري و الاستدلال في ذلك، كنقص خبرتها في تقنيات التحري في العالم الإلكتروني الافتراضي،مقابل ما تتسم به تلك الأدلة من طبيعة معنوية يمكن إخفاؤها، تغييرها و إتلافها بكل سهولة وسرعة فائقة[1]، و هذا ما قد يشكل دافعا كافيا لانتفاء سبب التفتيش الذي يعتبر شرطا جوهريا لصحة إجراء التفتيش.

ب – محل التفتيش.

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة كالمسكن أو الشخص أو السيارة أو الرسائل ... وبالتالي فقد يكون محل ذلك التفتيش إمّا مسكنا أو شخصا أو سيارة... مع مراعاة الإجراءات القانونية المقررة.

ومحل التفتيش في جرائم الحاسب الآلي يعتبر النافذة التي تطل بها الأنترنت على العالم والشبكة التي تشمل في مكوناتها الخادم [2]، والمزودالآلي[1]وغيرها.

1:رشاد خالد عمر، المشاكل القانونية والتقنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، ب ط، الإسكندرية، 2013، ص 130.

2:الخادم هو الجهاز الرئيسي أو المسؤول في الشبكة وباقي الأجهزة المتصلة بالشبكة هي عبارة عن عملاء لأنها تتطلب

وتجدر الإشارة هنا إلى أن مثل هذا المحل لا يكون قائما بذاته، وإنما يشمل المكان أو العقار ما ويكون بصحبة مالكه أو حائزه، ولذلك وجب على ضابط الشرطة القضائية عند استصداره لإذن التفتيش أن يحدد محل ذلك لإجراء تحديدا دقيقا وذلك الغرض منه وإلا كان باطلا.

إن إجراء التفتيش في الجريمة المعلوماتية تحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش العادية (التقليدية) لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفةبملفات أجهزة الإعلام الآلي وأماكن إخفاء المعلومات فيها لأنه يسهل أتلافها كليا أو جزئيا، كما يصب تحديد مكان الدليل[2]

وبالتالي ففي إطار جرائم الأنترنت يقع التفتيش على موضوعين إثنين هما:

- تفتيش مكونات الحاسب الآلي (المادية والمعنوية).
- تفتيش الشبكات المعلوماتية المتصلة بالحاسوب، التفتيش عن بعد.

I. تفتيش مكونات الحاسب الآلي:

قبل الغوصفي إجراءات التفتيش لابد من تعريف الحاسب الآلي: وهو جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال أو إخراج معلومات.[3]

I. 1- تفتيش المكونات المادية للحاسب الآلي:

تخضع المكونات المادية لنظام المعالجة الآلية للمعطيات لإجراءات التفتيش المنصوص عليها في المادة 44 من (ق.إ.ج.ج) [1]أي أنه يجوز مراعاة مكان وجود ذلك الحاسوب أثناء

خدمات معينة منه.

1:المزود الآلي هو المزود الذي يوفر لعملائه إمكانية الوصول إلى الأنترنت.

2:هذا ما نصت عليه المادة 163 من (ق.إ.ج.ج): إذا رأى قاضي التحقيق ... انه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة ما يزال مجهولا، إصدار أمر بأن لا وجه للمتابعة.

3:محمد هماجهومجالهيتي، جرائم الحاسوب، ط1، دار المناهج للنشر والتوزيع، ب ط، الإسكندرية، 2012، ص 22.

مباشرة ذلك الإجراء، فيما إذا كان مكانا عاما أو خاصا كمسكن المتهم فلا يجوز تفتيشه إلا في الحالات التي يجوز فيها تفتيش مسكنه، و بنفس الضمانات المقررة قانونا و كذا المادة 64 من نفس القانون، فلا يجوز القيام بإجراء التفتيش إلا بإذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق وبعد الحصول على رضا صريح من صاحب المسكن، و يجب كتابته بخط صاحب الشأن و توقيعه، و في حالة العكس يثبت أن صاحب الشأن لا يعرف الكتابة في المحضر التنويه عن رضائه، أمّا إذا تعذر على صاحب الشأن الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، و إذا امتنع عن ذلك أو كان هاربا استدعى الضابط لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.[2]

كما يجب أن يتم ذلك الإجراء في المواعيد المحددة في القانون وهي من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا، إلاّ في الحالات الخاصة فيما يتعلق بالجرائم الخطيرة ومن بينها الجريمة المعلوماتية التي لا تشترط المواعيد وإنّما في كل وقت من الليل والنهار (24 ساعة).[3]

إلاّ أن المشرع الجزائري بمناسبة التعديل الذي ألحقه على (ق.إ.ج.ج)بالقانون رقم 22/06المؤرخ في 2006/12/20 استثنى بموجب الفقرة الثالثة من المادة 45وكذا الفقرة الثانية من المادة 47والفقرة الثالثة من المادة 64تطبيق هذه الضمانات عند إجراء التفتيش بمناسبة تحقيق مفتوح بخصوص الجريمة المعلوماتية.

1:تنص المادة 44 من (ق.إ.ج.ج) على: لا يجوز لضابط الشرطة القضائية إجراء تفتيش إلا بموجب إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق ويتضح من نص المادة أن التفتيش يقع على الأشياء والأوراق التي لها علاقة بالجريمة.

2:أنظر: المادة 01/45 من (ق.إ.ج.ج) .

3: أنظر: المادة 47 من (ق.إ.ج.ج).

ويفهم من استقراء هذه المواد أن المشرع لا يشترط حضور الشخص الذي يشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه [1] وغيرها من الضمانات التي استثناها المشرع في بعض الجرائم ومن ينتهك الجريمة المعلوماتية (جرائم أنظمة المعالجة الآلية للمعطيات) بموجب الفقرة الثالثة من المادة 47 من (ق.إ.ج.ج).

I. 2- تفتيش المكونات المعنوية للحاسب الآلي:

يتعلق الأمر بالتفتيش عن الجريمة التي وقعت على المكونات المعنوية للحاسوب ويقصد بها أنظمة الكومبيوتر والبيانات المخزنة فيه التي جرى التلاعب فيها أو تغييرها وغيرها من الوسائط التي تساعد على تخزين المعلومات.[2]

وكذلك وأن الأمر يتعلق بمدى صلاحية نظم الحاسوب للتفتيش وبالأجهزة المختصة بتفتيش نظام الحاسوب والأنترنت.[3]

أما مدى صلاحية معطيات الحاسوب فهو أمر تفوضه طبيعة الجريمة المرتكبة، والرأي المستقر عليه، أن معطيات الحاسوب تصلح لتفتيش عن الأدلة الجرمية وضبطها لأن الغاية من التفتيش هو الحصول على دليل خاص بالجريمة وكشف الغموض الذي أحاط بها.[4]

1: أنظر: المادة 64 والمواد 44 إلى 47 .

2: خالد عياد حلمي، إجراءات التحري والتحقيق في جرائم الكومبيوتر والأنترنت، ط 01، دار الثقافة للنشر والتوزيع، عمان، 2011، ص159.

3: نبيلة هبة هروال، المرجع السابق، ص 224.

4: عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية لجرائم الكومبيوتر والأنترنت، ط 1، دار الفكر الجامعي، الإسكندرية، 2006، ص159.

إنّ الطابع المعنوي للبيانات والمعلومات المخزنة على الحاسوب [1]والتي يمكن القيام بتفتيشها إذا كانت مخزنة على حاسوب المتهم، فإن الإشكال هنا في حالة ما إذا كان حاسوب المتهم مرتبطا بحاسوب آخر داخل دولة أو خارجها، فهل يجوز إجراء التفتيش في هذه الحالة؟ وهل يجوز تفتيش حاسوب الآخرين والكشف عن الوسائط الإلكترونية؟

وبالتالي يرى البعض أن التفتيش يمتد إلى سجلات البيانات الموجودة في موقع آخر يشترط أن تكون البيانات الخاصة ضرورية بإظهار الحقيقة.

وهو ما تبناه القانون المقارن حول تفتيش الأنظمة المعلوماتية، فقد منحت المادة 251 من (ق.إ.ج.ج. اليوناني) سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع الدليل، وكذلك المادة 487 من القانون الكندي [2]والإنجليزي[3]والفرنسي[4]والولايات المتحدة الأمريكية.[5]

1: محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلومات لجرائم الكومبيوتر والأنترنت، ب ط، منشأة المعارف شركة جلال للطباعة، الإسكندرية، 2006، ص 36.

2: نصت المادة 487 من القانون التي منحت سلطة إصدار إذن الضبط أي شيء طالما تتوافر أسس معقولة للاعتقاد أن الجريمة ارتكبت أو يشتبه في ارتكابها...

3: ينص القانون الإنجليزي صراحة على تفتيش نظم الحاسوب في جرائم الولوج غير مصرح به على أنظمة الحاسوب والتعديل الغير مصرح به دون إذن.

4: يرى بعض الفقهاء في فرنسا أن الشخصيات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا بالمعنى المألوف للمصطلح ولذا لا يمكن ضبطه.

5: تم تعديل القاعدة رقم 34 من القواعد الفدرالية الخاصة بالإجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة الحاسوب والكشف عن الوسائط الإلكترونية.

وبالتاليفإن النصوص القانونية التي أرست القواعد التي تحكم التفتيش تم سنها قبل أن يعرف القانون الأشياء المادية، وبالتالي فالنصوص التقليدية لا يمكن إعمالها مباشرة على النظم المعلوماتية لأن قيامها على الأشياء المادية سيكون منافيا لشرعية الإجرائية.[1]

وهو ما أقرته اتفاقية بودابست في المادة 01/09 من القسم الرابع على أنه: يمكن لكل دولة طرق الحق في أن تسن القوانين ماهو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى:

- نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة فيه.
- الوسائط التي يتم تخزين معلومات الكومبيوتر بها مادامت مخزنة في إقليمها.

يتضح موقف المشرع الجزائري من خلال القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، حيث أجازت المادة 05 منه للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها بغرض التفتيش ولو كان عن بعد إلى كل منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها أو في أي منظومة تخزين معلوماتية.

ويقصد التفتيش ولو كان عن بعد تفتيش حاسوب المتهم عندما يكون متصلا بغيره من الحواسيب عبر شبكة أخرى في دولة أخرى.

وطبقا للمادة 02/05 من القانون 09/04 أجاز المشرع تنديد التفتيش إلى هذه المنظومة بعد إعلام السلطة القضائية المختصة مسبقا بذلك متى وعت الضرورة إلى الاعتقاد وبأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه الأخيرة يمكن الدخول

1: سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير، جامعة باتنة، 2012، ص147.

إليها من المنظومة الأولى في إطار إقليم الدولة، وإذا تبين أن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن التفتيش أو الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة.[1]

II. تفتيش الشبكات المعلوماتية المتصلة بالحاسوب، التفتيش عن بعد.

✍ السلطة المختصة بالتفتيش:

يختص قاضي التحقيق أصلا بإجراء التفتيش تساعده النيابة العامة بتوليها تتبع الجرائم واتخاذ الجرائم واتخاذالإجراءات الملائمة بصددها تمتخطر قاضي التحقيق الذي يتولى مباشرة التحقيق، فالنيابة توجه الاتهام وقاضي التحقيق يباشر إجراءات التحقيق بما فيها التفتيش.

بقد نصت المادتان 81 و 82 من قانون الإجراءات الجزائية على أنه يجوز لقاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد به أشياء من شانها أن تفيد التحقيق وإظهار الحقيقة.

ولقد أجازت المادة 83 من قانون الإجراءات الجزائية لقاضي التحقيق القيام بنفسه بالتفتيشفي أي مكان آخر وبالتالي أي مسكن آخر غير مسكن المتهم ليضبط أدوات الجريمة أو ما نتج عن ارتكابها وكل شيء يفيد كشف الحقيقة، كما منحته المادة 83 من قانون الإجراءات الجزائية الحق في إنابة أحد ضباط الشرطة القضائية لقيام بهذا التفتيش إذ استحل على قاض التحقيق تنفيذه بنفسه.

وطبقا للشروط التي نصت عليها المواد 138 إلى 142 من قانون الإجراءات الجزائية والملاحظ أن المشرع الجزائري قد قيد قاضي التحقيق في منح الإنابة بشرط استحالة التفتيش ومن الممكن أن يتم التفتيش بمعرفة ضابط الشرطة القضائية في الجرائم المتلبس بها ولقد

1:أنظر: المادة 02/05 من القانون 09/04، مرجع سابق.

نصت المادة 15 من قانون الإجراءات الجزائية وعلى أعضاء الضبطية القضائية الذين هم صفة ضابط الشرطة القضائية إذ نص القانون على ضرورة إجراء التفتيش من طرف ضابط يساعده أعوان ولكن التفتيش يتم بحضوره وتحت إشرافه وإلا وقع باطلا.[1]

الشروط الشكلية:

أ – إجراء التفتيش بحضور أشخاص معينين بالقانون.

غني عن البيان أن التفتيش فيه إطلاع على أسرار الغير التي تحرم أغلب التشريعات الإجرائية الاطلاع عليها، لذلك فإنه من مطالعة التشريعات المقارنة نجد أن بعضها أوجب عملية التفتيش الذي تجريه الضبطية القضائية المشتبه فيه أو شهود وفي تشريعات أخرى حضور أشخاص معينين في القانون في حالات معينة أو جازت في أحوال أخرى إجراء التفتيش دون حضور أحد، وهناك تشريعات سكتت تماما عن التعرض لهذا الشرط.

وإن كان المشرع الجزائري من التشريعات الإجرائية التي أوجبت ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقاتها بحضور المشتبه فيه عندما يتم تفتيش مسكنه من طرف الضبطية القضائية، وإن تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش [2] إلاّ أنه بموجب التعديل الذي الحقه على قانون الإجراءات الجزائية القانون رقم 22/06 استثنى تطبيق هذه الشروط حضور المشتبه فيه أو الشاهدين عندما يتعلق الأمر بالجرائم

1:عبد الله أوهايبية، شرح قانون من قانون الإجراءات الجزائية الجزائري، دار الهومة، دون طبعة، الجزائر،2004، ص 250.

2:أنظر: المادة 45من قانون الإجراءات الجزائية الجزائري.

المعلوماتية[1] و هو ما يعدإقرار من المشرع بذاتية هذا النوع من الجرائم و ما يتطلبه التحقيق بشأنها من بسط نوع من السرية أثناء جمع الدليل الرقمي بالإضافة إلى الإسراع في استخلاصه قبل فقدانه.

ب – الميعاد الزمني لإجراء التفتيش.

المشرع الجزائري ذهب إلى حضر تفتيش المساكن وقد حكمها في أوقات معينة وحدد ميقات تنفيذ الخروج من هذا الميقات ويصبح إجراؤه في أي ساعة من ساعات الليل والنهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها في المواد من 342و348 من قانون العقوبات المرتكبة في أماكن معينة[2]، أو في حالة رضا صاحب المسكن صراحة.

وفي نطاق التفتيش المتعلق بالجرائم المعلوماتية فإن الاستثناء الوارد بالفقرة الثانية من المادة 47 من قانون الإجراءات الجزائية والمتعلق بجواز إجراء ضابط الشرطة القضائية للتفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق ينوع معين من الجرائم، فقد شمل هذا الاستثناء الجرائم المعلوماتية حيث جاء في نصها: ...عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطن، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و....فإنه يجوز إجراء التفتيش ...في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناءا على إذن مسبق من وكيل الجمهورية المختص..[3]

ج – محضر التفتيش:

1:أنظر: الفقرة الأخيرة من المادة 45من قانون الإجراءات الجزائية الجزائري.

2:أنظر: المادة 47من قانون الإجراءات الجزائية الجزائري.

3:سعيداني نعيم، مرجع سابق، ص 153.

باعتبار أن التفتيش عمل من أعمال التحقيق، ينبغي تحرير محضر يثبت فيه كل ما تم من إجراءات، وما ترتب عن هذا التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا لهذا المحضر وبالتالي فإنه لا يشترط لصحتهإلا ما تستجوبه القواعد العامة في المحاضر عموما، كأن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثنيها هذا المحضر.

وبالنسبةلتفتيش نظم الحاسوب فإنه يستلزم بالإضافة إلى ما سب ق ذكره، ضرورة إحاطة قاضي التحقيق أو عضو النيابة العامة بتقنية المعلومات، مع وجوب أن يكون هناك شخص متخصص في الكومبيوتر يرافقه للاستعانة به في مجال الخبرة الفنية، فحضور الخبير يساعد على صياغة مسودة محضر التحقيق.[1]

الفرع الثاني: المعاينة.

هي إجراء من إجراءات التحقيق، تتطلب سرعة الانتقال إلى محل الواقعة الإجرائية لمباشرتها بغرض إثباتها وتقديم للمحقق صورة حقيقة عن مكان وقوع الجريمة.

1. تعريف المعاينة:

1: خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009، ص 224،225.

تعني المعاينة مشاهدة وإثبات الحالة في مكان الجريمة، أي مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، ويطلق عليها في العادة إثبات حالة، بمعنى إثبات حالة الأشخاص والأشياء ذات الصلة بالحادث.[1]

تنص بالفقرة الثانية من المادة 79 من قانون الإجراءات الجزائية أنه: يجوز لقاضي التحقيق الانتقال إلى مكان وقوع الجرائم لإجراء جميع المعينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له حق في موافقته ومن خلال هذه المادة نلاحظ أن المعاينة في الإجراءات الجزائية يتولى قيامها النيابة العامة وقضاةالتحقيق.[2]

والمعاينة كأصل تتم بالانتقال إلى محل الجريمة أما فيما يخص جرائم الأنترنت والجرائم الإلكترونية تتم عن طريق العالم الافتراضي، بحيث يستطيع المحقق القيام بالمعاينة، وكما يجب على المكلف بالقيام بالمعاينة لأن يجعل في إجرائها وذلك تفاديا من فقدان الأدلة.[3]

فهناك فرق بين المعاينة والانتقال، فالمعاينة تكون مكان وقوع الجريمة إذ تتم بانتقال المحقق إلى مسرح الجريمة للوقوف على حالته عقب وقوع الجريمة للسيطرة على معالمها، ويشمل معالم الجريمة حالة بعدمكان وقوع الجريمة وحالة الجاني والمجني عليه، فذلك بوصف شامل ودقيق وضبط الآثار للأدلة المادية واستظهارها.[4]

1:فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، دون طبعة، مصر،1999، ص 103.

2:الأمر رقم 155/66 المؤرخ في 18 صفر علم 136 الموافق لـ 08 يونيو 1966 يتضمن قانون الإجراءات الجزائية ج. ر.ج.ج عدد 48 الصادرة بتاريخ 11 يونيو 1966 المعدل والمتمم بالقانون رقم 07/17 المؤرخ في 27 مارس 2017 ج. ر.ج.ج عدد 20 صادرة بتاريخ 29 مارس 2017.

3:حسين محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة الدكتوراه في الحقوق، كلية الحقوق، جامعة عين الشمس، ص 154.

4:عبد الفتاح عبد اللطيف الجبارة، الإجراءات الجنائية في التحقيق، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2015، ص 150

2. أهمية المعاينة:

للمعاينة أهمية كبيرة تتمثل في أمرين وهما:

الأول يتمثل في جمع الأدلة الناتجة عن الجريمة، والأمر الثاني يتمثل في وقوف المحقق أمام مسرح الجريمة لتحقيق عن كيفية وقوع الجريمة، ولذلك تعتبر المعاينة الدليل المباشر الذي يطمئن غليه المحقق باعتبارها تؤدي إلى الوصول على الحقيقة.[1]

إلا أن رغم أهميتها في الجرائم التقليدية إلاّ أنها لا تملك نفس الأهمية في مجال الحصول على الدليل الرقمي، وذلك لأن الجرائم الإلكترونية غالبا ما ترتب آثارها، أما الدليل الرقمي فهو دليل غير مرئي، وكذلك سهولة إزالة الدليل وذلك بتعديله أو محوه.[2]

كما أن هناك حالات استثنائية لا يلزم أن تكون المعاينة فيها فمثلا جريمة السب العلني تقع بالقول فقط.[3]

3. كيفية إجراء المعاينة على مسرح الجريمة الإلكترونية:

عند العلم بوقوع الجريمة فإن أول ما يقوم به الضابط القضائي هو الانتقال إلى مسرح الجريمة،لأن هذا الأخير من أهم ما يكون في التحقيق الجنائي، ومكان وجود الآثار والأدلة المادية، وينبغي التعامل في هذا الإطار مع مسرح الجريمة الإلكترونية على أنه مسرحان هما:

- **مسرح تقليدي:** ويشمل هذا المسرح جميع المكونات المادية للحاسب الآلي، ويمكن أن يحتوي على آثار مادية مثل بصمات الجاني أو وسائط تخزين رقمية، أو أوراق.

1:حسن محمد إبراهيم، مرجع سابق، ص 155.

2:عائشة بن قارة مصطفى، مرجع سابق، ص 81.

3:عائشة بن قارة مصطفى، مرجع نفسه، ص 82.

- **مسرح افتراضي:** ويقع داخل العالم الافتراضي (الرقمي) لجهاز الحاسب الآلي، ويحتوي على جميع المعلومات والبيانات الرقمية المخزنة فيه والتي تقيد في التحقيق.[1]

ونتيجةلاختلاف مسرح الجريمة الإلكترونية عن غيره من الجرائم، وهذا راجع لتوافره على الأدلة الإلكترونية ذات الطبيعة غير المرئية، مما يستوجب تعامل خاص مع هذا النوع من المسارح ويكون ذلك باتباع مجموعة من القواعد الفنية، قبل الانتقال لمسرح الجريمة الإلكترونيةوأهمها:

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

- الحصول على الاحتياجات الضرورية من أجهزة وبرامج الاستعانة بها في الفحص والتشغيل مثل برنامج معاجلة الملفات((xtree pro goldوبرنامج النسخ ((la plink، وبرنامج(en case)، ويستخدم هذا البرنامج بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفدرالية الأمريكية، ويسميها الخبراء حقيقة الأدلة الرقمية.

- تأمين التيار الكهربائي من الانقطاع المفاجئ، لأن هذا الأمر له العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء غلق جهاز الكومبيوتر، ومنه ضياع كل العمليات التي كان يتم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة. [2]

ومن الإجراءات التي يتعين اتباعها عند المعاينة ما يلي:

- القيام بتصوير جهاز الحاسب الآلي الذي ترتكب من خلاله الجرائم، وكذا كل ما يتصل به من أجهزة طرفية، ومحتوياته وأوضاع المكان الذي توجد فيه بصفة عامة.

1:فاطمة زهراء بوعناد، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول (بدون دار نشر)، الجزائر، 2013، ص 68.

2:عائشة بن قارة مصطفى، مرجع سابق، ص 85،86.

- العناية الدقيقة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام والمواقع بشبكة المعلومات، ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام.
- إجراء الاختبارات اللازمة قبل نقل أي معلومة من مكان وقوع الجريمة بهدف التأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارج ي، حتى لا يحدث أي إتلاف للبيانات المخزنة.
- القيام بحفظ المستندات الخاصة بالإدخال، وكذلك مخرجات الحاسوب الورقية التي لها صلة بالجريمة، ورفع ما قد يوجد عليها من بصمات وآثار مادية.
- ربط الأقراص الكمبيوترية التي ربما تحمل الأدلة، مع جهاز يمنع الكتابة أو التسجيل عليها مما يتيح للمحققين قراءة بياناتها دون تغييرها.
- التحفظ على محتوياتسلة المهملات والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها.[1]

ومنه نقول أنّ المعاينة تعتبر إجراء مهم من إجراءات الحصول على الدليل الإلكتروني أثناء مرحلة التحقيق ولا يمكن الاستغناء عنها.

