

جامعة عمار ثليجي - الأغواط -

كلية الحقوق والعلوم السياسية

قسم الحقوق

مشروعية الدليل التقني في الإثبات الجنائي

مذكرة مكملة لنيل شهادة الماستر تخصص القانون الجنائي والعلوم الجنائية

إشراف الدكتور :

* ملياني عبد الوهاب

من إعداد الطالب :

سعدون أحمد

لجنة المناقشة :

- الدكتورة عكاكة فاطمة الزهراء..... رئيسا

- الدكتور ملياني عبد الوهاب..... مشرفا و مقورا

- الدكتور بطيمي حسين..... مناقشا و ممتحنا

السنة الجامعية : 2020-2019

جامعة عمار ثليجي – الأغواط –

كلية الحقوق و العلوم السياسية

قسم الحقوق

مشروعية الدليل التقني في الإثبات الجنائي

مذكرة مكملة لنيل شهادة الماستر تخصص القانون الجنائي و العلوم الجنائية

إشراف الدكتور :

* ملياني عبد الوهاب

من إعداد الطالب :

سعدون أحمد

السنة الجامعية : 2019-2020

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

شكر و تقدير

بداية الحمد و الشكر لله الواحد الأحد ، الذي أعاني و بإذنه وفقني
لإنجاز هذا البحث البسيط.

كما أتقدم بجزيل الشكر و العرفان إلى كل أساتذة و موظفي قسم
الحقوق بجامعة عمار ثليجي بالأغواط ، نظير الجهودات المبذولة لنشر
رسالة العلم النبيلة ، كما أتقدم بجزيل الشكر إلى الدكتور / ملياني عبد
الوهاب ، الذي أشرف على هذا البحث المتواضع ، و رافقنا منذ البداية
بكل جدية و اهتمام كبيرين دون تردد مصرا على انجاز هذا العمل بكل
صدق و أمانة ، لا يسعني أن أقول له إلا جزاك الله كل خير ، كما أتقدم
بالشكر إلى لجنة المناقشة التي وافقت على مناقشة هذا الموضوع ، كما لا
يفوتني أن أشكر جميع زملائي الطلبة لما قدموه لي من مساعدة طيلة المشوار
الدراسي .

إهداء

أهدي هذا العمل المتواضع إلى الوالدين الكريمين أطال الله في
عمريهما ، و زوجتي الغالية " إيمان " و إخوتي و أخواتي و أبناء الأخت
(خير الدين ، خلود ، ضحى) و الأصدقاء و الزملاء ، خاصة رئيسي في
العمل السيد / علي حناشي ، و الأخ الذي لم تلده أمي " بودية نصر الدين
" و إلى الدكتور المشرف " ملياني عبد الوهاب " و كل أساتذة قسمي
الحقوق بجامعة الأغواط و تيارت .

مقدمة

مقدمة

لقد شهد العالم تطورا تكنولوجيا هائلا في العديد من المجالات منذ اختراع الحاسب الآلي ، الذي يتضمن تقنيات عالية أدت إلى الاعتماد عليه في مجالات العمل المختلفة ، خاصة مع استمرار التطور الحاصل على هذا الجهاز بسرعة واستمرار ، ولقد لامست هذه الإضافات الحياة العامة و الخاصة للأفراد ، بحيث أصبحت مرتبطة بها ارتباطا وثيقا نتيجة اعتماد الدول عليها في تسير شؤونها ، فقد تم اعتماده بشكل كبير في المرافق العمومية و المؤسسات على اختلاف أشكالها و أنواعها ، لأجل تحسين و سرعة سيرها و كذا تقديم الخدمات لمواطنيها ، و مثال ذلك ظهور الحكومة الالكترونية على سبيل المثال ، كما أدى التطور الهائل الحاصل على تقنية الاتصالات مع تطور تقنيات الحاسوب إلى اعتماد الحكومات و الأفراد اعتمادا كبيرا على تنفيذ العديد من المهام نتيجة لخصيات عديدة منها السرعة و التكلفة الأقل ، مع التزايد المتواصل لهذه التقنيات كلما تطورت خدماتها و ظهرت تقنيات أخرى جديدة¹.

و مع اعتماد تقنية المعلومات و الاتصالات في حياة الأفراد و تعاملاتهم اليومية نتج عن ذلك استخدام إيجابي و سلبي لتلك التقنيات ، نتيجة لما تتضمنه من معلومات و خصوصيات لها قيمة بالنسبة للأشخاص الطبيعية و المعنوية العامة و الخاصة ، الأمر الذي أدى بالمجرمين إلى استغلال هاته التقنيات لتنفيذ أغراضهم الإجرامية باعتبارها أسهل و أقل خطورة لاقتراف جرائمهم ، من خلال ارتكاب جرائم تقليدية بواسطة تقنية حديثة ، أم ابتداء جرائم جديدة لا تقع

1 - ملياني عبد الوهاب ، أمن المعلومات في بيئة الأعمال الالكترونية ، أطروحة دكتوراه في القانون العام ، جامعة

أبو بكر بلقايد تلمسان، الجزائر، السنة 2016-2017 ، ص 2.

مقدمة

على قالب الجرائم التقليدية و التي اصطلح عليها بالجرائم الالكترونية ، هذه الجرائم ارتبطت بتقنية نظم المعلومات و الاتصالات¹.

و بناءا على ذلك ، تطورت نظرية الإثبات في وسائل و طرق الإثبات الجنائي و في طريقة التعامل مع الأدلة المستخلصة من التحقيقات ، خاصة لما تتميز به هذه الأدلة من خصائص و مميزات ، لكونها مرئية و ذات خصائص مرتبطة بالبيئة التقنية التي تنشأ فيها ، و هو ما يتطلب وسائل و أساليب تناسبها للاستقصاء عنها أو استخلاصها ، أو لحفظها و حمايتها من التلف الضياع ، وفق إجراءات محددة مسبقا من طرف المشرع ، بالإضافة إلى ضوابط تحكم هذه الإجراءات و يجب على الجهات القائمة بالتحقيق التقيد بها ، حتى تكون هذه الأدلة التقنية متوافقة مع طبيعة الجرائم المرتكبة ، مع مراعاة اعتبارات العدالة و ضمانات المتهم في مرحلتي التحقيق و المحاكمة ، ثم الحفاظ على الحقوق و الحريات العامة و الخاصة .

ثم لابد من ضمان قبول هذه الأدلة من قبل المحكمة ، ليس باعتبارها صالحة للإدانة ، بل باعتبارها أدلة قانونية مشروعة كافية لتكوين قناعة القاضي سواء بالإدانة أو البراءة .

لما سبق ذكره ، و يجب علينا النظر في مشروعية الأدلة التقنية من جانبها الإجرائي من جهة ، و مدى كفايتها في تكوين قناعة القاضي الجنائي من جهة

1 - ملياني عبد الوهاب ، المرجع السابق ، ص 3.

مقدمة

أخرى ، بالإضافة إلى دورها في إثبات جرائم تقنية المعلومات عامة ، و من هذا المنطلق تظهر لنا أهمية البحث التي نوجزها في النطاق الأساسية التالية :

- التعرف على الإجراءات المستحدثة من قبل المشرع لمواجهة جرائم تقنية المعلومات ، مع الوقوف على مدى كفاية الإجراءات التقليدية في مواجهة الجرائم الحديثة الناجمة عن تقنية المعلومات .

- الوقوف على مدى توفيق المشرع الجزائري في الإجراءات المستحدثة لمواجهة هذا النوع من الجرائم ، و مدى اعتمادها من قبل القاضي الجنائي في تكوين قناعته .

- من خلال تناول الجوانب الإجرائية فيما يتعلق بالدليل التقني ، و مختلف الاجراءات التقليدية و المستحدثة الخاصة بالبحث عنه ، و كذا الآليات المخصصة للوقاية من الجرائم المعلوماتية و مكافحتها ، التي سنوضحها من خلال تطرقنا لموضوع الدراسة.

و عليه يمكننا تحديد الأهداف التي نتطرق إليها الدراسة في النقاط التالية:

- حيث نهدف إلى الوقوف على مفهوم الدليل التقني ، و تحديد خصائصه عن باقي الأدلة الأخرى ، مع إبراز فاعليته في إثبات جرائم تقنية المعلومات .

مقدمة

- تحديد الآليات الخاصة بالتحري و التحقيق في جرائم المعلوماتية،
والأساليب المعتمدة لاستخلاص الدليل من تقنية المعلوماتية .

- التعرف على الأجهزة المساعدة لجهات التحقيق و فاعليتها في
استخلاص الدليل التقني .

ومن هنا يظهر لنا جليا سبب اختيارنا لهذا الموضوع حيث يعتبر من
أهم المواضيع التي ينبغي توضيحها ، خاصة في ظل تجريم المشرع الجنائي
الاعتداء على المعلوماتية أو ارتكاب جرائم تقليدية بواسطتها .

حيث أن عملية الإثبات الجنائي للجرائم المعلوماتية تركز على الدليل التقني
باعتباره وسيلة مستحدثة لإثبات هذا النوع من الجرائم .

هذا بالإضافة إلى الانتشار الواسع لهذا النوع من الجرائم في المجتمع
الجزائري مؤخرا بصورة ملفتة للانتباه ، مما يستوجب معرفة إجراءات البحث
و التحري المقررة من طرف المشرع لمكافحتها .

أضف إلى ذلك دور الدليل الجنائي في إثبات الجرائم ، كونه الأداة الفعالة
للكشف عن مرتكبي الجرائم ، حيث بدونه يفلت الفاعلين من العقاب ، ما يؤدي
إلى ارتفاع نسبة الجرائم ، ناهيك عن الخسائر المادية الناجمة عنها ، هذا
بالنسبة للأسباب الموضوعية أما بالنسبة للأسباب الشخصية التي دفعتني إلى
اختيار هذا الموضوع ، فتعود في مجملها إلى الاهتمام في مجال المعلوماتية
بصفة عامة من جهة ، و من جهة أخرى الرغبة في معرفة الإجراءات الخاصة

مقدمة

باستخلاص الدليل التقني و كيفية القيام بها ، لكون الموضوع له علاقة وطيدة بوظيفتي .

إضافة إلى أنني تلقيت تكوين سابقا في مجال المعلوماتية درجة تقني مستغل المعلوماتية .

و مما سبق تفصيله كانت هذه الدراسة القانونية التحليلية معتمدة أساسا على المناهج التي تتناسب و طبيعة موضوع الدراسة و مع المعطيات المبينة أعلاه كي تتلاءم مع الأهداف المرجوة ، و نظرا لخصوصية الموضوع اعتمدنا على مجموعة من المناهج المعتمدة في الدراسات القانونية التي تكمل بعضها البعض للإحاطة بكل جوانب البحث محل الدراسة لهذا اعتمدنا المناهج التالية :

المنهج الوصفي الذي يصف الظاهرة ، لفهم أصلها و حقيقتها العلمية و القانونية ، كذلك **المنهج الاستدلالي** من خلال قراءة النصوص القانونية لمعرفة الإجراءات المستحدثة لاستخلاص الدليل التقني ، مع تحديد الجهات المكلفة بذلك و الأجهزة المساعدة لها ، إضافة إلى **المنهج الاستقرائي** لملاحظة و دراسة الجزئيات حتى يتسنى لنا تكوين فكرة عامة عن الموضوع .

و وفقا لما سبق ، و بالنظر إلى طبيعة الموضوع ، خاصة اعتماد تقنيات المعلومات في المعاملات اليومية للجميع بما فيها الدولة ، هذا الذي رافقه عدة مسائل قانونية لمواكبتها من حيث حمايتها و قمع الجرائم المرتكبة عليها ، و من بين المسائل القانونية المطروحة تلك المتعلقة بالبحث و التحري عن الجرائم المعلوماتية التي تركز أساسا في إثباتها على الدليل التقني المتميز عن باقي أدلة

مقدمة

الاثبات الأخرى ، حيث خصه المشرع بجملة من الإجراءات المستحدثة ، و من منطلق ما سبق يمكننا طرح الإشكالية التالية : هل يمكن الإقرار بنجاعة الاعتماد على الدليل التقني للوصول إلى مكافحة جنائية فعالة في جرائم المعلوماتية ؟

و لعرض أفكار الموضوع محل الدراسة وجب علينا دراسة البحث وفق خطة منهجية قسمناها إلى فصلين رئيسيين تناولنا في الفصل الأول الطبيعة القانونية للدليل التقني ، حيث تطرقنا في المبحث الأول الإطار المفاهيمي للدليل التقني، و في المبحث الثاني المكانة الإجرائية للدليل التقني في الإثبات الجنائي .

أما الفصل الثاني فنعالج فيه القواعد الإجرائية الكفيلة بالحصول على الدليل التقني ، حيث تناولنا في المبحث الأول القواعد الإجرائية التقليدية الكفيلة بالحصول على الدليل التقني، وفي الثاني القواعد الإجرائية الحديثة للحصول على الدليل التقني .

و خلصت إلى خاتمة تضمنتها مجموعة من النتائج و الاقتراحات حول الموضوع محل الدراسة .

الفصل الأول الطبيعة القانونية للدليل التقني

قبل الخوض في دراسة موضوع مشروعية الدليل التقني في الإثبات الجنائي ، وجب علينا التطرق إلى تحديد طبيعته القانونية من خلال تحديد الإطار المفاهيمي له ، و من ثم إبراز مكانته الإجرائية ضمن الإثبات الجنائي ، و هو ما سنتناوله ضمن الفصل الأول .

المبحث الأول: الإطار المفاهيمي للدليل التقني .

تتركز عملية الإثبات الجنائي للجرائم المعلوماتية على الدليل التقني الجنائي ، ذلك أنه الوسيلة الأساسية لإثبات هذا النوع من الجرائم ، و هو محور اهتمام موضوع بحثنا هذا ، لذا سنتناول في هذا المبحث مفهوم الدليل التقني (المطلب الأول) ، و نتناول محل الدليل التقني ضمن (المطلب الثاني).

المطلب الأول : مفهوم الدليل التقني

الدليل التقني مصطلح مركب من كلمتين ، الأولى تتمثل في الدليل و الثانية هي التقني ، و على هذا الأساس سنخصص (الفرع الأول) لتعريف الدليل و (الفرع الثاني) خصصناه لتعريف التقنية ، ليكون (الفرع الثالث) لتحديد تعريف الدليل التقني و مميزاته .

الفرع الأول : تعريف الدليل

أولاً - الدليل لغة : هو المرشد و ما يتم به الإرشاد، و ما يستدل به ، و الدليل، الدال، و الجمع أدلة ، و كذلك يعني تحقيق الحق بالبينه ، و البينة هي الدليل أو الحجة ¹.

1 - جميل صليبا ، المعجم الفلسفي للمصطلحات القانونية ، دار المناهج للنشر و التوزيع ، ط 1، الأردن، 1990،

ثانيا - الدليل اصطلاحا : هو ما يلزم من العلم به علم شيء آخر، و غايته أن يتوصل العقل إلى التصديق اليقيني فيما كان يشك في صحته ، أي التوصل به إلى معرفة الحقيقة.¹

ثالثا - الدليل قانونا : أغلب التشريعات و منها التشريع الجزائري ، نجد أنها لم تضع تعريف للدليل الجنائي ، و تركت المسألة للفقهاء ، إذ عرفوا الدليل الجنائي بأنه " معلومة يقبلها المنطق و العقل يتم الحصول عليها بإجراءات قانونية و المسائل الفنية أو المادية أو القولية ، و يمكن استخدامها في أي مرحلة من مراحل التحقيق و المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه .²

الفرع الثاني : تعريف التقنية

الدليل التقني يتكون من مصطلحين الأول يتمثل في الدليل و الثاني هو التقنية ، و بعد تعريف الدليل في الفرع السابق نتطرق من خلال هذا الفرع إلى التعريف بالتقنية .

أولا - التقنية لغويا

تتناظر كلمة (تقنية) في اللغة الفرنسية (technologie) ، و تتكون من مقطعين (Techno) و تعني أسلوب مختص بفن أو مهنة أو حرفة ، و (Logie) و تعني العلم ، و يقابله في اللفظ الانجليزي (Technology) الذي يأخذ نفس المعنى ، و عليه فإن المفهوم اللغوي للتقنية هو علم الحرف و الصناعات .

1 - محمد أمين البشري ، الأدلة الجنائية الرقمية مفهومها و دورها في الإثبات ، المجلة العربية للدراسات الأمنية و التدريب ، المجلد 17 العدد 33 ، الإمارات العربية المتحدة ، سنة 2002 ، ص 106 .

2 - محمد أمين البشري ، التحقيق في الجرائم المستحدثة ، جامعة نايف العربية للعلوم الأمنية ، مركز الدراسات و البحوث ، الرياض سنة 2004 ، ص 231 .

و عرفت التقنية أيضا بأنها المعدات و الأجهزة و المكائن و المعادلات الفنية التي يمكن توظيفها في تأدية مهمة أو وظيفة.¹

ثانيا - التقنية قانونا

يقصد بالتقنية الحديثة في هذه الدراسة تلك الأجهزة الخاصة بالإثبات للأدلة الجنائية و التي تتيح باستخدامها إنجاز أعمال و نتائج هامة في الإثبات الجنائي.²

الفرع الثالث : استخلاص تعريف للدليل التقني و تحديد مميزاته

نتناول من خلال هذا الفرع تعريف الدليل التقني في العنصر الأول ، و من ثم تحديد مميزاته في العنصر الثاني و فق ما يلي :

اولا - تعريف الدليل التقني

يعرف الدليل التقني بأنه " معلومات يقبلها المنطق و العقل و يعتمدها العلم ، يتم الحصول عليها وفق إجراءات قانونية و علمية بترجمة البيانات الحاسوبية المخزنة في أجهزة النظم المعلوماتية و ملحقاتها و شبكات الاتصال و يمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه" ، أو أنه " الدليل المأخوذ من أجهزة الكمبيوتر و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة و هي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات و الأشكال و الرسوم و ذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون ."³

الملاحظ على هذه التعريفات السابقة أن منها من اعتبر الدليل التقني كل معلومات يتم إعدادها أو تخزينها بشكل رقمي كما لو كانت محملة على وسيط معين يمكن قراءته عن

1 - فيصل مساعد العنزي ، أثر الإثبات بالوسائل التقنية الحديثة على حقوق الإنسان ، رسالة ماجستير في العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2007 ، ص 10 .

2 - نفس المرجع السابق ، ص 11 .

3 - ملياني عبد الوهاب ، المرجع السابق ، ص 246.

طريق الآلة و التي عند تنفيذها في نظام المعلومات تؤدي إلى إنجاز وظيفة ما ، و هو بهذا يتلاقى مع البرنامج أي لا وجود للتفرقة بين الدليل التقني و البرنامج ، فبالرغم من أن كلا المكونان يتفقان في مسألة الالتصاق بتقنية المعلومات من حيث تكوينهما ، فهما عبارة عن آثار معلوماتية يتركها مستخدم الانترنت ، و يظهران في شكل رئيسي هو الشكل الرقمي ، فالمعلومات داخل النظام المعلوماتي و مهما كان شكلها فهي تتحول إلى طبيعة رقمية ، من خلال تقنية الترقيم التي تتعلق بترجمة أو تحويل أي مستند معلوماتي مؤلف من نصوص أو صور أو أصوات أو بيانات إلى نظام ثنائي في تمثيل الأعداد قوامه الرقمان الواحد و الصفر ، إلا أن الفرق بين الدليل التقني و البرنامج يكمن في الوظيفة التي يؤديها كل واحد منهما ، فالأخير له دور في القيام بمختلف العمليات التي يحتويها النظام ، ذلك أنه لا يقوم بعمله إلا عن طريق مجموعة من البرامج عن طريق إعطاء أوامر بذلك ، أما الدليل التقني فدوره يكمن في معرفة كيفية حدوث جرائم الاعتداء على النظام المعلوماتي ، لأجل نسبتها إلى مرتكبها .¹

في حين ذهب التعريف إلى اعتبار الدليل التقني للأدلة المستخلصة من الكمبيوتر ، و عليه فالمعلومات التي تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية أي التي لا زالت لم تفصل عن أجهزة الحاسب الآلي و الخوادم و المضيفات و الشبكات بمختلف أنواعها ... لا تصلح لأن توصف بالدليل التقني و هو قول غير دقيق في نظرنا ، هذا بالإضافة إلى أن الكمبيوتر ليس وحده من يقوم بالمعالجة الآلية للمعلومات من حيث ان الهواتف المحمولة و البطاقات الذكية كبطاقة الذاكرة الخارجية تقوم بالدور ذاته و لهذا فإن قصر الدليل التقني في الكمبيوتر و أجهزته يعد تعريفا يشوبه النقصان .

و لما سبق نقدم تعريف للدليل التقني بأنه " المعلومات المخزنة في النظام المعلوماتي بجميع مكوناته ، أو المتنقلة عبره بأي طريقة إلكترونية ، و التي من الممكن تجميعها و تحليلها باستخدام تكنولوجيا خاصة لتظهر في شكل مخرجات ورقية أو إلكترونية أو

1 - ملياني عبد الوهاب ، المرجع السابق ، ص 246.

معروضة على شاشة النظام أو غيره من الأشكال ، لإثبات وقوع الجريمة في إطار الإجراءات المعمول بها " ¹.

و لما كان هذا الدليل يتكون من معطيات و معلومات في شكل إلكتروني غير ملموس و غير محسوس متواجدة في الأجهزة و المعدات ، فهو يحتاج إلى جوانب تقنية للتعامل معه ، و كدليل يحتاج إلى بيئته التقنية للبحث عنه و استخراجه ، و لذلك فهو دليل يخضع للمنطق العلمي.

ثانيا - مميزات الدليل التقني : نتناول أهم مميزات الدليل التقني وفق ما يلي :

أ- الدليل التقني دليل رقمي : إن الأدلة المستنبطة من البيئة التقنية هي أدلة رقمية ، لكون البيئة التقنية تنتج نبضات رقمية على القطع الصلبة التي تشكل الحاسوب ، و لكي يكون هناك دليل رقمي يجب أن يكون مستنبطا من البيئة التقنية ، و إلا لا وجود لدليل رقمي خارج البيئة التقنية ، و هي في إطار جرائم المعلوماتية ممثلة في العالم الرقمي أو العالم الافتراضي و هو العالم الكامن في الحاسوب و المضيفات و الخوادم و الشبكات التي يتم تداول الحركة فيه عبرها .

و نتيجة لذلك فإنه اكتسب مميزات عن الدليل المادي من حيث قابليته للنسخ ، بحيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل و لها نفس القيمة العلمية ، و هذه الخاصية لا تتوفر في أنواع الأدلة الأخرى مما يشكل ضمانا شديدة الفعالية للحفاظ على الدليل ضد الفقد و التلف و التغيير ، بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله و ذلك لإمكانية مقارنته بالأصل باستخدام البرامج و التطبيقات الصحيحة ².

1 - ملياني عبد الوهاب ، ص 247.

2 - نفس المرجع السابق ، ص 122.

ب - الدليل التقني دليل إلكتروني : إطار الإثبات الجزائي يعتبر الدليل التقني ذلك الدليل المأخوذ من أجهزة الحاسب الآلي و ما شابهها و الذي يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ، يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة ، و يتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء ، و هو مكون رقمي في أشكال متنوعة ، مثل : النصوص المكتوبة أو الصور و الأصوات و الأشكال و الرسوم ، و عليه فإن الدليل التقني هو دليل إلكتروني¹.

ج - الدليل التقني يصعب التخلص منه : إن القاعدة التي تسري على كافة هيكلية تكنولوجيا المعلومات ، هي أنه كلما حدث اتصال بتكنولوجيا المعلومات عن طريق ادخال بيانات إلى ذلك العالم ، فإنه من الصعب التخلص منها و لو كان ذلك باستخدام أقوى أدوات الإلغاء ، فمحاولة التخلص من الأدلة باستخدام خصائص التخلص من الملفات في الحاسوب كخاصية (Remove.Delet.Erase...) لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة إذ تتوفر برمجيات ذات الطبيعة التقنية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب².

د - الدليل التقني ذو طبيعة رقمية ثنائية : كما اشرنا سابقا أن الدليل التقني هو دليل رقمي لكونه وليد البيئة التقنية دون سواها ، فإن الآثار التي يتركها مستخدم النظام المعلوماتي تشمل الرسائل المرسله منه أو التي تم استقبالها و كافة الاتصالات التي تمت من خلال الحاسب الآلي سواء كانت في شكل نصوص أو حروف أو أرقام أو صور أو فيديو تتحول إلى صيغة رقمية ، حيث تركز تكنولوجيا المعلوماتية الحديثة على تقنية الترميز التي تعني ترجمة أو تحويل أي معلومات إلى نظام ثنائي في تمثيل الأعداد يفهمه

1 - محمد نافع فالح رشدان العدوانى ، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية (دراسة مقارنة بين القانونين الكويتي و الأردني) ، رسالة ماجستير في القانون العام ، جامعة الشرق الأوسط ، سنة 2015 ، الأردن، ص 20 .

2 - سعيداني نعيم ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة ماجستير في العلوم القانونية ، تخصص علوم جنائية ، جامعة الحاج لخضر باتنة ، الجزائر ، ص124.

الحاسب الآلي ، قوامه الرقمان (0) ، (1) فأى شيء في العالم الرقمي يتكون من الصفر و الواحد ، فالكتابة مثلا في النظام الرقمي ليس لها الوجود المادي الذي نعرفه و إنما مجموعة من الأرقام التي ترجع إلى النظام الثنائي ، و هما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها و تفاعلها من الطاقة.

إن هذه الخصائص جعلت منه الدليل الأفضل لإثبات الجرائم المعلوماتية لأنه من طبيعة الوسط الذي ارتكبت فيه ، سواء كانت مرتكبة بواسطة نظام المعالجة الآلية أو كانت تشكل اعتداء و مساسا على نظام المعالجة الآلية.¹

المطلب الثاني : أنواع الأدلة التقنية و تقسيماتها

تعريف الدليل التقني يحتم علينا تحديد أنواعه و أشكاله حتى يتسنى فهم الهيئة التي يتخذها للحكم على قيمته القانونية فيما بعد ، لذا سنتطرق إلى أنواعه ، ثم الأشكال التي يبدو عليها على النحو التالي :

الفرع الأول - أنواع الدليل التقني : يمكن تقسيم الدليل التقني لنوعين رئيسيين هما :

أولاً- أدلة أعدت لتكون وسيلة إثبات: وهذا النوع من الأدلة الرقمية يمكن إجماله فيما يأتي:

أ- السجلات التي تم إنشاؤها بواسطة الآلة تلقائياً ، و تعتبر هذه السجلات من مخرجات الآلة التي لم يساهم المستعمل في إنشائها مثل سجلات الهاتف و فواتير أجهزة الحاسب الآلي.

ب- السجلات التي جزء منها تم حفظه بالإدخال و جزء تم إنشاؤه بواسطة الآلة و من أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة و تتم معالجتها من خلال برنامج خاص، مثلا

1 - سليمان غازي العتيبي ، درجة توافر البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة ، رسالة ماجستير ، جامعة نايف للعلوم الأمنية ، كلية الدراسات العليا ، السعودية ، 2010 ، ص 35 .

كإجراء العمليات الحسابية على تلك البيانات.¹

ثانيا - أدلة لم تعد لتكون وسيلة إثبات : و هذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص ، أي أنها أثر يتركه الجاني دون أن يكون راغبا في وجوده ، و يسمى هذا النوع من الأدلة بالبصمة الرقمية ، و هي ما يمكن تسميته أيضا بالآثار المعلوماتية الرقمية ، و هي تتجسد في الآثار المعلوماتية الرقمية ، و هي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسله منه أو التي يستقبلها و كافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.

و الواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل من صدر عنه ، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة و لو بعد فترة زمنية من نشؤها ، فالاتصالات التي تجرى عبر الانترنت و المرسلات الصادرة عن الشخص أو التي يتلقاها ، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك.² و تبدو أهمية التمييز بين هذين النوعين فيما يأتي :

أ- حيث أن النوع الثاني من الأدلة التقنية هو الأكثر أهمية من النوع الأول لكونه لم يُعد أصلا ليكون أثرا لمن صدر عنه ، و لذا فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجريمة و مرتكبها.

يتميز النوع الأول من الأدلة الرقمية بسهولة الحصول عليه لكونه قد أُعد أصلا لأن يكون دليلا على الوقائع التي يتضمنها ، في حين يكون الحصول على النوع الثاني من الأدلة بإتباع تقنية خاصة لا تخلو من صعوبة و تعقيد.

ب- و كما أن النوع الأول قد أُعد كوسيلة إثبات لبعض الوقائع فإنه عادة ما يُعتمد إلى حفظه للاحتجاج به لاحقا و هو ما يقلل من إمكانية فقدانه ، و هذا على عكس النوع الثاني

1 - أمحمد طارق الجملي ، مجلة الحقوق ، المجلد 12، العدد1، جامعة بنغازي ليبيا ، بدون سنة النشر ، ص 46.

2 - نفس المرجع السابق ، ص 46.

حيث لم يُعد ليحفظ و هو ما يجعله عرضة للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز مثلاً.¹

الفرع الثاني : تقسيمات الأدلة التقنية بحسب مكان وجودها

يمكن تقسيمها إلى الأنواع الأساسية التالية :

أولاً- الورق و مخرجات الطابعة :

غالباً ما تترك الجرائم الواقعة على الأموال أو على الأشخاص آثار من الأوراق والمستندات بالغة الأهمية التي يتم حفظها في الحاسب الآلي ، فالكثير ممن يقومون بطباعة المعلومات بهدف المراجعة أو التأكد من الشكل العام أو صحة المستند موضوع الجريمة ، فالطابعات و أجهزة الحاسب الآلي ذات السرعة الفائقة تطبع الكثير من الأوراق في وقت يسير ، لذلك يعد الورق من الأدلة الرقمية التي يتم من خلالها بحث و تفتيش مسرح الجريمة ، و للورق أربعة أنواع هي :

أ- المسودة التي يتم إعدادها بخط اليد مثل تصور للعلمية التي يتم برمجتها.

ب- أوراق تالفة و التي يتم طباعتها للتأكد من برمجة العملية ، و من ثم رميها في سلة المهملات .

ج- الأوراق التي تتم طباعتها و الاحتفاظ بها لأغراض تفيد الجريمة .

د- الأوراق الأساسية و المحفوظة في الملفات العادية أو دفاتر الحسابات و خاصة التي يتم تزويرها من أجل تنفيذ الجريمة.²

ثانياً - الأجهزة الالكترونية :

نتطرق في هذا العنصر إلى تحديد الأجهزة الالكترونية من خلال تعريفها و دور كل منها ضمن المنظومة المعلوماتية ، باعتبارها قد تتوفر على أدلة تقنية تساعد في الكشف

1 - أمحمد طارق الجملي ، المرجع السابق ، ص 47.

2 - معمش زهية و غانم نسيم ، الإثبات الجنائي في الجرائم المعلوماتية ، مذكرة ماستر في الحقوق ، جامعة باتنة ، السنة الجامعية 2012-2013 ، ص 50،51 .

عن جرائم المعلوماتية ، بحيث تتمثل هذه الأجهزة فيما يلي :

الحاسب الآلي و ملحقاته: لتحديد الجريمة على أنها جريمة معلوماتية مرتبطة بالمكان أو بالشخص يفترض وجود حاسب آلي ، حيث بإمكان خبير الحاسب الآلي التعرف على الجهاز و مواصفاته مع تمييزه عن غيره من أجهزة الحاسب الآلي الأخرى ، بالإضافة إلى كيفية تحديد أسلوب التعامل معه أثناء الضبط و التحريز .

أ- الطابعات : و هي التي يتم بواسطتها استخراج ما تم طباعته ، و تختلف أنواعها من حبرية إلى ليزيرية ، ملونة و غير ملونة ، غالبا ما تستخدم في مجال التقنية المعلوماتية .

ج- الموديم : هي الوسيلة التي يمكن من خلالها لأجهزة الحاسوب الآلي الاتصال ببعضها البعض عبر خطوط الهاتف ، كما يقوم كذلك بإرسال الفاكس و الرد على المكالمات الهاتفية ، و تبادل البيانات و تعديلها ، و يأخذ أشكال متنوعة مرتبطة بتطور تقنية المعلومات .

د- الهاتف النقال: يعتبر جهاز إلكتروني حجمه صغير يفيد التواصل بين الأشخاص، و قد تطور في الآونة الأخيرة ، فأصبح يتمتع بأشكال و مميزات أحدث أجهزة الحاسب الآلي اليوم ، و أطلق عليه تسميات عدة منها الجوال ، المحمول ، الخليوي و النقال.....الخ.¹

ثالثا- أمثلة الدليل التقني : يمكن أن نذكر كأمثلة عن الأدلة التقني ما يلي :

أ- بروتوكول (TPC/IP) ، يعتبر من أهم و أشهر البروتوكولات المستخدمة في شبكة الانترنت و الاتصالات ، كما يعد جزء أساسي من الانترنت و يتكون من مايلي:

1 - سيدي محمد لبشير ، دور الدليل الرقمي في إثبات الجرائم المعلوماتية - دراسة تحليلية تطبيقية- ، رسالة ماجستير في العلوم الشرطية ، تخصص التحقيق و البحث الجنائي ، كلية الدراسات العليا ، جامعة نايف للعلوم الامنية ، الرياض 2010 ، ص 15 .

- بروتوكول (User Datagram Protocol/UDP) .

- بروتوكول (Transmission Control Protocol / TCP) .

- بروتوكول (Internet Protocol / IP) .

و من مميزات هذه البروتوكولات ، أنها تقوم معا بنقل المعلومات الخاصة بالمستخدم وفقا لنظام هيكلية تبادل المعلومات المعروف باسم (TCP/IP With OSI).

حيث يقوم بروتوكول (TCP) بتسليم و استقبال المعلومات المطلوب إرسالها أو إعادة إرسالها في حالة الضرورة ، بتنسيق من بروتوكول (UDP) الذي صمم من أجل مواجهة بعض التطبيقات التي لا تستخدم (TCP) ، كما أن تطبيقات كل من (UDP/TCP) أعدت أيضا لمواجهة المسائل المألوفة أثناء عملية تبادل المعلومات و التي تتمثل في إخفاء معدات الحاسوب (Hard Ware) و تأخر المعلومات ، و اشتباك و ازدحام الشبكات و الأخطاء التي قد تتكرر أو تتوالى ، و بعد تقسيم المعلومات إلى حزمة معلوماتية (Soft Ware Package) من طرف (TCP) ، يقوم بروتوكول (IP) بعنوان المعلومات مع إضافة معلومات أخرى ، فتصبح (Soft Ware Package) التي تحتوي على حزمة (TCP/IP) ، و أثناء اتصال الحاسب الآلي بالانترنت يأخذ عنوان خاص يسمى IP Adresses و كل عنوان مكون من جزأين ، الأول يتضمن أرقام الشبكة ، و الثاني يتعلق بأرقام مزود الخدمة .

ب- الكوكيز (Cookies) 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 عنوان (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 الهروب منها لأن بدونها لا يستطيع تصفح الانترنت.¹

1 - معمش زهية و غانم نسيمية ، المرجع السابق ، ص53.

المطلب الثالث : محل الدليل التقني

نتطرق من خلال هذا المطلب إلى تحديد محل الدليل التقني ضمن (الفرع الأول)، ثم إبراز خصائص هذا المحل ضمن (الفرع الثاني) .

الفرع الأول : تحديد محل الدليل التقني

عبر المشرع الجزائري عن الجريمة المعلوماتية في القانون 04-15 بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، معبرا في ذلك عن النظام المعلوماتي بنظام المعالجة الآلية للمعطيات ، ذلك أن الجريمة المعلوماتية ترتكب بواسطة و على النظام المعلوماتي ، و عليه فهذا الأخير هو محل الدليل التقني باعتباره البيئة التقنية التي ينشأ فيها نتيجة لوقوع الجريمة عليه أو بواسطته .¹

و يعرف نظام المعلومات information system بأنه مجموعة من العناصر المتداخلة و المتفاعلة مع بعضها و التي تعمل على جمع المعطيات و معالجتها لتشكل لنا المعلومة الالكترونية و من ثم تخزينها و بثها و توزيعها ، بغرض صناعة أو أخذ القرارات و تنسيقها ، إضافة إلى تحليل المشكلات و النظر في الموضوعات المعقدة .²

و قد عرف المشرع الجزائري النظام المعلوماتي بموجب الفقرة "ب" من المادة 2 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها بأنه " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها

1 - رابحي عزيزة ، الأسرار المعلوماتية و حمايتها الجزائية ، أطروحة دكتوراه علوم في القانون الخاص ، جامعة

أبوبكر بلقايد تلمسان ، السنة الجامعية 2017-2018 ، ص 52 .

2 - ملياني عبد الوهاب ، المرجع السابق، ص 30 .

البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين"¹

الفرع الثاني : خصائص النظام المعلوماتي باعتباره محل الدليل التقني

من خلال التعاريف السابقة يتضح لنا أن النظام المعلوماتي مجموعة مكونة من حاسوب و معدات و برمجيات معزولة أو مرتبطة عبر شبكات الاتصال أو متقاربة ، التي تضمن عن طريق برنامج تنفيذ المعالجة الآلية للبيانات ، كما أنه يشمل القيام بتسجيل المعطيات ، و كذا الإجراءات المتعلقة بتسجيل البيانات أو بوضعها في ذاكرة الحاسوب ، و عمله يمر وفق المراحل التالية :

- تأمين المدخلات المطلوبة من البيانات التي توضع في الحاسوب بوسائل خاصة.
- معالجة البيانات المدخلة و تحويلها من شكلها الأولي إلى نتائج مفهومة و قابلة للاستخدام تكون في شكل مخرجات أو معطيات .
- تأمين المخرجات من المعلومات المطلوبة لمستخدميها أو لمن يحتاجها ، و هنا لابد أن تنقل تلك المعلومات من وحدة المعالجة المركزية إلى وسيلة إخراج مناسبة كشاشة الحاسوب ، أو الطابعةإلخ .
- التغذية الراجعة كون المعلومات المخرجة لنشاط محدد قد تكون بدورها مدخلات ثانية بغرض إعادة معالجتها مع بيانات أخرى من داخل ذاكرة الحاسوب ، و لأغراض مخرجات أخرى .

و حتى يتضح لنا مفهوم هذا النظام و عمله وجب علينا التطرق إلى مكوناته المتمثلة فيما يلي :

1 - الفقرة "ب" من المادة 2 من القانون 04-09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، الجريدة الرسمية العدد 47 ، لسنة 2009 ، المعدل للأمر 66-156 المتضمن قانون العقوبات الجزائري .

أولا - العنصر البشري

الذي يلعب دورا هاما في النظام للقيام بالمعلومات و الإجراءات ، فبدونه لا يستطيع النظام المعلوماتي العمل ، فهو حلقة أساسية في مكونات النظام المعلوماتي ، و من مكونات العنصر البشري نجد المستخدمين النهائيين و الاختصاصيين الفنيين المسؤولين عن تشغيل و إدارة نظم المعلومات فنيا و منهم محللو النظم و مطورو البرمجيات و مشغلو النظام و مهندسو الصيانة إلخ .¹

ثانيا - الحاسب الآلي

يعرف بأنه عبارة عن جهاز إلكتروني مركب من المكونات المادية و المكونات المنطقية أو البرمجية ، يتم توصيلها و توجيهها باستخدام أوامر خاصة لمعالجة و إدارة المعلوماتية ، عن طريق تنفيذ عمليات أساسية تتمثل في استقبال المعطيات المدخلة إليه ، و معالجة المعطيات إلى معلومات ، و إظهار المعلومات المخرجة ، حيث يتميز بالسرعة و سعة التخزين ، و إعطاء نتائج دقيقة ، كما انه قابل للبرمجة لتحسين الأداء الوظيفي له ، إضافة إلى إمكانية التعامل عن بعد عن طريق وسائل الاتصال السلكية و اللاسلكية و هو ما يعرف بشبكة المعلوماتية.²

ثالثا - المعلومات الالكترونية

تتمثل معلومات الجهاز بصفة عامة في البيانات و النصوص ، الصور و الأشكال و الرموز ، و قواعد البيانات و برامج الحاسوب ، كما أنها مجموعة من البيانات و المعطيات التي قد تمت معالجتها و تحليلها و تلخيصها و تجريبيها لتحقيق الأهداف المرجوة منها و استخدامها في المجالات المختلفة ، أي أنها البيانات المجهزة في شكل

1 - ملياني عبد الوهاب ، المرجع السابق ، ص 31.

2 - نفس المرجع ، ص 32.

منظم و مفيد بتسلسل منطقي .¹

و تعرف المعلومات بوجه عام "أنها الصورة المحمولة للبيانات المنظمة و المعالجة بطريقة تسمح باستخلاص نتائج نهائية " .²

رابعاً - شبكة المعلومات (الانترنت)

تعتبر وسيلة تواصل و تبادل المعلومات ، فهي نظام للتخاطب بين الحواسيب تسمح بنقل الملفات و البرامج و البيانات ، التي تكون مكتوبة أو أصوات أو صور في شكل معلومات إلكترونية بين حاسوبين أو أكثر في أماكن متباعدة و في زمن قصير جداً ، فهي تساعد على ربط الاتصال بين الأفراد و الجماعات لإنجاز الأعمال عن بعد بالاعتماد على توجيه المعلومات من المرسل إلى المستقبل .³

الفرع الثالث: المواجهة التشريعية لإعتداء على النظام المعلوماتي

الجريمة المعلوماتية و ما يصاحبها من أضرار من جهة ، و محاولة المشرع لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى ، لهذا نجد المشرع قام بحركة تشريعية رغبة للتصدي لهذه الجريمة و هو ما سنتناوله وفق ما يلي :

أولاً- القوانين العامة في مجال مكافحة الجريمة المعلوماتية

أ-مكافحة الجريمة المعلوماتية وفق الدستور : كفل الدستور الجزائري حماية الحقوق الأساسية و الحريات الفردية ، و أن تسهر الدولة على عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية بسن نصوص تشريعية أوردها في قانون العقوبات و قانون الإجراءات الجزائية و قوانين خاصة ، غايتها ردع كل مساس بهذه الحقوق ، و من بين المبادئ الدستورية نجد المواد التالية :

1 - رابحي عزيزة ، المرجع السابق ، ص 59.

2 - ملياني عبد الوهاب ، المرجع السابق ، ص 38.

3 - نفس المرجع ، ص 46، 47.

- المادة 38 التي تنص على " الحريات الأساسية و حقوق الإنسان و المواطن مضمونة" ، و بالتالي المشرع سعى لحماية الحقوق من جميع أشكال الانتهاكات.¹

بينما نصت المادة 44 على ما يلي " حرية الابتكار الفكري و الفني و العلمي مضمونة للمواطن ، حقوق المؤلف يحميها القانون ، لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ و الإعلام إلا بمقتضى أمر قضائي ، الحريات الأكاديمية و حرية البحث العلمي مضمونة و تمارس في إطار القانون ، تعمل الدولة على ترقية البحث العلمي و تثمينه خدمة للتنمية المستدامة للأمة".²

كما تنص المادة 46 على " لا يجوز انتهاك حرمة حياة المواطن الخاصة ، و حرمة شرفه، و يحميها القانون ، سرية المرسلات و الاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز بأي شكل من الأشكال المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ، و يعاقب القانون على انتهاك هذا الحكم ، حماية الأشخاص الطبيعيين في مجال معالجة المعطيات الطابع الشخصي حق أساسي يضمنه القانون و يعاقب انتهاكه".³

كما أكدت المادة 47 على مايلي " تضمن الدولة عدم انتهاك حرمة المسكن ، فلا تفتيش إلا بمقتضى القانون ، و في إطار احترامه ، و لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".⁴

يفهم من سياق هذه النصوص أن المشرع سعى إلى حماية الحياة الخاصة من كل أشكال الاعتداءات .

1 - المادة 38 من القانون رقم 01-16 ، المؤرخ في 06 مارس 2016 المتضمن التعديل الدستوري ، الجريدة الرسمية العدد 14، لسنة 2016.

2 - المادة 44 من القانون رقم 01-16 ، المتضمن التعديل الدستوري ، نفس المرجع.

3 - المادة 46 ، المتضمن التعديل الدستوري، نفس المرجع.

4 - المادة 47 ، المتضمن التعديل الدستوري، نفس المرجع.

ب- مكافحة الجريمة المعلوماتية وفق قانون العقوبات

تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي ، كنتيجة حتمية لما أفرزته ثورة المعلوماتية من أشكال جديدة للإجرام ، مما دفعه إلى تعديل قانون العقوبات¹ و إدراج القسم السابع مكرر ، الذي تضمن 08 مواد (من المادة 394 مكرر إلى المادة 394 مكرر7) ، تحت "عنوان المساس بأنظمة المعالجة الآلية للمعطيات" و نص على الجرائم المذكورة أعلاه .²

1 - قانون العقوبات الصادر بموجب الأمر رقم 66-156 المؤرخ في 08 جوان 1966 ، المتضمن قانون العقوبات ، الجريدة الرسمية العدد 49 ، لسنة 1966 .

2 - تنص المادة 394 مكرر على " يعاقب بالحبس من 3 أشهر إلى سنة 1 و بغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .."

- تنص المادة 394 مكرر 1 " يعاقب بالحبس من 6 أشهر إلى 3 سنوات و بغرامة من 50.000 دج إلى 200.000 دج ، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.."

- تنص المادة 394 مكرر 2 " يعاقب بالحبس من شهرين 2 الى ثلاث سنوات و بغرامة من 1000.000 دج إلى 5000.000 دج كل من يقوم عمدا و عن طريق الغش بما يأتي : 1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم ، 2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم .

- تنص المادة 394 مكرر 3 " تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الددفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد"

- تنص المادة 394 مكرر 4 " يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي"

- تنص المادة 394 مكرر 5 " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"

ج- مكافحة الجريمة المعلوماتية وفق قانون الإجراءات الجزائية

قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لمواكبة التطور المعلوماتي الذي لحق بالجريمة المعلوماتية ، محاولة منه تطويقها و القضاء عليها ، أو على الأقل الحد من انتشارها ، حيث وضع قواعد و أحكام خاصة لسلطة التحقيق ، الغرض منها مواجهتها ، من خلال استحداث أساليب خاصة في قانون الإجراءات الجزائية متمثلة في التسرب و اعتراض المرسلات ، المراقبة الالكترونية ..إلخ ، نتطرق إليها بشيء من التفصيل في عنوان خاص من خلال الفصل الثاني .¹

- تنص المادة 394 مكرر 6 " مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها"

- تنص المادة 394 مكرر 7 " يعاقب على الشروع في ارتكاب الجرح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنة ذاتها"

1 - القانون 06-22 ، المؤرخ في 20 ديسمبر 2006 ، المؤرخ في 20 ديسمبر 2006 ، المعدل و المتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 ، المتضمن قانون الإجراءات الجزائية الجزائري ، الجريدة الرسمية العدد 84 لسنة 2006 ، حيث تنص المادة 93 مكرر 2 " دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) الى خمس (5) سنوات وبغرامة من 100.000 دج إلى 200.000 دج، كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة"

- تنص المادة 93 مكرر 3 " دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين (2) الى خمس (5) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهني الصحة"

ثانيا - القوانين الخاصة في مجال مكافحة الجريمة المعلوماتية

نظرا لاتساع نطاق الجريمة الالكترونية ، و تعدد أنواعها ، و على أساس القانون الجنائي التقليدي غير قادر على استيعاب الجرائم المعلوماتية الحديثة ، أدى الأمر بالمشروع الجزائري إلى استحداث قوانين خاصة لمواكبة هذا النوع من الجرائم.

أ- قانون البريد و المواصلات السلوكية و اللاسلوكية:

سعى المشرع من خلال القانون 03-2000 المحدد للقواعد العامة المتعلقة بالبريد و بالمواصلات السلوكية و اللاسلوكية¹ ، مواجهة هذه الظاهرة الإجرامية ، ضمن الفصل

1 - القانون رقم 03-2000 المؤرخ في 05 أوت سنة 2000 ، المحدد للقواعد العامة المتعلقة بالبريد و بالمواصلات السلوكية و اللاسلوكية ، الجريدة الرسمية العدد 48 لسنة ، لسنة 2000 .