الفرع الثالث: الخبرة

الاستعانة بالخبراء يعتبر من الإجراءات التي يلجا إليها القضاة وسلطات التحقيق كلما استعصى عليهم الأمر، ومن بين المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة الإلكترونية لأن حكمها يكون مبنيا على المنطق العلمي ومعيبا إذا لم يستند إلى الخبرة الفنية وذلك تحقيقا لمبدأ التخصيص.

1:عائشة بن قارة مصطفى، مرجع سابق، ص 86،87.

1. تعريف الخبرة:

يقصد بها مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة علمية لا تتوفر لديه.[1]

كما يعرف الخبير الإلكتروني بأنه الشخص الذي تعمق في دراسة الأعمال الإلكترونية وتخصص في أدائه فترة زمنية طويلة مما اكسبه خبرة علمية، بحيث اصبح ملما بتفصيلاته مما جعله متفوقا على الشخص العادي، و جعله قادرا على إبداء الراي الإلكتروني في الأمور المتصلة بهذا العمل و يشترط في هذا الخبير أن يكون لديه المؤهل العلمي و الخبرة العلمية، إلاّ أنّ الشخص الذي يعمل في هذا المجال لمدة طويلة الزمن و اصبح يتقن القواعد الفنية يمكن اعتباره خبير حتى و إن لم يتوفر فيه الجانب العلمي، عكس الذي يكون لديه المؤهل العلمي و لا يزاول هذه المهنة فلا يستطيع أن يكون خبيرا.

وعلى الخبراء الذين تكون لهم علاقة بالتحقيق الجنائي الإلكتروني أن يكونوا على معرفة بلغات البرمجة وأنظمة التشغيل الجديدة، وكذا تصميم البرامج وتشغيلهومعرفة الجديد منها، وكذلك تحليل البرامج وأنظمة التشغيل وأيضا أن يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على اختراق الشبكة.[2]

1:صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة تخرج لنسل شهادة الماجستير، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، 2013، ص 88.

2:مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، مصر،2009، ص 221،222.

2. الضوابط التي تحكم عمل الخبير في مجال الجريمة الإلكترونية.

مما لا شك فه عند قيام الخبير بمزاولة مهامه، يجب أن تتوفر مجموعة نمن الضوابط القانونية والفنية، فأما الضوابط القانونية هي أن يتم اختياره من قائمة الخبراء المعدة سالفا، وهو ما نصت عليه المادة ﴿144﴾ من قانون الإجراءات الجزائية بحيث يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة... و استثناء يجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول و يجب على الخبير أيضا أن يكون أدى اليمين القانونية و ذلك لكي لا يترتب على عمله البطلان، و هو مانصت عليه المادة ﴿145﴾ من نفس القانون، و ذلك بأن يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس.[1]

وبعدذلك يقوم الخبير بمزاولة مهامه المحددة له، وبعد انتهائه من عمله بعد تقريرا كتابيا مفصلا لما توصل إليه من نتائج، ويودعه خلال المدة المحددة له الأمر أو الحكم بالندب.

وأما الضوابط الفنية فيجب على الخبير أن يكون ملما بكل ما يتعلق بالحاسب الآليوملحقاته[2]، بالإضافة إلى وجوب تمكنه وفهمه البيئة التي يعمل فيها، والقدرة على أداء المهام الموكلة له دون أن يترتب على ذلك ضررا لدليل الجنائي الرقمي المراد استخلاصه.

3. أهمية الخبرة في البحث عن الدليل الرقمي.

نظم المشرع الجزائري أعمال الخبرة في قانون الإجراءات الجزائية في المواد ﴿143﴾ إلى ﴿156﴾ من قانون الإجراءات الجزائية ، واعتبارها من إجراءات البحث عن الدليل، بحيث نصت

1: إبراهيم بلعيات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، بدون طبعة، دار الخلدونية، الجزائر،2012، ص 304.

2: عبد الفتاح بيومي حجازي، المرجع السابق، ص 330.

المادة 143 من نفسالقانون على ما يلي: "لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة، أو من تلقاء نفسها أو من الخصوم".[1]

وكما تكمن أهمية الخبير في البحث عن الدليل وأنها وسيلة من وسائل التي تهدف إلى الكشف عن بعض الدلائل.[2]

وتبرز أهميتها أيضا في مجال الجرائم الإلكترونية، أنه في مجال غياب الخبير تعجز الشرطة القضائية في كشف غموض الجريمة، وكما تعجز أيضا جهات التحقيق في جمع الأدلة المتعلقة بالجريمة، وذلك يعود لنقص الكفاءات والتخصصات اللازمة لتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبه بواسطتها الجريمة وما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل والإهمال عند التعامل.[3]

كما أشار المشرع الجزائري في نص المادة 04/05 القانون رقم 04/09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: "يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".[4]

1:الأمر رقم 155/66، مرجع سابق.

2:يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، جامعة محمد بوضياف، مسيلة، 2016،2017، ص 34.

3:القانون رقم 04/09، مرجع سابق.

4:الأمر رقم 155/66، مرجع سابق.

ومن خلال هذه المادة نجد أن سلطات التفتيش يمكن أن تستعين بشخص له دراية خاصة بعمل المنظومة المعلوماتية وتكمن أهمية الخبرة في هذه المادة في مجال التحقيق في الجريمة المعلوماتية.[1]

يستهدف هذا الإجراء استخدام القدراتالعلمية أو الفنية لشخص، والتي لا تتوفر لدى رجال القضاة أو المحقق، من أجل الكشف عن دليل أو قرينة تفيد معرفة الحقيقة بشأن وقوع أو نسبتها للمتهم.[2]

4. أنواع الخبرة في مجال المعلوماتي:

4. 1- الخبرة الخاصة:

تعتبر الخبرة الفردية من اهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والأنترنت فالمؤسسات الكبرى المتخصصة في هذا المجال تعمل جاهدة على الاستعانة بأشخاص ثبتت كفاءتهم في مجال الحاسب الآلي والأنترنت، فهناك من الدول تقوم بمحاولة التعرف على قراصنة الذين تحولوا مع مرور الزمن إلى رموز وطنية من جراء تحركاتهم عبر الشبكة الإلكترونية.[3]

4. 2- الجهات التعليمة:

يمكن مواجهة الجريمة المعلوماتية عن طريق المؤسسات التعليمية والتيتهدف بدورها إلى تطوير العلم والقضاء على المشكلات التي تواجه الإنسانية، حيث يتم تدعيمها ماديا ومعنويا حتى تكون أفضل سبيل للمواجهة، وأنشأت العديد من المؤسسات التعليمية منها دراسات الكومبيوتر في

1:عبد الفتاح بيومي حجازي، مرجع سابق، ص 331.

2:رشيدة بوكر، مرجع سابق، ص 424.

3:عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، 2004، ص 1035.

جامعة "ستافرورد" ومعهد التكنولوجيا في "ماساشوستش" والذي وفر خبراء على درجة عالية من التفوق.[1]

4. 3-جهات الضبط القضائي:

قامت بعض الدول وأهمها الولايات المتحدة الأمريكية بإعداد أجهزة متخصصة للخبرة في إجراء الخبرة على الأنترنت، العابر نشاطها الإطار الدولي في هذا المجال المتمثل في منظمة الإنتربول.

حيث أن آخرنشاط مؤسستي في هذا الإطار هو الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية«FBI» أطلق عليه المعمل الإقليمي الشرعي للحاسوب، وأصبح مقر خبرة عامة متعددة النواحي القضائية، هدفه مكافحة التصعيد الخطير في الجرائم المعلوماتية من خلال التصنيف والتحليل للدليل الرقمي، وأهم دور يقوم به هذا المعمل هو التقاء العديد من منظمات الضبط القضائي من أجل التعاون فيما بينها.[2]

المطلب الثالث: الإجراءات الحديثة في جمع الأدلة الجنائية الرقمية.

تم الحديث في المطلب السابق عن مجموعة من الإجراءات التقليدية للحصول على الدليل الإلكتروني واتضح أن هناك صعوبات تحيط بهذه الإجراءات في سبيل استخلاص الدليل الإلكتروني، ولهذا أصبح من اللازم على التشريعات أن تواكب التطور التكنولوجي، من خلال استحداث قواعد إجرائية تتماشى مع طبيعة الدليل الإلكتروني الخاصة، وهذا من أجل تسيير عمل الإجراءات التقليدية، أو تبني إجراءات حديثة مستقلة قائمة بذاتها.

1:خالد ممدوح إبراهيم، مرجع سابق، ص 424.

2:عمر محمد أبو بكر بن يونس، مرجع سابق، ص1038،1037.

الفرع الأول: التسرب.

إنّ التسرب من الناحية الأمنية هو تلك العملية المحضر لها والمنظمة قصد التوغل داخل وسط لمعرفة أو استعلام عن نشاط جرمي ومعرفة أدق التفاصيل فيه وحضو صيانة، أمّا من الناحية القانونية المشرع الجزائري حدد مقصودا لهذا الإجراء بموجب المادة 56 مكرر12 من قانون الإجراءات الجزائية على أنه: "قيام ضابط الشرطة القضائية أو عون تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة أشخاص مشتبه في ارتكاب جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك".[1]

و يلاحظ مما سبق ذكره أن التسرب عملية معقدة تتطلب أن يدخل العون المكلف بالعملية في اتصالبالأشخاص المشتبه فيهم و يربط معهم علاقة من أجل تحقيق الهدف النهائي من العملية، و تتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية التي تسرب إليها.[2]

1. شروط القيام بعملية التسرب.

لقد قدم المشرع جملة من الشروط يجب مراعاتها عند القيام بعملية التحري والتحقيق في الجرائم، وذلك باعتبارها من أخطر الإجراءات التي تؤدي إلى انتهاك حرمة الحياة الخاصة للفرد وذلك حسب نص المادة39 من الدستور.[3]

أ الشروط الشكلية لقيام عملية التسرب.

- أن يكون صادر بإذن قضائي إمّا وكيل الجمهورية أو قاضي التحقيق المختص.

1:أنظر: المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري.

2:سعيداني نعيم، آليات البحث والتحري في الجريمة المعلوماتية، مرجع سابق، ص169.

3:باعتبار أنّ حرمة الحياة الخاصة هو حق مكفول دستوريا وكذا في الاتفاقيات التي صادقت عليها الجزائر ولذلك حدد القانون ضوابط الإجراء عملية التسرب.

- أن يكون الإذن مكتوبا وإلاّ وقع تحت طائلة البطلان.[1]
- ذكر اسم الضابط الذي تتم عملية التسرب تحت مسؤولية أو عون الشرطة القضائية باعتباره مساعدا له.[2]
- المدة المطلوبة لعملية التسرب 04 أشهر محددة قانونا قابلة للتجديد ويمكن توقيفها حتى انتهاء المدة المحددة لها.[3]

ب –الشروط الموضوعية لقيام عملية التسرب.

- تحديد الجريمة وهي تلك الجرائم التي لا تخرج عن تلك المذكورة على سبيل في المادة 65 مكرر 05، وهي جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد.
- أن يكون الإذن الذي أصدرته الجهات القضائية مسببا وذلك أنه بالتسبيب يتبين من خلاله الأشياء التي جعلت الجهات القضائية المختصة بإصدار هذا الأمر، وكذلك الأشياء التي جعلت ضابط الشرطة القضائية باللجوء للقيام بهذا الإجراء الذي يكون ضمن موضوع الإذن.
- يستلزم عند القيام بإصدار الإذن بالتسرب من طرف الجهات القضائية المختصة بإظهار جميع الأدلة اللازمة.[4]

2. كيفية استخدام التسرب في الجريمة الإلكترونية.

1:أنظر المادة 65 مكرر 05 من قانون رقم 22/06 المعدل لقانون الإجراءات 66. 155.

2:أنظر المادة 65 مكرر 16 من تعديل 2006 لقانون الإجراءات الجزائية.

3:أنظر المادة 65 مكرر 15 فقرة 03 تعديل 2006 لقانون الإجراءات الجزائية.

4:سعيد نعيم، آليات البحث والتحري في الجريمة المعلوماتية، مرجع سابق، ص176.

تتم عملية التسرب في نطاق الجريمة الإلكترونية بدخول الضابط وأعوان الشرطة القضائية في العالم الافتراضي، وذلك باختراقهم للمواقع الإلكترونية والمشاركة في المحادثات مع المشتبه فيهم، وظهورهم كأنهم فاعلين أصلين، وذلك بمعرفتهم على كيفية اختراق المواقع وكيف يتم ارتكاب هذه الجرائم، وذلك للاستفادة وجمع الأدلة المراد تحصيلها.[1]

3. الأفعال المقررة بعملية التسرب:

تناول المشرع الجزائري هذه الأفعال في نص المادة 65 مكرر 14 التي تنص على ما يلي: "يمكن لضباط وأعوان الشرطة القضائية المرخص لهم إجراء عملية التسرب والاستخلاص الذين يسخرونهم لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بمايلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق، أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل أو التخزين، أو الإيواء، أو الحفظ أو الاتصال."

ومن خلال هذا النص يتبين أن طبيعة هذه الأفعال تستوجب من القائمين به مشاركة إيجابية ومثلاحيازة متحصلات الجريمة بحيث أن هذه الأفعال لها تأثيرات على المسؤولية الجزائية "دون أن يكونوا مسؤولين جزائيا".

ولكي تتحقق عملية التسرب والوصول إلى الهدف المرجو من هذه العملية، يجب أن تتم العملية في سرية تامة، وذلك من أجل عدم اكتشاف الهوية الحقيقية لضباط وأعوانالشرطة القضائية من قبل المجرمين.

1:يوسف جفال، مرجع سابق، ص 37.

لذلك منح له المشرع الجزائري حماية وذلك في نص المادة 65 مكرر 16 الفقرة 02 من قانون الإجراءات الجزائية على أنه: يعاقب كل من يكشف هوية ضابط وأعوان الشرطة القضائية بالحبس من سنتين (02) إلى خمس (05) سنوات وبغرامة تقدر بـ 50.000 دج إلى 200.000دج.[1]

الفرع الثاني: اعتراض المراسلات.

لقد أغفل المشرع الجزائري في قانون الإجراءات الجزائية تعريف لاعتراض المراسلات، و اكتفى بوضع تنظيم لعملية اعتراض المراسلات في المواد 65 مكرر 05 إلى غاية المادة 65 مكرر 10 من القانون المذكور، و لا يغني هذا أن يرمي المشرع بالقصور، لأنّ وضع التعريفات ليس عمل المشرع إنّما هو من اختصاص الفقه.[2]

نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية إن المقصود باعترا ض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق القنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض، مع العلم أن هذا النص هو إعادة صيانة المادة 100 من قانون الإجراءات الجزائية الفرنسي.

عرفت لجنة خبراء البرلمان الأوربي بمناسبة اجتماعها المنعقد "بسترسبورغ" في 2006/10/06 لدراسة أساليب التحري التقنية وعلاقتهابالأفعال الإرهابية عملية اعتراض

1:الأمر رقم 155/66، المتضمن قانون الإجراءات الجزائية، مرجع سابق.

2: l'article (100) sitruple «… autorités peuvent intercepter et la transcrire de correspondances émises par la voie des télécommunications..» voir la loi N° 1062 ,de 15/11/2001, portant code de procédures pénales français jore، 2001 16/11/2001

المراسلات بأنها :"عملية مراقبة سرية المراسلات السلكي ة واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب الجريمة". [1]

1. خصوصية اعتراض المراسلات:

تتسم عملية اعتراض المراسلات بخصوصية، ولكي تتسم بهذه الأخيرة توافر عنصرين و هما:

- **عنصر موضوعي:** وهو ما يتعلق بموضوع الرسالة في حد ذاته، وذلك يعني أن تكون الرسالة ذات طابع شخصي وسري.
- **عنصر شخصي:** والمراد به هو تحديد المرسل إليه ورغبته في عدم السماح للغير بالاطلاع على مضمون الرسالة.

فإذا تم توفير هذين العنصرين في الرسالة فتصبح هذه الرسالة خاصة، ولها خصوصيتها وسريتها المحمية في القانون، وذلك طبقا لنص المادة "39" من الدستور، ولا تشكل أهمية لنوع وشكل الرسالة، ولا تشكل أيضا أهمية في طريق نقلها أوتوصيلها.

وكما أنه يمكن لضابط الشرطة القضائية اللجوء إلى اعتراض المراسلات، إلا بعد أخذ إذن مكتوب من وكيل الجمهورية، أو قاضي التحقيق، ويجب أن يكون مكتوبا، ومسببا حسب نص المادة "65 مكرر 07". [2]

2. شروط اعتراض المراسلات.

أ –الحصول على إذن مكتوب:

1:بوكر رشيدة، مرجع سابق، ص 442.

2:يوسف جفال، مرجع سابق، ص 39.

تعتبر السلطة القضائية عموما هي المختصة بإصدار هذا الإذن، ويعد هذا الأمر ضمانة ضرورية حتى يكون هذا الأمر مشروعا، هذا ما نص عليه القانون الفرنسي، فالمشرع استلزم صدور الإذن بالاعتراض من قاضي التحقيق المختص، أو من القاضي الجزائي، وحرمان النيابة العامة من إصدار هذا الإذن حتى لا يكون أي تعسف من طرفها، إلا في حالة ما إذا كانت النيابة العامة تتولى التحقيق بنفسها.

وفي المقابل المشرع الجزائري أجاز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وذلك في المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

وبالنظر إلى الطبيعة الخاصة التي يتمتع بها الدليل الإلكتروني من حيث سرعة فقده وزواله، نجد أنه من اللزوم التحقيق من شروط وجوب استئذان النيابة العامة للقاضي الجزائي حتى تتمكن من مباشرة الاعتراض بنفسها في جريمة من الجرائم الإلكترونية التي تتولى التحقيق فيها، وهذا كسبا للوقت، وحفاظا على الدليل.[1]

ب –تسبيب الإذن الصادر باعتراض الاتصالات الإلكترونية.

يجوز للقاضي إصدار الإذن بمراقبة الاتصالات الإلكترونية كما سبق، من خلال أعمال الاستدلال التي قام بها مأمور الضبط القضائي و ما يراه من ضرورة هذه المراقبة، لما لذلك من أهمية في ظهور الحقيقة في جريمة ما خاصة الجريمة الإلكترونية، و ينتج هذا التسبيب بصفة عامة من مدى اقتناع القاضي بجدية التحريات التي اتخذها ضابط الشرطة القضائية، و السبب في ضرورة

1:أشرف عبد القادر قنديل، مرجع سابق، ص 188-189.

تسبيب الإذن القضائي يرجع إلى كون هذا الإجراء يمس بحريات الأفراد، فهو استثناء على القاعدة العامة والمتمثلة في حرمة الحياة الخاصة للمواطنين و حقهم في سرية مراسلاتهم.[1]

ج تحديد الجرائم محل الاعتراض والمراقبة.

إن الاستعانة بعملية اعتراض أو مراقبة المراسلات الإلكترونية لغرض التحقيق غير مسموح في كافة الجرائم، إنما مجال تطبيقها يتوقف عند نوع محدد فقط:

- الجرائم المذكورة على سبيل الحصر في نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية وهي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد والجرائم الماسة بأنظمة المعالجة الآلية.[2]

- الجرائم المنصوص عليها في الفقرات أ، ب، ج، القاضي الجنائي من المادة 04 من القانون رقم 04/09 المتمثلة في الأفعال الموصوفة بجرائم الإرهاب أو التخريب، الاعتداءات على منظومة معلوماتية الماسة بأمن الدولة، بما فيها تلك التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني.[3]

وتجدر الإشارة إلى أن المشرع لم يحدد نوع الجرائم التي تندرج ضمن الفقرة ج من المادة 04 أعلاه والتي يصعب وصول التحريات والتحقيقات القضائية الجارية في شأنها إلى نتيجة تهم هذه الأبحاث دون اللجوء إلى المراقبة الإلكترونية وهو ما يفتح المجال أمام جميع جرائم القانون العام لكي تكون محلا للمراقبة الإلكترونية كلما كان هذا الإجراء ضروريا.

1: شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة مكملة لنيل شهادة الماستر في الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2016-2017، ص64.

2: أنظر: المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

3: أنظر: المادة 04 من قانون رقم 09 / 04 ، مرجع سابق.

د -سرية الإجراءات وكتمان السر.

أي ينبغي أن تنفذ عملية الاعتراض والمراقبة في سرية تامة دون علم أو رضا المشتبه فيه أو صاحب الأماكن، مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة 45 فقرة 04 من قانون الإجراءات الجزائية.

وينبغي التنبيه كذلك، إلى أن المشرع الجزائري لم يشير صراحة إلى كيفية وضع الأدلة المحصل من عملية اعتراض ومراقبة المواصلات (التسجيلات السمعية البصرية، البيانات الرقمية) في أحراز مختومة، مما يطرح التساؤل حول مدى اعتبارها من قبيل الأشياء المضبوطة التي تخضع لأحكام المادة 84 من قانون الإجراءات الجزائية وحكم المادة 05/45 من ذات قانون.[1]

علما بأن هذه التسجيلات والبيانات تعتبر أدلة إثبات رقمية أصلية تقتضي الشرعية الإجرائية، حفظها بطريقة خاصة بوضعها في أحراز مختومة تضمن عدم التلاعب والعبث فيها بالحذف والإضافة، وضمها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها للكشف عن الحقيقة.

ومن ذلك كانت الحاجة إلى فتح المشروع المجال أمام سلطات التحقيق والاستدلال للاستعانة بذوي الاختصاص سواء عن طريق تسخير كل ما لديهم درايةو مؤهلات في مجال سيوتكنولوجيات الإعلام و الاتصال من أجل تزويدهم بالمساعدة الفنية و التقنية الممكنة لتسهيل و إنجاح أية عمليةمن عمليات التحقيق بما فيها المراقبة الإلكترونية للاتصالات كما هو منصوص

1:أنظر: المادة 84 من قانون الإجراءات الجزائية على أنه: "... ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة.."

في المادة 05 الفقرة الأخيرة من القانون رقم 04/09[1]، أو عن طريق تكليف هؤلاء المختصين باستعمال الوسائل التقنية المناسبة و الضرورية للحيولة دون الوصول إلى المعطيات التي تشكل محل الجريمة أو تحتوي أدلة لها، الموجودة داخل المنظومة المعلوماتية، و منع الاطلاع عليها أو نسخها أو تهريبها أو تدميرها وفقا لما تقتضيه المادتين 07 و08 من القانون رقم 04/09.

1. طرق اعتراض المراسلات

يعد البريد الإلكتروني أهم وسيلة في إطار التراسل الإلكتروني، من ثم فعلية الاعتراض عادة ما تنص عليه، بحيث أن هذه الرسائل تحتوي على العديد من المعلومات، كتاريخ إنشاء الرسالة، وتاريخ إرسالها، أو تلقيها، وعنوان المرسل والمرسل إليه، ولكن تبقى المعلومات التي تحتوي عليها حاشية رسائل البريد الإلكتروني «email Head» هي الأهم، كما تتضمن على عنوان Ip/ مرسل الرسالة، بحيث أن هذا العنوان يحتوي على معلومات تتمثل في الكومبيوتر الذي تتم إرسال الرسالة منه.[2]

الفرع الثالث: المراقبة الإلكترونية.

تم استحداث هذا الإجراء بموجب القانون رقم 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[3]

لم يعرف المشرع الجزائري إجراء المراقبة الإلكترونية بل ترك أمر تعريفها للفقه، ومنه فتعرف أنّها: عمل أمني له نظام معلومات إلكتروني، يقوم فيه المراقِب (بكسر القاف) بمراقبة المراقَب

1: أنظر: المادة 05 من القانون رقم 04/09، مرجع سابق.

2: يوسف جمال، مرجع سابق، ص 39.