- تنص المادة 127 من نفس القانون على " تطبق العقوبات المنصوص عليه في المادة 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه والذي في إطار ممارسة مهامه يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال ، تسري نفس العقوبات على كل شخص مرخص له بتقديم خدمة مواصلات سلوكية و لاسلوكية وكل عامل لدى متعاملي الشبكات العمومية للمواصلات السلوكية و اللاسلوكية والذي في إطار ممارسة مهامه وزيادة على الحالات المقررة قانونا ينتهك بأي طريقة كانت سرية المراسلات الصادرة أو المرسله أو المستقبله عن طريق المواصلات السلوكية و اللاسلوكية أو الذي أمر أو ساعد في ارتكاب هذه الأفعال.

يعاقب.... أو بإحدى هاتين العقوبتين كل شخص غير الأشخاص المذكورين في الفقرتين السابقتين، ارتكب أحد الأفعال المعاقب عليها بموجب هاتين الفقرتين"

علاوة على العقوبات المنصوص عليها في الفقرات 1 و 2 و 3 المشار إليها أعلاه، يمنع المخالف من ممارسة كل نشاط أو مهنة في قطاع المواصلات السلوكية و اللاسلوكية أو قطاع البريد أو في قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين سنة إلى خمس (5) سنوات.

تنص المادة 128 من نفس القانون على " تعاقب كل مخالفة لحق استعمال التخصيص كما هو مبين في المادة 63 من هذا القانون ..."

تنص المادة 129 من نفس القانون على " يعاقب ... كل متعامل استعمل علامة بريد، غير المتعامل المستفيد من نظام التخصيص."

تنص المادة 130 من نفس القانون على " يعاقب ... كل من يقطع عمدا كابلا بحريا أو يسبب له تلفا قد يوقف أو يعطل المواصلات السلوكية و اللاسلوكية كليا أو جزئيا. تطبق هاتان العقوبتان على كل من يحاول ارتكاب هذه الجناه ، لا تطبق

هذه الأحكام على الأشخاص الذين يكونون قد أجبروا على قطع كابل بحري أو إتلافه بسبب الضرورة الآتية، لحماية حياتهم أو ضمان سلامة سفينتهم "

-تنص المادة 131 من نفس القانون على " يعاقب بالحبس .. أو بإحدى هاتين العقوبتين، كل من ينشيء أو يستغل شبكة عمومية للمواصلات السلكية و اللاسلكية دون الرخصة المنصوص عليها في المادة 32 من هذا القانون أو مواصلة ممارسة النشاط خرقة لقرار التعليق أو سحب هذه الرخصة.

تنص المادة 132 من نفس القانون على" لمادة 132 : يعاقب بالحبس ... بإحدى هاتين العقوبتين، كل من ينشيء أو يعمل على إنشاء شبكة مستقلة دون الترخيص المنصوص عليه في المادة 39 من هذا القانون"

- تنص المادة 133 من نفس القانون على" يعاقب بغرامة كل شخص يقوم بإشهار لغرض بيع تجهيزات أو معدات للمواصلات السلكية واللاسلكية دون أن يكون متحصلا على الاعتماد لمنصوص عليه في المادة 41 من هذا القانون "

- تنص المادة 134 من نفس القانون على" يجوز للمحكمة كذلك عند النطق بالعقوبة من أجل إحدى الجرائم المنصوص عليها في المواد من 131 إلى 133 من هذا القانون بمصادرة المعدات والمنشآت المشكلة للشبكة أو التي تسمح بتقديم الخدمة، كما يجوز لها الأمر بإتلافها على نفقة المحكوم عليه والحكم بمنع طلب منح رخصة أو ترخيص جديد مدة سنتين.

- تنص المادة 135 من نفس القانون على " يعاقب بالحبس ... أو بإحدى هاتين العقوبتين، كل شخص يصدر عمدا عن طريق لاسلكي كهربائي إشارات أو يصدر نداءات نجدة كاذبة أو خادعة يجوز الحكم بمصادرة الأجهزة ، مع مراعاة حقوق الغير حسني النية ، يعاقب بنفس هذه العقوبة كل شخص حول أو عمل على تحويل خطوط المواصلات السلكية و اللاسلكية أو يستغل خطوط المواصلات السلكية و اللاسلكية المحمولة .

- تنص المادة 136 من نفس القانون على " يعاقب .. كل شخص يقوم بإرسالات لاسلكية كهربائية باستعمال ، عمدا ، رمز نداء في السلسلة الدولية مخصص لإحدى محطات الدولة أو لكل محطة أخرى مرخص بها"

- تنص المادة 137 من نفس القانون على" يعاقب بالعقوبات المنصوص عليها في المادة 137 من قانون العقوبات، كل شخص يفشي أو ينشر أو يستعمل دون ترخيص من المرسل أو المرسل إليه مضمون المراسلات المرسله عن طريق اللاسلكي الكهربائي أو يخبر بوجودها"

- تنص المادة 138 من نفس القانون على " يعاقب كل شخص يرتكب عملا ماديا ضارا بخدمة المواصلات السلكية و اللاسلكية أو يخرب أو يتلف بأي شكل كان الأجهزة أو المنشآت أو وصلات المواصلات السلكية و اللاسلكية. ، يحكم عليه علاوة على ذلك، بناء على طلب المتضرر بتعويض الضرر بما في ذلك فوات الربح المحدث للمستغل العمومي أو لكل متعامل مرخص له ، تحد د تقييم هذا الضرر الجهة القضائية التي تم رفع الدعوى أمامها"

- تنص المادة 139 من نفس القانون على " يعاقب في حالة انعدام التصريح المنصوص عليه في المادة 40 من هذا

الثاني المعنون بالأحكام الجزائية في المواد (من المادة 127 إلى المادة 144) ، الذي نص على سلوكيات إجرامية جديدة و أحال أيضا بعض السلوكيات إلى قانون العقوبات .

ب- قانون التأمينات الاجتماعية:

أراد المشرع من وراء القانون 08-01 المتمم للقانون 83-11 ، المتعلق بالتأمينات الاجتماعية كذلك تنظيم الجريمة الالكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية تخص البطاقة الالكترونية ، حيث نص على تجريم عدد من السلوكيات ضمن المواد (من المادة 93 مكرر 2 إلى المادة 93 مكرر 6) ، دون الإخلال بالعقوبات

-
- القانون بالحبس ..وبغرامة ... أو بإحدى هاتين العقوبتين ، .وفي حالة العود، تضاعف هذه العقوبة مرتين"
- تنص المادة 140 من نفس القانون على" لمادة 140 : يعاقب ... كل من يقوم، تهاونا أو خطأ أو خرقا للتنظيمات، بقطع كابل بحري أو يسبب له تلفا قد يوقف أو يعطل المواصلات السلوكية و اللاسلوكية كلياً أو جزئياً."
- تنص المادة 141 من نفس القانون على " ... كل من يمتنع عن تقديم الوثائق الضرورية لتحرير محاضر المعاينة"
- تنص المادة 142 من نفس القانون على " يعاقب .. 1- قائد السفينة القائم بتصليح أو مدّ كابل بحري الذي لا يراعي قواعد الإشارات المعتمدة لاتقاء الاصطدامات ، 2- قائد أية سفينة لا ينسحب أو لا يبتعد بميل ملاحي على الأقل عن السفينة القائمة بمد أو تصليح كابل بحري عندما يلاحظ أو يكون بوسعه ملاحظة هذه الإشارات، 3- قائد أية سفينة لا يبتعد عن خط الطواف بربع ميل ملاحي على الأقل عندما يرى أو عندما يكون بوسعه أن يرى الطوافي الدالة على موقع الكوابل"
- تنص المادة 143 من نفس القانون على " يعاقب بالحبس ..1- قائد أية سفينة يرمي المرساة على بعد أقل من ربع ميل ملاحي من كابل بحري والذي بوسعه أن يحدد موقعه بواسطة خطوط الطوافي أو غيرها ، أو كان قد ربط السفينة بطواف مخصصة للدلالة على موقع الكابل ، باستثناء حالات القوة القاهرة ، 2 - صاحب أي مركب صيد، لا ينأى بأجهزته أو شبابه بقدر ميل ملاحي على الأقل عن السفينة القائمة بمد أو تصليح كابل بحري ، غير أن لمراكب الصيد التي تلمح السفينة أو بوسعها أن تلمح الإشارات المعتمدة للسفينة، وقصد الامتثال للإنذار، الأجل الضروري للانتهاء من العملية الجارية على ألا يتجاوز هذا الأجل 24 ساعة ، 3- صاحب أي مركب صيد لا ينأى بأجهزته أو شبابه بقدر ربع ميل ملاحي على الأقل عن خط الطوافي المخصصة للدلالة على الكوابل البحرية"
- تنص المادة 144 من نفس القانون على " يمنع تقليد و استعمال المطبوعات المستعملة من طرف المستغل العمومي أو من طرف كل متعامل آخر مرخص له ، يعاقب على خرق هذه الأحكام طبقا للمواد 220 و ما يليها من قانون العقوبات"

المنصوص عليها في التشريع المعمول به .¹

ج- قانون خاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها :

يعتبر القانون 04-09 المحور الأساسي للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات و الاتصال و مكافحتها ، حيث تضمن الإجراءات الخاصة بالتحري عن هذه الجرائم و حالات اللجوء إليها ، و القيود الواردة على هذه الإجراءات ، كما نص أيضا

1 - من القانون 01-08 ، المؤرخ في 23 جانفي 2008 ، المتمم للقانون رقم 83-11 المؤرخ في 02 جويلية 1983 ، المتعلق بالتأمينات الاجتماعية ، الجريدة الرسمية العدد 04 لسنة 2008

- تنص المادة 93 مكرر 2 " دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين (2) إلى (5) و بغرامة من 100.000 دج إلى 200.000 دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهني الصحة "

- تنص المادة 93 مكرر 3 " دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين (2) إلى (5) و بغرامة من 500.000 دج إلى 1000.000 دج ، كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لمهني الصحة ، يعاقب بنفس العقوبة ، كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لمهني الصحة ، يعاقب بنفس العقوبة ، على المحاولة في ارتكاب الجرح المذكورة في الفقرتين الأولى و الثانية أعلاه "

- تنص المادة 93 مكرر 4 " دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين (2) إلى (5) و بغرامة من 500.000 دج إلى 5.000.000 دج ، كل من ينسخ أو يصنع أو يحوز أو يوزع بطريقة غير مشروعة البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لمهني الصحة "

- تنص المادة 93 مكرر 5 " يعاقب كل شخص معنوي يرتكب احدى الجرح المنصوص عليها في المادتين 93 مكرر 3 و 93 مكرر 4 أعلاه ، بغرامة تساوي خمس 5 مرات المبلغ الأقصى للغرامة المقررة للشخص الطبيعي "

- تنص المادة 93 مكرر 6 " دون الاخلال بحقوق الغير حسن النية ، يحكم بمصادرة الأجهزة و الوسائل المستعملة و كذا غلق المحلات و أماكن الاستغلال التي تكون محل للجرح المنصوص عليها في المادتين 93 مكرر 3 و 93 مكرر 4 أعلاه ، في حالة ما إذا كان المالك على علم بذلك "

إلى كفاءات القيام بهذه الإجراءات ، و الآليات المسخرة لسلطات التحقيق للكشف عن هذه الجرائم ، و التي كما ذكرنا سنتطرق إليها بشيء من التفصيل في جزء خاص بها .¹

د- قانون البريد و الاتصالات الالكترونية:

في ذات الشأن صدر القانون 04-18 ، المحدد للقواعد العامة المتعلقة بالبريد و المواصلات الالكترونية² ، الذي تضمن أيضا أحكام جزائية في الباب الرابع منه في المواد

- 1 - القانون 04-09 ، المتعلق بالجرائم المتعلقة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، المرجع السابق.
- 2 - القانون 04-18 ، المؤرخ في 10 ماي 2018 ، المحدد للقواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، الجريدة الرسمية العدد 27 لسنة 2018.
- تنص المادة 164 من نفس القانون على " يعاقب كل شخص ينتهك سريه المراسلات المرسله عن طريق البريد أو الاتصالات الالكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها"
- نص المادة 165 من نفس القانون على " يعاقب بالحبس أو بالغرامة أو بإحدى هاتين العقوبتين كل متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال ، تسري نفس العقوبات على كل متعامل للاتصالات الالكترونية يحول في بأي طريقه كانت المراسلات الصادرة أو المرسله أو المستقبله عن طريق الاتصالات الالكترونية أو ساعد في ارتكاب هذه الأفعال ، و يمكن الجهة القضائية أيضا النطق بواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 9 من قانون العقوبات"
- تنص المادة 166 من نفس القانون يعاقب بالحبس وبغرامة أو بإحدى هاتين العقوبتين كل عون مستخدم من طرف متعامل يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال في إطار ممارسه مهامه ، يعاقب بنفس العقوبات كل شخص مستخدم لدى متعامل للاتصالات الالكترونية في أي طريقه كانت المراسلات الصادرة أو المرسله أو المستقبله عن طريق الاتصالات الالكترونية أو أمر أو ساعد فرتكه هذه الأفعال"
- تنص المادة 167 من نفس القانون على " يعاقب كل شخص غير المذكورين في المادتين 165 و 166 احد الأفعال في المادتين السابقتين"
- تنص المادة 168 من نفس القانون على " يعاقب كل شخص غير المستفيد من نظام التخصيص ويمارس نشاطات تخضع لنظام التخصيص يعاقب بنفس العقوبة كل متعامل غير بريد الجزائر يستعمل علامة 'بريد' "
- تنص المادة 169 من نفس القانون على " يعاقب بالحبس .. بغرامة .. أو بإحدى هاتين العقوبتين كل شخص يقدم خدمات البريد من دون الحصول على الترخيص المنصوص عليه في المادة 34 من هذا القانون"
- تنص المادة 170 من نفس القانون على " يعاقب في حالة انعدام التصريح المنصوص عليه في المادة من هذا القانون بالحبس .. بغرامة ، أو بإحدى هاتين العقوبتين "
- تنص المادة 171 من نفس القانون على " يعاقب بالحبس .. وبغرامة ، أو إحدى هاتين العقوبتين كل من ينشئ أو يستغل شبكة اتصالات الكترونية مفتوحة للجمهور دون الرخصة المنصوص عليها في المادة 123 ، أو مواصلة

- ممارسة النشاط خرقاً لقرار التعليق أو سحب هذه الرخصة "
- تنص المادة 172 من نفس القانون على " يعاقب بالحبس ...و بغرامة ، أو بإحدى هاتين العقوبتين كل من يوفر خدمات الاتصالات الالكترونية المفتوحة للجمهور دون الترخيص العام المنصوص عليه في المادة 131 من هذا القانون ، و يعاقب بنفس العقوبة كل من كل من ينشئ أو يستغل أو يعمل على إنشاء شبكة خاصة دون الترخيص المنصوص عليه في المادة 138 من هذا القانون "
- تنص المادة 173 من نفس القانون على "يعاقب في حالة انعدام التصريح المنصوص عليه في المادة 135 من هذا القانون بالحبس ..و بغرامة ، أو إحدى هاتين العقوبتين "
- تنص المادة 174 من نفس القانون على " يعاقب بغرامة ..كل شخص يقوم بتوزيع التجهيزات أو معدات الاتصالات الالكترونية بمقابل أو بدون مقابل أو يقوم بإشهار لغرض بيعها دون أن يكون متحصلاً مسبقاً على شهادة المطابقة المنصوص عليه في المادة 143 من هذا القانون "
- تنص المادة 175 من نفس القانون على " يعاقب بالحبس ..و بغرامة ، أو بإحدى هاتين العقوبتين كل شخص حول خطوط الاتصالات الالكترونية أو يستغل خطوط الاتصالات الالكترونية المحولة "
- تنص المادة 176 من نفس القانون على " يعاقب بالحبس ..و بغرامة ، كل شخص يقوم بإرسالات لاسلكية كهربائية باستعمال عمدا رمز نداء في السلسلة الدولية مخصصاً لإحدى محطات الدولة أو لأي محطة أخرى مرخص بها "
- تنص المادة 177 من نفس القانون على " يعاقب بالحبس ..و بغرامة ، كل شخص يرتكب عملاً مادياً ضاراً بخدمة الاتصالات الالكترونية أو يخرب أو يتلف ، بأي شكل كان ، الأجهزة أو المنشآت أو وصلات الاتصالات الالكترونية "
- تنص المادة 178 من نفس القانون على " يعاقب بالحبس ..و بغرامة ، أو بإحدى هاتين العقوبتين ، كل شخص يصدر عمداً عن طريق لاسلكي كهربائي إشارات أو نداءات نجدة كاذبة أو خادعة ، و يجوز الحكم بمصادرة الأجهزة ، مع مراعاة الغير حسن النية "
- تنص المادة 179 من نفس القانون على " يعاقب بالحبس ..و بغرامة ، كل من يقطع عمداً كابل بحري أو يسبب له تلفاً قد يوقف أو يعطل الاتصالات الالكترونية كلياً أو جزئياً ، و لا تطبق هذه الأحكام على الأشخاص الذين أجبروا على قطع كابل بحري أو أو إتلافه بسبب الضرورة الآنية لحماية حياتهم أو حياة الآخرين أو ضمان سلامة سفينتهم "
- تنص المادة 180 من نفس القانون على " يعاقب بالحبس ..و بغرامة ، كل شخص يقطع تهاوناً أو خطأ كابل بحرياً أو يسبب له قد يوقف أو يعطل الاتصالات الالكترونية كلياً أو جزئياً "
- تنص المادة 181 من نفس القانون على " يعاقب بالحبس ..و بغرامة ، أو بإحدى هاتين العقوبتين كل من لا يبلغ السلطات المختصة عن تسببه في قطع كابل بحري أو تلفه "
- تنص المادة 182 من نفس القانون على " يعاقب بغرامة ..1- قائد السفينة القائم بتصليح أو مدّ كابل بحري الذي لا يراعي قواعد الإشارات المعتمدة لاتقاء الاصطدامات..، 1- قائد أية سفينة لا ينسحب أو لا يتعد بميل (1) ملاحى، على الأقل، عن السفينة القائمة بمد أو تصليح كابل بحري، عندما يلاحظ أو ي كون بوسعه ملاحظة هذه الإشارات، 2- قائد أية سفينة لا ينسحب أو لا يتعد بميل (1) ملاحى، على الأقل، عن السفينة القائمة بمد أو تصليح كابل بحري، عدا يلاحظ أو يكون بوسعه ملاحظة هذه الإشارات 3- قائد أية سفينة لا يتعد عن خط الطوافي ربع (1/4) ميل ملاحى، على الأقل، عندما يرى أو يكون بوسعه أن يرى الطوافي الدالة على موقع الكوابل "
- تنص المادة 183 من نفس القانون على " يعاقب بالحبس ..1- قائد أية سفينة يرمي المرساة على بعد أقل من ربع

(من المادة 164 إلى المادة 188) ، تصب جلها على السلوكات المرتكبة في البيئة التقنية. للإشارة القانون المذكور أعلاه ، ألغى الأحكام المخالفة له لا سيما منها أحكام القانون رقم 03-2000 ، وأبقى أحكام النصوص التطبيقية له ، إلى حين صدور النصوص التنظيمية المتخذة لتطبيق هذا القانون، حسب المادة 189 من القانون 04-18 .¹

هـ- قانون حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي

في ذات السياق أيضا ، جسد المشرع الجزائري من خلال القانون 07-18 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، مواجهة

(1/4) ميل ملاحي من كابل بحري وبوسعه أن يحدد موقعه بواسطة خطوط الطوافي أو غيرها، أو كان قد ربط السفينة بطوافه مخصصة للدلالة على موقع الكابل باستثناء حالات القوة القاهرة ، 2- صاحب أي مركب صيد، لا ينأى بأجهزته أو شبابه بقدر ميل (1) ميل ملاحي ، على الأقل ، عن السفينة القائمة بمد أو تصليح كابل بحري ، غير أن لمراكب الصيد التي تلمح السفينة أو بوسعها أن تلمح الإشارات المعتمدة للسفينة ، وقصد الامتثال للإنذار ، لأجل الضروري لانتهاء من العملية الجارية على ألا يتجاوز هذا الأجل الأربع والعشرين (24) ساعة ، 3- صاحب أي مركب صيد لا ينأى بأجهزته أو شبابه بقدر ربع (1/4) ميل ملاحي ، على الأقل، عن خط الطوافي المخصصة للدلالة على الكوابل البحرية.

- تنص المادة 184 من نفس القانون على " يمنع التقايد والاستعمال غير المرخص للمطبوعات المستعملة من طرف المستغل العمومي أو من طرف كل متعامل آخر مرخص له ، يعاقب على كل خرق لهذه الأحكام طبقا للمواد 220 وما يليها من قانون العقوبات "

- تنص المادة 185 من نفس القانون على " يجوز للجهة القضائية كذلك، عند النطق بالعقوبة من أجل إحدى الجرائم المنصوص عليها في المواد 171 إلى 173 من هذا القانون ، أن تحكم بمصادرة التجهيزات والمنشآت المكونة للشبكة أو التي تسمح بتقديم الخدمات، وكذا بمنع المطالبة من جديد برخصة أو ترخيص عام جديد لمدة سنتين (2) "

- تنص المادة 186 من نفس القانون على " يعاقب بالعقوبات المنصوص عليها في المادة 394 مكرر 8 من قانون العقوبات، كل متعامل مشار إليه في المادة 118 من هذا القانون لا يقوم رغم إنذاره من طرف سلطة الضبط بالتدخل الفوري لمنع النفوذ إلى شبكات و/أو خدمات الاتصالات الإلكترونية "

- تنص المادة 187 من نفس القانون على " يعتبر الشخص المعنوي مسؤولا جزائيا عن الجرائم المذكورة في هذا القانون طبقا للقواعد المنصوص عليها في قانون العقوبات "

- تنص المادة 188 من نفس القانون على " في حالة العود، تضاعف العقوبات المنصوص عليها في هذا القانون "

1 - تنص المادة 189 من القانون 04-18 ، المرجع السابق ، على " تلغى كل الأحكام المخالفة لهذا القانون لاسيما منها أحكام القانون رقم 03-2000 ، المؤرخ في 05 أوت سنة 2000 الذي يحدد القواعد المتعلقة بالقواعد بالبريد و الموصلات السلكية و اللاسلكية ، المعدل و المتمم ، و كذا أحكام المادة 53 من الأمر رقم 01-10 المؤرخ في 26 أوت 2010 المتضمن قانون المالية التكميلي لسنة 2010 "

الجرائم المتعلقة بالمعطيات الرقمية ، من خلال أحكام جزائية ضمن الفصل الثالث من الباب السادس في المواد (المادة 54 إلى المادة 74) ، دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع المعمول به .¹

- 1 - القانون 07-18 ، المؤرخ في 10 جوان 2018 ، المتعلق بحماية المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، الجريدة الرسمية العدد 34 لسنة 2018 .
- تنص المادة 54 من نفس القانون على " دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول ، يعاقب على خرق أحكام المادة 2 من هذا القانون بالحبس ...و بغرامة.."
- تنص المادة 55 من نفس القانون على " يعاقب بالحبس ..و بغرامة .. كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقاً لأحكام المادة 7 من هذا القانون ، ويعاقب بنفس العقوبة كل من يقوم بمعالجة معطيات ذات طابع شخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة، لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنياً على أسباب شرعية"
- تنص المادة 56 من نفس القانون على " يعاقب بالحبس ..و بغرامة .. كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون، ويعاقب بنفس العقوبات كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له.
- تنص المادة 57 من نفس القانون على " يعاقب بالحبس ..و بغرامة .. كل من قام، دون الموافقة الصريحة للشخص المعني و في غير الحالات المنصوص عليها في هذا القانون، بمعالجة المعطيات الحساسة"
- تنص المادة 58 من نفس القانون على " يعاقب بالحبس ..و بغرامة ..، أو بإحدى هاتين العقوبتين، كل من قام بإنجاز أو باستعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها"
- تنص المادة 59 من نفس القانون على " يعاقب بالحبس ..و بغرامة .. كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة"
- تنص المادة 60 من نفس القانون على " يعاقب بالحبس ..و بغرامة .. كل من سمح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي"
- تنص المادة 61 من نفس القانون على " يعاقب بالحبس ..و بغرامة ..، أو بإحدى هاتين العقوبتين، كل من عرقل عمل السلطة الوطنية ، 1- بالاعتراض على إجراء عملية التحقق في عين المكان، 2- عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة، 3- عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح.
- تنص المادة 62 من نفس القانون على " دون الإخلال بالأحكام الجزائية التي يستدعي تطبيقها طبيعة المعلومات المعنية ، يعاقب الشخص

المشار إليه في المادتين 23 و 27 من هذا القانون ، لإفشائه معلومات محمية بموجب هذا القانون ، بالعقوبات المنصوص عليها في المادة 301 من قانون العقوبات"

- تنص المادة 63 من نفس القانون على " يعاقب بالحبس ..و بغرامة ..، أو بإحدى هاتين العقوبتين، كل من يلج، دون أن يكون مؤهلاً لذلك إلى السجل الوطني المنصوص عليه في المادة 28 من هذا القانون"

- تنص المادة 64 من نفس القانون على " كل مسؤول عن المعالجة يرفض دون سبب مشروع ، حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض المنصوص عليها في المواد 32 و 34 و 35 و 36 من هذا القانون"

- تنص المادة 65 من نفس القانون على " دون الإخلال بالعقوبات الأشد المنصوص عليها في التشريع الساري المفعول ، يعاقب بغرامة ..، المسؤول عن المعالجة الذي يخرق الالتزامات المنصوص عليها في المادتين 38 و 39 من هذا القانون" يعاقب بنفس العقوبة كل من قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص"

- تنص المادة 66 من نفس القانون على " يعاقب بالحبس ..و بغرامة ..، أو بإحدى هاتين العقوبتين، مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية، خلافا لأحكام المادة 43 من هذا القانون"

- تنص المادة 67 من نفس القانون على " يعاقب بالحبس ..و بغرامة ..، كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقاً لأحكام المادة 44 من هذا القانون"

- تنص المادة 68 من نفس القانون على " يعاقب بالحبس ..و بغرامة ..، كل من قام، في غير الحالات المنصوص عليها قانوناً، بوضع أو حفظ في الذاكرة الآلية، المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن"

- تنص المادة 69 من نفس القانون على " يعاقب بالحبس ..و بغرامة ..، كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص مكلف، بالنظر إلى مهامه، بمعالجة معطيات ذات طابع شخصي، يتسبب أو يسهل، ولو عن إهمال، الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك"

- تنص المادة 70 من نفس القانون على " يعاقب الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون، وفقاً للقواعد المنصوص عليها في قانون العقوبات"

- تنص المادة 71 من نفس القانون على " يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات، كما يمكن الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة والتي نتج عنها ارتكاب الجريمة ، يؤهل أعضاء ومستخدمو السلطة الوطنية لمعاينة مسح هذه المعطيات"

- تنص المادة 72 من نفس القانون على " يصادر محل الجريمة بغرض إعادة تخصيصه أو تدميره في إطار احترام التشريع الساري المفعول، يتحمل المحكوم عليه مصاريف إعادة التخصيص أو التدمير"

المبحث الثاني : المكانة الإجرائية للدليل التقني في الإثبات الجنائي

نتناول من خلال هذا المبحث مفهوم الإثبات الجنائي و علاقته بالجرائم المعلوماتية ضمن (المطلب الأول) ، ثم نحدد ضمن (المطلب الثاني) الأجهزة المكلفة بالحصول على الدليل التقني .

المطلب الأول : مفهوم الإثبات الجنائي و علاقته بالجرائم المعلوماتية

نتطرق في هذا المطلب إلى تعريف الإثبات الجنائي في (الفرع الأول) ، ثم إبراز علاقته بالإثبات الجنائي في (الفرع الثاني) ، و من خلال (الفرع الثالث) نتناول حجية الإثبات بالدليل التقني .

الفرع الأول : تعريف الإثبات .

أولا - الإثبات لغة:

جاء في لسان العرب المحيط أن الإثبات مأخوذ من : ثَبَتَ الشَّيْءُ يَثْبُتُ ثَبَاتًا وَ ثُبُوتًا فهو ثابتٌ وَ ثَبِيْتُ ، وَ أَثْبَتَهُ هو ، وَ ثَبَّتَهُ بمعنى¹ .

- تنص المادة 72 من نفس القانون على " يعاقب على محاولة ارتكاب إحدى الجنح لمنصوص عليها في هذا القانون، بنفس العقوبات المقررة للجريمة التامة"

- تنص المادة 74 من نفس القانون على " في حالة العود، تضاعف العقوبات المنصوص عليها في هذا الفصل"

1 - كوثر أحمد خالد ، الإثبات الجنائي بالوسائل العلمية ، مكتب التفسير للنشر و الإعلان / أربيل ، الطبعة الأولى ، سنة 2007 ، ص 31 .

ثانيا - التعريف الفقهي للإثبات

يعني إقامة الدليل أمام القضاء بالطرق القانونية التي حددها القانون على وجود واقعة قانونية ترتبت آثارها ، أما الإثبات الجزائي ، فهو وسيلة لإقرار الوقائع التي لها علاقة بالدعوى ، و ذلك وفقا للطرق التي حددها القانون أو إقامة الدليل على وقوع الجريمة و على نسبتها إلى المتهم .

و لكن في الحقيقة يتسم الإثبات بصفة مميزة و هي إظهار الحقيقة سواء عن طريق إدانة المتهم بالتهمة المنسوبة إليه أو براءته منها ، و عليه يكون للإثبات وظيفة مزدوجة ، و ليس وظيفة اتهام الناس فقط كما يلاحظ ذلك من التعريفات السابقة.¹

و يعرف الإثبات الجنائي بأنه إقامة الدليل اليقيني على صحة حدوث الوقائع الجنائية المؤثرة في وقوع ماديّات الجريمة و قيام معنوياتها ، كما تطلبها القانون بجميع ظروفها و نسبتها إلى المتهم بارتكابها، و ذلك وفق الضوابط التي أخضعها لها المشرع و التي يراعي فيها التوازن بين مصلحة المجتمع في معاقبة المذنب و مصلحته في المحافظة على حريات أفراد.²

ثالثا - موقف المشرع الجزائري من تعريف الإثبات

اكتفى المشرع الجزائري بتحديد وسائل الإثبات التي تناقش أمام القاضي الجزائي ، و كرسها في المواد 213 إلى 237 من قانون الإجراءات الجزائية ، تجسيدا لمهمته المتمثلة في سن القوانين ، تاركا تعريف الإثبات للفقهاء .

الفرع الثاني: علاقة الإثبات بالجرائم المعلوماتية

ظهور تكنولوجيا المعلومات كان له نتائج سلبية أهمها ظهور نمط جديد من الجرائم تعرف بالجرائم المعلوماتية ، الأمر الذي حتم على التشريعات مواجهة هذا النوع من

1 - كوثر أحمد خالند ، نفس المرجع السابق ، ص 31.

2 - شعبان محمود محمد الهواري ، أدلة الإثبات الجنائي ، دار الفكر و القانون ، الطبعة الأولى ، ليبيا، سنة 2013، ص 3.

الجرائم عن طريق استحداث نصوص تجريبية في هذا المجال .
فجرائم المعلوماتية كغيرها من الجرائم الأخرى يستوجب إثباتها و لإقامة الحجة على مرتكبيها النوع من الجرائم ، كما أن عملية الإثبات تركز أساساً على الأدلة لإثبات الجرائم كونها السبيل الوحيد الذي يقود إلى برهان صحة الواقعة أو الوقائع المجرمة ، و جاء قانون الإجراءات الجزائية بأحكام و ضوابط لعمليات البحث عن تلك الأدلة و كيفية جمعها و تأمينها بطرق مشروعة ، مما أسفر عن نوع جديد من الأدلة يعرف بالأدلة التقنية كنتيجة طبيعية لجرائم تقنية المعلومات تعتبر وسيلة لإثباتها.¹

الفرع الثالث: نظم الإثبات

تعد نظم الإثبات من أكثر النظم الجزائية تطوراً ، إذ مرت بمراحل عدة مسيرة لمراحل التطور الاجتماعي ، و هي : المرحلة البدائية² ، و المرحلة الدينية³ ، و مرحلة الأدلة القانونية⁴ ، و مرحلة الاقتناع الشخصي للقاضي ، و أخيراً مرحلة الأدلة العلمية و

1 - اللواء د.محمد البشري ، الأدلة الجنائية الرقمية مفهومها و دورها في الإثبات ، المجلة العربية للدراسات الأمنية و التدريب ، المجلد 17 العدد 33 ، الإمارات العربية المتحدة ، سنة 2002 ، ص 91، 92 .

2 - المرحلة البدائية هي مرحلة ما قبل وجود التنظيم الاجتماعي و وجود الدولة ، حيث كان الفرد يأخذ حقه بنفسه حسب قوته الجسدية أو قوة المجموعة التي ينتمي إليها ، و ما ميز هذه المرحلة أن الضعيف لا حق له ، و مع الوقت تجمع الناس و قبائل و أصبح الانتقام من المعتدي إذا كان من عشيرة أخرى ، و ما ميز أدلة الإثبات في هذه المرحلة هو الخضوع للنظام التجريبي البدائي القائم على الميول و التأثيرات الشخصية البحتة .

3 - خلال المرحلة الدينية كانت الإثبات قائماً على الابتغال إلى الآلهة ، حيث اعتقد الناس آنذاك أن الآلهة لها القدرة على كشف الحقيقة و تحديد المجرم ، و من ثم فهي تكافئ الأخيار و تعاقب الأشرار و أنها تنتقم للضعيف عن طريق أناس وسطاء ينقلون طلبات الأفراد إلى الآلهة و يتلقون الجواب و يأمرهم الناس بالتنفيذ ، فساد مذهب الإثبات الديني ، و أهم وسائل الإثبات في هذه المرحلة هي اليمين الحاسمة ، و الابتلاء ، المبارزة القضائية .

4 - الأدلة القانونية تعود جذورها إلى العصر الروماني ن ثم انتشر في أوروبا في القرون الوسطى و زاد اتساعاً على أيدي البربر الذين جاءوا بمبادئ ساعدت في تقوية نظام الأدلة القانونية ، و ارتكزت الفكرة الأساسية لهذا النظام على

هي المرحلة التي ينتسب إليها موضوع بحثنا هذا عامة .

و هكذا تطورت وسائل الحصول على الأدلة بمرورها بمراحل عدة تتفق في كل عصر من العصور و تطور الفكر الإنساني .

و كان من نتائج هذا التطور قيام نظامين للإثبات ، هما: نظام الإثبات الحر و نظام الإثبات القانوني ، فضلا عن بروز بواذر نظام آخر هو نظام الإثبات العلمي¹.

أولاً: نظاما الإثبات الحر و القانوني

أ- جوهر نظام الإثبات الحر يتمثل في أن الاقتناع الشخصي للقاضي هو وحده الذي يتحكم في قرار القاضي الجنائي ، و هذا الاقتناع لابد أن يصدر بكل حرية من ضمير القاضي الذي يكون حراً من جهة اختيار الدليل من بين الأدلة المتعددة ، و من جهة أخرى في تقديرها ، و بعبارة أخرى فهو يكرس مبدأ حرية القاضي في الاقتناع ، كما أنه غير مطالب بتبيان سبب اقتناعه بدليل دون الآخر ، مما يستبعد كل تدخل من طرف المشرع لتقييم مسبق لهذه الأدلة .

ب- بالنسبة لنظام الإثبات القانوني الحقيقة القضائية محددة مسبقا بقواعد قانونية ، بمعنى أن المشرع هو الذي يضبط وسائل الإثبات فيقر قواعد قانونية تبين للقاضي الجنائي وسائل الإثبات المقبولة ، كما تبين موقع هذه الوسائل في السلم التدريجي و قوتها الثبوتية. فدور القاضي يقتصر على مراعاة تطبيق القانون من حيث توفير دليل الإثبات ، فإذا لم يتوفر فإنه لا يجوز له يحكم بالإدانة حتى و لو كان لديه اقتناع شخصي ، و الظاهر أن دور القاضي في هذا النظام هو دور ثانوي يقتصر على مدى توفر الأحكام القانونية المتعلقة بالإثبات و التحقق من مراعاة الشروط القانونية الممهدة للحكم ، فإذا توفرت فإن

المشرع الذي له الدور الإيجابي في عملية الإثبات بحيث يحدد مسألة قبول أدلة معينة و استبعاد أخرى ، كما أنه حجية الأدلة مسبقا .

1 - كوثر أحمد خالد ، المرجع السابق ، ص 31.

القاضي ملتزم بالحكم بالإدانة .¹
ثانيا - نظام الإثبات العلمي

يقصد به الاستعانة بالأساليب العلمية و الفنية التي كشف عنها العلم الحديث في مجال إثبات الجريمة و نسبتها الى مرتكبها أو تبرئته من التهمة المنسوبة إليه ، و استنادا إليه يمارس الخبير دورا رئيسيا ، و تعد القرائن القضائية أهم الأدلة ، و التي تخضع للفحص العلمي الدقيق لاستنباط ما يثبت الإدانة أو البراءة بشكل قاطع .

إن ما يبرر قيام هذا النظام هو أن المجرمين أنفسهم بدأوا باستغلال نتائج التقدم العلمي و تطور التكنولوجيا في ارتكاب الجرائم أو إخفاء معالمها على نحو يصعب معه كثيرا كشفها و معرفة مرتكبيها ، اذ لم يتردد المجرمون في الاستعانة بالوسائل العلمية التي تتيح لمشروعهم الإجرامي أداء أفضل سواء كان ذلك في ابتكار أنواع جديدة من الجرائم أو لمجرد ضمان طرق جديدة لارتكاب الجرائم التقليدية و إخفاء معالمها .

من المعلوم أن الجرائم التي ترتكب في العصر الحديث لم تكن معروفة من قبل ، كالجرائم التي تستخدم بواسطة أجهزة الكمبيوتر ، لاسيما عن طريق شبكات الانترنت ، فهناك نشاطات غير قانونية ترتكب على شبكات الانترنت من قبل أشخاص يخفون هوياتهم الحقيقية وراء ما يسمى بتقنية التشفير ، و هي عبارة عن تقنية تستخدم لحجب المعلومات و كتمها ، و توثيق صحتها من خلال تقنية خاصة تعمل على مزج البيانات أو خلطها على أسس رياضية معينة ، ثم إعادة تلك البيانات في حالة مقروءة .²

1 - محمد مروان ، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري ، الجزء الأول ، ديوان

المطبوعات الجامعية ، الجزائر ، سنة 1999 ، ص 34-39 .

2 - محمد مروان ، نفس المرجع السابق ، ص 39.

ثالثا : موقف المشرع الجزائري من أنظمة الإثبات

أ- موقف المشرع الجزائري من أنظمة الإثبات بصفة عامة

حسم المشرع الجزائري موقفه من أنظمة الإثبات بشكل جلي من خلال نصي المادتين (212 و 307) من قانون الإجراءات الجزائية ، حينما نص في المادة (212) منه على أنه " يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك ، و للقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي " و نص في المادة (307) من نفس القانون على أنه " القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم و لا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما ، و لكنه يأمرهم أن يسألوا أنفسهم في صمت و تدبر ، و يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم و أوجه الدفاع عنها و لم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم .

هل لديكم اقتناع شخصي ؟¹.

بالنظر إلى نصي المادتين يتضح جليا أن المشرع الجزائري تبني كأصل عام نظام الإثبات الحر أو الاقتناع الشخصي للقاضي الجزائري ، و الذي منح من خلاله للقاضي الجزائري في مجال تقدير الأدلة وفقا لقناعته الذاتية ، و فتح أمامه باب الإثبات على مصرعيه كي يستلهم عقيدته من أي موطن يراه ، دون أن يطالبه بتقديم مبرر لذلك ، و هو ما نستشفه من قول المشرع ضمن نص المادة 212 من قانون الإجراءات الجزائية بقوله " ..يحوز إثبات الجرائم بأي طريقة من طرق الإثبات ... " ، و في الوقت نفسه و على سبيل الاستثناء نجده أخذ بنظام الإثبات المقيد أو ما يسمى كذلك بأنظمة الأدلة القانونية في إثبات بعض الجرائم ، أين اشترط لإثباتها أدلة قانونية محددة مسبقا على سبيل الحصر بقوله أيضا في نص المادة 212 من نفس القانون " .. ما عدا الأحوال التي ينص فيها القانون على غير ذلك .. " ، كما هو الشأن بخصوص جريمة الزنا المنصوص

1 - براهيم جمال ، التحقيق الجنائي في الجرائم الالكترونية ، أطروحة دكتوراه في العلوم تخصص القانون ، جامعة مولود معمري - تيزي وزو ، الجزائر، سنة 2018 ، ص 168 .

عليها في المادة (339) من قانون العقوبات ، حيث حدد أدلة إثبات الجريمة ضمن نص المادة 341 من نفس القانون التي تنص على مايلي " الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها المعاقب عليها بالمادة 339 يقوم إما على محضر قضائي أحد رجال الضبط القضائي عن حالة تلبس و إما بإقرار وارد في رسائل أو مستندات صادرة من المتهم و إما بإقرار قضائي.

و قد تأكد الأخذ بنظام الإثبات الحر كذلك بطريقة غير مباشرة في العديد من نصوص قانون الإجراءات الجزائية ، فيما يخص جهات الحكم ، نذكر منها الفقرة الأولى من نص المادة (235) التي تنص على أنه " يجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة " ، و كذلك الفقرة الأولى من المادة (286) ...له (رئيس الجلسة) سلطة كاملة في ضبط حسن سير الجلسة و فرض الاحترام الكامل و اتخاذ أي إجراء يراه مناسباً لإظهار الحقيقة .."¹

من خلال ما سبق التطرق إليه يتضح لنا أن المشرع الجزائري لم يقيد القاضي الجزائري بتحديد الأدلة مسبقاً، بل فتح له المجال لاقتناعه الشخصي كأصل عام ، إلا في حالات استثنائية ، نظراً لخصوصيات بعض الجرائم كما أشرنا إليه سابقاً.

ب - موقف المشرع الجزائري من الإثبات في جرائم المعلوماتية بوجه خاص

المشرع الجزائري لم يضع أي نصوص قانونية صريحة بهذا الخصوص حيث تم الاستناد في هذا الموضوع للمادة 212 من قانون الإجراءات الجزائية السابق الإشارة إليها ، و التي أطلق من خلالها مبدأ حرية الإثبات ، لكن المشرع أدرك أن هذا لا يكفي لوحده ، فيما بعد وضع القانون رقم 04/15 المؤرخ في 10 نوفمبر 2004 ، المتمم و المعدل للأمر 156/66 المتضمن قانون العقوبات و الذي خصص القسم السابع مكرر منه تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات " و لقد جاء في عرض أسباب

1 - براهيمى جمال ، المرجع السابق ، ص 168.

هذا التعديل مواكبة التطور التكنولوجي و المعلوماتي و انتشار وسائل الاتصال الحديثة التي أدت بدورها إلى ظهور أشكال جديدة للإجرام ، و كذلك يهدف هذا القانون إلى توفير حماية جزائية للأنظمة المعلوماتية و أساليب المعالجة الآلية للمعطيات ، و كان هذا القانون كنتيجة حتمية لما أفرزته ثورة تقنية المعلومات التي مست مصالح جديدة غير تلك التي يحميها قانون العقوبات ، فقد تطرق المشرع الجزائي إلى تجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات من خلال تعديل قانون العقوبات بموجب القانون 04/15 ، الذي تضمن تسعة مواد تطرق المشرع من خلالها إلى حماية و سرية و سلامة المعلومات و نظم معالجتها و ذلك من المواد 394 مكرر إلى 394 مكرر 8 .¹

بعدها تدخل المشرع الجزائي لحماية التعاملات الرقمية حين وضع القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و من خلال هذا القانون أدرج المشرع طريقة ضبط الأدلة التقنية و التي تتخذ صورتين ، الصورة الأولى² تكمن في نسخ المعطيات محل البحث عن تخزين المعلومات الرقمية على أن تكون هذه المعطيات مهياة بشكل يجعلها قابلة لحجزها و وضعها في أحرار حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية ، و الصورة الثانية³ تتمثل في الاستعانة بالتقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي

1 - نور الهدى محمودي ، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية ، مجلة الباحث للدراسات الأكاديمية ، العدد الحادي عشر ، جوان 2017 ، ص 922.

2 - تنص المادة 6 على " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية ..."

3 - تنص المادة 7 " إذا استحال إجراء الحجز وفقا لما هو منصوص في المادة 6 أعلاه ، لأسباب تقنية ، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية ، أو إلى نسخها ، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة .

تحويلها هذه المنظومة أو القيام بنسخها ، و يكون ذلك في حالة صعوبة الحصول على هذه الأدلة وفقا للصورة الأولى.

و هذا يعني أن الدليل التقني يخضع في ضبطه و تحريزه إلى قواعد تحريز الأدلة الجنائية عموما ، إلا أنه و نظرا إلى الطبيعة الخاصة له فإن عملية الحصول عليه تحتاج لبعض الإجراءات الخاصة التي تحافظ عليه و تحميه من العبث به و تغييره ، و هذا ما أشارت إليه المادة 06 في فقرتها 3 (ج) من القانون رقم 04/09 و التي تلزم السلطات المعنية بعملية ضبط الدليل الرقمي أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية ، و أن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات ¹.

و الملاحظ أن تخصيص المشرع الجزائي لهذه الجرائم قسما خاصا في قانون العقوبات دلالة على إقراره بأنها ظاهرة مستجدة و متميزة عن الجرائم التقليدية الأخرى من حيث المصالح التي تطلها و كذا من حيث مبنائها و طبيعتها و محلها ، و من ثم لا يمكن إدراجها تحت أي نوع من الجرائم التقليدية.

كما أنه لم يميز في وضعه لهذه النصوص القانونية نوعية المعلومات التي تطلها الجريمة فيما إذا كانت معلومات تتصل بمصالح اقتصادية أو مالية أو مسائل أمنية ، و ذلك سعيا من المشرع الجزائي إلى تعميم الحماية للمعلومات بكافة أنواعها ما عدا تشديد العقوبة إذا كانت المعلومات المستهدفة متعلقة بالدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام .

و منه يتضح لنا أن المشرع الجزائي و من خلال القانون رقم (04-09) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها أية استثناءات أو أوضاع خاصة بهذا الصدد ، مما يوحي بأن الأدلة التقنية

1 - نور الهدى محمودي ، المرجع السابق، ص 922.

مقبولة في مجال الاعتداء على نظم المعالجة الآلية بصفة خاصة ، حيث يمثل مظهرا من مظاهر اعتناق المشرع لمبدأ حرية الإثبات و الاقتناع.¹

الفرع الرابع - حجية الإثبات بالدليل التقني

بالنسبة للمشرع الجزائري فقد بينا فيما سبق بأنه أجاز إثبات الجرائم بأية طريقة من طرق الإثبات ماعدا الجرائم التي قد يتطلب إثباتها دليلا معينا ، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن إليه ، و لكن السؤال الذي يثار هنا هو هل تتصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي الجزائري إلى الأدلة المستخرجة من الوسائل الالكترونية أو ما يسمى بالأدلة التقنية والرقمية؟

بالرجوع إلى القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجده خاليا من أية أحكام خاصة تتعلق بحجية المخرجات الالكترونية في الإثبات ، ومن هنا فسكوت المشرع عن هذا الأمر هو تفسير لنيته في إخضاع هذه الأدلة مثلها مثل باقي الأدلة الأخرى للقواعد العامة.²

وإذا أخذنا في الحسبان بأن الجرائم المعلوماتية تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكل الأفعال الإجرامية الأخرى التي ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام الاتصالات الالكترونية كما صرحت المادة 02 من القانون رقم 04-09 ، فإن ذلك يعني أن الإجرام المعلوماتي قد يأخذ وصف المخالفة أو الجنحة أو الجناية بحسب طبيعة الجرم المرتكب.