3: مصطفى محمد يوسف، المراقبة الإلكترونية عبر شبكة الأنترنت (دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية)، دار الكتب القانونية، بدون طبعة، مصر، ص 192.

(بفتح القاف) بواسطة الأجهزة الإلكترونية وعبرشبكة الأنترنت، لتحقيق غرض محدد وإفراغ النتيجة في ملف إلكتروني، وتحرير تقارير بالنتيجة.[1]

بناء على التعريف السابق، يمكن القول أن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات و المعلومات، عن المشتبه فيه [2]، بحيث يقوم بها مراقب إلكتروني يتمثل في ضابط من ضباط الشرطة القضائية ذي كفاءة تقنية عالية، و باستخدام تقنيات و برامج إلكترونية فيها، لذا و بالرجوع إلى القانون رقم 04/09 الذي سبق ذكره، نجد أنّ المشرع الجزائري لم يعتبر هذا الإجراء طريقة من طرق الحصول على الدليل الجنائي الرقمي فقط، بل أدرجه أيضا ضمن التدابير الوقائية من الجريمة المعلوماتية، التي يمكن أن ترتكب بواسطة المعلوماتية إلى جانب إمكانية القيام بإجراء مراقبة الاتصالات الإلكترونية في إطار التحريات القضائية من أجل الوصول إلى الأدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء فإنه يمكن كذلك تطويع هذه التقنية لكي تعمل في بيئة رقمية لغرض الوقاية من احتمال وقوع في جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة.[3]

2. شروط القيام بعملية المراقبة الإلكترونية.

باعتبار المراقبة وسيلة من وسائل الإجرائية لجمع الدليل الرقمي في مجال الجريمة الإلكترونية فقد أحاطها المشرع بجملة من الشروط وهي:

ما أكده القانون 04/09 سابق الذكر في المادة 04 الفقرة (05) أنه: "لا يجوز إجراء عمليات المراقبة إلاّ بإذن مكتوب من سلطة قضائية مختصة" بمعنى أنّه لا يمكن اللجوء أو تنفيذ العملية إلاّ بعد الحصول على إذن من قبل السلطات المختصة.

1:نبيلة هبة هروال، مرجع سابق، ص 199.
2:نعيم سعيداني، مرجع سابق، ص 39.
3:نعيم سعيداني، نفس المرجع، ص 199.

كما أشارت المادة 04/ج من القانون المذكور أعلاه: أن لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية بمعنى أن يتم اللجوء إلى المراقبة عندما تتطلب الضرورة في تحقيق و عند وجود صعوبة الوصول إلى النتيجة تهم مجريات التحري و التحقيق دون اللجوء إلى المراقبة الإلكترونية.[1]

3. حالات اللجوء إلى عملية المراقبة الإلكترونية.

لقد نص المشرع الجزائري من خلال نص المادة 04 من القانون 04/09[2]، على الحالات التي يتوافرها يمكن اللجوء إلى المراقبة الإلكترونية المنصوص عليها في المادة03:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توافر معلومات عن اتصال اعتداء على المنظومة على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تخدم الأبحاث دون اللجوء إلى مراقبة الاتصالات الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية.

قانون الإجراءات الجزائية أنه:

1: بن قدوم سوهيل، الدليل الرقمي في الاثبات الجنائي، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2017-2018، ص 34.

2: أنظر: المادة 04 من قانون رقم: 04/09، مرجع سابق.

أنه:👌يجوز لقاضي التحقيق الانتقال إلى مكان وقوع الجرائم لإجراء جميع المعينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له حق في موافقته👌

المادة 👌79👌 من قانون الإجراءات الجزائية أنه: 👌يجوز لقاضي التحقيق الانتقال إلى مكان وقوع الجرائم لإجراء جميع المعينات اللازمة أو القيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له حق في موافقته 👌

الفصل الثاني

الفصل الثاني: القيمة القانونية للدليل الرقمي و تقديره أمام القضاء.

إن التطور التكنولوجي و تزاوجه مع نظام الاتصالات أفرز ميلاد عالم الافتراضي الذي فرض نفسه بقوة في جميع نواحي الحياة، و قوام هذا العالم الرقم صفر، و واحد و صاحب هذا التطور عديد من الأفعال المقترنة بسوء النية، نالت المعطيات التي تمت معالجتها آليا اصطلح عليها بالجرائم الإلكترونية التي تزايدت معدلاتها و امتداد أثارها على كافة مجالات الحياة بسبب ارتباطها بشبكة الأنترنت، اضطرت التشريعات إلى ترشيد إجراءات متطورة لتصبح نافذة في مواجهة هذه الجرائم وهو ما يسمى بالدليل الإلكتروني(الرقمي) الذي يعتبر من الأدلة الجنائية الخاصة التي ظهرت بظهور الجريمة الإلكترونية بهدف إثباتها، باعتبارها الوسيلة الوحيدة لإثبات هذه الجرائم.

نظرا للخصائص و مميزات الاستثنائية التي تتمتع بها و سرعة محوها من المسرح الجريمة، فإن أجهزة القضاء الجنائية وجدت نفسها أمام تحديات قانونية و عملية جديدة غير معهودة فيما يخص فهم الطبيعة الخاصة لهذه الأدلة الإلكترونية المنتشرة في بيئة افتراضية و أساليب البحث و التحري عنها، و كذا كيفية التعامل معها بشكل يبقى على طبيعتها الأصلية و لا يفقدها قيمتها الاستدلالية، و هو الأمر الذي دفع الفقه الجنائي إلى التدخل لرفع الإبهام عن هذه المسألة من خلال تحديد مفهوم الدليل الرقمي وخصائصه و أنواعه، مراحله و كذا مشروعيته.

ولم يتوقف الأمر عند هذا الحد، بل أثارت الظاهرة إجرامية التقنية العديد من المشكلات الأخرى في خضوعها لأحكام قانون الإجراءات الخاصة بجرائم التقليدية لا تثير صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأالإقناع الشخصي للقاضي الجزائي، وكذا الضوابط التي تحكم هذا المبدأ ومشكلات الاختصاص القضائي في مثل هذه الجرائم، وهوالأمر الذي سيكون محور الدراسة في المبحث الثاني.

المبحث الأول:ماهية الدليل الرقمي كدليل إثبات في المواد الجنائية.

نظرا لحداثة الجريمة الإلكترونيةوارتباطها بتكنولوجيا فإنه من الضروري لجوء الجاني إلى استخدام أساليب خاصة عند ارتكابها وتقنيات حديثة، ومن جهة أخرى فعلى الجهات المتخصصة إثبات هذه الجريمة استخدام تقنيات علمية لاكتشافها، غذ يعتبر الدليل الإلكتروني دليل جنائي خاص الذي ظهر بهدف إثبات هذه الجرائم فكان من الضروري معرفة معنى الدليل الإلكتروني لكي يسهل توضيح كل الجوانب المتعلقة به.

والوقوف عند خصائص الدليل الإلكترونيالتي تعتبر في غاية الأهمية باعتبار أنها تميز الدليل الإلكتروني وذلك من خلال ما يلي:

المطلب الأول: ماهية الدليل الإلكتروني.

لقد أثرَت الثورة العلمية على نوعية الجرائم التي صاحبتها وظهور أنماط مستحدثة من الجرائم عرفت بالجرائم المعلوماتي، فإنها في المقابل أيضا أثرَت على إثباتها فأصبحت الأدلة التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير قادرة على إثبات هذا النوع من الجرائم الذي يحتاج إلى طرق تقنية تتناسب مع طبيعتها، بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوبة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات طبيعة فنية وعلمية خاصة.

الفرع الأول:تعريف الدليل الرقمي وتقسيماته.

أولا: تعريف الدليل الرقم.

يعرف البعض الدليل الرقمي على أنه:" الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتباره أمام القضاء.

وهو مكون رقمي لتقديم المعلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكالوالرسوم، وذلك من أجل الربط بين الجريمة والمجرموالمجني عليه بشكل قانوني يمكن الأخذ به أمام أجهزة إنفاد وتطبيق القانون.[1]

كما عرف أيضا أنه:" ذبذبات أو نبضات إلكترونية «Impulsions électroniques» مسجلة على وسائط أو دعائم مادية" [2]أو أنه:" الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكةالأنترنتوالأجهزةالإلكترونيةالملحقة والمتصلة به وشبكات الاتصال، من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة."[3]

وعرف أيضا بأنه:" معلومات يقبلها المنطق والعقلويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعملية بترجمة البيانات الحاسوبي ة المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل شيء أو تشخص له علاقة بجريمة أو جان أو مجني عليه."[4]

وهناك أيضا من يعرف الدليل الرقمي بأنه:" يشمل جميع المعلومات والبيانات الرقمية التي يمكن أن تثبت أن هناك جريمة قد ارتكبت أو توجد علاقة بين الجريمة والجاني، أو توجد علاقة بين الجريمة

1: ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكومبيوتر والأنترنت، ب ط، دار الكتب القانونية، مصر، 2006، ص 88.

2: نفسه، ص 176.

3: خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 230

4: محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، السعودية،2004، ص 243.

والمتضرر منها، والبيانات الرقمية هي مجموعة من الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت، والتي جرى تخزينها أو إرسالها عبر جهاز الإلكتروني.[1]

ثانيا: تقسيماته.

للدليل الرقمي أشكال مختلفة، وقد قسمها البعض إلى الأقسام الأساسية التالية:

1 -الأدلة الرقمية الخاصة بأجهزة الحاسب الآلي وشبكاتها.

2 -الأدلة الرقمية بالشبكة الدولية للمعلومات " الأنترنت"

3 -أدلة خاصة ببروتوكولات تبادل ونقل المعلومات بين أجهزة الشبكة العالمية للمعلومات

وبالتالي هذا التقسيم يتطابق مع تقسيم الجريمة عبر الحاسب الآلي.[2]

وقد قررت وزارة العدل الأمريكية لسنة 2002 أن الدليل الرقمي يمكن تقسيمه كالتالي:

1 -المسجلات المحفوظة في الحاسب الآلي وتشمل الوثائق والملفات المكتوبة والمحفوظة كالبريد الإلكتروني وملفات معالجة الكلمات مثل «WinWord»، ورسائلوغرف المحادثات عبر الأنترنت.[3]

1: the Technical Working Group for Electronic Crime Scene Investigation, Electronic Crime Scene Investigation of justice the unites states of America,2001,p 06.

2: ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 88.

3: عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بأدلة رقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول للعلوم وأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 13.

2 المسجلات التي تم إنشاؤها وإعدادها بواسطة الحاسوب، و هي تعد مخرجات الحاسوب، والتي لم يشارك الأشخاص فيها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي «Files».[1]

3 المسجلات التي تم حفظ جزء منها بإدخال جزء تم إنشاؤه عن طريق الحاسب الآلي، ومنها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيها مباشرة إلى برامج أوراق العمل، و بعد ذلك تم معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها تلقائيا مثل:« Excel»

المطلب الثاني:خصائص الدليل الرقمي.

يتميز الدليل الرقمي بجملة من الخصائص تميزها عن غيره من الأدلة الجنائية التقليدية ويرجع سبب هذا إلى استخراجه من البيئة الافتراضية فلها خصائص علمية ومواصفات قانونية، فهذه الأخيرة مرتبطة أساسا بطبيعة البيئة التي يتواجد فيها التي انعكست على طبيعة هذه الأدلة وجعله يتصف بالخصائص التالية:

الفرع الأول: الدليل الرقمي دليل علمي.

الدليل الإلكتروني هو الواقعة التي تنبئ عن وقوع جريمة أو فعل مشروع، وهذه الواقعة مبناها علمي، من حيث أن مبنى العلم الافتراضي علمي، وهذه الخاصية مفادها أن الدليل الإلكتروني لا يمكن الحصول عليه ولا الاطلاع على فحواه غلا باستخدام أساليب علمية.[2]

1: خالد عياد الحلبي، مرجع سابق، ص 243.

2:فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون، مصر، 2010، ص 684.

يتطلب في استخلاص الدليل الجنائي الرقمي وتحليله طرقا غير تقليدية، بحيث يتم إجراء تجاري علمية وتقنية على جهاز الحاسب الآلي الذي استخدم فيه الجريمة معينة.[1]

وعليه عند ما يتم البحث عن الدليل الجنائي الرقمي، يجب أن تكون هذه العملية في إطار جغرافيا النظام الافتراضي «géographique information systèmes» الخاضعة لقوانين الإعلام الآلي أو البيئة المعلوماتية ككل.[2]

يتصف الدليل الإلكتروني بأنه علمي لأنه مشكل من معطيات الإلكتروني ة غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات ذات المبنى العلميوأن ما يسري على الدليل يسري على الدليل الإلكتروني[3]، و إذاكان الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة إذ يستبعدها تعارضه مع القواعد العلمية السلمي، فإن الدليل الإلكتروني له الطبيعة ذاتها، و يجب أن لا يخرج مما توصل إليه العلم الإلكتروني الرقمي و إلا فقد معناه.[4]

الفرع الثاني: الدليل الرقمي دليل تقني.

يعد الدليل الرقمي ذو طبيعة تقنية و هذا ما يميزه عن الدليل التقليدي، من حيث أن التقنية لا تنتج سكينا يتم من خلاله معرفة القاتل أو اعترافا مكتوبا أو ما قدم كرشوة أو بصمة أصبع، بل تنتج التقنية نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه، و هذا ما جاء به المشرع البلجيكي بمقتضى القانون الصادر في 22 نوفمبر

1:فتنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، دراسة تأصيلية تطبيقية (رسالة ماجستير)، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العلي، السعودية، 2012، ص 74.

2:عمر محمد أبو بكر يونس، الدليل الرقمي، دون طبعة، دون دار نشر، مصر، 2006، ص 7.

3:عمر محمد أبو بكر يونس، مرجع سابق، ص 977.

4:علي محمود علي حمودة، الأدلة المحصلة على الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العربي الأول، الأدلة الجنائية والطب الشرعي المنظم بالرياض في الفترة الممتدة بين 122 و14 نوفمبر 2008، ص 01، 45، 22.

2000 بتعديل قانون التحقيق الجنائي من خلالإضافة المادة (39) التي أجازت ضبط الأدلة الرقمية مثل نسخ المواد المحذوفةفي نظم المعالجة الآلية للبيانات بقصد عرضه على الجهات القضائية. [1]، و عليه ما يميز الدليل الرقمي على أنواع الأدلة الأخرى أنه يمكن أن يستخرج نسخ من الدليل الرقمي مماثلة و مطابقة الأصل و لها نفس القيمة العلمية و الثبوتية، و هذا ما يكفل وجود ضمانة قوية و فعالة للحفاظ على الدليل ضد الفقدان و التلف و التغيير من خلال وضع نسخ طبق الأصل من الدليل[2]،بالضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله، و ذلك لإمكانية مقارنته بالأصلالأساليب و برامج و التطبيقات الصحيحة.

كما تظهر أهمية تقنية الدليلالإلكتروني في الدور الذي تقوم به التقنية في كشف الدليل الإلكتروني، وهذه العلاقة تقتضي اهتمام من ناحيتين، الأولى ضرورة الاهتمام بتقنية البرامج التي تتعامل مع الدليل الإلكتروني من ناحية اكتسابه أو التحفظ عليه، وتحليله، وتقديمه، والثانية هي أن هذه البرامج في حد ذاتها يجب أن تكون مقبولة من قبل المحكمة، وهذا ما يستدعي الإشارة إليه في محضر الاستبدال والتحقيق إلى التقنية في الحصول على هذا الدليل.

فإن إطلاق صفة الإلكتروني تعني أن يكون هناك توافق بين الدليل الموجود وبين البيئة التي يعيش فيها فلا وجود للدليل الإلكتروني خارج بيئة التقنية أو الإلكترونية.[3]

الفرع الثالث: صعوبة التخلص من الدليل الرقمي.

تعد هذه الخاصية أهم ميزة يتميز بها الدليل الإلكتروني عن غيره من الأدلة المادية و إذا كان من اليسير جدا التخلص من الأدلة المادية نهائيا دون إمكانية استعادتها كالوثائق و الأشرطة بتمزيقها

1:عمر محمد أبو بكر يونس، مرجع أعلاه، ص 7.

2:أنظر: عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص15.

3:فتحي محمد أنور عزت، مرجع سابق، ص 650.

وحرقها، أو بصمات الأصابع بمسحها من موضعها، أو حتى الشهود بقتلهم أو تهديدهم بعد الإدلاء بالشهادة، فإن الحال غير ذلك بالنسبة للأدلة الإلكترونية [1] لأن موضوع التخلص من الدليل الرقمي باستعمال أو الاستعانة بخصائصالتخلص من المستندات في الحاسب الآلي و الشبكة الإلكترونية لا تعتبر من العوائق التي تحيل دون استرداد الملفات، حيث أنه تتوفر برمجيات من ذات الطبيعة الرقمية يمكن من خلالها استرجاع كامل الملفات التي تم من قبل إلغاؤها أو محوها من الحاسب الآلي أو إظهارها، و هذا ما يعني صعوبة إخفاء الجاني لجريمته.[2]

كما يعتبر نشاط الجاني في سبيل محو الدليل الذي يدينه دليلا أيضا، وهذا لأن فعله هذا أي محاولته لإخفاء الدليل يتم تسجيله في الكومبيوتر، ويمكن استخلاصه كدليل إدانة ضده.[3]

و بالتالي فإن خاصية صعوبة التخلص من الدليل الإلكتروني تقابلها مسالة أخرى هي أن هذا الدليل نتيجة لمرونته و ضعفه، فإن يسهل إتلافه أو فقدانه أو كما يطلق عليه « spoliation of évidence » بمعنى إمكانية التخلص منه بغير الحذف و الإلغاء، و بالنظر في هذه المسألة أي إمكانية إتلاف الدليل الإلكتروني، هي في الواقع ليست حقيقية، و إنما القول بإمكانية إتلاف معناه أنه يوجد قصور في القدرات التكنولوجية لدى مؤسسات العدالة، مما ينبغي وجود العمل على التطور المستمر لنظم العدالة بالإضافة لتطور قدرات القائمين على مهامها و أعمالها.[4]

1:محمد الأمين البشري، مرجع سابق، ص 26،27

2: عمر محمد أبو بكر يونس، مرجع سابق، ص 981،982

3: عائشة بن قارة، مرجع سابق، ص 63.

4: هلال أمينة، مرجع سابق، ص 13.

الفرع الرابع: الدليل الرقمي متنوع ومتطور.

إن مصطلح الدليل الجنائي الرقمي يشمل جميع البيانات الرقمي ة التي يمكن تداولها رقميا بمختلف أشكالها و أنواعها [1] سواء كانت هذه الأدلة متعلقة بالحاسب الآلي أو غيرها منه الأجهزة، أو شبكة الأنترنت، أو شبكات الاتصال السلكية و اللاسلكية، و منه فالآثار الرقمية [2] المستخلصة من الحاسب الآلي أو شبكة الأنترنت، تكون ثرية جدا و متنوعة بما تحتويه من معلومات عن وقائع قد تشكل جريمة ما، و ترتقي إلى أن تصبح دليل براءة أو إدانة، و من بين هذه المعلومات صفحات المواقع الإلكترونية المختلفة، البريد الإلكتروني، النصوص و الصور و الفيديوهات الرقمية، الملفات المخزنة في الكومبيوتر الشخصي و المعلومات المتعلقة بمستخدم شبكة الأنترنت و غيرها.[3]

بالإضافة إلى أن الدليل الإلكتروني له خاصية رصد المعلومات عن الجاني وتحليلها في ذات الوقت، ومن خلال إمكانية تسجيله لتحركات الفرد، وتسجيل عاداته وسلوكياته وبعض الأمور الشخصية، ولذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.[4]

فيما يخص التنوع المتعلق بالدليل الإلكتروني، نجد أنه يظهر بطريقة علنية في هيئات مختلفة الأشكال، كان تكون بيانات غير مقروءة، كما هو الأمر في حالة المراقبة عبر الشبكات والملفات أو الخوادم، وقد يكون الدليل الإلكتروني مفهوما للأشخاص كما كان وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة، أو معدة بنظام التسجيل السمعي

1:eoghan Casey, file system forensic analysis, Pearson education (INC), unites states America,2005,p06.

2: يقصد بالآثار الرقمية التي يتركها مستخدم أجهزة الحاسب الآلي أو شبكة الأنترنت والتي تشكل دليلا جنائيا ببراءته أو إدانته وعليه فمصطلح الآثار الرقمية مصطلح اعم وأشمل من مصطلح الدليل الجنائي الرقمي.

3: ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 22.

4:عائشة بن قارة مصطفى، مرجع سابق، ص 64.

المرئي، أو أن تكون مخزنة في نظام البريد الإلكتروني، وهذه الخاصية تستوجب مواكبة التطور في عالم التكنولوجيات.[1]

المطلبالثالث:مراحل وأنواع الدليل الرقمي في إثبات الجنائي.

إن الدليل الرقمي هو جوهر الإثبات في الجريمة المعلوماتي، وبالتالي فإن الدليل الرقمي له عدة أنواع وهذا راجع إلى أنه ذو أهمية بالغة في مجال الإثبات الجنائي في الجرائم المعلوماتية، لهذا تمر الأدلة الجنائية الرقمية في سيرها للإثبات الجنائي في الجرائم المعلوماتية، لهذا تمر الأدلة الجنائية الأخرى بعدة مراحل، وكل مرحلة من هذه المراحل تتميز عن غيرها، وسوف نتطرق إلى مراحل الدليل الرقمي في إثبات الجنائي (الفرع الأول)، وأنواع وأمثلة الدليل الرقمي (الفرع الثاني).

الفرع الأول: مراحل الدليل الرقمي في إثبات الجنائي.

أولا: مرحلة التحرير.

يتم في هذه المرحلة التحرير و الاحتفاظ بالأدلة الموجودة عن طريق إرسالها إلى المختبر الجنائي بطرقة لا تمكنها من التلف أو الكسر أو الإفساد، كما يتم أيضا التقاط الصور الفوتوغرافية أو بواسطة الفيديو لجميع آثار الجريمة كالحواسب و ملحقاتها و البصمات و كل الأشياء التي تفيد في إظهار التحقيق، و التي تم العثور عليها في مسرح الجريمة المعلوماتية، و أثناء هذه المرحلة يكون المحقق أو الخبير في وضع لا يعرف أي نوع من البيانات يمكن من خلالها الحصول على الدليل الجنائي الرقمي، و عليه الحفاظ على النظام الرقمي و كامل القيم الرقمية ليتم تحديد الضرورية منها الاستخلاص الدليل لاحقا، و كذلك يستلزم نسخ جميع البيانات المخزنة داخل الحاسب الآلي موضوع الجريمة إلى

1:فتحي أنور عزت، مرجع سابق، ص 651،652.

حاسب خاص بالمختبر الجنائي الرقمي للاعتماد عليه، بالإضافة إلى نسخ البيانات المخزنة داخل جهاز الحاسب الآلي المشكوك فيه.[1]

ثانيا: مرحلة التحليل.

يتم في هذه المرحلة القيام بالفحص و التحليل لجميع الآثار المرتبطة و المستمدة من مسرح الجريمة، و يشمل ذلك القيم الرقمية لتحديد نوع الدليل، حيث يتم الفحص في محتويات الوثائق، الملفات والمسارات واستعادة المحتويات التي تم حذفها، و يجب أن يتم الفحص بالصيغة العلمية عن طريق استخدام البرامج و التطبيقات الخاصة بتحليل نظام الملفات و المسارات، بالإضافة على ذلك يمكن من خلال تحضير قائمة البيانات المحذوفة و عرض البيانات المخزنة في شكل (format) للاستفادة منها و الأمر المهم جدا في هذه المرحلة وجوب قيام فحص و التحليل على نسخ مطابقة الأصل لعدم تغيير خصائص الملفات، حيث يتم الحفاظ بالنسخة الأصلية مضبوطة من أجل التحقيق و التدقيق على أن البيانات الموجودة مطابقة للأصل و لم يطرأ عليها أي تغيير أو حذف.

ويهدف من وراء قيام عملية الفحص والتحليل إلى استنباط ثلاثة من الأدلة:

- دليل الإدانة ((iculpatory évidence : و يعد الدليل المؤكد و المستند إلى وجود فكرة معينة على ارتكاب و إسناد الجريمة موضوع التحقيق.
- دليل البراءة ((exculpatory évidence:ويعتبر الدليل الذي يخالف فكرة ارتكاب الجريمة موضوع التحقيق.

1:ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 124.

✍ دليل محايد ((évidencetampering: هو الدليل الغير مرتبط بالإدانةولا بالبراءة، بل يستعان به في إثبات انه لم يطرأ أي تعديل أو تغيير في النظام الرقمي للحاسب الآلي لاستبعاد استخدام محتوياته أو الاستعانة به كدليل.[1]

ثالثا: مرحلة التقدم والعرض.

هي المرحلة التي يتم من خلالها تقديم وعرض النتائج التي تم التوصل غليها عن طريق التحقيقات والفحصوالتحليل الفني على جهة المحكمة المختصة، ويطبق على عملية هذه المرحلة النظام الجنائي المطبق في تلك الدولة.

وسيتلزم الأمر موثوقية الأدلة الجنائية الرقمية لضمان مصداقيتها، حيث أنه يسمكن توثيق الأدلة الجنائية الرقمية بالعديد من الوسائل المختلفة منها التصوير بالفيديو والقيام بنسخ الملفات المخزنة في الأقراص أو في الحاسب الآلي، كما يستوجب أيضا تدوين التاريخ والوقتوتوقيع الشخص الذي قام بإجراء الحفظ عند حفظ الأدلة الرقمية، بالإضافة على اسم ونوع نظام التشغيل والمعلومات المسجلة في الملف المحفوظ وقسم البرنامج أو الأوامر التي استعملت في إعداد النسخ.

فالتوثيق يفيد تأكيد مصداقية الدليل و عدم القيام بتعديله أو تغييره، مثل شهادة الأفراد المسؤولين عن جمع الأدلة بمطابقة الأدلة التي قاموا بتحصيلها و الحفاظ عليها مع تلك الأدلة المقدمة و المعروضة لجهة الحكم، كذلك يمكن الاستفادة من التوثيق في حالة إعادة تكوين مسرح الجريمة، باعتبار ا، أجهزة الحاسب الآلي و ملحقاتها تتشابه مما يصعب إعادة تنظيمها في حالة انعدام وجود توثيق فوتوغرافي أو توثيق الفيديو سليم و مفصل بتحديد الإجراء و المكونات بأوضاعها و حالتها الأصلية بدقة، و بالتالي يعتبر التوثيق من ضمن إجراءات حفظ الأدلة على غاية الانتهاء من إجراء

1:ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 125.

التحقيق و المحاكمة لاحتوائه على تحديد دقيق على الجهات التي تحفظ الأدلة، بالإضافة إلى إعداد رسالة التصنيف الحسابي و التي تستعمل لمضاهاة الأدلة الجنائية الرقمية الرسمية مع النسخ من اجل التأكد من صحتها وأنها لم تتعرض للتحريف أو التعديل، فهي تعتبر مجموعة من الأحرف و الأرقام المركبة و المنظمة بصيغة حسابية خاصة تمثل كل نوع من البيانات الرقمية، فهي حالة إدخال ملف الدليل الرقمي على رسالة التصنيف تكون قراءة الملف مطابقة لقراءة النسخة فنتيجة المضاهاة تكون قراءة مختلفة و مغايرة للنسخة الأصلية.[1]

رابعا: مرحلة القبول.

إن أمر قبول الأدلة الجنائية الرقمية المستخرجة من الوسائل الإلكترونية في المحاكم يعتمد على المبادئ القانونية التي تنظم عملية الإثبات أمام تلك المحاكم و بعبارة أخرى أن سلطة القاضي الجنائي في تقدير أدلة الإثبات تختلف من دولة إلى أخرى حسب ما تخضع له قواعد الإثبات في كل دولة، حيث يتضح وجود نظامين للأدلة الإثباتية، نظام الإثبات المحدد أو المقيد و أطلق عليه أيضا نظام الأدلة القانونية أين تكون الأدلة فيه محصورة و مقيدة من طرف المشرع، أما النظام الثاني هو نظام الأدلة الإقناعية و المسمى أيضا بحرية الإقناع.

إذن فإن مرحلة قبول الأدلة الجنائية الرقمية في الإثبات موقوف إلى مدى توافر هذا الدليل في النصوص القانونية بالنسبة لنظام الأدلة الإقناعية[2]

1: سيد محمد بشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية، رسالة ماجستير في العلوم الشرطية تخصص التحقيق والبحث الجنائي، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض،2002، ص 87،88.
2: ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 127،128.

الفرع الثاني: أنواع وأمثلة الدليل الرقمي.

أولا: أنواع الدليل الرقمي.

1)– الأدلة الجنائية الرقمية التي أعدت لتكون وسيلة إثبات.

ينقسم هذا النوع من الأدلة الجنائية على قسمين، القسم الأول يتمثل في المعلومات والبيانات المنشئة تلقائيا من طرف الحاسب الآلي، أمَا القسم الثاني فإنها يتمثل في المعلومات والبيانات ذات طبيعة المختلطة.

أ – المعلومات والبيانات المنشئة تلقائيا من طرف الحاسب الآلي.

وتتمثل في جميع المعلومات والبيانات الرقمية التي تم إنشاؤها بواسطة جهاز الحاسب الآلي أو أي جهاز آخر، ولا دخل للمستخدم في إنشاؤها [1]أو السجلات التي تعتبر من مخرجات جهاز الحاسب الآلي مثل فواتير البطاقات البنكية المعدة آليا.[2]

ب –المعلومات والبيانات ذات طبيعة المختلطة.

وهي المعلومات والبيانات الرقمية التي تم حفظ جزء منها بالإدخال، وجزءآخر تم إنشاؤه بواسطة الحاسب الآلي[3]

لذا، فكلا النوعين السابق ذكرهما تكمن أهميتهما من حيث انهما أعدا سلفا بغرض جعلها وسيلة لإثبات بعض الوقائع التي تتضمنها، ولهذا يتم حفظ هذه المعلومات والبيانات الرقمية

1:عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، مرجع سابق، ص14.

2:خالد عياد الحلبي، مرجع سابق، ص234.

3:عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، نفسه، ص14.

للاحتجاج بها لاحقا، وذلك للتقليل من إمكانية فقدانها، كما يكون من السهل الحصول عليها عند الحاجة.[1]

2)-الأدلة الجنائية الرقمية التي تعد لتكون وسيلة إثبات.

هذا النوع من الأدلة الجنائية الرقمية نشا دون إرادة المستخدم، و دون أن يكون راغبا في وجودها[2]، و تتجسد هذه الأدلة في الآثار التي يتركها المستخدم عند استعماله للحاسب الآلي أو شبكة الأنترنت بحيث تشمل الرسائل المرسلة منه أو التي يستقبلها و كافة الأفعال التي قام بها من خلال جهاز الحاسب الآلي أو شبكة الأنترنت.[3]

ثانيا: أمثلة الدليل الرقمي.

يمكن أن نذكر كأمثلة عن الأدلة الرقمية ما يلي:

1)- بروتوكول ((HPC/IP:

يعتبر من أهم وأشهر البروتوكولات المستخدمة في شبكة الأنترنت والاتصالات، كما يعد جزء أساسي من الأنترنت ويتكون ممايلي:

- بروتوكول ((User Protocol/UDP.
- بروتوكول ((transmission contrôle Protocol/TCP.
- بروتوكول ((Internet Protocol/TP.

1:نعيم سعيداني، مرجع سابق، ص 129.

2:خالد عياد الحلبي، مرجع سابق، ص 234.

3:ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 21.

ومن مميزات هذه البروتوكولات، أنها تقوم معا بنقل المعلومات الخاصة بالمستخدم وفقا لنظام هيكلة التبادل المعلومات المعروف باسم ((TCP/IP with OSI.[1]

حيث يقوم بروتوكول ((TPC بتسليم واستقبال المعلومات المطلوب إرسالها أو إعادة إرسالها في حالة الضرورة، وبتنسيق من بروتوكول ((UDPالذي من أجل مواجهة بعض التطبيقات التي تستخدم ((TPC، كما أن التطبيقات كلا من ((UDP/TPC أعدت أيضا لمواجهة المسائل المؤلفةأثناء عملية تبادل المعلومات والتي تتمثل في إخفاء الهاردوير وتأخر المعلومات، واشتباك وازدحام الشبكات والأخطار التي قد تتكرر أو تتالى، وبعد تقسيم المعلومات من حزمة معلوماتية (الباكت) من طرف ((TCP يقوم بروتوكول ((TPبعنونة المعلومات المرفقة مع إضافة معلومات أخرى، فتصبح (الباكت) المحتوى على حزمة ((TCP/IP، وأثناء اتصال الحاسب الآلي بالأنترنت يأخذ عنوان خاص يسمى ((IP Adresses و كل عنوان مكون من جزئين، الجزء الأول يتضمن أرقام الشبكة، و الثاني يتعلق بأرقام مزود الخدمة.[2]

2)– الكوكيز ((Cookies :

و هي مجموعة من الملفات أو السجلات النصية التي يرسلها الخادم ((Server عن طريق الاتصال به بواسطة القرص الصلب لحاسب المستخدم، حيث أنها تمكن من تسجيل العنوان ((IP الخاص بالحاسب الآلي، و تحديد موقعه الجغرافي و نظام التشغيل، و التاريخ و فترة الاتصال و الصفحات التي تم اكتشافها، و كلمة المرور مع اسم المستخدم، و بالتالي تعد الكوكيز أداة يتم من خلالها جمع البيانات التعريفية الخاصة بالمستخدم، حيث لا يمكن لهذا الأخير تصفح الأنترنت إلا بها.[3]

1:سيدي محمد لبشير، مرجع سابق، ص 72.

2:ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 99،102.

3:سيدي محمد لبشير، مرجع سابق، ص 73.

المطلب الثالث: مشروعية الدليل الرقمي من حيث الوجود.

بناء على مبدأ مشروعية الدليل الجنائي، يجب على القاضي أن يستمد اقتناعه بالإدانة من أدلة صحيحة ومشروعة[1]، و ذلك من خلال ضرورة اتفاق الإجراءمع القواعد القانونية و الأنظمة الثابتة للمجتمع، و الهدف من ذلك هو تقرير الضمانات الأساسية للفرد و حماية حرياتهم و حقوقهم الشخصية من تعسف سلطة التحقيق في غير الحالات التي رخص القانون فيه بذلك [2]، و منه فقاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا مراعاة إعلانات حقوق الإنسان و المواثيق و الاتفاقيات الدولية و قواعد النظام.[3]

الفرع الأول: المقصود بمشروعية الوجود.

ويقصد بها وجود الدليل الرقمي أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الاستناد إليه في تكوين عقيدته، ولعل المعيار الذي يتمدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي هو قبول الدليل الرقمي يتمثل في طبيعة نظام الإثبات السائد في الدولة، غذ تختلف النظم القانونية في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات.[4]

1:نصر الدين مروك، محاضرات في الإثبات الجنائي (النظرية العامة للإثبات الجنائي)، الجزء الأول، دار الهومة، الجزائر، 2003، ص 519.

2:كمال محمد عواد، الضوابط الشرعية في الثبات والقانونية للأدلة الجنائية (في الفقه الإسلامي والقانون الوصفي)، الطبعة الأولى، دار الفكر الجامعي، مصر،2011، ص 165.

3:أحمد عبد الاله هلالي، حجية المحرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة) في بحوث مؤتمر القانون والكومبيوتر والأنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة،2004، ص 429.

4:سعيداني نعيم، مرجع سابق، ص 208.

الفرع الثاني: موقف المشرع الجزائري من الدليل الرقمي.

لقد عرفت التشريعات الإجرائية الجزائية نظامين رئيسيين للإثبات هما:

✍ نظام الإثبات المقيد وفيه يقوم المشرع بتحديد أدلةالإثبات حصرا أو كذا القوة الإثباتية لكل دليل من الأدلة على قناعة المشرع بها، وهو ما يعرف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، فتحدد للقاضي الأدلة التي يجوز له قبولها واللجوءإليها في الإثبات، ولا سبيل للإسناد على أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات.

✍ نظام الإثبات الحر والذي يقوم على أساس حرية الإثبات فلا يقوم المشرع بتحديد الأدلة بل يكون للقاضي دور إيجابي في البحث عن الأدلة وتقدير قوتها الثبوتية حسب قناعته بها، فلا يلزمه القانون بأدلة للاستنا د إليها في تكوين قناعته فله أن يبني هذه القناعة على أي دليل وإن لم يكن منصوصا عليه، بل إن المشرع في مثل هذا النظام لا يحتفل بالنص على أدلة الإثبات فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، و القاضي هو الذي يختار من بين ما يطرح عليه ما يراه صالحا للوصول إلى الحقيقة، و هو في ذلك يتمتع بمطلق لقبول الدليل أو رفضه وإذا لم يطمئن غليه فلا يتدخل المشرع في تحديد القيمة الإقناعية للدليل و لذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل انحصار دور المشرع.[1]

وعلى هذا الأساس واسترشادا بما سبق ذكره فإن النظم القانونية التي تتبنى نظام الأدلة القانونية لا يمكن في ظلها الاعتراف للدليل الرقمي بأية قيمة إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين قناعته.[2]

1:أحمد عبد الاله، مرجع سابق، ص 29.

2:طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية المنعقدة

أما بالنسبة للنظم القانونية التي تعتمد نظام الإثبات الحر كما هو الحال عليه في القانون الجزائري[1] المادة 212 من قانون الإجراءات الجزائية، والقانون الفرنسي المادة 427 من قانون الإجراءات الجزائية)، فإنه لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود على اعتبار أن المشرع لا يعتمد سياسة النص على قائمة لأدلة الإثباتفالأساس هو حرية الأدلة، لذلك فمسالة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه لتقدير القاضي.

و في هذا الصدد فإن المشرع الجزائري كغيره من التشريعات المنتمية إلى نظام الإثبات الحر لا تجد قد قيد 58 نصا خاصا تحظر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي، و هو أمر منطقي طالما أن المشرع الجزائري يستند إلى مبدا حرية الإثبات، حيث لم يتضمن القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام و الاتصال و مكافحاته أية أوضاع خاصة وترك الأمر للقواعد العامة و منها أن الأصل في الأدلة المشروعية وجودها و من ثم فإن الدليل الرقمي سيكون مشروعا من حيث الوجود اصطحابااللأصل و من جهة أخرى فإنه و طبقا لمبدأ المشروعية الإجرائية فلا يكون الدليل مقبول و لا يكون كذلك إلا إذا كان مشروعا بأن تم البحث عنه و الحصول عليه وفقا لطرق مشروعة.[2]

في 28،29/10/2009، الأكاديمية للدراسات العليا، طرابلس، ص 23.

1: هناك العديد من الأسباب التي تبرز الأخذ بمبدأ حرية الإثبات في نطاق نظرية الإثبات الجزائي، منها أن حرية الإثبات التي يقتنع ويطمئن إليها حتى يتسنى له أداء رسالته في إرساء العدالة بين المتقاضين، بالإضافة إلى أن الإثبات الدعوى الجزائية يرد على وقائع مادية يصعب بل قد يستحيل الحصول على دليل مسبق لها وذلك بعكس الدعوى المدنية التي يود الإثبات على تصرفات قانونية يسهل إعداد دليل مسبق بشأنها.

2: سعيداني نعيم، مرجع سابق، ص 201.

المبحث الثاني: تقدير الدليل الرقمي

بالرجوع إلى نص المادة 212 من قانون الإجراءات الجزائية التي تجسد فيها إرادة المشرع الجزائري تبني النظام الحر، نجدها تكرس قاعدتين تكمل إحداهما الآخر، ومهتمتان لإعمال هذا النظام وتحديد سلطة القاضي الجزائي في قبول أدلةالإثبات، وهاتان: قاعدة الاقتناع الحر للقاضي الجزائي، وقاعدة حرية اختيار وسائل الإثبات الجزائي.

وإذا كان الدليل الإلكتروني ذو صبغة عليمة، هو الأوفروالأنسب في إثبات الجريمة المعلوماتية، فالسؤال المطروح هنا هو ما مدى إمكانية إعمال القاضي الجزائي الجزائري لمبدأ الاقتناع الشخصي حيال هذا الدليل؟ وما مدى حريته في الأخذ أو عدم الأخذ به بوصفه دليلا علميا دقيقا طبقا لأحكام المادة 212 المذكور أعلاه.

المطلبالأول: سلطة القاضي الجنائية بالدليل الرقمي

تقوم سلطة القاضي الجزائري في تقدير الدليل الرقمي أساسا على أحد أهم المبادئ القضائية مبدأ الاقتناع القضائي، هذا المبدأ الذي بموجبه يملك القاضي سلطة تقديرية واسعة في تقديره للدليل الرقمي وتكويناقتناعه.[1]

الفرع الأول: ماهية اقتناع القاضي الجزائي بالدليل الرقمي.

إن الأدلة الرقمية سواء تلك المتواجدة في هيئة ورقة يتم إنتاجها عن طريق الطابعات أو الرسوم، أو كانت في شكل مخرجات رقمية مثل الأشرطةوالأقراص الممغنطة أو الضوئية وأسطوانات الفيديو، أووغيرها من الأشكال غير التقليدية، وإما أن تكون مخرجات مرئية يتم عرضها على شاشة الحاسوب

1: بن فريدة محمد، الدليل الجنائي الرقمي وحجيّته أمام القضاء الجزائي (دراسة مقارنة)، مجلة سداسية متخصصة محكمة، السنة الخامسة، الجلد 09، عدد 01، بجاية، 2011، ص 289،297.

وتخضع جميعها لنظام الأدلة المعنوية الذي تأخذ به اغلب التشريعات المقارنة حديثا والذي يقوم على مبدا الاقتناع الشخصي للقاضي الجزائي.

أولا: تعريف الاقتناع الشخصي للقاضي الجزائي.

هو الإيمان العميق والركون إلى صحة الوقائع التي يقدما الأطراف المقارنة والتي اعتمدها القاضي وتنتج عنها أثارا عميقة في نفسية القاضي الجزائي، تتركه يصدر حكمه عن قناعة وحريةوإحساس كبير بإصابته في حكمه.[1]

ولقد أشار المشرع الجزائري على هذه المسالة 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]

وكما تطرق المشرع الجزائري على مبدأإلى مبدأ الاقتناع القضائي نص المادة 212 من قانتون الإجراءات الجزائية الجزائري على:المادة يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عاد الأحوال الشخصية التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ويطبق المبدأ أمام 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 بها في أحكام محاكمها وسيتم تناول اهم الأنظمة القانونية وأهم

1: سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، بدون طبعة، دار الكتب القانونية، مصر، 2014، ص 280.

2: هلال آمنة، مرجع سابق، ص 28.

3: القانون رقم 155/66 يتضمن الإجراءات الجزائية، مرجع سابق.

الأحكام القضائية التي طبقت المبدأ دون أن ننسى موقف كل من التشريع والقضاء الجزائري، ففيهذا الصدد سيتم دراسة الأساس القانوني لمبدأ الاقتناع، ثم الأساس القضائي لمبدأ الاقتناع القضائي.

أ -الأساس القانوني لمبدأ الاقتناع القضائي.

حرصت الكثير من التشريعات على جعل مبدا الاقتنا ع القضائي عنوانا للإثبات الجزائي حيث يستند إليها القاضي في حكمه، فقد اقر المشرع الجزائري ذلك في قانون الإجراءات الجزائية على مبدأ الاقتناع الشخصي للقاضي الجزائي، وجسّده بنصوص واضحة، وهذا ما ورد في المادة 307 من قانون الإجراءات الجزائية الجزائري: يتلو الرئيس قبل مغادرة قاعة الجنايات التعليمات الآتية التي تعلق فصلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة...".

كما أوردته المادة 01/212 من نفس القانون الذي يتضمن توجيه القسم من الرئيس إلى المحلفين فيما يخص إجراءات انعقاد محكمة الجنايات.[1]

ومن بين التشريعات التي أخذت بهذا المبدأ نجد القانون الفرنسي الذي يقرّ على مبدأ الاقتناع الشخصي للقاضي الجزائي لأول مرة و ذلك ما جسده في المادة 343 من قانون الإجراءات الجزائية.[2]، في شأن التعليمات التي تلقى على محكمة الجنايات ثم ألغى هذا الأخير بموجب القانون الصادر 25 نوفمبر غلا 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 أنه: "على المحلفين أن يحلفوا يمينا بأن يحكموا بالعدل لأدلة الاتهام و وسائل الدفاع على ضمائرهم و اقتناعهم الداخلي مع النزاهة و التي يتمتع بها

1: محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي، ب. ط، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 427.

2:بن فردية محمد، مرجع سابق، ص 308.

الإنسان حر مستقيم، و أيضا كما خول المشرع لرئيس محكمة الجنايات سلطة تفويضية بمقتضاها يمكنه أن يتخذ كافة الإجراءات التي يعتقد أنها مفيدة للكشف عن الحقيق، حيث لا يقدم عليه سوى ضميره و شرفه حسب نص المادة 310 من قانون الإجراءات الجزائية الفرنسي.

كما نصت المادة 01/427 من قانون الإجراءات الجزائية الفرنسي : فيما عدا الحالات التي ينص عليها القانون خلاف ذلك تثبت الجرائم بكل وسائل الإثبات ويقضي القاضي بمقتضى اقتناعه الشخصي.

أما التشريعات العربية أخذت بهذا المبدأ فقد تناول القانون المصري مسالة الاقتناع في المواد 01/291، 300، 01/302 من قانون الإجراءات الجزائية المصري.[1]

وتنصالمادة 01/302 من قانون الإجراءات الجزائية المصري على أنه: يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حرياته.[2]

ونستخلص مما سبق أن أغلب التشريعات المعاصرة تأخذ بمبدأ الاقتناع القضائي مع اختلاف في الصياغة بين التشريعات اللاتينية والتشريعات الأنجلوسكسونية ،ولكن ليست في النص بل هو التعبير في جانبه العملي الذي يقره في حكمه خاضعا بذلك لضميره دون تقييده بأي قيد ما عدا القيود والضوابط التي وصفها القانون.

ب –الأساس القضائي لمبدأ الاقتناع القضائي.

قضت المحكمة العليا الجزائرية في الشق الجزائي بهذا المبدأ و جاء في عدة أحكام و منها مايلي:من المقرر قانونا أنه لا يطالب من القضاة المشكلين لمحكمة الجنايات أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم الشخصي، و لا يرسم لهم بها قواعد يتعين عليهم أن

1:بن قدوم سهيل، مرجع سابق، ص 69،70.
2:بن فردية محمد، مرجع سابق، ص 310.

يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، من ثم البقي على الحكم المطعون فيه بحر القانون غير سديد مما يستوجب رفضه، و لما كان الثابت في قضية الحال أن الحكم الصادر من محكمة الجنايات بالبراءة كان بأغلبية الأصوات و أن الأسئلة قد طرحت بصفة قانونية و أن الأجوبة المعطاة كانت حسب الاقتناع الشخصي للقضاة الذي لا يخضع لرقابة المحكمة العليا و متى كانت كذلك استوجب رفض الطعن.[1]

و جاءت 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 و من ثم فإن القضاة بما يخالف خذا المبدأ يعد خرقا للقانون، و لما كان الثابت في قضية الحال أن القضاة الاستئناف ناقشوا أدلة الإثبات و أوجه دفاع المتهم و اقتنعوا بعدم صحة دفاعه فيما يخص النكران للتهمة المنسوبة غليه علما أن الجريمة لم تكن من الجرائم التي ينص فيها القانون على إثباتها بنص خاص يكونوا قد طبقوا القانون تطبيقا سليما، و متى كان الأمر كذلك استوجب رفض الطعن".[2]

وكما جاء في قرار آخر أنه : "يمكن للقاضي تأسيس اقتناعه على أية حجة حصلت مناقشتها حضوريا أمامه".[3]

كذا:"لا يمكن للقضاة الموضوع أن يؤسسوا قرارهم إلاّ على الأدلة المقدمة لهم أثناء المرافعات والتي تم مناقشتها حضوريا".[4]

1:المحكمة العليا الجزائرية، قرار صادر بتاريخ 1987/06/30 الملف رقم 50977، المجلة القضائية، العدد الثالث، 1991، ص 199.

2:المحكمة العليا الجزائرية، قرار صادر بتاريخ 1991/01/29 الملف رقم 70690، المجلة القضائية، العدد الثالث، 1991، ص 199.

3:ر.غ.ج، 09 جويلية 1990 مجموعة قرارات غ.ج ، ص 153، المجلة القضائية، العدد الثالث، 1993، ص 282.

4:ر.غ.ج.م، 1989/03/28 الملف رقم 647،56، المجلة القضائية، العدد الثالث، 1993، ص 291.

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 اقتناعهوذلك ما جاءت به المادة 427 من قانون الإجراءات الجزائية الفرنسي.[1]

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 بديل معين.[2]

وسنستخلصمما 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 اقتناعه الشخصي.

ثانيا: ممارسة القاضي الجزائي لمبدأ الاقتناع الشخصي بالدليل الرقمي.

إن ممارسة القاضي الجنائي لمبدأ الاقتناع الشخصي فيما يخص الدليل الرقمي تتجسد هذه مظاهر 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 لا سيما تشريعات الدول اللاتينية لم يتناول مسالة الدليل الرقمي كمسألة مستقلة في الإثبات، وإنّما يخضعها للمبادئ العامة في الإثبات، فمثلها مثل أي دليل آخر فالأدلة الرقمية ليست استثناء من الأدلة الأخرى فهي تخضع للقواعد العامة و على ما استقرت عليه الأحكام القضائية، و عليه سيتم تناول هذه الجزئية كالاتي:

1:بن فريدة محمد، مرجع سابق، ص 313.

2:بن فريدة محمد، مرجع نفسه، ص 313.

1. مظاهر ممارسة القاضي الجنائي لمبدأ الاقتناع بالنسبة للدليل الرقمي.

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

أ – سلطة القاضي الجنائي في تقدير الأدلة الرقمية بذاتها.

يظهر من أحكام محاكم النقض أن القاضي الجنائي أن يستعد الدليل و يطرحه إن لم يطمئن إليه، و أن يأخذ به كاملا أو يأخذ بالجزء الذي يطمئن إليه و يقتنع بصحته [2]، و هو الأمر الذي ينطبق على الأدلة الرقمية سواء كانت في بيئتها الرقمية إما على شكل مخرجات طباعة أو اتخذت شكل صور أو مقاطع الفيديو.

ب –حرية القاضي الجنائي في استبعاد الأدلة.

للقاضي الجنائي أن يستبعد في مجال تقديره ما لم يطمئن غليه عند ممارسة سلطته في الدعوى موضوعيا[3]، و يعود عدم الاطمئنان القاضي لقيمة الدليل الذي يطرحه تكمن في ضعف الدليل المستبعد في الأدلة على الحقيقة التي يسعى الحكم في جعلها عنوانا له بذلك القضاء، أو لأن هنالك

1: محكمة التمييز الكويتية 1976/06/30، المجلة القضائية العربية، الأمانة العربية لمجلس وزراء العدل العرب، العدد الأول، السنة الأولى، نيسان 1984، ص 326،327.

2: شيماء عبد الغاني، الحماية الجنائية للتعاملات الإلكترونية، بدون طبعة، دار الجامعة الجديدة، الإسكندرية،2007، ص 85.

3: جباري عبد المجيد، دراسة قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دون طبعة، دار هومة، الجزائر، 2012، ص 122.

أدلة أخرى تدحض الدليل المستبعد، أو لأن هناك أدلة اقوى منه في الإثبات و كفاية في تكوين قناعة المحكمة، كما قضت به محكمة تمييز دبي[1]

2. حرية القاضي الجنائي بالأخذ بالدليل.

هذه الحرية لها صور عديدة فالقاضي يستطيعالأخذبمبدأ الاقتناع القضائي ما يتعلق بالدليل فالقاضي يأخذ به كاملا أو يأخذ بجزء منه دون الجزء الآخر، وأنيأخذ به لمتهم دون شريكه، وأن يأخذ بالدليل في حالة تعدد التهم دون التهم الأخرىوهكذا كما قضت عليه محكمة دبي في قرارها.[2]

3. سلطة القاضي الجنائي في تقدير الأدلة الرقمية من حيث مصدرها.

إن سيادة مبدا 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 يعتمد بما جمعه الاستدلالات التي يحررها ضباط الشرطة المختصون، و له أيضا سلطة عدم الاعتداد بها [4] ، كما له أن يرفض تقرير خبرة أجريت في مرحلة التحقيقات بتعيين من قاضي التحقيق ، إذا فالقاضي يقدر الدليل بحسب

1:محكمة تمييز دبي، ✍ وزن أقوال الشهود وتقديرها من حق محكمة الموضوع المنزلة التي تراها وتقدره التقدير الذي يطمئن إليه وللمحكمة أن تعود على ما قاله شهود الإثبات وتعرض عما قاله شهود النفي، فقضاؤها بالإدانة استنادا على أدلة الثبوت يقيد دلالة أنها طرحت شهادتهم ولم ترى الأخذ بها✍.

2:محمد علي العريان، الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2011، ص 45.

3:محكمة التمييز دبي: :✍أنه من المقرر قانونا أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك و من ثم فإن القضاة بما يخالف خذا المبدأ يعد خرقا للقانون، و لما كان الثابت في قضية الحال أن القضاة الاستئناف ناقشوا أدلة الإثبات و أوجه دفاع المتهم و اقتنعوا بعدم صحة دفاعه فيما يخص النكران للتهمة المنسوبة غليه علما أن الجريمة لم تكن من الجرائم التي ينص فيها القانون على إثباتها بنص خاص يكونوا قد طبقوا القانون تطبيقا سليما، و متى كان الأمر كذلك استوجب رفض الطعن✍.

4:شيماء عبد الغني، مرجع سابق، ص 94،95.

اقتناعه لا حسب الدليل ذاته، على أنه وجب عليه تنسيب الحكم إثر رفضه لهذا النوع من المحاضر كي لا يتعسف القاضي في استعمال حقه[1]

الفرع الثالث: الضوابط التي تحكم الاقتناع الشخصي بالدليل الرقمي.

إنّ الأصل العام أن القاضي الجنائي حر في تقديره للأدلة المطروحة عليه في الدعوى عملا بمبدأ الاقتناع الشخصي، فهو غير ملزم بإصدارحكم الإدانة أو البراءة لتوافر دليل معين طالما انه لم يقتنع به، و هذا الأمر وضعت له ضوابط حيث لا تعطي لهذا القضاء الجنائي مطلق الحرية التي يتمتع بها لغاية يراها المشرع ضرورة.[2]

وعلى ذلك فإن دراستنا للضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني الذي يتأسس عليه هذا الاقتناع القضائي.

أولا: الضوابط المتعلقة بمصدر الاقتناع

إنّ اقتناع القاضي الجنائي بالأدلة الإلكترونية يحكمه ضابطان، يتمثل الأول في أن يكون هذا الدليل الإلكتروني مقبولا، وأمّاالثاني يجب أن يكون الدليل الإلكتروني قد طرح في الجلسة للمناقشة.

1. ضابط أن يكون الدليل الإلكتروني مقبولا.

على القاضي الجنائي أن يستمد اقتناعه من أدلة مقبولة ومشروعة، فلا يجوز الاستناد على دليل استمد من إجراء باطل وإلاّ بطل معه الحكم فهذا الضابط مكمل لقيد مشروعية الدليل الإلكتروني.[3]

1:محمد علي العريان، المرجع أعلاه، ص 52.

2:بلهولي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة لنيل شهادة ماجستير، جامعة الحاج لخضر، كلية الحقوق و العلوم السياسية، قسم الحقوق، باتنة، 2011، ص 91.

3:أشرف عبد القادر قنديل، مرجع سابق، ص، 235 ،236.

و كما سبق و ذكرنا فإن القاضي الجنائي حر في تقدير الدليل الإلكتروني المقبول في الدعوى الذي تم الحصول عليه بطريقة مشروعة، و بالتالي فان مسالة قبول هذا الدليل أي الدليل الإلكتروني لابد أن تحضيبالأهمية، لاعتبارها ركيزة في مبدأ حرية القاضي الجنائي في تقدير الدليل الإلكتروني، لأن محل هذه الحرية هو الأدلة المقبولة، فالتطبيق الحسن للقانون يفوض على القاضي أن يكون اقتناعه من دليل الإلكتروني مقبول، و يستبعد في المقابل سائر الأدلة الإلكترونية غير مقبولة، لأنها لا يمكن أن تدخل عنصرا من عناصر تقديره.[1]

فمشروعية الدليلالإلكتروني تعد ضمانا كبيرا للحرية الفردية، وللعدالة أيضا،كما أنها تحمل القائمين على تجميع أدلة الإدانة على القيام بعملهم بكل نزاهة، فليست الإدانة عي الغاية، فالغاية هي تحقيق العدالة والكشف عن الحقيقة، ولا يهدم قرينة البراءة التي تتحقق عن طريق الاقتناع اليقيني المبني على أدلة صحيحة ومشروعة.

ولذلك فلا بد أن يستمد القاضي الجنائي اقتناعه الذاتي في مجال الإثبات للجرائم الإلكترونية، من دليل الإلكتروني مشروع ومقبول، فلا يجوز الاعتماد على دليل استمد من إجراء باطل، وإلا بطل معه الحكم، لأنّ ما بنيّ على باطل فهو باطل.[2]

2. ضابط ضرورة طرح الدليل الإلكتروني في الجلسة للمناقشة

بصفة عامة يجب على القاضي أن يستمد اقتناعه من أدلة طرحت بالجلسة، وخضعت للمناقشة من طرف الخصوم.[3]

1:عائشة بن قارة مصطفى، المرجع السابق، ص 268.

2:عائشة بن قارة مصطفى، المرجع نفسه، ص 269.

3:أشرف عبد القادر قنديل، المرجع السابق، ص 236.

فمن الأسس التي تقوم عليها الأدلة أن القاضي لا يمكن أن يباشر سلطته في تقدير هذه الأدلة ما لم تطرح هذه الأدلة في الجلسة وبحضور الخصوم وتتم مناقشتها، وغاية ذلك حتى يتاح لكل طرف من الدعوى أن يواجه خصمه بما لديه من أدلة إزاءه، ويبين موقفه منها.

ومن مقتضيات هذا الضابط أن تعرض أدلة الدعوى جميعا في جلسة المحاكمة وتطرحلمناقشات،فالشاهد يدلي بشهادته والمتهم يذكر اعترافه ويقرأ تقرير الخبير.[1]

فهذه القاعدة تعني أن القاضي لا يؤسس اقتناعه إلا على عناصر الإثبات التي طرحت في جلسات المحكمة، وخضعت لحرية مناقشة أطراف الدعوى إعمالا بمبادئ المحاكمةالجزائية المتمثلة في الشفوية بحسب المواد 300، 304، 353 من قانون الإجراءات الجزائية الجزائري و مبدا العلنية بحسب المواد 285،344،355،399من قانون الإجراءات الجزائية الجزائري، و كذا مبدأ المواجهة بحسب المادة 2/212 من نفس القانون و هذه المناقشة تستجيب لضرورة احترام حقوق الدفاع بإعفاء فرصة للمتهم لأجل الاستفسار حول كل وسيلة من وسائل الإثبات المقدمة أمام القاضي الجنائي هذا من جهة، و من جهة ثانية فإن المناقشة الحضورية هي مطلب منطقي، لأنها تنطوي على فحص شامل وجماعي لكل وسيلة إثبات.

وإن كان القاضي يحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، إلاّ أنه مقيد بأن تكون الأدلة التي كونت عقيدته معروضة للبحث في الجلسة، حتى يتمكن أطراف الدعوى من الاطلاع عليها ز إبداء رأيهم فيها، فعلى القاضي أن يطرح للمناقشة كل دليل قدم فيها حتى

1: فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، الأردن،2010، ص 250، 254.

يكون للخصوم على بينة مما تقدم ضدهم من أدلة، ومن ثم يبطل الحكم، إذا كان مبناه دليلا لم يطرح للمناقشة، أو لم تتح للخصوم فرصة إبداء الرأي فيه، ومن باب أولي إذا لم يعملوا به أصلا.[1]

فمن القواعد الأساسية في الإجراءات الجزائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبر عنه بوضعية الدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشة، وكِلا الأمرين يجب توافرهما.

وعِلّة هذه القاعدة هي مبدأ الشفوية في المحاكمة الجنائية، وهومبدأ أساسيفي الإجراءات الجزائية، و تقتضيه أولى بديهيات العدالة، حيث يجعل القاضي غير مكتفي، على ما دو ن في محاضر التحقيق وإنما يستوجب علبه أنت يسمع الشهود و اعتراف المتهم بنفسه و ما يدلي به الخبراء و يطرح جميع الأدلة الأخرى للمناقشة الشفوية، فلا يكون هناك وسيط بين الدليل و القاضي، و غاية ذلك حتى لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة ضده و بين موقفه منها، مما يفيد القاضي في تكوين قناعته من حصيلة هذه المناقشات التي تجري أمامه في الجلسة.

ولا يختلف الأمر بالنسبة للدليل الإلكتروني، سواء كان على شكل بيانات معروضة على شاشة الكومبيوتر أو مدرجة في حاملات البيانات أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مستخرجة في شكل مطبوعات، كل هذا عليه أن يكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة.[2]

وضابط وضعية الدليل الإلكتروني يقوم على عنصرين أساسيين، حيث يتمثل العنصر الأول في إتاحة الفرصة للخصوم للاطلاع على الدليل الإلكترونيوالرد عليه، أما العنصر الثاني فهو يتمثل في أن يكون الدليل الإلكتروني أصل في أوراق الدعوى.

1:عائشة بن قارة مصطفى، المرجع السابق، ص 269،271.

2:بلهلولي مراد، المرجع السابق، ص 113،114.

بالنسبة للعنصر الأول ففحواه أنه يجب على القاضي مبدئيا أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم، حتى يكونوا على بينة مما يقدم ضدهم من أدلة ليتمكنوا من مواجهة هذه الأدلة والرد عليها، وهذااحتراما لحقوق الدفاع، الذي يعد أحد المظاهر الأساسية لدولة القانون و النظم الديمقراطية[1] و يتيح مبدأ المواجهة تجسيد هذا الأخير، حيث يقتضي مبدأ الدفاع حضور كل خصم في الدعوى وأن يطلع خصمه على ما لديه من أدلة، و أن يواجه بها، و أن يناقش كل منهما أدلة الطرف الآخر، و مبدأ المواجهة يجب أن تتوافر فيه نوعين من ضمانات.

حيث أن الضمانة الأولى تكون سابقة على عملية المواجهة ذاتها بين الأطراف في الجلسة، وهو يتضمن ضرورة إحاطة المتهم علما بالتهمة المنسوبة إليه، وأن يمنح له بالاستعانة عند الاقتضاء بالمترجم.

أما النوع الثاني من الضمانات فيتم أثناء عملية المواجهة ذاتها، وهي الأكثر تأثيرا في الدعوى العمومية، إذ يلزم أن يسمح لكل طرف بتقديم ما لديه من مستندات، وسؤال الشهود والخبراءوأن يطلب اتخاذ أي إجراء يقدر فائدته، وإثارة أي دفوع، أو إيداع أي مذكرات، ثم حق كل طرق في مناقشة تقرير الخبير ودحض ما ورد به.

و لهذا فإنه لا يجوز للقاضي الجنائي بعد مناقشة هادئة، و مجادلة حرة متكافئة من كل صاحب حق مشروع في الدعوى.[2]

أما بالنسبة للعنصر الثاني من ضابط وضعية الدليل الإلكتروني، يتمثل في أن يكون للدليل الإلكترونيأصل أوراق الدعوى حتى يكون اقتناع القاضي الجنائي مبنيا على أساس.

ومن أجل ذلك أوجب المشرع تحرير محضر الجلسة للإثبات وقائع الدعوى الجزائية وأدلتها لكي يتمكن قاضي الموضوع، أو أي شخص من الخصوم من الرجوع إلى هذا المحضر إذا ما رغبوا في

1:عائشة بن قارة مصطفى، المرجع السابق، ص 269،271.

2:أشرف عبد القادر، المرجع السابق، ص 237.

استيضاح أي الوقائع الثابتة بهدف منع التحكممن طرف القضاة الجنائيين وتحقيقا للعدالة، بالإضافة إلى ذلك فغن الغرض أيضا هو تمكين المحكمة المطعون أمامها من مراجعة الحكم المطعون فيه وتقديره من حيث الخطأ والصواب.[1]

وضابط وضعية الدليل الإلكتروني تترتب عليه نتائج من أهمها عدم جواز أن يقضي القاضي الجنائيبناءا على علمه الشخصين أي عدم جواز استناده على معلوماته الشخصية التي يكون قد حصل عليها من خارج نطاق الدعوى المطروحة عليه، والتي من الممكن أن تؤثر في تكوين قناعته عند تقديره لأدلتها.[2]

وهذا يعني أن المعلومات الشخصية التي يحوزها القاضي والتي يمتنع عليه القضاء استنادا إليها هي معلومات تتصل بصورة أو بأخرى بالدعوى التي ينظر فيها، ومن الممكن أن تؤثر على تقديره لأدلتها، ذلك لأنها لم تحصل بالطريق الذي رسمه القانون وهو أن يكون لها أصلا في الأوراق.

ويرى البعض أن أساس هذه القاعدة، أنه يترتب على حق الخصوم في مناقشة الأدلة التي تقوم في الدعوى أنه يجوز للقاضي أن يقضي بعلمه، وهذا لأن علة القاضي هما دليلا في الدعوى، ولما كان للخصوم حق مناقشة هذا الدليل يقتضي أن ينزل القاضي منزلة الخصوم فيكون خصما وحكماوهذا لا يجوز.

و يرجع البعض الآخر أساس هذه القاعدة إلى ضرورة احترام حقوق الدفاع، إذ أن المعلومات الشخصية التي يستند عليها القاضي تعد في الحقيقة مفاجأة للخصوم إن لم تناقش بمعرفتهم و لم يتم إثباتها في إطار إجراءات الخصومة، و يذهب رأي ثالث إلى منع القاضي من الحكم علمه الشخصي لا يرجع إلى مبدا حق الخصم في مناقشة الأدلة التي تقدم في الدعوى، و إنما يرجعإلى أن ما شاهده

1:أشرف عبد القادر، مرجع نفسه، ص 238.

2:فاضل زيدان محمد، المرجع السابق، ص 258.

القاضي أو علمه أو سمعه مما يتصل بوقائع الدعوى سوف يؤثر حتما في تقدير القاضي للأدلة، بل أنه قد يشمل هذا التقدير، و هو في هذه الحالة لا يصلح أن يكون قاضيا و إلا اعتبر قاضيا و شاهدا في آن واحد، و لهذا ينص القانون على أن القاضي الذي سبق أن يشهد في آن واحد، و لهذا ينص القانون على أن القاضي الذي سبق أن شهد في قضية ما لا يصلح أن يكون قاضيا لها.[1]

ولهذا فانه ضمانا لنزاهته وحياده، فإذا ما توفرت لديه معلومات شخصية حول الدعوى المطروحة أمامه، فعليه في هذه الحالة أن يتنحى عن الفصل فيها ويتقدم للمحكمة كشاهد عادي تاركا الفرصة للخصوم لمناقشة المعلومات التي حصل عليها.

و لكن يجوز له أن يستند إلى المعلومات العامة التي يفترض بالكل أن يعلم بها، و التي يكسبها القاضي من خبرته أو ثقافته العامة مما لا تلتزم المحكمة قانونيا ببيان الدليل عليه، فهي لا تعد من قبيل المعلومات الشخصية المحظورة على القاضي أن يبني حكمه عليها، إلا أن ما ينبغي الإشارة إليه أن هذه القاعدة يجب إلاّ تتعارض مع الدور الإيجابي للقاضي في البحث عن الحقيقة أو حريته في الاستعانة بكافة وسائل الإثبات، طالما أنه يطرح الأدلة المتحصل عليها للمناقشة بين أطراف الدعوى، فالحظر يقع على المعلومات التي يستقيها القاضي بصفته الشخصية و ليس بصفته القضائية.

وهذه القاعدة يرد عليها استثناء أنه يجوز للقاضي أن يحكم بما رآه أو سمعه بنفسه في حالة ارتكاب جنحة أو مخالفة في الجلسة، أي جرائم الجلسات وهو مانصت عليه المادة 569 من قانون الإجراءات الجزائية الجزائري.[2]

ومنه لا يجوز للقاضي أن يبني اقتناعه على هذه المعلومات الشخصية لأنها لم تكن موضع مناقشة شفاهية بحضور أطراف الدعوى، بل ستكون لهم مفاجأة إن لم تناقش بمعرفتهم و لم يتم

1:فاضل زيدان محمد، المرجع السابق ، ص 259.
2:بلهلولي مراد، المرجع السابق، ص 116، 117.

إثباتها في اطار إجراءات الخصومة مما يؤدي إلى عدم احترام حقوق الدفاع هذا من جهة، و من جهة ثانية يكون القاضي قد جمع في شخصه صفتين متعارضتين، صفة الشاهد و صفة القاضي و هذا ما لا يجيزه القانون و يرتب عليه بطلان الحكم، و يرجع السبب في ذلك أن من مستلزمات تقدير القاضي الجنائي لأدلة بصفة عامة و الدليل الإلكتروني على الخصوص، خلو ذهنه موقف الخصوم منه حينما يستطيع القاضي من خلال هذه المناقشة الوصول إلى التقدير السليم، و في هذا الشأن المتعلق بهذه القاعدة يقول الفقيه الإنجليزي " sydneyfipson " : ليس للقاضي و لا للمحلف أن يتصرفا على أساس من علمهما الخاص بالقضية لكن إن كان لديهما وقائع مادية يريدان الإدلاء بها فيجب أن يحلفا كشهود فإذا حلفا على هذا النحو فليس للقاضي بخلاف المحلف، أن يحكم على أساس من شهادته[1]

كما تجدر الإشارة في هذا المقام أنه ليس للقاضي أن يبني اقتناعه عل رأي غيره، إلا إذا كان هذا الغيرمن الخبراء وقد ارتاح ضميره إلى التقرير المحرر منهفأراد الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون أصدر حكمه بناءا عليه يكون متولدا من عقيدته هو وليس من تقرير الخبير.[2]

فمن غير الجائز أن يحول القاضي الجنائي على رأي الغير، بل يجب أن يستمد هذا الاقتناع من مصادر يستقيها بنفسه من التحقيق في الدعوى، وتطبيقا لهذه القاعدة لا يجوز له أن يحيل الحكم في شأن واقعة الدعوى ومستنداتها إلى دعوى أخرى لم تكن ضمن الدعوى التي ينظر فيها ولاالمطروحة بالجلسة.