اعتبارا لذلك ، فإن كان مبدأ الاقتناع القضائي عام النطاق لدى كافة أنواع المحاكم الجزائية سواء كانت محاكم الجنايات أم الجنح أم المخالفات ، وبدون تفرقة بين القضاة و

1 - نور الهدى محمودي ، المرجع السابق، ص 169.

2 - براهمي جمال ، المرجع السابق ، ص 176.

المحلفين ، وأنه يمتد كذلك ليشمل إلى جانب جهات الحكم جهات التحقيق و الإحالة ، إلا أن قواعد بيان عناصر تقدير القاضي للدليل تختلف حسب اختلاف وصف الفعل المجرم .

فإذا كان الفعل الإجرامي يحمل وصف جنائية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها وفقا لمحضر قناعتها دون أن يكون قضاتها مطالبين بتسبيب أو تعليل أحكامهم ودون أن تكون لجهات الطعن في ذلك رقابة عليهم ، أما إذا أخذ الفعل المجرم وصف جنحة، فإن القاضي في هذه الحالة يكون مطالبا ببيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه ، والذي يكون محل رقابة من قبل جهات الطعن ، وليس المراد بالالتزام القاضي بالتسبيب هنا أن يبين في حكمه لماذا اقتنع و الكيفية التي استمد بها اقتناعه ، و العلة في اقتناعه بها ، لأن ذلك يدخل في نطاق السلطة التقديرية المعترفة له قانونا، إنما المراد هو حمله على الإفصاح عن مصادر اقتناعه توطئة للنظر فيما إذا كان من شأنها أن تؤدي منطقيا لما انتهى إليه¹.

وعليه فقاضي الموضوع في مواد الجرح مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات بما فيها وسائل الإثبات الالكترونية التقنية ، والتي قد تأخذ شكل محاضر معدة بمناسبة استجواب أو تفتيش ، مراقبة الكترونية أو اعتراض مراسلات ، أو شكل تقرير خبرة محرر بمناسبة معاينة وفحص الأدلة المضبوطة من أجهزة أو دعامات الكترونية.

فأما ما يتعلق بالمحاضر، فالمرجع الجزائري اعتبرها كقاعدة عامة مجرد استدلالات ما لم ينص القانون على خلاف ذلك ، ولا تكون للمحضر أية قوة إثبات إلا إذا كان صحيحا من حيث الشكل ، وتم إعداده من طرف واضعه أثناء مباشرة أعمال وظيفته وأورد فيه موضوعا داخلا في نطاق اختصاصه ، غير أن المحاضر التي يخول القانون إعدادها بموجب نص خاص لإثبات جنح معينة كمحاضر الجلسات في المحاكمة ومحاضر التحقيق الصادرة عن قاضي التحقيق فإنها تتمتع بحجية ما لم يدحضها دليل عكسي و قد

1 - براهيم حمال ، المرجع السابق ، ص 177 ، 178.

سوى المشرع من خلال هذه الأحكام بين المحاضر المعدة حول الجرائم المعلوماتية وتلك المتعلقة بأية جريمة تقليدية أخرى ، وترك تقدير قيمتها الاستدلالية للقاضي الجزائي .

وأما بالنسبة لتقارير الخبرة فشأنها شأن باقي أدلة الإثبات تخضع لمناقشة و تقدير قاضي الموضوع ، كما استشف من نص المادة 215 من قانون الإجراءات الجزائية التي تنص على أنه " لا تعتبر... والتقارير المثبتة للجنايات أو الجرح إلا مجرد الاستدلالات.." وهو المعنى الذي أكدته المحكمة العليا في عدة قراراتها ومنه ما تضمنه القرار المؤرخ في 14 نوفمبر 1981 بأن " تقرير الخبرة ليس إلا عنصرا من عناصر الاقتناع يخضع لمناقشة الأطراف و تقدير قضاة الموضوع" 1.

ومع هذا فالطبيعة العلمية والفنية التي تتميز بها الجرائم الالكترونية ، بالإضافة إلى نقص ثقافته الفنية في هذا المجال غالبا ما تفرض على القاضي الجزائي الجزائري الاستناد في تكوين اقتناعه وبدون تردد على الخبرة الفنية والتقدير بالنتائج المفضي إليها في تقرير الخبرة ، ولا يمكنه طرحها واستبعادها إلا إذا قدر أن ما تحتويه من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة والمنطق العلمي ، إذ حدث وأن اكتفى القاضي الجزائي في عدة قضايا بالخبرة وحدها للفصل في وقائع ذات طابع تقني بحث دون أن يتعرض لمناقشة نتائجها.

خلاصة الأمر، أن موقف المشرع الجزائري من الإثبات بالأدلة التقنية هو على العموم موقف التشريعات التي أخذت بنظام الإثبات الحر، إذ أجاز الإثبات في المسائل الجزائية بكافة وسائل الإثبات ، أيا كان نوعها أو طبيعتها، على نحو تكون فيه جميع الأدلة متساوية ومتساندة في قيمتها التدليلية ، ومقبولة أمام القضاء الجزائي من حيث المبدأ، خاضعة لتقدير وموازنة قاضي الموضوع الذي يكون له مطلق الحرية في أن يأخذ عقيدته من أية بيئة أو قرينة يرتاح إليها، وله أن يبني اقتناعه من أدلة وي طرح غيرها.

فلا وجود في ظل التشريع الجزائري ، لأدلة يحظر مقدما على القاضي الجزائي قبولها يتولد معه اقتناعه يكون مبدئيا مقبولا ، وبالتالي فليس ثمة ما يمنع القاضي من قبول

1 - براهيمى جمال ، المرجع السابق ، ص 179.

الأدلة الالكترونية تسجيلات وبيانات ومخرجات الحاسب الآلي ، كأدلة يدخل تقدير قيمتها الإثباتية في دائرة اقتناعه ما دام أنها تتوافر على شروط المشروعية والسلامة من العبث والخطأ¹.

المطلب الثاني: الأجهزة المكلفة بالحصول على الدليل التقني

نتطرق في هذا المطلب إلى الأجهزة المكلفة بالتحقيق في جرائم المعلوماتية ، باعتبارها من الوسائل المهمة و المسخرة لغرض مكافحة هذا النوع المستحدث من الجرائم ، التي تتمثل في هجمات و سلطات و أجهزة أمنية تعتبر أداة فعالة في الحد من هذا النوع من الجرائم .

الفرع الأول: الأجهزة العامة المكلفة بالحصول على الدليل التقني

إن الحديث عن الدليل التقني يفرض علينا التطرق إلى الأجهزة المكلفة بالحصول عليه ، و هذا ما سنتطرق إليه من خلال هذا الفرع ، حيث نتناول الهيئات و الأجهزة المخولة قانونا بالحصول على الدليل التقني كالتالي :

أولاً- الهيئات القضائية الجزائية المختصة

أنشأت بموجب القانون 04-14 ، المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية ، و تختص الجهات القضائية طبقا للمواد 37-329-40 من قانون الإجراءات الجزائية بالجرائم الماسة بالمعالجة الآلية للمعطيات ، اختصاصا إقليميا موسعا طبقا للمرسوم التنفيذي 06-348 المؤرخ في 05 جانفي 2006.

إمكانية قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال المرتكبة في الخارج حتى و لو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني حسب المادة 15 من القانون 09-04.²

1 - براهيم جمال ، المرجع السابق ، ص 180.

2 - مولود ديدان ، قانون الإجراءات الجزائية ، الأمر 11-02 ، دار بلقيس الجزائر ، سنة 2012، ص 18 .

أ - توسيع صلاحيات الضبطية القضائية : عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، كما يمكن تمديد الاختصاص المحلي على كامل الإقليم الوطني حسب المادة 16 من قانون الإجراءات الجزائية ، كما يمكن القيام بتفتيش المحلات السكنية و غير السكنية في كل ساعة من ساعات الليل و النهار بإذن من وكيل الجمهورية في كل ساعة من ساعات الليل و النهار طبقا لنص المادة 47 من قانون الإجراءات الجزائية.¹

ب - أساليب التحري الخاصة: تتمثل فيما يلي :

- القيام باعتراض المرسلات الالكترونية ، طبقا لنص المادة 65 مكرر 5 من قانون الإجراءات الجزائية ، المدرج بموجب القانون رقم 06-22 ، المؤرخ في 12 ديسمبر 2006.

- القيام بالتسرب وفقا للمادة 65 مكرر 11 من قانون الإجراءات الجزائية .

- القيام بتفتيش المنظومة المعلوماتية طبقا لنص المادة 5 من القانون 09-04.

- حجز المعطيات المعلوماتية ، المادة 6 من القانون 09-04 .

- نسخ المعطيات على دعامة تخزين الكترونية .

- إمكانية منع الوصول إلى معطيات تحتويها المنظومة .

- منع الاطلاع على المعطيات التي يشكل محتواها جريمة.²

ثانيا- المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني

أنشأ بموجب المرسوم الرئاسي رقم 04-183 المتضمن إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني ، حيث نصت المادة الأولى منه على "

1 - بن نعم خالد أمين ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر في الحقوق ، تخصص قانون جنائي ، جامعة عبد الحميد بن باديس مستغانم ، الجزائر ، سنة 2019 ، ص 41.

2 - بن نعم خالد أمين ، المرجع السابق ، ص 42.

يحدث معهد وطني للأدلة الجنائية و علم الإجرام للدرك الوطني ، يدعى في صلب النص " المعهد " .¹

أ - تعريفه: عرفته المادة 2 من نفس المرسوم بما يلي : " المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلال المالي " .

و يوضع تحت وصاية وزير الدفاع الوطني و يمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه ، و بهذه الصفة ، فإنه يخضع إلى جميع الأحكام التشريعية و التنظيمية المطبقة على المؤسسات العسكرية " .

حددت مهام المعهد بموجب المادة 4 من نفس المرسوم ، و من أهمها إجراء الخبرات و الفحوص العلمية في إطار التحريات الأولية و التحقيقات القضائية ، و هذا بغرض إقامة الأدلة من بينها الأدلة التقنية التي تسمح بالتعرف على مرتكبي جرائم المعلوماتية ، بالإضافة إلى رصد و مراقبة و تتبع عمليات الاختراق و القرصنة المعلوماتية ، و كذا اكتشاف المعلومات المسروقة و تفكيك البرامج المعلوماتية ، تقديم المساعدة أثناء القيام بالتحريات ، المشاركة في الدراسات للتقليل من الإجرام ، تصميم بنوك معطيات ، المشاركة في الفحوص و الخبرات بصفته هيئة ، المبادرة بالبحوث ، المشاركة في الملتقيات و الندوات على الصعيدين الوطني و الدولي ، تنظيم دورات التكوين .²

1 - المادة الأولى ، من المرسوم الرئاسي رقم 04-183 ، المؤرخ في 26 جوان 2004 ، يتضمن إحداث المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني و تحديد قانونه الأساسي ، الجريدة الرسمية العدد 41 لسنة 2004.

2 - تنص المادة 4 من المرسوم الرئاسي على " يكلف المعهد بما يأتي : ، إجراء.. الخبرات و الفحوص العلمية..بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات و الجنج ..تقديم مساعدة علمية...المشاركة في الدراسات و التحاليل..تصميم بنوك معطيات..المشاركة في ..تحديد السياسة الجنائية..المبادرة بالبحوث المتعلقة بالإجرام..العمل على ترقية..أساليب التحريات..المشاركة في الملتقيات ..تنظيم دورات تحسين المستوى"

ب - تنظيم المعهد : حسب المادة 6 من نفس المرسوم " يتكون المعهد من الهياكل الآتية :

- مديرية للأدلة الجنائية.
- مديرية للدراسات و البحوث الإجرامية.
- مصلحة للتنظيم و المناهج .
- مصلحة للإدارة و الوسائل .

ثالثا - المعهد الوطني للبحث في علم التحقيق الجنائي التابع للمديرية

العامة للأمن الوطني (المعهد الوطني للشرطة الجنائية)

أنشأ المعهد الوطني للأدلة الجنائية و علم الإجرام بموجب المرسوم الرئاسي رقم 432-04 ، المؤرخ في 29 ديسمبر 2004¹ الذي نص في المادة الأولى منه على " ينشأ معهد وطني للبحث في علم التحقيق الجنائي يدعى في صلب النص "معهد" .

أ - تعريفه: عرفته المادة 2 من نفس المرسوم على أن " المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلال المالي " ²، و وضع المعهد تحت وصاية الوزير المكلف بالداخلية و يتبع المديرية العامة للأمن الوطني حسب المادة 3 من نفس المرسوم ، كما حدد مقره بمدينة الجزائر ، مع إمكانية نقله أي مكان آخر من التراب الوطني ، بقرار من الوزير المكلف بالداخلية ، حسب المادة 4 من نفس المرسوم.

حددت مهام المعهد بموجب المادة 5 من نفس المرسوم المذكور أعلاه ، المتمثلة عموما في القيام بعمليات التحليل ، من خلال تحليل الأدلة التقنية المأخوذة من مسرح الجريمة الإلكترونية أو عن طريق البحث عن الدليل التقني عن بعد بواسطة الشبكات من خلال برامج أو تطبيقات خاصة تستعين بها لتحديد هوية مرتكب الجريمة و مكان تواجده ، التكوين و تحسين المعارف ، المساهمة في وضع مراجع في مجال علم التحقيق

1 - المرسوم الرئاسي رقم 432-04 ، المؤرخ في 29 ديسمبر 2004 ، يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي ، الجريدة الرسمية العدد 84 لسنة 2004.

2 - المادة 2 ، نفس المرجع السابق.

الجنائي ، إعداد بنك معطيات في مجال التحقيق الجنائي ، القيام بالدراسات و الأبحاث في علم التحقيق الجنائي ، القيم بالشراكة مع المعاهد و الجامعات المتخصصة على الصعيدين الداخلي و الخارجي.. إلخ.¹

ب - تنظيم المعهد : نصت المادة 7 من نفس المرسوم المشار إليه أعلاه ، و جاء في مضمونها ما يلي: " يضم تنظيم المعهد ما يلي :

- قسم علمي.
 - قسم تقني.
 - مصلحة قاعدة المعطيات .
 - مصلحة الإدارة و الوسائل.
 - يتوفر المعهد زيادة على ذلك على مخابر جهوية .
- تجسيدا لما جاء في المرسوم 04-432 ، أنشأت المديرية العامة للأمن الوطني أربع مخابر جهوية للشرطة العلمية و التقنية في وهران ، قسنطينة ، بشار ، تمنراست ، و لمواكبة التطور الحاصل في مختلف أشكال الإجرام قامت سنة 2007 بتدعيم مخابر الشرطة العلمية و التقنية بأقسام مختصة في الأدلة التقنية ، تكمن مهامها في استغلال الأجهزة الالكترونية التي يشتهب استعمالها في ارتكاب الجرائم و ذلك بهدف استخراج المعطيات المخزنة بداخلها و التي من شأنها أن تساعد المحققين في التحقيق و التي تشكل في ذاتها أدلة إقناع.²

1 - تنص المادة 5 من المرسوم الرئاسي رقم 04-432 ، المرجع السابق ، على " يتولى المعهد المهام الآتية : تحليل المؤشرات المادية.. إعداد تقارير الخبرة .. القيام بأعمال التكوين .. المساهمة في وضع مراجع في مجال علم التحقيق الجنائي .. القيام بالتسيير الممرکز لوثائق الإثبات و للعينات المرجعية ذات العلاقة ببنوك المعطيات .. تطوير..برتوكولات الخبرة الخاصة بالأدلة المتعلقة بعلم التحقيق الجنائي..القيام ..بكل دراسة أو بحث في علم التحقيق الجنائي..القيام بنشر الوثائق و أعمال الدراسات و البحث ذات الصلة بالنشاطات العلمية و التقنية..القيام بالشراكة العلمية.. "

2 - علاوي محمد ، دور الأمن المعلوماتي في الحد من الجريمة المعلوماتية ، مذكرة ماستر في الحقوق ، تخصص قانون جنائي ، جامعة محمد خيضر بسكرة ، السنة الجامعية 2016-2017 ، ص 105، 106.

كما تم استحداث فرقة مكافحة الجرائم المعلوماتية على مستوى المصالح الولائية للشرطة القضائية بأمن الولايات .

الفرع الثاني : الأجهزة المتخصصة المكلفة بالحصول على الدليل التقني

نتناول ضمن هذا الفرع الأجهزة العامة المكلفة بالحصول على الدليل التقني المتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، و السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ، وفق مايلي :

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و

الاتصال و مكافحتها .

نص المشرع في المادة 13 من القانون 04-09 المتضمن القواعد الخاصة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، على ضرورة إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، كما نصت الفقرة الثانية من نفس المادة على أن تحديد تشكيلة الهيئة و تنظيمها و كفاءات سيرها عن طريق التنظيم.¹

1 - التعريف بالهيئة: أنشأت بموجب القانون 04-09 المذكور أعلاه ، و عرفت عن طريق التنظيم بموجب المادة 2 من المرسوم الرئاسي رقم 15-261² ، على أنها " الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي ، توضع لدى الوزير المكلف بالعدل ، و حدد مقر الهيئة بالجزائر العاصمة ، حسب نفس المرسوم³ .

1 - تنص المادة 13 من القانون 04-09 ، المرجع السابق ، على " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ن تحدد تشكيلة الهيئة و تنظيمها و كفاءات سيرها عن طريق التنظيم "

2 - المادة 2 من المرسوم الرئاسي رقم 15-261 ، المؤرخ في 08 أكتوبر 2015 ، المحدد لتشكيلة و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، الجريدة الرسمية العدد 53 لسنة 2015 .

3 - المادة 3 من المرسوم الرئاسي 15-261 ، نفس المرجع.

- 2 - مهام الهيئة : حددت الهيئة ضمن المادة 14 من القانون 09-04¹ المشار إليه أعلاه ، حيث تتولى خصوصا المهام الآتية:
- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحته.
 - مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام و الاتصال بما في ذلك تجميع المعلومات و إنجاز الخبرات القضائية .
 - تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و تحديد مكان تواجدهم.
- بالإضافة إلى الاختصاصات المحددة بموجب المادة 04 من نفس المرسوم الرئاسي 15-261² .

ب - السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

- استحدث المشرع الجزائري السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب المادة 22 من القانون 18-07³ ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .
- 1 : تعريفها : عرفت المادة 22 المذكورة أعلاه ، على أنها سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي يشار إليها "بالسلطة الوطنية" ، حدد مقرها

1 - المادة 14 من القانون 09-04 ، المرجع السابق.

2 - المادة 4 من المرسوم الرئاسي رقم 15-261 ، المرجع السابق .

3 - تنص المادة 22 من القانون 18-07 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية العدد 34 ، على " تنشأ لدى رئيس الجمهورية ، سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي يشار إليها أدناه " السلطة الوطنية" يحدد مقرها بالجزائر العاصمة ، تتمتع السلطة الوطنية بالشخصية المعنوية و الاستقلال المالي و الإداري ، تقيّد ميزانية السلطة الوطنية في ميزانية الدولة و تخضع للمراقبة المالية طبقا للتشريع المعمول به "

بالجزائر العاصمة ، تتمتع بالشخصية المعنوية و الاستقلال المالي و الإداري .¹

2 - مهامها : حدد المشرع الجزائري مهام السلطة الوطنية بموجب المادة 25 من نفس القانون ، التي نصت على أنه " تكلف السلطة الوطنية بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون ، و ضمان عدم انطواء استعمال تكنولوجيا الإعلام و الاتصال على أي أخطار تجاه حقوق الأشخاص و الحريات العامة و الخاصة" و تتمثل مهامها في هذا الصدد لا سيما في :

- منح التراخيص و تلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إعلام الأشخاص المعنيين و المسؤولين عن المعالجة بحقوقهم و واجباتهم .
- تقديم الاستشارات للأشخاص و الكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.
- تلقي الاحتجاجات و الطعون و الشكاوي بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي و إعلام أصحابها بمآلها .
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص إليها في هذا القانون.
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.
- الأمر بإغلاق معطيات أو سحبها أو إتلافها .
- تقديم أي اقتراح من شأنه تبسيط و تحسين الإطار التشريعي و التنظيمي لمعالجة المعطيات ذات الطابع الشخصي .
- نشر التراخيص الممنوحة و الآراء المدلى بها في السجل الوطني المشار إليه في المادة 28 من هذا القانون .

1 - المادة 22 من القانون 07-18 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع

الشخصي، المرجع السابق .

- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.
- إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون .
- وضع معايير في مجال المعطيات ذات الطابع الشخصي.
- وضع قواعد السلوك و الأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

في إطار ممارسة مهامها ، تعلم السلطة الوطنية النائب العام المختص فورا ، في حالة معاينة وقائع تحتل الوصف الجزائي.

تعد السلطة الوطنية تقريرا سنويا حول نشاطها ترفعه إلى رئيس الجمهورية.¹

ب - المنظومة الوطنية لأمن الأنظمة المعلوماتية

استحدثت المنظومة بموجب المرسوم الرئاسي رقم 20-05 ، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.²

أولا - تعريفها : عُرِفَت المنظومة بموجب المادة 2 من نفس المرسوم على أنها " المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية ، و تشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية و تنسيق تنفيذها"³.

كما نصت المادة 3 من نفس المرسوم على ما يلي "تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني ، ما يأتي :

- مجلس وطني لأمن الأنظمة المعلوماتية ، يدعى في صلب النص "المجلس" و يكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية ، و الموافقة عليها و توجيهها.
- وكالة لأمن الأنظمة المعلوماتية تدعى في صلب النص "الوكالة"، و تكلف بتنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

1 - المادة 25 من القانون 07-18 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، المرجع السابق.

2 - مرسوم رئاسي رقم 20-05 ، المؤرخ في 20 جانفي 2020 ، المتعلق بوضع بمنظومة وطنية لأمن الأنظمة المعلوماتية ، الجريدة الرسمية عدد 04 لسنة 2020.

3 - المادة 2 من مرسوم رئاسي رقم 20-05 ، المتعلق بوضع بمنظومة وطنية لأمن الأنظمة المعلوماتية ، نفس المرجع.

و لممارسة مهامه يتوفر المجلس بالإضافة إلى الوكالة ، على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال.¹

الفرع الثالث : دور مزودي الخدمات في التحري عن الجرائم الماسة بالمعالجة الآلية للمعطيات

إن توصيل خدمات الاتصالات السلكية و اللاسلكية كالهاتف و الشبكات الرقمية المتمثلة في الانترنت ، يتطلب توافر مجموعة من الفاعلين على رأسهم مقدمو الخدمات ، المعرفين ضمن المادة 2 الفقرة "د" من القانون 04-09:

- أي كيان عام أو خاص يقدم لمستعملي خدماته ، القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام اتصالات.

- و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمات الاتصال المذكورة أو لمستعمليها .²

و تجدر الإشارة إلى أن المشرع في تعريفه لمقدمي الخدمات قد جمع ثلاثة أنواع من الوسطاء يسمح تدخلهم بتوصيل خدمات تكنولوجيا المعلوماتية بأنواعها إلى مستعمليها و هم مقدمو(متعهدي خدمة التوصيل) ، متعهدي الإيواء ، مقدمو المضمون .³

1 - المادة 3 من المرسوم الرئاسي رقم 05-20 ، المتعلق بوضع بمنظومة وطنية لأمن الأنظمة المعلوماتية ، المرجع السابق.

2 - المادة 2 من القانون 04-09 ، المرجع السابق .

3 - عفاف خديري ، الحماية الجنائية للمعطيات الرقمية ، أطروحة دكتوراه في القانون الجنائي ، جامعة العربي تبسي تبسة ، الجزائر ، سنة 2017-2018 ، ص 141.