1:عائشة بن قارة مصطفى، المرجع السابق، ص 274، 275.

2:عائشة بن قارة مصطفى، المرجع السابق، ص 275.

كما يجب عليه أن يخضع لأي تأثير خارجي كتأثير رجال الصحافة مثلا أو الفقهاء ورجال الدين، لأن الإثبات في المواد الجزائية يقوم على اقتناع القاضي بنفسه بناءا على ما يجري في الدعوى من تحقيق.[1]

فالقاضي لا يجوز له أن يعتد برأي غيره مهما كانت صفته إلا إذا كان خبيرا ذو كفاءة عالية فغالبية القضاة الجنائيين تنقصهم الثقافة الفنية والتقنية فيما يتعلق بهذا الدليل المستحدث فالدليل الإلكتروني من الأدلة الصعبة على القاضي الجنائي، في بناء اقتناعه لأن في مجال المعلوماتيةولهذا جاز القاضي الجنائي أن يبني اقتناعه بناءا على ما يقدمه الخبير.

ثانيا: الضوابط التي تتعلق بالاقتناع الذاتي.

إنّ مبدأ الاقتناع القضائي الذي تبناه المشرع الجزائري، يتيح للقاضي الجنائي حرية كبيرة في تقدير عناصرالإثبات بما في ذلك الدليل الإلكتروني، بل لله أهم نتيجة تترتب على هذا المبدأ الهام، لذلك فإن تقدير كفاية أو عدم الكفاية الدليل الإلكتروني في إثبات الجريمة الإلكترونية ونسبتها إلى فاعلها أمر تختص به محكمة الموضوع المعروض عليها هذا الدليلولا تخضع في ذلك لرقابة المحكمة العليا.

غير أنه لا يعني أن وقائع الدعوى لا تخضع لرقابة المحكمة العليا، وإنما هي تراقب المنطق القضائي لمحكمة الموضوع التي تنظر في وقائع القضية المتعلقة بهذا الدليل، ولذلك عن طريق رقابتها لصحة تسبيب الحكم، لذلك قالت المحكمة العليا أنه يلزم لصحة سلامة اقتناع قاضي الموضوع بالدليل الإلكتروني، أن يكون مبنيا على الجزم واليقين، دون الظن والترجيحوالاحتمال، وأن يكون متلائما المحكمة العليا مقتضيات العقل والمنطق.[2]

1:بلهلولي مراد، المرجع السابق ، ص 117.

2:عائشة بن قارة مصطفى، المرجع السابق، ص 275.

ولهذا ستكون دراستنا أولا حول بلوغ الاقتناع القضائي درجة اليقين، ثم التطرق إلى كون هذا اليقين متلائما مقتضيات العقل والمنطق.

ضابط بناء الاقتناع القضائي على اليقين.

تهدف الخصومة الجنائية إلى معرفة الحقيقة المطلقة مما يقتضي أن يصدر حكم القاضي عن اقتناع يقينيبصحة ما ينتهي إليه من وقائع، لا بمجرد الظن والاحتمال لأن الشك يفسر لصالح المتهم أخذا بقاعدة أساسية أن الأصل في الإنسان البراءة، وشرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستقي منها هذا اليقين أدلة تقليدية أو مستحدثة كالدليل الإلكتروني.

فالقاعدة العامة في الإثبات الجنائي أن الأحكام تبنى على الجزم و اليقين، و لا تبنى على الظن و الاحتمال، و أن المحكمة ملزمة في حالة وجود الشك أن تحكم ببراءة المتهم طبقا للقاعدة القائلة بأن يفسر الشك لصالح المتهم، لأن الأصل في الإنسان البراءة و هذا يقين لا يزول إلاّبيقين مثله أو أقوى منه، فالإدانة لا يمكن إقامتها على مجرد ظنون أو تخمينات، بل لابد من التثبيت و اليقين الذي يبقى الأصل و هو براءة الإنسان، وعدم قدرة الأدلة الإدانة على أحداث القطع يترتب على هذا الأمر استمرار حالة البراءة التي يكفي تأكيد وجودها مجرد الشك في ثبوت تلك الأدلة.[1]

واليقين يعّرف في اللغة على أنه هو العلم وزوال الشك، و عدم وجود أدنى ريبة، أما في الاصطلاح فقد عرفه الفقهاء بأنه اعتقاد القاضي بأن ما وصل إليه هو الحقيقة و الوصول إلى اليقين يتم عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال وقائع الدعوى و ما يرتبه ذلك من تصورات في ذهنه ذات درجة عالية من تأكيد، و عندما يصل القارئ أو أطراف الدعوى و كذا

1: بلهلولي مراد، المرجع السابق ، ص 118.

القاضي إلى هذه المرحلة من اليقين، فإنه يصبح مقتنعا بالحقيقة فاليقين هو وسيلة الاقتناع ثمرة اليقين، و ليس اليقين في حد ذاته.[1]

فاليقين عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الصول إلى هذا اليقين عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي، من خلال ما يعرض عليه من وقائع الدعوى وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة ثقة عالية من التأكد.[2]

وعندما يصل القاضي لهذه المرحلة من مراحل اليقين فإنه يكون قد وصل إلى الحقيقة الواقعية وينطبق اليقين على الواقعة الإجرامية في ذهن القاضي، مما يولد لديه حالة ذهنية أو عقلية تحدث انطباعا عن كيفية حدوث تلك الواقعة.

وهذ اليقين يرتكز عليه القاضي في الوصول إلى اقتناعه واقتناع أطراف الدعوى، يتميز بجملة من الخصائص التي تضفي عليه صفة الوضوح و التحديد، و لعل أهمها اتسامه بصفة الذاتية، و ذلك لأنه نتيجة عمل و استنتاج الضمير الذي عند تقديره للوقائع المطروحة عليه كما أن اليقين الذي يصل غليه القاضي ليس يقينا مطلقا، بل يقينا نسبيا، و من ثم النتائج التي يمكن التوصل غليها تكون عرضة للتنوع و الاختلاف في التقدير من قاضي إلى آخر، لأن الجرم و اليقين المراد توفره في مجال الإثباتالجنائي،هو اليقين النسبي القائم على التدليل و التسبيب، لا اليقين المطلق لأن ذلك ليس بمقدور البشر، و لذلك فإن المطلوب من القاضي أن يبني عقيدته على أساس احتمالات ذات درجة عالية الثقة، و لكن يجب أن تبني على الجزم و اليقين لا على الحدس و التخمين، فلا يصلح سندا لإدانة أن يذكر القاضي في حكمه أنه يرجح ارتكاب جريمته ثم يدلل على أسباب هذا اليقين.[3]

1:عائشة بن قارة مصطفى، المرجع السابق، ص 277، 278.

2:مروك نصر الدين، المرجع السابق، ص 491.

3:بلهلولي مراد، المرجع السابق، ص 119، 120.

و القاضي الجنائي في سبيل وصوله إلى اليقين عليه أن يتبع كيفية معينة، حيث أن المطلوب عند الاقتناع ليس اليقين الشخصي للقاضي فحسب، و إنما كذلك اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قوتها في الاقتناع، و هو بهذا المفهوم يقوم على عنصرين أحدهما شخصي و يخلص في ارتياح ضمير القاضي و اطمئنان نفسه إلى إدانة المتهم على سبيل الجرم و اليقين، و الثاني موضوعي يخلص في ارتكانهذا الارتياح على أدلة من شأنها أن تقضي لذلك وفقا لمقتضيات العقل و المنطق، بحيث لا يكون عمل القاضي ابتداعا و انتزاعا من الخيال.

والعلة من وراء اقتضاء هذا القيد هو أن يحكم بالإدانة لشخص أمر جد خطير وتترتب عليه آثار جسيمة ويمكن أن ينال حريته أو شرفه أو مال، بل قد يكون حقه في الحياة، فضلا على أن القانون قد جعل الأحكام الباتة عنوانا للحقيقة، لذلك وجب أن تكون تلك الأحكام مبنية على الجرم واليقين.[1]

و إذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالأدلة التقليدية عن طريق المعرفة الحسية التي تدركها الحواس، أو المعرفة العقلية التي يقوم عن طريق المعرفة الحسية التي تدركها الحواس، أو المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل و الاستنتاج فإن الجرم بوقوع الجريمة الإلكترونية و نسبتها إلى المتهم المعلوماتي تتطلب نوعا جديدا من المعرفة، و هي المعرفة العلمية للقاضي بالأمور المعلوماتية لا سيما و أن القاضي الجنائي يلعب دورا إيجابيا في الإثبات الجنائي، و قد يؤدي الجهل في بعض الأحيان إلى التشكيك في قيمة الدليل الإلكتروني و من ثم يقضي بالبراءة، لا سيما أن الشك يستفيد منه المتهم المعلوماتي في مرحلة المحاكمة، و هذا يؤدي إلى إفلات المجرمين من العقاب و من تطبيق القانون.

1:عائشة بن قارة مصطفى، المرجع السابق، ص 278.

ويترتب على اللزوم بلوغ الاقتناع كان معنى ذلك اقتناعه بتأرجحبين ثبوت التهمة ومسؤولية المتهم عنها، وبين عدم ثبوتها أو عدم مسؤولية المتهم، وهذا الاقتناع المتأرجح يعني الشك في ثبوت التهمة مما يستوجب على القاضي أن يحكم بالبراءة.

ومن أهم نتائج مبدا الاقتناع اليقيني هي استثناء حالة البراءة من شرط الاقتناع اليقيني، فإذا كان الأصلمن الإنسان البراءة، فإنه يجب لإدانته أن يقوم الدليل القاطع على ارتكابه الجريمة سواء كانت تقليدية أو مستحدثة، كالجريمة الإلكترونية، بحيث يقتنع القاضي إقتناعا يقينيا بارتكابها ونسبتها للمتهم، أما فيما يتعلق بالحكم بالبراءة، و هذا إعمالا لمبدأ تفسير الشك لصالح المتهم.[1]

في حالة وجود الإدانة لابد من اليقين حتى يتم الحكم بإدانة المتهم، باعتبار أنها إثبات لخلاف الأصل وهو افتراض البراءة، فلا يمكن إثبات خلاف هذا الأصل إلا باليقين التام، في حيث أن الحكم بالبراءة هو مجرد تأكيد لهذا الأصل.

2-1. ضابط ملائمة الاقتناع القضائي لمقتضيات العقل والمنطق.

إن القاضي في تكوين اقتناعه وإن كان حرّا في اختباره للأدلة التي يطمئن إليها، وهذا في حكمه إلا أن هذا الأمر مشروط بأن يكون استنتاج القاضي للحقيقة الواقعة وما كشف عنها من أدلة لا يخرج من مقتضيات العقل والمنطق.[2]

فيجب أن يكون استخلاص محكمة الموضوع لواقعة الدعوى استخلاصا معقولا سائغا، ومعيار معقولية الاقتناع هو أن يكون الدليل بما في ذلك الدليل الإلكتروني مؤيدا إلى ما رتبه الحكم عليه من غير تعسف في الاستنتاج، ولا تنافر مع مقتضيات العقل والمنطق.

1: عائشة بن قارة مصطفى، المرجع السابق، ص 279.

2: شحط عبد القادر، نبيل صقر، الإثبات في مواد الجزائية، بدون طبعة، دار الهدى للطباعة والنشر والتوزيع، الجزائر، ص29.

ومع ذلك تجدر الإشارة إلى أن تقييد القاضي الجنائي عند تقديره للدليل الإلكترونيبضوابط معينة سواء كانت متعلقة بهذا الدليل ذاته أو متعلقة بالاقتناع، غير كافية لضمانة منع الاستبداد والتحكم، بل من اللزوم في إطار معتدل بهدف الوصول إلى الحقيقة الواقعية، باعتبارها غرض الدعوى الجزائية، وتتمثل هذه الوسيلة في مراقبة المحكمة العليا لسلطة القاضي الجنائي التقديرية.[1]

ومنه نقول أنّه صحيح أن الإثبات الجنائي يقوم على حرية الإثبات من طرف القاضي الجنائي إلاّ أنّ هذه الحرية لو تركت على مطلقها سيكون هناك تعسف في استعمال السلطة من طرف القاضي الجنائي.

المطلب الثاني: مشكلات الاختصاص القضائي في الجرائم المعلوماتية

تعتبر الجرائم المعلوماتية من الجرائم التي تثير مشكلة الاختصاص القضائي على المستوى المحلي أو الدولي، وتعني مشكلة الاختصاص المحلي في الجرائم المعلوماتية تنازع الاختصاص بين أكثر من جهة قضائية داخل إقليم الدولة، أمّا مشكلة الاختصاص الدولي تعني تنازع الاختصاص بين أكثر من دولة[2] وهذا سيتم تناوله من خلال ما يأتي:

الفرع الأول: الاختصاص القضائي الداخلي.

يسمى هذا النوع من الاختصاص الداخلي أو الإقليمي، بحيث يختص القضاء الوطني في الفصل في الدعوى الجزائية دون سواه، كما يقوم بتحديد إطار جغرافي أو دائرة الاختصاص مكاني تتحدد بمنطقة معينة من إقليم الدولة، لهذا ينقسم الاختصاص المكاني أثناء ارتكاب الجريمة إلى مكان وقوع الجريمة، أو مكان إقامة المتهم، أو مكان القبض على المتهم.[3]

1:عائشة بن قارة مصطفى، المرجع السابق، ص 281.

2:حسين الجندي، شرح قانون الإجراءات الجزائية، دون طبعة، دون دار نشر، دون بلد نشر،1990، ص 687.

3:أنظر المادتين 37 و 329 من قانون الإجراءات الجزائية الجزائري.

وقد قضت المادتين 37 و 329 من قانون الإجراءات الجزائية الجزائري على أن: الاختصاص القضائي المكاني يتطلب توافر حالة من الحالات التالية:

- أن تكون إقامة المتهم أو أحد شركائه المشتبه بهم في دائرة اختصاص عضو النيابة العامة أو قاضي التحقيق، ويتحدد مكان إقامة بوقت وقوع الجريمة.
- أن يكون القبض قد ألقي على أحد المتهمين أو المشتبه بهم في نطاق تلك الدائرة.[1]

وتثار مشكلة الاختصاص القضائي المحلي بالنسبة لجرائم المعلوماتية في حالة ما إذا ارتكبت الجريمة في أكثر من نطاق الاختصاص محلي داخل الإقليم الوطني للدولة، بسبب طبيعة الجريمة وشبكة المعلوماتية، فالجريمة في هذه الحالة سواء تمثلت بجريمة الدخول أو إتلاف بيانات الحاسب الآلي أو أنظمة المعالجة الآلية للمعطيات وغيرها، وقد وقعت بكامل أركانها في نطاق اختصاص المحاكم الجزائرية.

و الحل المناسب لهذه المشكلة هو تمديد الاختصاص القضائي داخلإقليم الدولة بما يتناسب وطبيعة الجريمة الإلكترونية، إذ يمكن تطبيق أي قاعدة من قواعد الاختصاص سواء اقترفت بمكان وقوع الجريمة، أو بمحل إقامة المتهم أو المشتبه فيه، أو بمكان وقوع الجريمة، أو محل إقامة المتهم في قضية فتكون مختصة بالنظر فيها دون غيرها، وز لها أن تمدد الاختصاص بشأن اتخاذ أي إجراء من إجراءات المحاكمة، بشرط أن يكون التمديد بموجب نص قانوني.[2]

وهذا ما جعل القانون الجزائري يمدد الاختصاص القضائي بالنسبة لبعض الجرائم التي نصت عليها المواد 37 و 47و 80 و 329 من قانون الإجراءات الجزائية الجزائري.

1:فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمن، أطروحة لحصول على شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر (1)، 2010، 2011، ص 373،376.

2:فايز محمد غالب، المرجع السابق، ص 375،376.

حيث تضمنت الفقرة الثانية من المادة 37 من هذا القانون إلى إجازة تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى في جرائم معينة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما أجازت المادة 47من نفس القانون لقاضي التحقيق الحق لقيام بعملية تفتيش أو حجز ليلا أو نهارا في جرائم محددة، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و ذلك في أي مكان على امتداد التراب الوطني أو بأمر ضابط الشرطة القضائية المختص بذلك، بالإضافة على نص المادة 3/329 من القانون سالف الذكر و التي سمحت بتمديد الاختصاص المحلي للمحكمة إلى دائرة الاختصاص المحاكم الأخرى في بعض الجرائم من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات [1] و من خلال النصوص القانونية السابقة يتضح أن التشريع الجزائريقد حسم المشكلة بالنسبة لتنازع الاختصاص القضائيين الجهات داخل الإقليم الوطني للدولة و هذا الاختصاص يتحدد من خلال ما يلي:

1. بنطاق ضرورة التحقيق: حيث نص المادة 80 من نفس القانون على أنه: "يجوز لقاضي التحقيق أن يقوم بجميع إجراءات التحقيق في نطاق اختصاص المحاكم المجاورة لنطاق اختصاص وفق الشروط التالية:

أ – ضرورة الانتقال خارج نطاق اختصاصه المكاني.

ب – إخطار وكيل الجمهورية بدائرة اختصاصه.

ج – إخطار وكيل الجمهورية بدائرة اختصاص المحكمة التي يستقبل إليها.

د – تبيان الأسباب التي جعلته يمدد دائرة اختصاصه المكاني في محضر معاينة."

2. كما يحدد الاختصاص وفقا لجرائم أخرى باعتبارها تشكل خطورة على أمن المجتمع، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، بحيث يمكن لوكيل الجمهورية تمديد اختصاصه المحلي إلى دائرة اختصاص محاكم أخرى، وكما أن لقاضي التحقيق أن يقوم بإجراء معاينة أو تفتيش أو حجز

1:أنظر المواد 37 و 47 و 80 و 329 من قانون الإجراءات الجزائية الجزائري.

على امتداد التراب الوطني، وكذلك يجوز تمديد اختصاص المحكمة إلى نطاق اختصاص المحاكم الأخرى.[1]

ولم يقتصر المشرع الجزائري تمديد الاختصاص القضائي على هذه الجرائم، بل أجاز تمديد الاختصاص والقيام ببعض الإجراءات عن بعد، حيث نصت المادة 05 من قانون رقم 04/09 على أنه: .... إذا كانت هناك أسباب تدعو الاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأنّ هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة، أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.[2]

الفرع ثاني: الاختصاص القضائي الدولي.

يعد الاختصاص القضائي الدولي بالنسبة للجرائم المرتكبة في نطاق المعلوماتية أكثر مشكلة بما عليه الوضع على مستوى إقليم الدولة الواحدة، على أساس أن الدولة بإمكانها وضع حد للمسألة كما سبق الذكر، على خلاف مشكلة الاختصاص القضائي على المستوى الدولي، باعتبار أن هذه الجريمة عبارة للحدود، بالإضافة إلى اختلاف التشريعات و النظم القانونية من دولة لأخرى، فقد يحدث أن ترتكب الجريمة في إقليم دولة ما من قبل أجنبي، و في هذه تخضع الجريمة لاختصاص الدولة الثانية على أساس مبدأ الشخصية، و قد تكون هذه الجريمة من الجرائم التي تهدد أمن و سلامة دولة أخرى، فتدخل عندئ في اختصاصها استنادا إلى مبدأ العينية.[3] و هذا سيتم التفصيل فيه فيما يلي:

1: فايز محمد راجح غلاب، المرجع السابق، ص 377،378.

2: أنظر الفقرة الثانية من المادة 05 من قانون رقم 04/09 ،المرجع السابق.

3: جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالأنترنت، دون طبعة، دار النهضة العربية،1998، ص 73.

أولا: الاختصاص القضائي الإقليمي

تختص المحاكم الجزائية في الدولة بالنظر في الجرائم التي تقع كلها أو جزء منها على إقليمها أيّا كانت صفة الشخص المتهم وبغض النظر عن جنسيته غير أن هذا المبدأ- الإقليمية- استثناءات منها عدم تطبيقه على رؤساء الدول ورجال السلك الديبلوماسي، إضافة إلى الاعتراف ببعض الأحكام الأجنبية بموجب نص قانوني أو معاهدة دولية.[1]

ويشترط القانون الجزائري تطبيق مبدأ الإقليمية أن تكون الجريمة أو أحد الأفعال المكونة لها قد تم ارتكابها في نطاق الإقليم الوطني للدولة، فيكفي لانعقاد الاختصاص للمحكمة الجزائرية أن ترتكب الجريمة بكامل أركانها في الجزائر أو أي فعل من الأفعال المكونة لها، ولا يه م بعد ذلك مكان وجود الجاني.[2]

وكذلك مبدأ الإقليمية يطبق على الجرائم المعلوماتية خاصة منها المرتكبة بواسطة الأنترنت و إلا أن هذا قد يثير مشكلة تنازع الاختصاص القضائي لأكثر من دولة، كما لو بث الجاني صور ذات الطابع الإباحي من إقليم دولة معينة و تم الاطلاع عليها في دولة أخر، ففي هذه الحالة يثبت الاختصاص وفقا لمبدا الإقليمية لكل دولة من الدول التي مستها الجريمة، لأن شبكة الأنترنت ليس لها مقر في دولة معينة، و لهذا يستطيع الأشخاص من كل دول العالم تبادل الأفكار و المعلومات بكل حرية، و لأجل ذلك فهي لا تخضع لرقابة أو سيطرة دولة معينة، مما يؤدي ذلك إلى عدم وجود قانون جنائي يتعلق بسيادة الدولة، وهنا تكمن المشكلة، و كذلك تعد إحدى مشكلات الاختصاص

1: حسين الجندي، المرجع السابق، ص 55.

2:راجع الفقرة 01 من المادة 03 من قانون العقوبات الجزائري، والمادة 586 من قانون الإجراءات الجزائية الجزائري.

القضائي عدم فاعلية المحاكمة عن الجرائم المعلوماتية نظرا لتداول الجرائم المرتكبة بواسطة الأنترنت، و هذا ما جعل منعها و العقاب عليها أمرا احتماليا في ظل الوضع الراهن للأنظمة القانونية.[1]

بالإضافة إلى أن من الصعوبات التي تؤدي إلى عدم إمكانية تطبيق الاختصاص القضائي القائم بمبدأ الإقليمية في مجال الجرائم المعلوماتية، حالة كون مزود الأنترنت تابع لمزود آخر كائن في بلد آخر، أو يكون المزود الرئيسي موجود في دولة بينما المزودات الفرعية في أكثر من دولة، والسؤال الذي يطرح نفسه أي من قضاء تلك الدول يكون مختصا، وأي من القوانين يكون واجب التطبيق؟[2]

أمام هذه المشكلات استلزم الأمر ضرورة وجود تعاون دولي لإقامة حد لمثل هذه الصعوبات من خلال معاهدات ثنائيةأو دولية بما يجعل قضاء الدولة التي بدأت في اتخاذالإجراءات أو الدولة الأكثر تضررا في الجريمة المعلوماتية هي المختصة، إضافة على تفعيل التعاون الأمني بين مختلف المؤسسات الأمنية فيما بينها عن طريق الإنتربول الدولي، بهدف تمكين الأجهزة الأمنية من الحصول على البيانات والمعلومات المتعلقة بتلك الجرائم، وتحديد مكان المجرم في الوقت المطلوب.[3]

ثانيا: الاختصاص القضائي الشخصي.

إن الاختصاص القضائي القائم على مبدا الشخصية يقتضي اختصاص الدولة التي يكون أحد أفرادها هو الجاني ويحمل جنسيتها أثناء ارتكابه جريمة في الخارج، وهذا ما يسمى بالاختصاص الإيجابي، إلا أنّ بعض الدول لم تقتصر على جنسية الجاني بل أضافت جنسية المجني عليه كمعيار

1: جميل عبد الباقي الصغير، المرجع السابق، ص 42،58.

2:عمر محمد أبو بكر بن يونس، المرجع السابق، ص 917.

3:مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، الطبعة الأولى، دار الكتب والوثائق القومية، المصرية، القاهرة،2000، ص 63.

لتطبيق قضائها على الجريمة التي ارتكبت ضد أفرادها في الخارج وهذا ما يسمى بالاختصاص السلبي.[1]

ولقد أدرج المشرع الجزائري في المادتين 582 و583 من القانون السالف الذكر على أنه يطبق النص الجزائي على كل من يحمل جنسية جزائرية، إذا توافرت فيه الشروط اللازمة منها:

- أن يكون الفعل مجرما في كلا من البلدين الجزائري و الأجنبي الذي افترض فيه الجريمة، و أن توصف الجريمة بجناية أو جنحة وفقا للقانون الجزائري، و كذلك ضرورة عودة المتهم إلى الجزائر، و أن يكون قد حكم عليه بحكم نهائي في الخارج، و أن تثبت قضاؤهللعقوبةفي حالة إدانته أو سقطت عنه العقوبة بالتقادم أو حصل العفو فيها، و يشترط أن يكونه الجاني وقت ارتكابه الجريمة يحمل الجنسية الجزائرية، و عليه يتم النظر في الجريمة المرتكبة منطوق المحكمة المختصة بموجب طلب من النيابة العامة بعد إخطارها من الشخص المضرور أو ببلاغ من السلطات المقرالذي ارتكبت فيه الجريمة.[2]

والجديربالذكر أن القانون الجزائري لا يعرف الوجه السلبي للاختصاص القائم على مبدا الشخصية، فجنسية المجني عليه ليست شرطا لتطبيق قضائه على الجريمة المرتكبة في الخارج ضد من يحمل جنسيتها، باستثناء أن تكون الجريمة المقترفة تحمل وصف جناية أو جنحة تكون قد ارتكبت على متن طائرة أجنبية وكان المجني عليه جزائري في حالة أن هبطت الطائرة في الجزائر بعد وقوع الجناية أو الجنحة أو القبض على الجاني بالجزائر.[3]

1:فايز محمد راجح غلاب، المرجع السابق، ص 385.

2:أنظر المادتين 582 و 583 من المادة 569 من قانون الإجراءات الجزائية الجزائري

3:أنظر الفقرة الثانية والثالثة من المادة 591 من قانون الإجراءات الجزائية الجزائري

وبالتالي فالاختصاص القضائي القائم على مبدأ الشخصية يثير العديد من المشكلات في مجال الجريمة بشكل عام والجريمة المعلوماتية بشكل خاص، والتي نوردها فيما يلي:

لا يطبق اختصاص قضاء الدولة للجريمة المرتكبة في الخارج من طرف من يحمل جنسيتها، إذا كان الفعل المجرم لا يحمل وصف جريمة في الدولة التي ارتكبت فيها، إذن فالاختصاص لا ينعقد بالنسبة للمعلومات و الصور التي ثبت عن الخارج باعتبارها غير مجرمة في بلد المنشأ، مع أنها جريمة في الدول التي يصلها البث، و في هذه الحالة عندما لا يكون القانون الوطني مختصا بالنظر في الدعوى فتثار المشكلة بالنسبة لمن أصابه الضرر في الجريمة، حيث يجب عليه الانتقال إلى الدولة التي ارتكبت فيها الجريمة لرفع دعواه أين تثار المشكلة بصورة أكبر كون الفعل غير معاقب عليه في هذه الدول[1]

إن تنفيذ العقوبات يصطدم بصعوبات كثيرة، ذلك أن العقاب على فعل وقع في الخارج لا يجد أساس له في ظل قلة الدول التي وقعت على اتفاقية تسليم المجرمين مقارنة بالكم الهائل من الدول التي تتعامل بالأنترنت، لذلك فمن الأصلح إيجاد قانون دولي جنائي على غرار القانون الدولي الخاص ليطبق على الجرائم الواقعة على الأنترنت أو بواسطتها.[2]

ثالثا: الاختصاص القضائي العيني.

يقوم الاختصاص القضائي القائم على أساس مبدأ العينة بالنظر في جرائم معينة، وهي تلك التي تمس أمنها ومصالحها دون النظر إلى مرتكب الجريمة إذا كان يحمل جنسية الدولة أم لا، وبغض النظر إذا كان مقترفيها متواجد في إقليمها أو خارجه، وكما أن أغلب التشريعات تقر بمبدأ

1:أحمد عبد الكريم سلامة، مرجع سابق، ص 38.

2:جميل عبد الباقي الصغير، المرجع السابق، ص 51.

الاختصاص القضائي العيني للفصل في أي قضية تتعلق بمصالحها وأمنها القومي ومن بين تلك التشريعات قانون العقوباتالفرنسي.[1]

و قد نص القانون الجزائري على مبدأ العينة في المادة 588 من قانون الإجراءات الجزائية التي تضمنت جواز متابعة كل أجنبي قام بالمساس بأمن و سلامة الدولة الجزائري، و لم يقتصر المشرع الجزائري على هذا النص، بل أضافة من خلال القانون الجديد رقم 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و الذي تضمن في إحدى مواده تمديد الاختصاص القضائي بالنسبة لهذا النوع من الجرائم حيث ورد النص كالتالي: "زيادة على قواعد الاختصاص المنصوص عليه في قانون الإجراءات الجزائية تخص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني".[2]

ومن خلال النصوص السالفة الذكر يتضح أن المشرع الجزائري قد تضمن اختصاص القضاء الوطني في كل من جرائم تزييف النقود والأوراق المصرفية الوطنية التي ارتكبت الواقعة الإجرامية في الخارج من طرف أجنبي، وكذلك الجرائم التي تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، فهذه الجرائم يمكن أن ترتكب بواسطة الأنترنت، وذلك في حالة كون الموقع الذي ارتكب من خلاله الواقعة الإجرامية يقع خارج إقليم الدولة.[3]، ومن تلك الجرائم نجد جريمة تسليم أو إنشاء أسرار الدفاع وجريمة الخيانة والتجسس وجرائم التعدي على الدفاع الوطني أو الاقتصاد الوطني وغيرها من الجرائم الماسة بالأمن القومي للدولة.[4]

1:فايز محمد راجح غلاب، المرجع السابق، ص 388.

2:المادة 15 من قانون رقم 04/09 ، مرجع سابق.

3:فايز محمد راجح غلاب، المرجع السابق، ص 388.

4:انظر المواد 64 و 83 من قانون العقوبات الجزائري.

غير أن تطبيق الاختصاص القضائي القائم على أساس مبدا العينة يثير العديد من المشكلات التي تعيق تنفيذه، وهي كالتالي:

✍ مشكلة تعارض الاختصاص بين مبدأي العينية والإقليمية، فهنا تثار مسألة تنازع الاختصاص ما بين الدولة التي ارتكب فيها الواقعة الإجرامية وفقا لمبدأ الإقليمية، والدولة الأخرى التي تعتبر تلك الجريمة من الجرائم التي يختص بها قضاؤها وفقا لمبدأ العينية، وبالتالي فقد يحاكم الشخص على جرمه مرتين.

✍ يعتبر كل من السلوك والنتيجة شرطي الجريمة في الجرائم المعلوماتية التي ترتكب عن طريق الشبكات، لذلك كل من محاكم مكان السلوك الإجرامي ومكان تحقق النتيجة الإجرامية مختصة بالنظر في الواقعة الإجرامية.[1]

فإذا تم البث مثلا لفيروس معين في مكان معين و تحققت النتيجة الإجرامية المتمثلة في تدمير المعلومات أو التلاعب بالبيانات أو تحويل الأموال أو غير ذلك من النتائج في مكان آخر، فإن الاختصاص سيكون لمحكمتين، الأولى مكان بث الفيروس و الثانية مكان تحقق النتيجة بالإضافة إلى ارتباط مشكلات الاختصاص و تطبيق القانون بصعوبات تتعلق بامتداد أنشطة الملاحقة و التحري والضبط و التفتيش خارج الحدود في الجرائم المعلوماتية، و ما يتطلبه ذلك إلى ضرورة تعاون دولي شامل لتحقيق التوازن بين مستلزمات المكافحة و وجوب حماية السيادة الوطنية.[2]

ومن خلال ما تم إيضاحه فإن مشكلة الاختصاص القضائي أصبحت معقدة نظرا لعدم وجود اتفاق دولي ينظم المشكلة، ذلك في ظل ما تتمتع به شبكة المعلوماتية من فقدان السيطرة والرقابة عليها وعلى المعلومات المتداولة عبرها، وبالتالي حبذا لو تم إعادة النظر بالنسبة الجرائم المعلوماتية، كما

1: جميل عبد الباقي الصغير، المرجع السابق، ص 63.

2: فايز محمد راجح غلاب، المرجع السابق، ص 391،392.

أنه لا مانع من تقرير نص يمكن من خلاله السماح لضباط الشرطة القضائية الانتقال عبر العالم الافتراضي للتعاون مع جهات ضبط دولية خارج مجال اختصاصه المكاني من أجل ضبط جرائم ذات الطابع الرقمي.[1]

المطلب الثالث: شروط قبول الدليل الرقمي.

نظرا للتطور العلمي الذي عرفه المجال الجنائي ومع بروز أدلة علمية حديثة، من بينها الدليل الرقمي الذي يعد كأفضل دليل الإثبات الجرائم الإلكترونيةوذلك يعود إلى نقص الثقافة العلمية، والأخذ به يجب توافر شروط مصداقيته، وكذا الاستعانة بأهل الخبرة والفصل في النزاعات في حالة ما استعصى عليه الأمر، ولهذا سنتطرق في هذا المطلب إلى مصداقية الدليل الرقمي، وإلى القيمة العلمية لدليل الرقمي على قناعة القاضي.

الفرع الأول: مصداقية الدليل الرقمي في الإثبات.

إذا كان الدليل الرقمي في الإثبات قيمة من الناحية العلمية، يجب توافر شروط مصداقيته، ولكن هذا لا يمكن أن يستبعد عن موضوع الشك من حيث سلامة العبث به من جهة، وكذا صحة الإجراءات المتبعة في الحصول عليه من جهة أخرى.

أولا: يقينية الدليل الرقمي:

يشترط في الأدلة المستخرجة من المنظومة المعلوماتية والأنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بموجبها بالإدانة ذلك أنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين [2]، و يمكن التوصل إلى ذلك من خلال ما يعرض من

1:عمر محمد أبو بكر بن يونس، المرجع السابق، ص 823.
2:علي حسن محمد طوابلة، المرجع السابق، ص 190.

الأدلة الرقمية على اختلاف إشكالها التي تتوافر عن طريق الوصول المباشر إليها أو بمجرد عرضها كمخرجات على شاشة الحاسوب، و يستطيع القاضي من خلال ما يعوض عليه من مخرجات إلكترونية (رقمية) وما ينطبع في ذمته من تصورات و احتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه، و كذا الوصول إلى يقينية هذه المخرجات عن طريق المعرفة الحسية التي تدركها الحواس من خلال ما يقوم به من استقراء و استنتاج ليصل إلى الحقيقة التي يهدف إليها و يجب أن يصدر حكمه استنادا إليها.[1]

ويتحقق اليقين للأدلة الرقمية أكثر بإخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته، وكذا صحة الإجراءات المتبعة في الحصول عليه من أجل تفادي تلك العيوب التي قد تشوبه، فمثلما يخضع الدليل الرقمي لقواعد وإجراءات معينة تحكم طرقا للحصول عليه فإنه يخضع لقواعد أخرى للحكم على قيمته الاستدلالية من الناحية العلمية وذلك راجع للطبيعة الفنية لهذا الدليل.[2]وتتمثل وسائل وتقييم الدليل الرقمي في:

1 تقييم الدليل الرقمي للتحقيق من سلامته من العبث.

ويمكن التأكد من سلامة الدليل الرقمي من وقوع العبث به بعدة طرق أهمها:

- فكرة التحليل التناظري الرقمي والتي من خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالأدلة الرقمية، ومن ثم يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا.[3]

1:خالد عباد الحلبي، المرجع السابق، ص 91.

2:فايز محمد راجح غلاب، المرجع السابق، ص 249.

3:طارق محمد الجملي، المرجع السابق، ص 22.

- استخدام عمليات حسابية خاصة تسمى الخوارزميا يلجأ على هذه التقنية في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي، أو في حالة أن العبث قد وقع على النسخة الأصلية إذ بالإمكان التأكد من سلامة الدليل الرقمي من التبديل والتحريفوالتغيير باستعمال هذه العمليات الحسابية.

- استعمال الدليل المحايد وهو نوع الأدلة الرقمية المخزون في البيئة الافتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول أي تعديل عليه في النظام الكمبيوتري.[1]

- إن نقص الثقافة المعلوماتية لدى القاضي الجزائي يستوجب عليه في هذه الحالة انتداب خبير من أجل الحصول على الدليل والتأكد من مصداقيته في مجال المعالجة الآلية للمعلومات وتحقيق اليقينية لهذا الدليل.

2 تقييم الدليل الإلكتروني في السلامة الفنية لإجراءات تحصيله.

إذا كانت نسبة الخطأ الفني في الحصول على الدليل الإلكتروني ضئيلة جدا لاعتباره تطبيقا من تطبيقات الدليل العلمي الدقيقة، و ذلك لا يعني أنها منعدمة تماما، إنما يظل الوقوع في الخطأ ممكنا أثناء استخلاصه و يكون ذلك إما بسبب الخطأ في استخدام الأداة المناسبة لاستخلاص الدليل، كالخلل في الشفرة المستخدمة، أو استعمال معلومات و مواصفات خاطئة، و إما بسبب الخطأ في استخدام أداة تقل نسبة عنمائةبالمائة (100%) مثل ما يحدث غالبا في وسائل اختزال المعطيات أو معالجتها بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.[2]

1: ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 391،392.

2: براهيمي جمال، إجراءات التحقيق في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم الجنائية، جامعة مولود

من أجل تجنب مثل هذه الأخطاء يمكن اتباع بعض الاختبارات والتطبيقات للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل الإلكتروني من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات والتي نلخصها فيما يلي:

أ - إخضاع الأداة المستخدمة في الحصول على الدليل لعدة تجارب بغية التأكد من دقتها في إعطاء النتائج المبتغاة:

ويكون ذلك باتباع اختبارين أساسيين يتم من خلالهما التأكد من أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الإلكتروني، وفي الوقت نفسه لم تضف غليها أي بيان جديد، وهو ما قد يعطي للنتائج المقدمة عن طريق هذه الأداة مصداقية في التدليل على الوقائع، ويتمثل هذان الاختبارين فيما يلي:

-**اختبار السلبيات الزائفة:** وفيه يتم إخضاع الأداة المستخدمة في الحصول على الدليل لاختيار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الإلكتروني دون إغفال أية بيانات مهمة عنه.

- اختبار الإيجابيات الزائفة: ومفاده إخضاع الأداة المستخدمة في الحصول على الدليل الإلكتروني لاختبار فني يمكن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.[1]

ب - الاستعانة بأدوات ذات تقنية عالية أثبتت التجارب العلمية نجاعتها في تقديم نتائج أفضل:

هناك دراسات وبحوث علمية متخصصة في مجال تقنية المعلومات حددت الأدوات السلمية التي يجب اتباعها في سبيل الحصول على الدليل الإلكتروني، وفي المقابل بينت كذلك الأدوات المشكوك في

معمري، تيزي وزو،2018،2017، كلية الحقوق والعلوم السياسية، قسم الحقوق، ص 155.

1:بوكر رشيدة، المرجع السابق، ص 501.

كفاءتها وحثت على اجتنابها، وعليه فاختيار أية أداة من هذه الأدوات من شأنه يؤثر على مصداقية المخرجات المستمدة منها.[1]

و منهنا يمكن القول بانه إذا سلمنا سابقا بإمكانية التشكيك في سلامة الدليل الإلكتروني بسبب قابليته للعبث و نسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن أن يقطع في شأنها برأي حاسم إذ لم يقطع به أهل الاختصاص، لذلك فإذا توفرت في الدليل الإلكتروني الشروط المذكورة سالفا بخصوص سلامته من العبث و الخطأ، فإن هذا الدليل لا يمكن رده استنادا لسلطة القاضي التقديرية[2]، لأن سلطة القاضي في ردّ الدليل استنادا لفكرة الشك يستلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، و هو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، فيقتصر دوره على بحث صلة الدليل بالجريمة فقط.

الفرع الثاني: مناقشة الدليل الرقمي.

إن حرية الدليل الجنائي مشروطة بأن يكون الدليل الذي يستند غليه القاضي قد طرحت مناقشته بالجلسة، ويكون كذلك متى كان له أصل ثابت في أوراق القضية المطروحة على القاضي[3]،وهو ما يجعل هذه الأدلة متاحة للخصوم لكي يتمكن كل خصم من إعداد دفاعه فإن كان الدليل في صالحه يدافع عنه وإن كان ضده يشك فيه ويضعفه، ولا يمكن للقاضي حينها أن

1:طارق محمد الجملي، المرجع السابق، ص 28.

2:هذا ما أكدته المحكمة الاتحادية الأمريكية في القضية المعروفة بـ(united states v. russe) لعام 1974 حينما قررت المحكمة أنه:" مع افتراض استخدام حاسب يؤدي وظائفه بشكل سليم، ومع توافر الثقة فيه وإمكانية التعويل عليه، فإن مخرجاته يجب أن تكون مقبولة كدليل على المعاملات التي أدخلت فيه" نقلا عن هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 182.

3:أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دون طبعة، دار النهضة العربية،1996، ص 392.

يؤسس اقتناعه ألا على العناصر الإثباتية التي طرحت في جلسات المحكمة وخضعت لحرية مناقشة أطراف الدعوى.

وهذا يعني أن الأدلة الرقمية المتحصلة لإثبات الجرائم المعلوماتية سواء كانت مطبوعة اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مصورات فلمية، كلها ستكون محى للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة،وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال البيئة الإلكترونية يجب أن يعرض في جلسة المحكمة ليس من خلال ملف الدعوى في التحقيق الابتدائي وإنما يعرض بصفة مباشرة أمام القاضي.

وهذهالأحكام تنطبق على كافة الأدلة المتولدة في الحسابات الإلكترونية فبالنسبة لشهود الجرائم المعلوماتية.[1]والذين كانوا قد سبق سماعهم في التحقيق الابتدائي فإنه يجب أن يتم إعادة سماعهم مرة أخرى من جديد أمام المحكمة، كذلك بالنسبة لخبراء المعلوماتية على اختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحكمة لمناقشتهم ومناقشة تقاريرهم التي خلصوا إليها.

ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم المعلوماتية بناءا على علمه الشخصي أو استنادا إلى راي الغير من الخبراء، وقد ارتاح ضميره إلى التقرير المحرر من قبله فقرر الاستناد إليه ضمن باقي الأدلة القائمة على أوراق الدعوى المعروضة عليه.

و الحديث في هذه المسالة يجرنا إلى مناقشة مدى تأثير الأصالة الرقمية [2]للدليل الرقمي على مبدأ قبوله من طرف القضاة، إذ تبرز هذه المشكلة بصورة جلية عندما يقوم المتهم بإزالة الدليل

1:الشاهد المعلوماتي هو الفني صاحب الخبرة والمتخصص في تقنية علوم الحاسب الآلي والذي يكون لديه معلومات جوهرية للولوج لنظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله.

2:هناك تمييز حقيقي بين الأصالة للدليل في طابعها المادي وبين الأصالة في طابعها الرقمي من حيث أن الأولى هي سوى تعبير عن وضعية مادية ملموسة كما هو الشأن في الورق المكتوب أو بصمة الأصبع أو الحدوث العيني للواقعة في حين أن الثانية ليست سوى تعداد غير محدود لأرقام ثنائية موحدة في الصفر الواحد.

الرقمي عن بعد، فيكون ما تبقى منه هو مجرد نسخة فقط يتم التوصل إليها عن بعد أيضا بطرق المراقبة الإلكترونية مثلا، و من ثم فالسؤال هنا هل يكفي ناتج المراقبة الإلكترونية وحده للقول بأن الدليل هنا هو دليل أصلي و بالتالي يقبل طرحه على القضاء و مناقشته ضمن أدلة الدعوى ذات السؤال ينطبق على حالة الدليل المسترد بعدما تم حذفه باستخدام خاصية الإلغاء.

إن مناقشة هذه المسألة من الناحية القانونية دفع بالتشريع المقارن أن يعتمد منطق افتراض أصالةالدليلالرقمي حيث نص قانون الإثبات الأمريكي في المادة 03/1003 أنه إذا كانت البيانات المخزنة في الحاسوب أو آلة مشابهة فإن أي مخرجات طابعة منها أو مخرجات مقروءة تبرز انعكاسا دقيقا للبيانات، و تعد بيانات أصليه و تبرز أهمية التسليم بمنطق افتراض أصالة في الدليل الرقمي على المستوى القانوني ذلك أن الطبيعة القانونية للدليل الرقمي لا تعبر عن قيمة أصليه بمجرد رفع محتواه من النظام المعلوماتي إذ يبقى متواجدا في كل مكان يتم استدعاؤه منه.[1]

النوع الثاني: القيمة العلمية لدليل الرقمي وتأثيرها على قناعة القاضي.

يعرف الدليل العلمي بانه ذلك الدليل الذي تقام عليه تجارب علمية لإثبات أو نفي واقعة فيها الشك، وفهمه يتطلب دراية خاصة لا يملكها القاضي في حكمه، وتكوينه القانوني المحض، والدليل الرقمي باعتباره تطبيقا من تطبيقات الدليل العلمي لا يمكن للقاضي أن ينازع في قيمته الإثباتيةوذلك لامتيازه بقوة الاستدلالية من الناحية العلمية.

1:محمد بوبكر بن يونس، المرجع السابق، ص 973.

فلتقدير القاضي براي العبير، فنجد أن الدليل الرقمي يعتبر من الأدلة العلمية التي يمكن للقاضي أن ينازع في القيمة و ذلك لتمتعه بقوة استدلالية، و هناك حجية قاطعة في الدلالة عن الوقائع الوضعية التي تتضمنه الأدلة، و كما يمكن التقلب من مشكلة الشك في مصداقية الدليل من خلال إخضاعه لتجارب تمكنه من التأكد من صحته، و أنه لا يمكن الخلط بين الشك الذي يشوب الدليل بسبب إمكانية العبث به، و كذا لوجود خطأ في الحصول عليه، و كذلك القيمة الاقتناعية به، و القاضي لا يمكن أن يفصل فيها باعتبارها مسألة فنية و الرأي هنا يعود إلى الخبير، فإذا سلم الدليل من العبث وتوافرت فيه كل الشروط، فإن على القاضي القبول بهذا الدليل، لذلك يرى هذا الاتجاه أن رفض القاضي لرأي الخبير فيكون تعارض مع رأيه و نفسه، و عليه فإن الدليل العلمي و منه الدليل الرقمي اصبح يقيد حرية القاضي في تقدير الأدلة، و يلزمه على الحكم حتى و لو لم يكن مقتنعا بصحة الواقعة المطروحة أمامه.[1]

و هناك من يناقد أنصار هذه النظرية و يؤكد أن الأدلة العلمية ليست دليلا مستقلا، بل هي عبارة عن قرائن إما أن يتخذ شكل قرينة قضائية يعتمد عليه وحده في الإثبات، و إما يتخذ شكل قرينة قضائية يعتمد عليه وحده في الإثبات، بل على القاضي الاستعانة بأهل الخبرة، إلا أن القاضي لا يمكن أو أن هناك مجالات لا يمكن لهذا الأخير، فمثلا إذا كان الدليل الرقمي لا يوافق ظروف و ملابسات التي وجد فيها، و كذلك لا يمكن للقاضي مباشرة حكمه بالإدانة أو البراءة إذ توفر الدليل الرقمي، فالدليل ليس آلية معدة لتقرير اقتناع القاضي على مسألة غير مؤكدة، فرأي هذا الاتجاه أن الدليل العلمي و الرقمي مهمًا على شأنهم في الإثبات الجنائي، إلا أنّ سلطة القاضي الجنائي محددة و

1: سعيداني نعيم، المرجع السابق، ص 218.