كما نص المشرع على التزامات مقدمو الخدمات ضمن المادة 10 من القانون 04-09 ، المتمثلة أساسا في مساعدة السلطات المكلفة بالتحريات القضائية ، حفظ المعطيات المتعلقة بالسير ضمن المادة 11 من نفس القانون ، إضافة إلى الالتزامات الخاصة بمقدمي خدمة الانترنت ضمن المادة 12 أيضا من نفس القانون.¹

1 - تنص المادة 10 من القانون 04-09 ، المرجع السابق ، على " في اطار تطبيق أحكام هذا القانون ، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ..بوضع المعطيات تحت تصرف السلطات المذكورة ، و يتعين على مقدمي الخدمات كتمان السر المهني ..تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق"

- تنص المادة 11 من نفس القانون على " ..يلتزم مقدمو الخدمات بحفظ: المعطيات التي تسمح بالتعرف على مستعملي الخدمة ، المعطيات ..الطرفية المستعملة للاتصال..الخصائص التقنية و كذا تاريخ و مدة الاتصال..المعطيات المتعلقة باخدمات التكميلية المطلوبة أو المستعملة و مقدميها..المعطيات التي تسمح بالتعرف على المرسل إليه ..إليهم الاتصال و كذا عناوين المواقع المطلع عليها ، بالنسبة لنشاطات الهاتف ، يقوم المتعامل بحفظ المعطيات ..التي تسمح بالتعرف على مصدر الاتصال و تحديد مكانه ..تحدد مدة الحفظ ..بسنة واحد من تاريخ التسجيل دون الاخلال بالعقوبات الادارية ..تقوم المسؤولية الجزائية للأشخاص الطبيعيين و المعنويين عند ما يؤدي ذلك الى عرقلة حسن سير التحريات القضائية ، و يعاقب الشخص الطبيعي بالحبس.. و بغرامة ..، يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات، تحدد كيفيات تطبيق الفقرات 1 و 2 و 3 ..عن طريق التنظيم"

- تنص المادة 12 من نفس القانون على " زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات الانترنت' ما يأتي: أ- التدخل الفوري لسحب المحتويات ..ب- وضع ترتيبات تقنية تسمح بحصر امكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام و الآداب العامة..."

تناولنا من خلال هذا الفصل ماهية الدليل التقني ، إضافة الى البيئة التي ينشأ فيها و المتمثلة في النظام المعلوماتي ، كما تطرقنا الى الحماية الجنائية التي أقرها المشرع الجنائي للنظام المعلوماتي .

في ذات السياق ، تناولنا علاقة الإثبات الجنائي بالجرائم المعلوماتية و الطبيعة التقنية للدليل المستتبط من نظم المعلوماتية ، مع إبراز حجية الدليل التقني في إثبات هذا النوع من المستحدث من الجرائم .

كما تم التطرق إلى الأجهزة المكلفة باستخلاص الدليل التقني ، و التي تتمثل في أجهزة عامة و أخرى خاصة لكل منها دور في استخلاص هذا الدليل وفق الاجراءات التي أقرها المشرع الجنائي .

الفصل الثاني

القواعد الإجرائية

الكفيلة بالحصول على الدليل التقني

المبحث الأول : القواعد الإجرائية التقليدية الكفيلة بالحصول على الدليل التقني

يصعب في غالبية الأنظمة القانونية الحالية أن نحدد إلى أي مدى تكفي الأساليب التقليدية لإجراءات جمع الأدلة من أجل مباشرة تحقيقات ناجحة في مجال جرائم المعلوماتية.

و مما لا شك فيه أن المشرع لم يجر استخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها : المعاينة ، الخبرة ، التفتيش و ضبط الأشياء ، والشهادة ، و مما لا شك فيه أيضا أن هذه القواعد عامة النطاق تنظم استخلاص الدليل في جميع الجرائم ، تقليدية كانت أم مستحدثة إلا أنها في الثانية قد تكون بحاجة إلى تطوير لكي تتناسب مع طبيعتها الخاصة و طبيعة الدليل الذي يصلح لإثباتها و هو ما سوف نتعرف عليه من خلال ما يلي : 1

المطلب الأول: المعاينة و الخبرة

نتناول من خلال هذا المطلب إجرائي المعاينة و الخبرة و توضيح دورهما في مجال إثبات جرائم المعلوماتية ، ضمن فرعين متتاليين .

الفرع الأول : المعاينة

عرف جانب من الفقه المعاينة بأنها " رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته و ضبط كل ما يلزم لكشف الحقيقة " و قد عرفها البعض بأنها " إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه و يجمع الآثار المتعلقة بالجريمة و كيفية وقوعها و كذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة " ، و أي كان تعريفها فهي تتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها من أجل إثبات حالته و ضبط الأشياء التي تفيد في إثبات وقوعها و نسبتها إلى فاعلها ، و الأصل في المعاينة أنها إجراء من إجراءات التحقيق ، و لذلك ففي غير حالات التلبس التي نص

1- سعيداني نعيم ، المرجع السابق ، ص 143 .

عليها القانون يلزم أن تقوم بها سلطة التحقيق أو تنتدب ضابط الشرطة القضائية للقيام بها ، و يقتضي ذلك تحرير محضر عن طريق كاتب ، لأنها من الإجراءات التي تستلزم تفرغا ذهنيا ، و تتبع في شأنها أيضا جميع القواعد التي تحكم إجراءات المحاكمة ، من إخطار الخصوم بمكان المعاينة و زمانها ليتمكنوا من الحضور أثناء إجراءاتها ، كما يمكن للمحكمة أن تقوم بإجراء المعاينة إذا ما رأت في ذلك سبيلا في كشف الحقيقة ، سواء كان ذلك من تلقاء نفسها أو بناءا على طلب الخصوم.¹

هذا فيما يخص الأحكام العامة للمعاينة ، و نتناول فيما يأتي المعاينة في الجريمة المعلوماتية ، و مدى أهميتها ، و القواعد التي يجب اتخاذها حتى تأتي المعاينة بثمارها و تفي بغرضها المنشود.

للمعاينة أهمية كبيرة في كشف غموض الكثير من الجرائم التقليدية ، إلا أن دورها في كشف غموض الجريمة المعلوماتية و ضبط الأشياء التي قد في إثبات وقوعها و نسبتها إلى مرتكبيها لا ترقى إلى نفس الدرجة من الأهمية ، و مرد ذلك إلى الاعتبارات التالية:

- إن الجرائم المعلوماتية قلما يتخلف عن ارتكابها آثار مادية كما في الجرائم التقليدية، فما ينتج عنها من أدلة ما هو إلا بيانات غير مرئية.
- تردد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنية الطويلة بين ارتكابها و اكتشافها مما يفسح المجال لحدوث إتلاف أو تغيير أو عبث بالآثار المادية ، مما يُدخل الشك على الدليل المستمد من المعاينة .

1-عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي دراسة مقارنة، رسالة ماجستير في الحقوق ، كلية الحقوق جامعة الإسكندرية ، مصر ، سنة 2009 ، ص 48.

- إمكانية تلاعب الجاني في البيانات أو محوها عن طريق التدخل من خلال وحدة طرفية ، حيث أن المشرع الجزائري قرر جزاءات على كل من يقوم بإجراء أي تغيير أو نزع أي شيء قبل الإجراءات الأولية للتحقيق القضائي¹ ، و الملاحظ أن هذه الأحكام و إن كانت تنصرف إلى أغلب الجرائم التقليدية ، إلا أنه يمكن تطبيقها عند معاينة مكونات الحاسوب ذات الطابع المادي كأشرطة الحاسوب و الكابلات و الأقراص و غيرها ، بخلاف معاينة المكونات غير المادية لأنها تتطلب إجراءات خاصة.²

و نظرا لما تتميز به الجريمة الالكترونية من خصائص ، فبإمكان سلطات التحقيق الاستعانة بالخبراء للفحص و إبداء الرأي الفني في الأمور التي تستعصي على هؤلاء فهمها و تفسيرها و ذلك حتى يمنع أي تشكيك في صحة الدليل المستمد منه.

و تتخذ المعاينة في الجرائم المعلوماتية عدة أشكال و ذلك حسب نوعية الجريمة المرتكبة ، ففي جرائم العدوان على الملكية الفكرية يتم إنزال نسخة من المصنف المعتقدى عليه أو التحفظ على نسخة منه و ذلك بطباعته و استخراجها في هيئة ورقية أو صلبة ، و حديثا تستخدم تقنية الطباعة على خشب أو بلاستيك خاص ، إلا أنه هناك طرقا عامة تتوافق مع طبيعة النظام المعلوماتي ، مثل وسيلة تصوير الشاشة ، و هو ما يعرف بطريقة تجميد مخرجات الشاشة، أو أن يكون ذلك عن طريق حفظ الموقع باستخدام خاصية الحفظ (Save as) المتوافرة في نظام التشغيل.³

1- تنص المادة 43 ، من الأمر رقم 66-155 ، المتضمن قانون الإجراءات الجزائية الجزائري ، المرجع السابق ، على "يحظر في مكان ارتكاب جناية على كل شخص لا صفة له أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي ...، غير انه يستثنى من هذا الحظر حالة ما إذا كانت التغييرات أو نزع الأشياء للسلامة أو الصحة العمومية أو تستلزمها معالجة المجني عليهم ، و اذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بالحبس من 3 أشهر إلى 3 و بغرامة من 1000 دج الى 10.000 دج .

2 - عائشة بن قارة مصطفى ، المرجع السابق ، ص 49 .

3 - نفس المرجع ، ص 50.

أولاً: كيفية إجراء المعاينة التقنية لمسرح الجريمة المعلوماتية : عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها المحقق هو الانتقال إلى مسرح الجريمة ، و ينبغي التعامل في هذا مع مسرح الجريمة المعلوماتية على أنه مسرحان هما :

أ- مسرح تقليدي : يقع خارج الحاسوب و الانترنت ، و يتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة و هو أقرب ما يكون إلى مسرح أية جريمة تقليدية ، قد يترك فيها الجاني آثار عدة ، كالبصمات و بعض متعلقاته الشخصية أو وسائط تخزين رقمية.

ب- مسرح افتراضي : يقع داخل البيئة التقنية ، و يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب و شبكة الانترنت ، في ذاكرة الأقراص الصلبة الموجودة بداخله.

و عملية الانتقال بالنسبة إلى المسرح الافتراضي لا يكون بالضرورة مادي ، و إنما عبر العالم الافتراضي ، حيث يستطيع المحقق أن يقوم بهذه المعاينة في مكتبه من خلال حاسوبه ، كما يمكنه أن يلجأ إلى الخبرة القضائية أو الخبرة الاستشارية أو إلى مقهى الانترنت ، و يمكنه اللجوء أيضا إلى مقر مزود الانترنت الذي يعد أفضل يمكن من خلاله إجراء المعاينة .¹

و نظرا لكون الجريمة المعلوماتية تتميز بوجود الأدلة ذات الطبيعة غير المرئية ، لذلك ينبغي تعامل خاص معه و يكون ذلك من خلال اتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة المعلوماتية أبرزها ما يلي:

1- توفير معلومات مسبقة عن مكان الجريمة ، نوع و عدد الأجهزة المتوقع مداخلتها و شبكات الاتصال الخاصة بها .

2- إعداد خريطة للموقع الذي تتم الإغارة عليه ، و إعداد خطة للهجوم على ذلك المكان و تكون موضحة بالرسومات .

3- إعداد فريق التفتيش من المتخصصين، على أن يكون هذا الفريق مرفقا بالإذن القضائي للقيام بالتفتيش، لأن أغلب الجرائم المعلوماتية تكون داخل أمكنة لها

1 - عائشة بن قارة مصطفى ، المرجع السابق ، ص 51، 50.

خصوصياتها.

4- الحصول على الاحتياجات الضرورية من أجهزة و برامج للاستعانة بها في الفحص و التشغيل مثل برنامج معالجة الملفات (Xtree Pro Gold) ، و برنامج النسخ (lap Link) ، و برنامج (Encase) الذي ينتج صوراً مطابقة من القرص الصلب ، و يستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفدرالية الأمريكية و يسميها الخبراء " حقيبة الأدلة الرقمية".

5- تأمين التيار الكهربائي من الانقطاع المفاجئ ، لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء غلق الكمبيوتر ، و بالتالي فقدان كافة العمليات التي كان يتم تشغيلها و اتصالات الشبكة و أنظمة الملفات الثابتة .¹ و من الإجراءات التي يتعين إتباعها عند إجراء المعاينة ما يلي :

1- القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريقه الجرائم و ما قد يتصل به من أجهزة طرفية و محتوياته و أوضاع المكان الذي يوجد به بصفة عامة مع العناية بتصوير أجزاءه الخفية و ملحقاته الأخرى.

2- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام ، و الآثار الالكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات ، و بوجه خاص السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال و نوع الجهاز الذي تم عن طريقه الولوج على النظام أو الموقع أو الدخول معه في الحوار.

3- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة و ذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة.

4- القيام بحفظ المستندات الخاصة بالإدخال و كذلك مخرجات الحاسوب الورقية ذات الصلة بالجريمة و رفع ما قد يوجد عليها من بصمات و آثار مادية.

5- ربط الأقراص الكمبيوترية التي ربما تحمل الأدلة التقنية ، مع جهاز يمنع الكتابة أو التسجيل عليها ، مما يتيح للمحققين قراءة بياناتها من دون تغييرها .

1 - عائشة بن قارة مصطفى ، المرجع السابق ، ص 51.

6- التحفظ على محتويات سلة المهملات ، و القيام بفحص الأوراق و الشرائط و الأقراص الممغنطة المحطمة المتواجدة فيها، و رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة .

7- الاستعانة بأهل الخبرة عند الضرورة.¹

ثانيا : معاينة أنظمة الاتصال بشبكة الانترنت : أحيانا لا يكفي معاينة مكونات الحاسب وحدها لاستخلاص الدليل التقني ، إنما يتطلب من المحقق فحص أنظمة اتصال الحاسب بشبكة الانترنت كذلك ، و يقصد بأنظمة الاتصال بشبكة الانترنت بالمفهوم الإجرائي ، تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالانترنت ، لذلك فعملية فحص أو معاينة هذه الأنظمة يشمل بالأساس فحص مسار الانترنت أو ما يعرف ببرتوكول الانترنت ، و النظام الأمني للشبكات ، و كذا فحص الخادم.²

أ- **فحص مسار الانترنت:** تتم هذه العملية من خلال تتبع الحركة التراسلية للنشاط الممارس عبر الانترنت باستخدام نظام فحص الكتروني يسمى علم البصمات المعاصر أو علم بصمات القرن الواحد و العشرين ، و ما يتم التوصل إليه بعد ذلك هو عنوان رقمي يطلق عليه (**Internet protocole adresse**) أو باختصار (**IP adresse**) ، و هو عبارة عن برتوكول لعنونة البيانات و المواقع في شبكة الانترنت يتم بمقتضاه التعرف على الحاسب الآلي الموصول بشبكة الانترنت من خلال عناوين عددية ، علما أن لكل حاسب آلي عنوانه (**IP adresse**) الوحيد الخاص به ، و كل عنوان (**IP**) مكون من جزأين الأول يشمل أرقام الشبكة و الثاني يشمل أرقام مزود الخدمة ، فالحاسب الآلي فور اتصاله بالانترنت يقوم تلقائيا باختيار البرتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات .

1 عائشة بن قارة مصطفى ، المرجع السابق ، ص 52.

2 - براهيم جمال ، المرجع السابق ، ص 64 .

و يشتغل البروتوكول (IP) بشكل متزامن مع بروتوكول آخر يدعى بروتوكول التحكم بالنقل (Trams mission control Protocol TCP) للاتصال بين عدة أجهزة من الحواسيب طورت أساسا لنقل البيانات الرقمية عبر شبكة الانترنت ، و يرتكز البروتوكولان معا (TCP/IP) على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Pachets) بين مختلف أنظمة الاتصالات السلكية و اللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها ، و حزمة المعلومات هي جزء من ملف معلوماتي حجم مصغر ثابت تحمل رقما خاصا و معلومات تعريفية لكل من المرسل و المرسل إليه ، و عند كل اتصال تتم قراءة جهة المقصد أو المرسل إليه ثم تتم إعادة الحزمة المارة عبرهما إلى الوصلات التالية الأقرب إلى جهة المقصد النهائية .¹

تبرز أهمية الاستعانة بالمعلومات و المصادر و العناوين التي يمكن أن يحتويها نظام البروتوكول (TCP/IP) للتحقيق في الجريمة الالكترونية في كونها تدل بصفة جازمة عن مصدر الجهاز المستخدم في ارتكاب الجريمة ، و تحدد الأجهزة التي أصابها الضرر من جراء الفعل الإجرامي و نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة ، كما أنها تساعد بالاطلاع على جميع المرسلات و المحادثات ، و كل ما تم نقله أو تبادله أو معالجته من بيانات عبر شبكة الانترنت ، و كذا الكشف عن مصدرها و تتبع مسارها إلى غاية نقطة وصولها ، و من ثم تحديد هوية المرسل و المرسل إليه اللذين قد يمثلان أول المشتبه فيهم .

لذلك أثبتت تقنية تتبع الحركة العكسية لمسار الانترنت جدواها للكشف عن المجرمين في أكثر من جريمة إلكترونية ، إذ بواسطتها تم الكشف و القبض على مبتكر فيروس ميليسا ، و كذا الشخص الذي ابتكر موقع خدمات 'بلومبرج' لأخبار المال الاحتياالي لكي يرفع أسعار السهم عن طريق الغش و الخداع ، كما أن القضاء أقر في عدة قضايا بمصادقية هذه التقنية في تحديد مسار العمل الإجرامي و مشروعية الأدلة المتحصل عليها من خلالها ، منها ما جاء في الحكم الذي تبنته محكمة باريس الابتدائية بتاريخ 22 ماي 2000 في قضية ياهو (yahoo) الشهيرة.

1 - براهيمي جمال ، المرجع السابق ، ص 65.

ب- **فحص الخادم (Serveur):** يعتبر الخادم من أهم نظم الاتصال بالانترنت ، فهو جهاز إلكتروني كبير مهمته ضمان حركة الاتصال بمواقع و صفحات الانترنت ثم استقبالها و تخزينها فيه على هيئة رقمية، فالخادم له وظيفة مزدوجة ، إذ يتولى من جهة ربط مستخدمي الانترنت بالمواقع و الصفحات التي يريدون الاطلاع عليها ، و يقوم من جهة ثانية باستضافة هذه المواقع و الصفحات و تخزينها على شكل بيانات رقمية ، و هو ما يجعله ليكون مصدرا غنيا جدا للأدلة الالكترونية الرقمية ، و يطلق عليه البعض موقع تخزين المعطيات الرقمية (Lieu de stockage des données numérisées) .¹

و للقيام بعملية فحص الخادم ينبغي على المحقق الالتزام بالضوابط المقررة لإجراء المعاينة وفق القانون المنفذ في النطاق الإقليمي الذي يوجد فيه ، و اتخاذ كافة التدابير التقنية و الفنية اللازمة للمحافظة على مسرح الجريمة كما أشرنا سابقا ، بالإضافة إلى لزوم الأخذ بعين الاعتبار مبدأ الغاية من البحث و التفتيش و بالتالي خلق مفارقة بين الخادم العام و الخادم الخاص بفئة تراسلية معينة ، غير أن الأمر لا يقف عند هذا النقطة لأن تقنية الانترنت تجعل من الممكن القيام بفحص الخوادم عن بعد باستخدام تقنيات حديثة في هذا المجال تجعل التوصل إلى محتوى حركة الاتصال بالخادم ذات مغزى ، و ربما أفضل من مجرد القيام بفحص الخادم ماديا.²

الفرع الثاني : الخبرة

تعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجأ إليها القضاء و سلطات التحقيق على حد سواء ، و ذلك كلما استعصى عليهم الأمر ، و من بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجرائم المعلوماتية ، حيث أنه لا يستطيع التعامل مع هذه الجرائم إلا شخص ذو دراية و خبرة في مجال الالكترونيات.³

1 - براهيمي جمال ، المرجع السابق ، ص 66.

2 - نفس المرجع ، ص 67.

3 - يوسف جفال ، التحقيق في الجريمة الالكترونية ، مذكرة ماستر، تخصص قانون جنائي ، جامعة محمد بوضياف المسيلة ، الجزائر ، السنة 2016-2017 ، ص 33.

و الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية و العلمية و التي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة.

و قد عرفها البعض بأنها الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه.

و الخبير هو كل شخص لديه دراية خاصة بمسألة من المسائل قد يستدعي التحقيق فحصها و يستلزم ذلك كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه فيمكن أن يستعين بالخبير كما هو الحال مثلا في تقرير فحص خطوط الكتابة في جريمة التزوير.¹

تكمن أهمية الخبرة في البحث عن الأدلة التي تقدمها لجهة التحقيق و القضاء و لسائر السلطات المختصة بالدعوى الجزائية ، لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة من المواد 143 إلى 156 من قانون الإجراءات الجزائية الجزائري و اعتبرها من إجراءات البحث عن الدليل ، حيث نصت المادة 143 " أنه لجهات التحقيق أو الحكم عند ما تعرض لها مسألة ذات طابع فني ان تأمر بندب خبير إما من تلقاء نفسها أو بناء على طلب من النيابة العامة و إما بطلب من الخصوم "

و إذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهات التحقيق ، فهي أوجب في مجال استخلاص الدليل التقني لإثبات الجرائم المعلوماتية حيث تتعلق بمسائل فنية أكثر تعقيدا ، يصعب على المحقق أن يشق طريقه فيها و يعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات ، و منذ ظهور الجرائم المعلوماتية فإن الضبطية القضائية و سلطات التحقيق عموما تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي و المنظومات المعلوماتية و ذلك بغرض كشف غموض الجريمة و تجميع أدلتها و التحفظ عليها ، أو مساعدة المحقق في إجلاء

1 - سعيداني نعيم ، المرجع السابق ، ص 165، 166.

جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق ، و يلاحظ أن نجاح الاستدلالات و أعمال التحقيق في هذه الجرائم يكون مرتها بكفاءة و تخصص هؤلاء الخبراء ، فإجرام الذكاء و الفن لا يكشفه إلا ذكاء و فن مماثلين، و تبرز أهمية الاستعانة بالخبير في مجال الجرائم المعلوماتية عند غيابه فقد تعجز الضبطية في كشف غموض الجريمة لنقص الكفاءة و التخصص اللازمين للتعامل مع الجوانب التقنية و التكنولوجيا التي ارتكبت بواسطتها الجريمة ، و هو ما قد يؤدي إلى تدمير الدليل و محوه بسبب الجهل أو الإهمال عند التعامل .¹

و نظرا لفائدة الخبرة في التحقيق فقد أشار المشرع الجزائري في المادة 150 الفقرة 05 الأخيرة من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها أنه يمكن للسلطات المكلفة بتفتيش المنظومة المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

المطلب الثاني : التفتيش و الشهادة

نتطرق من خلال هذا المطلب إلى إجرائي التفتيش و الشهادة ، لإبراز دورهما في عملية التحقيق خاصة في مجال جرائم المعلوماتية ، و توضيح ضوابطهما المقررة قانونا، ضمن فرعين متتاليين .

الفرع الأول - التفتيش

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة ، تحقق وقوعها في محل يتمتع بحرمة ، و ذلك وفقا للضمانات و القيود القانونية المقررة .

1 - المادة 143 من قانون الإجراءات الجزائية ، المرجع السابق .

و أن ضبط الأدلة هو النتيجة الطبيعية التي ينتهي إليها التفتيش و التي يتم الحصول عليها أثناءه.

و على ذلك فإنه يتضح لنا أن هذا الإجراء ما هو إلا وسيلة للإثبات المادي ، ذلك أن التفتيش يستهدف ضبط أشياء مادية تساعد في إثبات وقوع الجريمة و إسنادها إلى المتهم المنسوب إليه ارتكابها ، كما أن رجال الضبطية القضائية قد تعودوا في الجرائم التقليدية على ضبط إلا الأشياء المادية ¹.