مسيطرة في الحقيقة و خلالها يمكن للقاضي أن يفسر الشك لصالح المتهم و أن يستبعد الأدلة التي يتم الحصول عليها بطريقة غير مشروعة و هو أمر ضروري و هذا ما جعل الحقيقة العلمية قضائية.[1]

وتكمن مهمة القاضي في التقرير الفني هي الرقابة القانونية على هذا التقرير وهو ما ورد في نص المادة 212 من قانون الإجراءات الجزائية كما أن المادة 215 من نفس القانون تؤكد أنّ: "لا تعتبر المحاضر والتقاريرالمثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك".

وهو الأمر الذي أخذ به المشرع الجزائري حيث بموجبه يقرر المبدأ الشخصي للقاضي الجزائي بجعله يبسط سلطته على جميع الأدلة بدون استثناء بما فيها تقرير الخبير.[2]

بحيث قضت المحكمة العليا هذا الاتجاه في أحد أحكامها: "إنّ تقرير الخبرة ليس إلا عنصرا من عناصر الاقتناع يخضع لمناقشة الأطراف ولتقدير قضاة الموضوع".

وكما أكدت في حكم آخر لها: "إنّ تقرير الخبرة لا يقيد لزوما قضاة الموضوع وإنما هو كغيره من أدلة الإثبات قابل للمناقشة والتمحيصومتروك لتقديرهم وقناعتهم".

وكما يلزم القاضي بالحقائق العلمية لا يسلب منه سلطة الرقابة القانونية على عناصر الدعوى بما فيها طرق الحصول على الدليل والظروف التي وجد فيها، فهي تدخل ضمن الاختصاصات الأصلية للقاضي، كما أنها تخضع أيضا لمبدأ تكافي الأدلة بحيث يمكن للقاضي استبعاد أي دليل علمي لا يتناسب مع ظروف الواقعة أو الجريمة.

وكما يمكن الاستعانة بمعطيات التطور العلمي في إطار الكشف عن الجريمة ويبقى للقاضي الحرية المطلقة في تقرير الدليل المعروض أمامه، والأخذ بما هو مناسب للواقع.[1]

1: سعيداني نعيم، مرجع سابق، ص 218.

2: الأمر رقم 155/66 يتضمن قانون الإجراءات الجزائية، مرجع سابق.

1:عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة ماجستير في الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة،2014، ص 57.

الخاتمة

الخاتمة:

لقد أصبح العالم يعيش في زمن من التطور التكنولوجي تزامنا معه ظهور ما يعرف بالإجرام المعلوماتي، هذا ما استوجب ظهور آليات ووسائل تقنية حديثة تتناسب وطبيعة هذه الجريمة لكشف الجريمة فظهر ما يعرف بالدليل الرقمي الذي فرض نفسه في مجال الإثبات الجنائي.

فمن خلال ما تم عرضه سابقا نخلص بأن:

إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات، وز التي تستهدف بشكل خاص المعلومات المختلفة في البيئة الرقمية.

تتميز الجرائم المعلوماتية بجملة من الصفات والخصائص تميزها عن غيرها من الجرائم التقليدية في ذاتية أركانها وأساليب ارتكابها والبيئة الافتراضية، واللامادية التي ترد عليها وخصوصية مرتكبيها.

لقد خول المشرع الجزائري عملية البحث والتحري في الجرائم المعلوماتية إلى الضبطية القضائية (الشرطة القضائية والدرك الوطني).

لقد نظم المشرع الجزائري كيفية الاستخلاص الدليل عن طريق إجراءات تتبع للوصول على هذه الغاية، و أهم هذه الإجراءات التي تم توضيحها من خلاق القوانين: التفتيش، المعاينة، الخبرة و هي يمكن اعتبارها أنها إجراءات تقليدية نظرا لفشل إجراءات البحث و التحري التقليدية، كان لابد من استحداث وسائل أخرى تتناسب و طبيعة الجريمة المستحدثة، و منه فقد استحدث المشرع الجزائري وسائل إجرائية و هي: اعتراض المراسلات و التسرب الذي جاء بهما القانون رقم 22/06 المؤرخ في 2006/12/20 المعدل و المتمم للأمر رقم 155/66 المتضمن قانون الإجراءات الجزائية الجزائري ، و من جهة أخرى تم استحداث الإجراء المتمثل في المراقبة الالكترونية الذي جاء به القانون رقم 04/09 المؤرخ في 20119/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

الدليل الجنائي الرقمي هو الدليل المستخلص من أجهزة الحاسب الآليوملحقاته، أو من شبكة الأنترنت أو أي جهاز آخر له خاصية المعالجة أو تخزين المعلومات.

كما أن الدليل الجنائي الرقمي يتميز عن باقي الأدلة الجنائية أخرى بأنه دليل علمي ذو طبيعة تقنية وأنه ذو طبيعة ثنائية وأيضا أنه دليل متنوع ومتطور.

لكي يكون للأدلة الجنائية الرقمية حجية في مجال الإثبات الجنائي يجب أن يكون قد تمالحصول عليه بطريقة مشروعة زيادة على ذلك يجب أن تكون هذه الأدلة غير قابلة للشك كما يجب أن يتم طرحها للمناقشة أمام جميع أطراف الدعوى العمومية وفي حالة عدم الأخذ بها يؤدي هذا إلى بطلان الإجراءات وعدم الأخذ بها كأدلة لإثبات الجريمة.

كما نلاحظ من خلال هذه الدراسة أن الإبقاء على سلطة القاضي الجنائي التقديرية في تقديره لهذه الأدلة العلمية والفنية على الرغم من علة شأنها ضرورية وحتمية لضمان تنقية الأدلة من الأخطاء وجعل الحقيقة العلمية حقيقة قضائية، ويظل القاضي هو الذي يحدد الحقيقة لأن من خلال هذه السلطة يستطيع أن يفسر الشك لصالح المتهم، وكذا استبعاد الأدلة الالكترونية التي يتم الحصول عليها بطرق غير مشروعة.

ومن خلال هذه النتائج نخلص إلى التوصيات التالية.

- وجوب الاهتمام بتدريب الخبراء والمحققينوالقضاء على التعامل مع الجرائم المعلوماتية.
- التوعية بشكل دائم عن طريق وسائل الإعلام عن مخاطر الجرائم المعلوماتية وأساليب المجرمين في ارتكابها.
- حرض بعض الدول التي لا تزال لم تضع بعد الاستخدام غير المشروع للحاسب الآلي داخل دائرة الإجرام أن تتسارع وتجرّم هذا السلوك وذلك من خلال الدخول في اتفاقيات ومعاهدات دولية تجرم هذا النوع من الإجراموذلك لضرورة تعزيز التعاون الدولي لمواجهة الجرائم المعلوماتية.
- إدراج موضوع الأدلة العلمية ومواد الأنظمة المعلوماتية في المقررات الدراسية سواء في الجامعات أو في معاهد التكوين الخاصة بالقضاء والشرطة لإزالة الغموض الذي يكتنف هذه الأدلة وحجيتها في الإثبات الجنائي.

- وجوب النص صراحة على الأدلة الالكترونية كأدلة إثبات في المجال الجنائي والاعتراف له بحجية قاطعة باعتبارها استثناء على سلطة القاضي الجنائي في تقدير الدليل.

قائمة المراجع

قائمة المصادر والمراجع:

أولا: المصادر

أ -القوانين.

1. القانون رقم 07/17 المؤرخ في 27 مارس 2017 جريدة رسمية عدد 20 صادرة بتاريخ 29 مارس 2017 المعدل و المتمم لقانون الإجراءات الجزائية الجزائري.
2. القانون رقم 04/09 المؤرخ في 14 شعبان 1430- 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتعلقة بالتكنولوجيا الإعلام والاتصال ومكافحتها جريدة رسمية عدد 47 صادرة بتاريخ 2009/06/16.

ب -الأوامر:

3. الأمر 02/15 المؤرخ في 07 شوال 1436 الموافق لـ 23 يوليو 2015 المعدل والمتمم للأمر رقم 66/155 المتضمن ق.إ.ج.ج.
4. الأمر رقم 155/66 المؤرخ في 18 صفر علم 136 الموافق لـ 08 يونيو 1966 يتضمن قانون الإجراءات الجزائية ج. ر.ج.ج عدد 48 الصادرة بتاريخ 11 يونيو 1966 المعدل والمتمم

ج-القرارات:

1. المحكمة العليا الجزائرية، قرار صادر بتاريخ 1991/01/29 الملف رقم 70690، المجلة القضائية، العدد الثالث، 1991.
2. المحكمة العليا الجزائرية، قرار صادر بتاريخ 1987/06/30 الملف رقم 50977، المجلة القضائية، العدد الثالث، 1991.
3. محكمة التمييز الكويتية 1976/06/30، المجلة القضائية العربية، الأمانة العربية لمجلس وزراء العدل العرب، العدد الأول، السنة الأولى، نيسان 1984.

ثانيا: المراجع.

أ المراجع العامة

1. إبراهيم بلعيات، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، بدون طبعة، دار الخلدونية، الجزائر، 2012.
2. ابن منظور جمال الدين، لسان العرب، دار الحياء التراث، لبنان، الجزء الثامن.
3. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص" ضد الأشخاص والجرائم ضد الأموال"، دار هومة، الجزائر، الجزء الأول، 2015.
4. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دون طبعة، دار النهضة العربية، 1996.
5. أمير فرح يوسف، القبض والتفتيش، الطبعة الأولى، مكتبة الوفاء القانونية، مصر، 2013.
6. بلهولي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة لنيل شهادة ماجستير، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة، 2011.
7. بوكرر رشيدة، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، ب ط، بيروت، 2012.
8. جباري عبد المجيد، دراسة قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دون طبعة، دار هومة، الجزائر، 2012.
9. حسين الجندي، شرح قانون الإجراءات الجزائية، دون طبعة، دون دار نشر، دون بلد نشر، 1990.
10. حسين محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الأنترنت، رسالة الدكتوراه في الحقوق، كلية الحقوق، جامعة عين الشمس.
11. شحط عبد القادر، نبيل صقر، الإثبات في مواد الجزائية، بدون طبعة، دار الهدى للطباعة والنشر والتوزيع، الجزائر.

12. شيماء عبد الغاني، الحماية الجنائية للتعاملات الإلكترونية، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، 2007.

13. عبد الفتاح عبد اللطيف الجبارة، الإجراءات الجنائية في التحقيق، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2015.

14. عبد الله أوهايبية، شرح قانون من قانون الإجراءات الجزائية الجزائري، دار الهومة، دون طبعة، الجزائر، 2004.

15. فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون، مصر، 2010.

16. فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، دون طبعة، مصر، 1999.

17. محمد زكي أبو عامر وعلي عبد القادر القهوجي، قانون العقوبات القسم الخاص، دار النهضة العربية، بدون طبعة، القاهرة، 1993.

18. محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي، ب. ط، ديوان المطبوعات الجامعية، الجزائر، 1999.

ب -المراجع المتخصصة

1. إبراهيمي سهام، الجريمة المعلوماتية، مذكرة تخرج لنيل الشهادة المدرسة العليا للقضاة، الدفعة الخامسة عشر، 2007/2004.

2. أحمد السمدان– النظام القانوني لحماية البرامج الكمبيوتر– مجلة حقوقي، الكويت،1987.

3. أحمد المناعسة، جرائم الحاسب الآلي والأنترنت (دراسة مقارنة)، ط 1، دار وائل للنشر والتوزيع، عمان،2001.

4. أحمد عبد الاله هلالي، حجية المحرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة) في بحوث مؤتمر القانون والكومبيوتر والأنترنت، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، 2004.

5. أسامة أحمد المناعسةوجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، عمان،2014.

6. أشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الإلكترونية ، دار الجامعة الجديدة للنشر، بدون طبعة، الإسكندرية، 2015.

7. براهيمي جمال، إجراءات التحقيق في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم الجنائية، جامعة مولود معمري، تيزي وزو، 2017،2018، كلية الحقوق والعلوم السياسية، قسم الحقوق.

8. بن فريدة محمد، الدليل الجنائي الرقمي وحجيّته أمام القضاء الجزائي (دراسة مقارنة)، مجلة سداسية متخصصة محكمة، السنة الخامسة، الجلد 09، عدد 01، بجاية، 2011، ص 289،297.

9. جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالأنترنت، دون طبعة، دار النهضة العربية، 1998.

10. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2011.

11. خالد عياد حلمي، إجراءات التحري والتحقيق في جرائم الكومبيوتر والأنترنت، ط 01، دار الثقافة للنشر والتوزيع، عمان، 2011.

12. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009.

13. رشاد خالد عمر، المشاكل القانونية والتقنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، ب ط، الإسكندرية، 2013.

14. سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، بدون طبعة، دار الكتب القانونية، مصر، 2014.

15. طوبي ميشال عيسى، التنظيم القانوني لشبكة الأنترنت، دار صادرة للمنشورات، بيروت، ط1، 2001.

16. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، ب ط، كلية الحقوق، جامعة الإسكندرية، 2006.

17. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.

18. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية لجرائم الكومبيوتر والأنترنت، ط 1، دار الفكر الجامعي، الإسكندرية، 2006، ص159.

19. عبد الفتاح مراد، شرح جرائم الكمبيوتر والأنترنت، بدون دار النشر، بدون طبعة.

20. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بأدلة رقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول للعلوم وأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.

21. علي محمود علي حمودة، الأدلة المحصلة على الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العربي الأول، الأدلة الجنائية والطب الشرعي المنظم بالرياض في الفترة الممتدة بين 122 و14 نوفمبر 2008.

22. عمر محمد أبو بكر يونس، الدليل الرقمي، دون طبعة، دون دار نشر، مصر، 2006.

23. فاطمة زهراء بوعناد، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول (بدون دار نشر)، الجزائر، 2013.

24. فتنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، دراسة تأصيلية تطبيقية (رسالة ماجستير)، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العلي، السعودية، 2012.

25. فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، ب ط، كلية الحقوق، جامعة الإسكندرية ،2016.

26. كمال محمد عواد، الضوابط الشرعية في الثبات والقانونية للأدلة الجنائية (في الفقه الإسلامي والقانون الوصفي)، الطبعة الأولى، دار الفكر الجامعي، مصر،2011.

27. محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، السعودية، 2004.

28. محمد عادل ريان، جرائم الحاسب الآلي وأمن البيانات بدون دار النشر، بدون طبعة، بيروت، 2002.

29. محمد عبد الله أبو بكر سلامة، موسوعة جرائم المعلومات لجرائم الكومبيوتر والأنترنت، ب ط، منشأة المعارف شركة جلال للطباعة، الإسكندرية، 2006.

30. محمد علي العريان، الجرائم المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2011،

31. محمد هماجهومجالهيتي، جرائم الحاسوب، ط 1، دار المناهج للنشر والتوزيع، ب ط، الإسكندرية، 2012.

32. مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، الطبعة الأولى، دار الكتب والوثائق القومية، المصرية، القاهرة، 2000.

33. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، مصر، 2009.

34. مصطفى محمد يوسف، المراقبة الإلكترونية عبر شبكة الأنترنت (دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية)، دار الكتب القانونية، بدون طبعة، مصر.
35. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكومبيوتر والأنترنت، ب ط، دار الكتب القانونية، مصر، 2006.
36. منبيلة هبة هروال، الجوانب الإجرامية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، ب ط، الإسكندرية، 2013.
37. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر، ط1، عمان، 2008.
38. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، بدون طبعة، 1992.
39. هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، إسبوط، ط1، 1994.
40. هلال عبد الله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ط1، 1997.
41. هلال عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، ب ط، دار النهضة العربية، القاهرة، 1997.
42. يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، جامعة محمد بوضياف، مسيلة، 2016،2017.
43. علي حسن طوابلة، التفتيش الجنائي على نظم الحاسوب والأنترنت، الطبعة الأولى، عالم الكتب الحديثة للنشر والتوزيع، الأردن، 2004.

ثالثا: المذكراتو الرسائل:

1. المويشير، تركي عبد الرحمن (2009)، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، الرياض، رسالة ماجستير، جامعة نايف الأمنية.

2. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس، 2004.

3. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمن، أطروحة لحصول على شهادة الدكتوراه في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر (1)، 2010، 2011.

4. بعرة سعيدة،الجريمة الإلكترونية على التشريع الجزائري (دراسة مقارنة)،تخصص قانون جنائي مذكرة مكملة من مقتضيات نبل شهادة الماستر في الحقوق كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016/2015

5. بن قدوم سوهيل، الدليل الرقمي في الإثبات الجنائي، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2017-2018.

6. سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، 2013/2012

7. سيد محمد بشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليلية تطبيقية، رسالة ماجستير في العلوم الشرطية تخصص التحقيق والبحث الجنائي، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2002.

8. شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة مكملة لنيل شهادة الماستر في الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2016-2017.

9. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة تخرج لنسل شهادة الماجستير، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، 2013، ص 88.

10. صيد خير الدين، مشروعية عمل الضبطية القضائية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمود خيضر، بسكرة، كلية الحقوق والعلوم السياسية، 2015/2014، ص عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة ماجستير في الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة،2014،

11. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير والعلوم الجنائية، 2011- 2012.

12. نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة 2015،2016.

رابعا: المجلات.

1. مجلة جامعة بابل، العلوم الإنسانية، المجلد14، العدد6، 2007، ص11

خامسا: المداخلات والملتقيات.

1. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية المنعقدة في 2009/10/28،29، الأكاديمية للدراسات العليا، طرابلس،

2. نصر الدين مروك، محاضرات في الإثبات الجنائي (النظرية العامة للإثبات الجنائي)، الجزء الأول، دار الهومة، الجزائر، 2003،

سادسا: باللغة الأجنبية.

1. L'article (100) sitruple «… autorités peuvent intercepter et la transcrire de correspondances émises par la voie des télécommunications..» voir la loi N° 2001،1062 ,de 15/11/2001, portant code de procédures pénales français jore 16/11/2001

2. eoghan Casey, file system forensic analysis, Pearson education (INC), unites states America,2005, p06.
3. the Technical Working Group for Electronic Crime Scene Investigation, Electronic Crime Scene Investigation of justice the unites states of America,2001.

سابعا: المواقع الالكترونية.

www.startimes.com

قائمة المحتويات

الفهرس:

شكر: .....

إهداء: .....

مقدمة: ..... أ

الفصل الأول: الجريمة الإلكترونية و إجراءات التحقيق فيها 11

المبحث الأول: مفهوم الجريمة الإلكترونية: 12

المطلب الأول: تعريف الجريمة الإلكترونية: 12

الفرع الأول: التعريف القانوني. 13

الفرع الثاني: التعريف الفقهي. 15

المطلب الثاني: خصائص الجريمة الإلكترونية. 17

الفرع الأول: أسلوب ارتكاب الجريمة المعلوماتية: 18

الفرع الثاني: خصوصية مجرمي المعلوماتية: 19

الفرع الثالث: الجريمة الإلكترونية عابرة الحدود. 20

الفرع الرابع: صعوبة اكتشافها وإثباتها. 21

المطلب الثالث: أثر الطبيعة القانونية الخاصة بالجريمة الإلكترونية على الإثبات الجزائي. 22

الفرع الأول: الطبيعة القانونية للمعلومات: 22

الفرع الثاني: أثر الطبيعة الخاصة بالجريمة الإلكترونية على الإثبات الجزائي: 24

المبحث الثاني: التحقيق في الجريمة. 27

المطلب الأول: الأجهزة المكلفة بالبحث والتحري في الجريمة المعلوماتية 27

الفرع الأول: التعريف اللغوي. 27

الفرع الثاني: التعريف الاصطلاحي. 28

المطلب الثاني: الإجراءات التقليدية في جمع الأدلة الجنائية الرقمية..... 29
الفرع الأول: التفتيش..... 29
الفرع الثاني: المعاينة..... 43
الفرع الثالث: الخبرة..... 47
المطلب الثالث: الإجراءات الحديثة في جمع الأدلة الجنائية الرقمية..... 52
الفرع الأول: التسرب..... 53
الفرع الثاني: اعتراض المراسلات..... 56
الفرع الثالث: المراقبة الإلكترونية..... 61
الفصل الثاني: القيمة القانونية لدليل الرقمي و تقديره أمام القضاء..... 62
المبحث الأول: ماهية الدليل الرقمي كدليل إثبات في المواد الجنائية..... 67
المطلب الأول: ماهية الدليل الإلكتروني..... 67
الفرع الأول: تعريف الدليل الرقمي وتقسيماته..... 67
المطلب الثاني: خصائص الدليل الرقمي..... 70
الفرع الثاني: الدليل الرقمي دليل تقني..... 71
الفرع الثالث: صعوبة التخلص من الدليل الرقمي..... 72
الفرع الرابع: الدليل الرقمي متنوع ومتطور..... 74
المطلب الثالث: مراحل وأنواع الدليل الرقمي في إثبات الجنائي..... 75
الفرع الأول: مراحل الدليل الرقمي في إثبات الجنائي..... 75
الفرع الثاني: أنواع وأمثلة الدليل الرقمي..... 79
المطلب الثالث: مشروعية الدليل الرقمي من حيث الوجود..... 82
الفرع الأول: المقصود بمشروعية الوجود..... 82

الفرع الثاني: موقف المشرع الجزائري من الدليل الرقمي. 83
المبحث الثاني: تقدير الدليل الرقمي 85
المطلب الأول: سلطة القاضي الجنائية بالدليل الرقمي..... 85
الفرع الأول: ماهية اقتناع القاضي الجزائي بالدليل الرقمي. 85
الفرع الثالث: الضوابط التي تحكم الاقتناع الشخصي بالدليل الرقمي. 93
المطلب الثاني: مشكلات الاختصاص القضائي في الجرائم المعلوماتية 106
الفرع الأول: الاختصاص القضائي الداخلي. 107
الفرع ثاني: الاختصاص القضائي الدولي. 109
المطلب الثالث:شروط قبول الدليل الرقمي..... 116
الفرع الأول: مصداقية الدليل الرقمي في الإثبات. 116
الفرع الثاني: مناقشةالدليل الرقمي. 120
الخاتمة:..... 127
قائمة المصادر والمراجع: 131
ملخص: .....

ملخص:

الجرائم المعلوماتية وإن كانت تبدو أنها منظمة بشكل كافي من المشرع الجزائري إلا أنها تثير العديد من الصعوبات وخصوصا ما يتعلق بالإثبات وشخص الجاني وخصوصا حينما يكون مقيما خارج الدولة لأنه من الصعب تحديد المسؤول جنائيا ويظهر ذلك جليا في حالة وقوع جريمة على شبكة الأنترنيت، لذلك يجب على التشريع ألا يكون قاصرا على تنظيم ما هو موضوعي فقط إنما عليه أن يصاحب ما هو موضوعي بما هو إجرائي لكي يتم تحقيق نوع من التوازن بين الحق وطريقة الوصول إليه.

Résumé :

Les crimes d'information, bien qu'ils semblent suffisamment organisés par le législateur algérien, soulèvent de nombreuses difficultés, notamment en ce qui concerne la preuve et la personne du coupable, en particulier lorsque celui-ci réside en dehors de l'État en raison de la difficulté d'identifier un officier criminel. Ainsi, la législation ne doit pas se limiter à l'organisation de ce qui est uniquement objectif, mais elle doit accompagner ce qui est matériel et procédural pour parvenir à une sorte d'équilibre entre le droit et le moyen d'y accéder.