من أجل هذا فإن تفتيش نظم المعالجة الآلية يعد من أخطر المراحل حال اتخاذ الإجراءات الجزائية ضد مرتكب الجريمة المعلوماتية ، لكون محل التفتيش فيها هو نظام المعالجة الآلية ذو الطابع غير المادي ، و لا يعد أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي ، فما مدى صلاحية مكونات نظام المعالجة الآلية كي تكون محلا يرد عليه التفتيش و ما هي الأشياء المضبوطة في ظل التفتيش في العالم الافتراضي ؟

أولاً- التفتيش في البيئة التقنية : يثور التساؤل حول إمكانية تطبيق القواعد العامة لتفتيش نظم الحاسوب و الانترنت ، ذلك أن هذا الإجراء يهدف إلى جمع الأدلة المادية في حين أن نظم المعلوماتية عبارة عن كيان معنوي ، و لا تتوفر له صفة المادة سواء تعلق ذلك ببرامج الحاسوب أو ما يشمل عليه من بيانات .

لكن من المعروف أن نظم المعالجة الآلية تتكون من مادية و أخرى غير مادية ترتبط بغيرها عبر شبكات اتصال بُعدية على المستوى المحلي أو الدولي.

و إذا كان التفتيش هو التنقيب في وعاء السر بقصد ضبط ما يفيد من الأسرار في كشف الحقيقة ، و أن جوهره هو كشف نقاب السرية عما تحويه نظم المعالجة الآلية من خفايا و أسرار و نوايا إجرامية ، و بالتالي إزاحة ستار الكتمان عنها للاستفادة منها في معرفة الحقيقة ، و إذا كان هذا المعنى لا يتقيد بالكيان المادي لوعاء السر ، فإن الأمر يتطلب منا البحث في مسألة المحل الذي ينصب عليه هذا الإجراء في مجال المعلوماتية.

1- سعيداني نعيم ، المرجع السابق ، ص 143.

أ- محل التفتيش في الجريمة المعلوماتية : يتكون النظام المعلوماتي من مكونات مادية (hard ware) و مكونات منطقية (soft ware) ، كما أن له شبكات اتصالات بُعدية سلكية و لاسلكية على المستوى المحلي و المستوى الدولي، فهل تخضع هذه الأخيرة للتفتيش ؟¹

1- تفتيش المكونات المادية لنظام المعالجة الآلية: إن التفتيش الواقع على المكونات المادية لنظام المعالجة الآلية لا توجد فيه أي مشكلة في التنفيذ لإمكانية ذلك و سهولته ، مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها و إمكانية إتلافها ، و تأتي سهولة هذا التفتيش لأنه يرد على أشياء مادية لا خلاف حول خضوعها للتفتيش طبقا لقواعد قانون الإجراءات الجزائية ، ففي نص المادة 44 من قانون الإجراءات الجزائية ورد بالمعنى أن التفتيش يرد على الأشياء ، و هي كلمة تنصرف في الأرجح على المكونات المادية ، و نفس القول ينصرف على ما جاءت به المادة 64 من نفس القانون بنصها " لا يجوز تفتيش المساكن....و ضبط الأشياء...".

و على هدي ذلك فإنه لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب ، و ذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب و ملحقاته ، سواء من الأماكن العامة أو الأماكن الخاصة ، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش ، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه و بنفس الضمانات المقررة قانونا.

إلا أن المشرع الجزائري بمناسبة التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 20 ديسمبر 2006 استثنى بموجب الفقرة الثالثة من المادة 45 و كذا الفقرة الثانية من المادة 47 و الفقرة الثالثة من المادة 64 تطبيق هذه الضمانات عند إجراء التفتيش بمناسبة تحقيق مفتوح بخصوص الجرائم المعلوماتية.

1 - رزيق محمد ، إجراءات المعاينة ، التفتيش و الحجز داخل المنظومة المعلوماتية ، مذكرة ماستر في القانون العام ، جامعة أكلي محند أولحاج ، البويرة ، الجزائر ، سنة 2018-2019 ، ص 16.

و يفهم من استقراء هذه المواد أن المشرع لا يشترط حضور الشخص الذي يشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه ، و أنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات الليل و النهار و دون حاجة إلى رضائه عند القيام بهذا الإجراء. و الملاحظ أن المشرع في هذه الحالة قد غلب المصلحة العامة على حريات الأفراد ، و مرد ذلك لاعتبارين :

- ذاتية الجريمة المعلوماتية المتمثلة في إمكانية اختفائها بسرعة فائقة.
- افتراض كون الدليل التقني هو الدليل الوحيد في الدعوى الجزائية و من ثم ارتكاز كل العملية الاتباتية على وجوده.¹

2 - تفتيش المكونات المعنوية لنظام المعالجة الآلية : إذا كان الأمر قد انتهى بنا إلى صلاحية المكونات المادية للنظم المعلوماتية كمحل يرد على التفتيش ، فإن امتداد ذلك إلى مكوناته غير المادية محل جدل حول مدى صلاحيتها لأن تكون موضوعا للتفتيش تمهيدا لضبط الأدلة .

فبالخلاف حاصل في مسألة أن التفتيش التحقيقي وسيلة للبحث عن الأدلة المادية ، إذ هو إجراء يسعى إلى ضبط الأدلة المتعلقة بالجريمة لتقديمها إلى المحكمة المختصة كدليل إدانة ، لذلك يثور الشك و التساؤل حول إمكانية اعتبار البحث عن أدلة الجريمة المعلوماتية في نطاق نظم الحاسوب نوعا من التفتيش باعتبار أن البيانات الالكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي و يستشعر الفقه صعوبة المسألة نظرا لغياب الطبيعة المادية للمعلومات في ذاتها مجردة من دعامتها المادية² ، و قد ذهب الفقه بهذا الشأن مسارين رئيسيين:

1- رزيق محمد ، المرجع السابق ، ص 17.

2 - عبد العظيم وزير ، شرح قانون العقوبات القسم الخاص ، جرائم الاعتداء على الأموال ، دار النهضة العربية القاهرة ، مصر ، سنة 1993 ، ص 40 .

1-2 المسار الأول : تتمثل فكرته في عدم إمكانية انسجام و تطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث و تنقيب عن الأدلة في برامج الحاسوب و بياناته.

فهناك جانب من التشريعات الإجرائية قد حدد هدف التفتيش في البحث عن الأشياء و ضبطها ، و هذا الشيء يقتصر بمفهومه على المال ذي الحيز المادي المحسوس و لا يمتد في نطاق شموله إلى الكيانات المنطقية ، و قد عملت الدول التي أخذت بهذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية .¹

2-2 المسار الثاني: يخلص أصحاب هذا المسار إلى أن برامج الحاسوب يمكن أن تطبق عليها خصائص و سمات المادة ، و بالتالي تدخل في نطاق الأشياء المادية و يستوي في ذلك أن تكون برامج نظام أو برامج تطبيقات ، مستنديين في ذلك إلى أن المادة هي كل ما يشغل حيزاً مادياً في ذاكرة الحاسوب و يمكن قياسه بمقياس معين و هو البايت (Byte) و الكيلو بايت (KB) ، و هكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن تخزينها فيها ، لذلك ذهب الفقه في تفسيره إلى الاستناد على الربط بين النصوص الإجرائية التي أوردت عبارة "أي شيء" و التي يقصد بها المادة و بين العلوم الطبيعية و مفهومها في البيانات المنطقية أو البرامج.²

غير أن النصوص القانونية التي أرست القواعد التي تحكم التفتيش تم سنّها قبل أن يعرف القانون الأشياء غير المادية ، لكن تقدم الفكر البشري و الذي رافقه أظهر للوجود قيماً اقتصادية و أشياء غير مادية ليس لها حيز محسوس ، لذلك فأى كانت المبررات التي ساقها معتقو المساواة بين الكيان و نقيضه فإن طبيعة البيانات و المعطيات المعالجة تتطلب قواعد خاصة تحكمها بدلاً من محاولة توسيع نطاق القواعد التقليدية ، و هذا من

1- علي حسن محمد الطويلة ، التفتيش الجنائي على نظم الحاسوب و الانترنت ، عالم الكتب الحديثة ، الأردن ، سنة 2004 ، ص 7.

2 - هلاي عبد الله أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، دراسة مقارنة ، دار النهضة العربية القاهرة ، سنة 1993 ، ص 40 .

خلال إجراء تعديل عليها من شأنه توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش و تضمينها من الأحكام بما يتلاءم و متطلبات هذه التقنية الجديدة ، فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا يمكن إعمالها مباشرة على النظم المعلوماتية لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الاجرائية .

و يتضح موقف المشرع الجزائري من خلال القانون 04/09 المتعلق الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، حينما أجاز صراحة تفتيش المنظومة المعلوماتية ، و ذلك بموجب المادة 05 منه التي نصت على أنه يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية .." الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها و كذا منظومة تخزين المعلوماتية".¹

3 - تفتيش الشبكة المعلوماتية المتصلة بالحاسوب "التفتيش عن بعد": تعرف الشبكة المعلوماتية بأنها مجموعة مكون من اثنين فأكثر من أجهزة الحاسوب و المتصلة ببعضها اتصالا سلكيا أو لاسلكيا ، و قد تكون هذه الأجهزة موجودة في نفس الموقع و تسمى بالشبكة المحلية (Lan) ، و قد تكون موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف و تسمى بالشبكة بعيدة المدى (Wan).²

و مع التطور التكنولوجي لثورة الاتصالات لم يعد نطاق الاتصالات محدودا في اقليم دولة واحدة ، بل امتد ليشمل كل أرجاء العالم بعد ظهور شبكة الانترنت و التي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لامركزية ، و يدخل في تركيب هذه الشبكة ملايين الحواسيب الموزعة عبر مختلف دول العالم.

و السؤال المطروح في هذا الصدد يتعلق بمدى خضوع شبكات نظام المعالجة الآلية للتفتيش و هي مسألة على درجة كبيرة من الخطورة تتعلق بالتفتيش عن بعد

1- سعيداني نعيم ، المرجع السابق ، ص 147.

2- نفس المرجع ، ص 148 .

(Perquisition A Distance) ، و ذلك نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة عن الموقع المادي للتفتيش ، و بالتالي فإن الحاسوب أو النهاية الطرفية التي يمكن أن ترتكب عليها أو بواسطتها الجريمة المعلوماتية تخضع للقانون الإجرائي الخاص بتلك المنطقة .

لذلك يثار التساؤل حول أثر تفتيش الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة، و نستطيع أن نميز في هذه الصورة بين احتمالين على النحو التالي :

3-1 اتصال حاسب المشتبه فيه أو المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة: و هنا يثور التساؤل حول مدى إمكانية امتداد الحق في التفتيش إلى أجهزة الحاسوب المتصلة بجهاز المشتبه فيه المتهم ، و في هذه الحالة عمدت بعض التشريعات الإجرائية إلى حل هذه المشكلة من خلال نصها على إجازة تفتيش نظم المعلومات المتصلة بالحاسوب الذي يجري فيه التفتيش (أي الشبكة و ما يتصل بها) ، و تسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة.

و يعتبر المشرع الجزائري من بين هذه التشريعات حيث نص في الفقرة الثانية من المادة 05 من القانون 04-09 بأنه "في حالة تفتيش منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الاولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".¹

3-2 اتصال حاسب المشتبه فيه أو المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة : و هنا من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبوا

1- المادة 05 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، المرجع السابق .

الجرائم بتخزين بياناتهم في أنظمة معلوماتية خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات التحقيق في جمع الأدلة.¹

فمن المشاكل الحقيقية التي تواجه جهات التحقيق في جمع الأدلة، حالة تطلب امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي تصدر عن جهاتها المختصة الإذن بالتفتيش ، و دخوله في المجال الجغرافي لدولة أخرى ، و هو ما يسمى بالتفتيش العابر للحدود ، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها و حدودها الإقليمية.

لذا فإن جانبا من الفقه يرى أن التفتيش الإلكتروني العابر للحدود ينبغي أن يتم في إطار اتفاقيات تعاون خاصة ثنائية أو دولية تجيز هذا الامتداد ، و أنه لا يجوز القيام به في ظل غياب تلك الاتفاقيات ، و وفقا لما جاء بتقرير المجلس الأوروبي فان الاختراق المباشر يعد انتهاكا لسيادة دولة أخرى ما لم توجد اتفاقية دولية في هذا الشأن ، فاسترجاع البيانات التي تم تخزينها في الخارج دون علم الدولة الأخرى أو رضاها يعد انتهاكا لسيادة الدولة الأخرى و خرقا للقوانين.²

و لمواجهة هذا الاحتمال نجد أن المشرع الجزائري قد أجاز تفتيش الأنظمة المتصلة حتى و لو متواجدة خارج الإقليم الوطني، و هو ما أورده في الفقرة الثالثة من نص المادة 05 من القانون 04-09 "....إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية طبقا للاتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل " .

ثانيا : ضوابط التفتيش

رغم اعتبار التفتيش من الإجراءات الجوهرية للبحث عن حقيقة الجرائم إلا أن معظم القوانين الإجرائية حرصت على إحاطته بجملة من الضمانات القانونية ، و ذلك تقاديا لتعسف سلطات البحث و الاستدلال و ما يمكن أن ينجر عنه من اعتداء على حقوق و

1- سعيداني نعيم ،المرجع السابق ، ص 150.

2- نفس المرجع ، ص 151.

حريات الأفراد و حرمة مساكنهم و حياتهم الخاصة من جهة ، و إحقاقا لحق الدولة ممثلة في المجتمع في كشف غموض الجرائم و متابعة مرتكبيها و توقيع العقاب عليهم من جهة أخرى .¹

أ- الضمانات الموضوعية للتفتيش الالكتروني : تتمثل هذه الضمانات في الشروط الواجب توافرها حتى يكون التفتيش صحيحا ، و تتلخص في ثلاث شروط أساسية هي :

1- سبب التفتيش : يعتبر عنصر السبب ضمانا قانونية لصحة و مشروعية إجراء التفتيش ، و يتحقق بوقوع جريمة ما يتم بموجبها توجيه الاتهام إلى شخص أو الأشخاص المراد تفتيشهم بناء على أدلة أو قرائن تفيد تورطهم في الجريمة ، عملا بمبدأ الشرعية الجزائية القاضي بأن " لا جريمة و لا عقوبة أو تدابير أمن بغير قانون " ، إذ بدون وقوع جريمة و توجيه الاتهام إلى شخص أو أشخاص معينين وفقا لأدلة كافية ، يكون التفتيش باطلا لانتفاء السبب الذي يبرره .²

و تطبيقا لما سبق ، فإن سبب التفتيش في الجرائم الالكترونية لا يتحقق إلا بتحقق العناصر الثلاثة التالية :

1.1- وقوع جريمة الكترونية تحمل وصف جنائية أو جنحة: اتفقت معظم التشريعات أنه لا يجوز لهيئات التحقيق مباشرة التفتيش إلا بعد التأكد من وقوع جريمة إلكترونية نص عليها القانون في نصوص التجريم و العقاب ، و أي تفتيش في جريمة محتملة الوقوع مستقبلا و لو أيقنت التحريات و الدلائل الجدية على أنها ستقع بالفعل ، يعد إجراء التفتيش غير مشروع مآله البطلان .

2- ابتسام بغو ، إجراءات المتابعة الجزائية في الجريمة المعلوماتية ، مذكرة ماستر تخصص قانون جنائي للأعمال ،

جامعة العربي بن مهيدي أم البواقي ، الجزائر ، السنة 2015/2016 ، ص 18 .

3- براهيم جمال ، المرجع السابق ، ص 31 .

غير أن المشرع الجزائري خرج عن هذه القاعدة من خلال المادة 05 من القانون 04-09 التي تجيز إمكانية اللجوء إلى تفتيش نظم المعلوماتية للوقاية من الجرائم ، أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة 04 من نفس القانون.¹ كما أنه لا يكفي وقوع جريمة معلوماتية للقول بمشروعية إجراء التفتيش طبقا للقواعد العامة ، بل لابد من أن تحمل هذه الجريمة وصف جنائية أو جنحة.

بالإضافة إلى ذلك ، فلا يمكن القيام بالتفتيش على بعض السلوكات المجرمة في دول أخرى ، و لازالت خارج نطاق التجريم في التشريع الجزائري ، و تبعا لذلك فإن اتخاذ أي إجراء من إجراءات التحقيق إزاء هذه الجرائم بما في ذلك التفتيش ، قد يكون مصيره البطلان طالما لم يركز على سبب مقبول قانونا ، ناهيك عما تتطلبه الإجراءات التقنية في حالة النص على تلك الجرائم من نصوص تتناسب مع حداثتها .

2.1- اتهام شخص أو أكثر بمساهمته في ارتكاب جريمة معلوماتية : يشترط لقيام سبب التفتيش إلى جانب وقوع جريمة معلوماتية تحمل وصف جنائية أو جنحة ، أن يتوفر في الشخص المراد تفتيشه أو تفتيش حاسبه أو مسكنه دلائل كافية توحي بأنه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أصليا أو شريكا ، مما يستوجب اتهامه بها ، و من هنا فعدم اكتشاف قاضي التحقيق لهوية المتهم في الشكوى تقيد ضد مجهول و يكون سببا لحفظ ملف القضية و إصداره لأمر بأن لا وجه للمتابعة ، و هو ما نصت عليه المادة 163 من قانون الإجراءات الجزائية الجزائري "إذا رأى قاضي التحقيق ...أنه لا توجد دلائل كافية ضد المتهم أو كان مقترف الجريمة ما يزال مجهولا ، أصدر أمرا بأن لا وجه لمتابعة المتهم"²

و يقصد بالدلائل في جرائم المعلوماتية " مجموعة من المظاهر أو الأمارات المعينة القائمة على العقل و المنطق و الخبرة الفنية و الحرفية للمحقق و التي ترجح نسبة الجريمة الالكترونية إلى شخص معين باعتباره فاعلا أصليا أو شريكا".

1- براهيمي جمال ، المرجع السابق ، ص32.

2- نفس المرجع ، ص 33.

و على هذا الأساس فسبب التفتيش في البيئة التقنية لا يتوقف على وقوع جريمة من الجرائم الالكترونية فقط ، إنما لابد أن يكون ذلك الوقوع مقترنا بنسبتها إلى شخص أو أشخاص معينين ، إما بصفتهم فاعلين أصليين أو شركاء .

3.1- توافر أمارات قوية توحى إلى وجود أدلة مادية تفيد في كشف الجريمة

لا يكفي وقوع جريمة من نوع جنائية أو جنحة منصوص عليها في القانون ، و توجيه الاتهام إلى شخص أو أشخاص معينين بمساهمتهم في ارتكابها لقيام سبب التفتيش في جرائم المعلوماتية ، إنما ينبغي أن تتوافر كذلك لدى المحقق أدلة و قرائن كافية على وجود لدى المتهم أو في المكان المراد تفتيشه أجهزة و أدوات استعملت في الجريمة أو أشياء متحصل منها ، أو أية معلومات أو بيانات أو مستندات تفيد في استجلاء الحقيقة .¹

و يتم الحصول على القرائن و الأمارات من خلال التحريات التي تجريها سلطات الضبط في مرحلة الاستدلال ، بعد ما يتم إخضاعها لتقدير السلطة المختصة بإصدار الإذن بالتفتيش التي تتأكد من مدى كفاية هذه القرائن لتبرير اللجوء إلى إجراء التفتيش.

2- محل التفتيش: يشترط كذلك لصحة و مشروعية التفتيش في الجرائم الالكترونية أن يقع على محل ، و يقصد بالمحل كل المكونات المادية و المعنوية و شبكات الاتصال المتعلقة بالوسائل الالكترونية.

و المحل في الجريمة المعلوماتية لا يكون قائماً بذاته ، بل يكون إما مقترنا بمكان معين كمسكن المتهم أو بشخص معين (مالك أو حائز) ، كما هو الشأن في الحاسب المحمول أو الهاتف النقال ، لذلك قبل مباشرة التفتيش يجب مراعاة طبيعة المكان الذي تتواجد فيه الوسائل الالكترونية المراد تفتيشها و كذا الضمانات القانونية المحاطة به ، لأن حكم تفتيش هذه الوسائل يتوقف غالباً على طبيعة المكان الذي تتواجد فيه .²

1- براهيمي جمال ، المرجع السابق ، ص 34.

2- عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر و الانترنت ، الطبعة الأولى ، دار الفكر الجامعي ، القاهرة مصر ، سنة 2006 ، ص 31.

و يشترط في المحل الذي يقع عليه التفتيش ، أن يكون معينا تعينا نافيا للجهالة ، و يكون مما يجوز فيه التفتيش ، فالشرط الأول هو نتيجة منطقية للمحافظة على حقوق و حرمان و حريات الأفراد ، لذا لا يمكن القيام بتفتيش كل الحواسيب المتواجدة في شركة ما أو الحواسيب المحمولة أو الهواتف النقالة الخاصة بكل أفراد العائلة الواحدة.¹

و أما الشرط الثاني ، فالقانون يستثني من التفتيش بعض الأشخاص و الأماكن مثل أشخاص و مساكن و سيارات أعضاء السلك الدبلوماسي و أعضاء المجالس النيابية ، و كذا مكاتب المحامين لتمتعهم بالحصانة ، و عليه فأى تفتيش لهذه الفئة أو الوسائل الالكترونية الموجودة بحوزتهم أو في منازلهم أو على متن سياراتهم يعد منافيا للقانون و مآله البطلان.

كذلك الحال بالنسبة للتفتيش عن بعد عبر شبكات الاتصال أو التفتيش الالكتروني الذي لا يستلزم الاعتداء المعنوي لحرمة المكان أو الشخص المراد تفتيشه ، فهو يخضع لقواعد الحصانة مثله مثل التفتيش المادي ، لأن الاعتداء المعنوي على الحياة الخاصة يرتب عادة الآثار نفسها التي يربتها الاعتداء المادي أو أكثر خطورة منه ، نظرا لكم الهائل من المعلومات و البيانات التي تحويها الوسائل الالكترونية الشخصية ، و التي يسهل الولوج إليها و الاعتداء على سريتها.

و تجدر الإشارة أن المشرع الجزائري في هذا الشأن استحدث نصوصا قانونية سمح من خلالها لسلطات التحقيق تفتيش الأنظمة المعلوماتية ، أو جزء منها ، و المعطيات المخزنة بتلك الأنظمة ، و جعلها محلا للتفتيش الالكتروني ، كما وسع نطاق هذا المحل بحيث لم يعد قاصرا على تفتيش الأجهزة الالكترونية تبعا لتفتيش المكان و الأشخاص ، بل جعله يمتد ليشمل التفتيش عن بعد داخل النطاق الإقليمي للدولة إلى نهاية طرفية أخرى التي يمكن الدخول إليها من المنظومة الأولى و ذلك كل ما استدعت

1- عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 32.

ضرورة التحقيق إلى ذلك.¹

3- السلطة المختصة بالتفتيش : لكي يكون التفتيش في الجرائم المعلوماتية أو غيرها من الجرائم صحيحا و منتجا لآثاره ، لابد أن يتم من طرف سلطات التحقيق الأصلية ، مع مراعاة الاختصاص المحلي الذي يتحدد عادة إما بمكان وقوع الجريمة ، و إما بمكان إقامة المتهم ، أو مكان القبض عليه.²

إلا أنه استثناء ، يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية و ذلك وفقا للشروط و الإجراءات المنصوص عليها في القانون ، و في هذه الحالة يشترط لصحة إجراء التفتيش الذي تقوم به الضبطية أن يكون بناء على إذن بالتفتيش صحيح ، صادرا من هيئة مختصة ، و في حالة تخلف هذه الشروط يصبح التفتيش غير مشروع.³

ب- الشروط الشكلية للتفتيش في البيئة التقنية

إن القواعد الشكلية لا تهدف الى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب ، و إنما تضيف إلى مقتضيات الإجراءات سياجا يحمي الحريات الفردية ، و أبرز هذه الشروط هي :

1 - تنص المادة 05 من القانون 04-09 ، المرجع السابق على " يحوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية ..بفرض التفتيش و لو عن بعد الى: أ- منظومة معلوماتية ..منظومة تخزين معلوماتية .."

2- تنص المادة 40 من قانون الإجراءات الجزائية الجزائري ، المرجع السابق على " يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها او بمحل القبض على احد هؤلاء الأشخاص حتى و لو كان هذا القبض قد حصل لسبب آخر ، يجوز تمديد الاختصاص المحلي لقاضي التحقيق الى دائرة اختصاص أماكن أخرى ، عن طريق التنظيم ، في جرائم .. و الجرائم الماسة بالمعالجة الآلية للمعطيات .."

3- تنص المادة 6/68 من قانون الإجراءات الجزائية الجزائري ، المرجع السابق ، على " ..و إذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق جاز له أن يندب ضباط الشرطة القضائية للقيام بجميع أعمال التحقيق ضمن الشروط المنصوص عليها في المواد من 138 إلى 142.."

1- إجراء التفتيش بحضور أشخاص معينين بالقانون: غني عن البيان أن التفتيش فيه اطلاع على أسرار الغير التي تحرم أغلب التشريعات الإجرائية الاطلاع عليها ، و المشرع الجزائري في هذا الشأن أوجب ضرورة حصول إجراء التفتيش المتعلق بالمساكن و ملحقاتها بحضور المشتبه فيه عند ما يتم تفتيش مسكنه من طرف الضبطية القضائية ، و إن تعذر ذلك بامتناعه عن حضور التفتيش أو كان في حالة فرار يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش ، إلا أنه بموجب التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 22/06 استثنى هذه الشروط إذا تعلق الأمر بالجرائم المعلوماتية ، و هو ما يعد إقرار من المشرع بذاتية هذا النوع من الجرائم و ما يتطلبه التحقيق بشأنها من بسط نوع من السرية أثناء جمع الدليل التقني بالإضافة إلى الإسراع في استخلاصه قبل فقدانه.¹

2- الميعاد الزمني لإجراء التفتيش في البيئة التقنية: اختلفت التشريعات الإجرائية في وقت تنفيذ التفتيش ، فمنها من حظر تفتيش المساكن ليلا إلا في أحوال معينة ، و منها من لم يقيد القيام بهذا الإجراء بوقت معين و ترك الأمر لتقدير القائم بالتفتيش لاختيار الوقت الملائم لتنفيذه ضمن المدة المحددة بالإذن .

فالمشرع الجزائري ذهب إلى حظر تفتيش المساكن و ما في حكمها في أوقات معينة و حدد ميقات تنفيذ هذا الإجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساء كأصل عام ، و هناك حالات استثنائية يجوز فيها الخروج عن الأصل و يمكن إجراؤه في أي ساعة من ساعات الليل و النهار² في بعض الجرائم على سبيل الحصر من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات .³

1- سعيداني نعيم ، المرجع السابق ، ص 153.

2 - تنص الفقرة 3 من المادة 47 من قانون الإجراءات الجزائية الجزائري ، المرجع السابق ، على " عندما يتعلق الامر بالجرائم المذكورة في الفقرة الثالثة اعلاه ، يمكن لقاضي التحقيق ان يقوم باية عملية تفتيش او حجز ليلا او نهارا و في أي مكان على امتداد التراب الوطني او يأمر ضباط الشرطة القضائية المختصين للقيام بذلك"

3 - إيتسام بغو ، المرجع السابق ص 19.

ثالثا- إجراءات ضبط الدليل التقني

إن ضبط المكونات المادية للحاسوب لا يثير مشاكل لدى الفقهاء في إمكانية ضبط هذه المكونات ، بل حتى إمكانية ضبط الحاسوب بشكل كامل لتأكيد الاحتفاظ بالدليل إذا كان مشغل الجهاز غير متعاون مع جهات التحقيق ، أما بالنسبة لمكونات الحاسوب المعنوية ، و لما فرض الواقع ضرورة أن يشمل التفتيش المكونات المعنوية للحاسوب ، لكن ليس بالكيفية المنصوص عليها بموجب النصوص التقليدية لانتفاء الطابع المادي عن هذه البيانات ، و على هذا الأساس استلزم التدخل التشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط لتشمل بجانب الأشياء المادية البيانات الالكترونية بكافة أنواعها و أنماطها.

و نظرا لعرضت الأدلة للإتلاف و الفساد لأي سبب من الأسباب المذكورة سابقا ، يتعين اتخاذ بعض الإجراءات الخاصة للحفاظ عليها و صيانتها من العبث ، و ذلك على النحو التالي :

وضع المشرع الجزائري في القانون 04-09 المتعلق بتكنولوجيات الإعلام و الاتصال و مكافحتها طريقتين لضبط الأدلة الالكترونية ، الأولى تكون عن طريق نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون هذه الأخيرة قابلة لحجزها و وضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية ، و الطريقة الثانية تكون باستعمال التقنيات المناسبة ، و حاليا يتم استخدام برامج متخصصة في النسخ مثل برامج (Lap Link) ، كما يوجد أسلوب تجميد التعامل بالحاسوب أو إحدى القطع المكونة له التي استخدمت في ارتكاب الجريمة ، و يتخذ هذا الأسلوب عدة مظاهر ، و يتم اللجوء إلى هذا الإجراء في حالة ما إذا كانت البيانات تتضمن خطرا أو ضررا بالمجتمع لمنع الوصول إليها .¹

1 - بن طالب ليندا ، الدليل الالكتروني و دوره في الإثبات الجنائي (دراسة مقارنة) ، أطروحة دكتوراه ، تخصص قانون ، جامعة مولود معمري تيزي وزو ، الجزائر ، سنة 2019 ، ص 67 .

الفرع الثاني : الشهادة

الشهادة بصفة عامة هي اثبات حقيقة واقعة معينة ، علم بها الشاهد من خلال ما شاهده أو سمعه أو أدركه بحواسه الأخرى عن تلك الواقعة بطريقة مباشرة ، و الشهادة تعد وسيلة اثبات أساسية في المسائل الجزائية ، لأنها تنص في الغالب على وقائع مادية تقع فجأة – يتعذر إثباتها إلا عن طريق الشهادة .

الشهادة لا تقل أهمية في الجرائم المعلوماتية عن باقي الإجراءات في الحصول على الدليل الإلكتروني ، فالقاعدة العامة بأن يلتزم الشاهد بالإفصاح بما يعلمه من معلومات بخصوص واقعة الجريمة و الفاعلين فيها ، و الإدلاء بكل ما يفيد في كشف الحقيقة من وقائع أخرى.¹

سنتطرق في هذه النقطة إلى المقصود بالشاهد في الجريمة المعلوماتية –الشاهد المعلوماتي- و التزاماته .

أولاً: المقصود بالشاهد المعلوماتي

الشاهد المعلوماتي يختلف عن غيره من الشهود في الجريمة التقليدية ، فغالبا ما يكون من أصحاب المعرفة التقنية للنظام المعلوماتي و ذلك بحكم عملهم ، و لا يقصد من ذلك أن يكون الشاهد خبيراً ، بل كلاهما يختلفان عن بعضهما البعض ، حيث يعد الخبير تقارير و آراء توصل إليها بتطبيق قوانين علمية أو أصول فنية ، أما الشاهد يقدم إلى القاضي معلومات حصلها بالملاحظة الحسية .

و يعرف الشاهد المعلوماتي بأنه " ذلك الشخص الفني صاحب الخبرة المعلوماتية و التخصص في التقنية و علوم الحاسب الآلي ، الذي تكون لديه معلومات أساسية و جوهرية هامة لازمة للولوج في نظام المعالجة الآلية للمعطيات إذا كانت مصلحة التحقيق

1 - ثيان ناصر آل ثيان ، إثبات الجريمة الإلكترونية ، رسالة ماجستير ، تخصص السياسة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، السعودية ، سنة 2012 ، ص 89 .

تقتضي التفتيش عن أدلة تتعلق بالجريمة داخله " ، و نذكر نماذج عن هؤلاء الشهود كما يلي :

- مشغلو الحاسوب: الشخص الذي تكون لديه خبرة كبيرة في استخدام جهاز الحاسب الآلي و مكوناته ، و هو المسؤول عن تشغيل الجهاز و معداته و الملحقات و المعدات المتصلة به.

- خبراء البرمجة: و هم مخطو البرامج ، متخصصون في كتابة أوامر البرامج الخاصة بجهاز الحاسب الآلي ، و هم فئتين ، مخطو البرامج التطبيقية و مخطو برامج النظم.

- المحللون : هم الذين يحللون الخطوات و يقومون بتتبع البيانات داخل النظام ، كما يقومون بتجميع بيانات النظام و دراستها و تحليلها و تقسيمها إلى وحدات .

- مهندسو الصيانة و الاتصالات: هم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته و شبكات الاتصال المتعلقة به. ¹

- مديرو النظم : و هم الذين لهم أعمال الإدارة في النظم المعلوماتية. إضافة إلى هذه الفئات ، هناك أشخاص آخرون يعدون بمثابة شهود في الجريمة المعلوماتية ، و هي فئة لها دور كبير في شبكة الانترنت إلى المستهلك من بينهم مقدمو الخدمات الوسطية في مجال المعلوماتية و الانترنت ، أيضا متعهدو الوصول و متعهدو الايواء و مسؤولو المنتج ، مسؤولو ناقل المعلومات و مسؤولو متعهد الخدمات ، كذلك مورد المعلومات و مؤلف الرسالة.

ثانيا : التزامات الشاهد المعلوماتي

تعد التزامات الشاهد المعلوماتي نفسها التزامات الشاهد في الجرائم التقليدية ، و من أهمها نذكر ما يلي :

أ-حضور الشاهد : إن لسلطة التحقيق كامل الحرية في أن تسمع الشهود هن الوقائع التي تثبت أو تؤدي إلى ثبوت الجريمة و ظروفها و إسنادها إلى المتهم أو براءته منها ،

1 - بن طالب ليندا ، المرجع السابق ، ص 70.

و لها كذلك أن تسمع شهادة الشهود الذين يطالب الخصم سماعهم ما لم ترى عدم الفائدة من سماعهم .¹

نص المشرع الجزائري في المادة 223 الفقرة 1 من قانون الإجراءات الجزائية الجزائري ، و التي تحيل إلى المادة 97 من القانون نفسه ، صراحة على عقاب الشاهد المتخلف عن الحضور أو رفض حلف اليمين أو أداء الشهادة ، كما أجاز القانون 15-03² في المادتين 14 و 15 منه اذا استدعى بعد المسافة أو تطلب ذلك حسن سير العدالة استجواب و سماع الاطراف عن طريق المحادثة المرئية عن بعد مع مراعاة احترام الحقوق و القواعد المنصوص عليها في قانون الإجراءات الجزائية.

ب-حلف اليمين: تنص المادة 227 من قانون الإجراءات الجزائية الجزائري على إلزامية تأدية الشاهد لليمين القانونية حسب الصيغة القانونية المنصوص عليها في المادة 93 من القانون نفسه ، و يترتب على مخالفة هذا الإجراء بطلان شهادته.³

للإشارة فإن الخبرة و الشهادة يصطلح عليهما بالإجراءات الشخصية ، و هي إجراءات تقليدية و إن كان بعضها مستحدث في الآونة الأخيرة ، و تسمى بالإجراءات الشخصية لكونها إجراءات يتدخل فيها بعض الأشخاص بحكم صفتهم ، و بواسطتهم يتم الحصول على الدليل.⁴

المبحث الثاني: القواعد الإجرائية الحديثة للحصول على الدليل التقني

من ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية ، ما جاء به في القانون 06-22 المؤرخ في 20/12/2006 المعدل و المتمم لقانون الإجراءات الجزائية (الأمر 66-155) من خلال إجرائي التسرب

1 - بن طالب ليندا ، المرجع السابق ، ص 71.

2 - القانون 15-03 مؤرخ في أول فيفري 2015 ، المتعلق بعصرنة العدالة ، الجريدة الرسمية العدد 06 لسنة 2015.

3 - بن طالب ليندا ، المرجع السابق ، ص 71.

4 - نفس المرجع السابق ، ص 69.

و اعتراض المرسلات ، ثم من خلال القانون 09-04 استحدث إجرائين آخرين و هما المراقبة الالكترونية و حفظ المعطيات المتعلقة بحركة السير .

المطلب الأول: التسرب و اعتراض المرسلات

الجريمة المعلوماتية من بين الجرائم التي يمكن فيها إلى إجرائي التسرب و اعتراض المرسلات إذا اقتضت ذلك ضرورات التحري أو التحقيق بشأنها، و تناول كلا الإجرائين وفق الفرعين التاليين :

الفرع الأول - التسرب

لقد حدد المشرع الجزائري نطاق هذا الإجراء بالجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 5 من قانون الإجراءات الجزائية ، من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .¹

أولاً- مفهوم التسرب: التسرب من الناحية الأمنية هو تلك العملية المنظمة المراد من القيام بها التوغل داخل وسط لمعرفة حقيقته معرفة جيدة من خلال نشاطه البارز و كشف الخفي فيه ، و يكون هذا الوسط محددا مسبقا بطبيعته و العمل من أجل الاستعلام عنه و معرفة أدق التفاصيل فيه و خصوصياته و أسرارته حسب تطلعات الجهات الأمنية و فائدة المصلحة ، أما من الناحية القانونية فالمشرع الجزائري حدد المقصود بهذا الإجراء بموجب المادة 65 مكرر 12 على أنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف² .

1 - سعيداني نعيم ، المرجع السابق ، ص 174.

2 - نفس المرجع السابق ، ص 175.

ثانيا- ضوابط التسرب في الجرائم الالكترونية : نظرا لخطورة هذا الإجراء على حرمة الحياة الخاصة للأفراد ، فقد قيده المشرع بجملة من الشروط و الضوابط الواجب اتباعها أثناء مباشرته و هي كالتالي :

أ-الضوابط الإجرائية: تتلخص الضوابط الإجرائية للتسرب الالكتروني في الإذن القضائي و كل ما يجب أن يتضمنه من أحكام ، إذ لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة المتمثلة حسب أحكام المادة (65 مكرر 11 ق إ ج) في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه ، على أن تتم العملية تحت الرقابة المباشرة للجهة المصدرة للإذن حسب الحالة لتفادي حدوث تجاوزات و تعسف في استعمال الحق.¹

كما أنه يشترط أن يكون الإذن بالتسرب مكتوبا و إلا كان الإجراء باطلا، لأن الأصل في العمل الإجرائي الكتابة ، و هو ما أكدته المادة(65 مكرر 15 ق إ ج)² .

ب-الضوابط الموضوعية: إلى جانب الضوابط الاجرائية المذكورة آنفا أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن ايجازها في عنصرين:

4.الأول وجوب التسبب ، المتمثل في المبررات و الحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن بإجراء التسرب ، و الدوافع التي جعلت الضبطية القضائية تلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق التي تكون ضمن الإذن بالتسرب.

5.أما الثاني يتعلق بتحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب ، و التي يجب أن لا تخرج عن نطاق الجرائم المحددة على سبيل الحصر التي يمكن القيام فيها بهذا الإجراء كما أشرنا سابقا.³

1 - براهيمي جمال ، المرجع السابق ، ص85.

2 - تنص المادة 65 مكرر 15 ، من قانون الإجراءات الجزائية ، المرجع السابق على " يجب أن يكون الإذن..مكتوبا و مسببا و ذلك تحت طائلة البطلان..."

3 - براهيمي جمال ، المرجع السابق ، ص 86.

ثالث- التسرب في مجال الجريمة المعلوماتية: يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي و ذلك باختراقه لمواقع معينة و فتح ثغرات الكترونية فيها ، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم و الظهور بمظهر الفاعل مثلهم ، مستخدما في ذلك أسماء أو صفات مستعارة و وهمية سعيا منه للإستفادة منهم حول كيفية اقتحام الموقع.¹

الفرع الثاني : اعتراض المرسلات السلوكية و اللاسلوكية

أولاً- مفهومه : من خلال نص المادة 65 مكرر 5 من قانون الاجراءات الجزائية ، نجد أن المشرع الجزائري يقصد باعتراض المرسلات ، اعتراض او تسجيل أو نسخ المرسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلوكية و اللاسلوكية ، و هذه المرسلات هي عبارة عن بيانات قابلة للإنتاج و التوزيع ، التخزين ، الاستقبال والعرض.

كما عرف المشرع الجزائري الاتصالات الالكترونية في القانون 09-04 في المادة 02 الفقرة "و" على أنها " تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة إلكترونية .²

و في هذا الصدد فإن المرسلات التي تصلح لإجراء اعتراضها يجب أن تتسم بالخصوصية ، و لكي تكون كذلك يلزم أن يتوافر لديها عنصران أساسيان هما :

- أ- عنصر موضوعي و يتعلق بموضوع و مضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي و سري أو خاص فيما تخبره .
- ب- و عنصر شخصي و المراد به إرادة المرسل في تحديد المرسل إليه و رغبته في عدم السماح للغير بالاطلاع على مضمون الرسالة .³

1 - بن نعم خالدين أمين ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، جامعة عبد الحميد بن باديس، مستغانم الجزائر ، سنة 2019 ، ص 93.

2 - سعيداني نعيم المرجع السابق ، ص 177 ، 178 .

3 - نفس المرجع ، ص 179 .

ثانيا- الشروط و الضمانات المقررة لاعتراض المرسلات السلكية و اللاسلكية: مما لا شك فيه أن أسلوب اعتراض المرسلات دون علم أصحابها يفيد في كشف الجريمة و يسهل إثبات كثير من الجرائم كتلك المتعلقة بالجرائم المعلوماتية ، فهو من جانب آخر يمثل انتهاكا لحرمة الحياة الخاصة للأفراد و اعتداء على سرية مراسلاتهم و اتصالاتهم التي كفلها الدستور و قانون العقوبات بالحماية ، و المشرع الجزائري كما مكن سلطات التحقيق من اعتراض المرسلات كأسلوب مستحدث للبحث عن الدليل من جهة ، أحاط هذا الإجراء بشروط قانونية تعمل على منعه التعسف و صون الحرية الفردية ، و تتمثل هذه الشروط في :

أ- ترخيص السلطة القضائية و مراقبتها لعملية التنفيذ: طبقا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المرسلات إلا بعد الحصول على إذن مكتوب و مسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي ، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن و هو ما يعد ضمانا لمشروعية هذا الإجراء .¹

و قد نصت المادة 65 مكرر 09 على أن عملية تنفيذ إجراء اعتراض المرسلات تتم تحت رقابة السلطة القضائية التي أذنت به ، و ذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو النائب من طرف القاضي المختص بإعداد محضرا عن كل عملية اعتراض للمرسلات ، وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض ، و يذكر في المحضر تاريخ و ساعة بداية هذه العمليات و الانتهاء منها .

ب- تحديد طبيعة المراسلة ومدة الاعتراض: و هو ما ورد صراحة في نص المادة 65 مكرر 7 التي نصت على انه يجب أن يتضمن الإذن باعتراض المرسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المرسلات المطلوب اعتراضها ، كما أن مدة الاعتراض يجب أن لا تتجاوز الأربعة أشهر قابلة للتجديد حسب تقدير السلطة

1 - المادة 65 من قانون الإجراءات الجزائية الجزائري ، المرجع السابق .

المصدرة للإذن وفقا لمقتضيات التحري و التحقيق.¹

المطلب الثاني : المراقبة الالكترونية و حفظ المعطيات

تعتبر المراقبة الالكترونية و حفظ المعطيات إجرائين يستعان بهما في البحث والتقصي في مجال الجرائم الالكترونية ، وقد استحدث المشرع الجزائري هذين الاجرائين بموجب القانون 04-09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و ذلك ما سنتطرق إليه من خلال هذا الفرع .

الفرع الأول - المراقبة الالكترونية

نتطرق من خلال هذا الفرع الى مفهوم المراقبة الالكترونية ، و شروط مراقبتها المقررة من قبل المشرع الجنائي كما يلي :

أولاً- مفهومها: لم يعرف المشرع الجزائري على غرار العديد من المشرعين إجراء المراقبة الالكترونية بل اكتفى بتحديد الاتصالات ، غير أن الفقه عرف هذا الإجراء على أنه " إجراء تحقيق مباشر خلسة ، و ينتهك سرية الأحاديث الخاصة ، تأمر به السلطة القضائية في الشكل المحدد قانونا ، بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها و يتضمن من ناحية استراق السمع إلى الحديث ، و من ناحية أخرى بواسطة أجهزة الكترونية مخصصة لذلك.²

و لقد نظم المشرع الجزائري هذا الإجراء في نص المادتين 3 و 4 من القانون 04-09 ، المذكور سابقا ، بحيث نصت المادة 3 على ما يلي " مع مراعاة الأحكام القانونية التي تضمن سرية المرسلات و الاتصالات ، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص

1 - سعيداني نعيم ، المرجع السابق ، ص 181 .

2 - ياسر الأمير فاروق ، مراقبة الأحاديث الخاصة في الإجراءات الجزائية ، دار المطبوعات الجامعية ، الطبعة 1 ، مصر 2009 ، ص 150 .

عليها في قانون الإجراءات الجزائية و في هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراء التفتيش و الحجز داخل منظومة معلوماتية".

كما بين ضمن المادة 4 من نفس القانون الحالات التي يمكن القيام فيها بعمليات المراقبة .¹

ثانيا- شروط المراقبة الالكترونية: نظرا لضرورة هذا الإجراء في التحري و التحقيق في مجال الجرائم المعلوماتية من جهة ، و خطورته على حرية الأفراد المكفولة دستوريا من جهة أخرى ، فقد وازن المشرع بين المصلحتين العامة و الخاصة و أحاط هذا الإجراء بجملة من الشروط يجب التقيد بها للقيام بهذا الإجراء ، و قد أكدها المشرع على هذه الشروط في المادة 04 من القانون 04-09 ، و التي تتمثل في وجوب الحصول على إذن مكتوب من السلطة القضائية المختصة ، كما يجب أن تكون هناك ضرورة للقيام بهذا الإجراء عند ما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري و التحقيق دون هذا الإجراء .

الفرع الثاني- حفظ المعطيات

تتمثل الإجراءات المتعلقة بالبيانات الساكنة في التحفظ العاجل على هذه البيانات ، ثم الأمر بتقديم بيانات معلوماتية متعلقة بالمشارك .

أولا - التحفظ العاجل على البيانات المخزنة : قبل الحديث عن هذا الإجراء و جب علينا التطرق إلى المقصود بمزودي الخدمات ، على أساس أنهم من يحوزون هذه البيانات و مدى التزامهم بالتعاون مع سلطات التحري و التحقيق . يقصد بمزودي الخدمات كل من يقدم خدمات إلى الجمهور بوجه عام في مجال

1 - تنص المادة 04 من القانون 04-09 ، المرجع السابق ، على " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية: أ- للوقاية من الأفعال صوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية...، ج- لمقتضيات التحريات و التحقيقات القضائية ..، د- في إطار تنفيذ المساعدة القضائية الدولية المتبادلة ..."

الاتصالات الالكترونية ، و التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود.¹

كما عرف المشرع الجزائري مقدمو الخدمات بموجب المادة 02 الفقرة "د" من القانون 04-09 بأنهم :

- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام الاتصالات.
- و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعملها.²

ثانيا - الأمر بتقديم بيانات معلوماتية متعلقة بالمشارك : أما التحفظ المعجل على البيانات يقصد به توجيه السلطة المختصة لمزودي الخدمة الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته ، في انتظار اتخاذ اجراءات قانونية أخرى كالقتيش أو الأمر بتقديم بيانات معلوماتية.

و يعتبر التحفظ على المعطيات إجراء أوليا تمهيدا ، الهدف منه هو الاحتفاظ بالمعطيات قبل فقدانها ، و من هذه البيانات المعلوماتية الواجب حفظها البيانات المتعلقة بحركة السير ، المعرفة ضمن المادة 2 الفقرة "هـ" من القانون 04-09 عى أنها " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات ، توضح مصدر الاتصال ، و الوجهة المرسل إليها ، و الطريق الذي يسلكه ، و وقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة".

أما بالنسبة للمعطيات الواجب حفظها فقد ألزم المشرع الجزائري مقدمو الخدمات بضرورة التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بحركة السير ، و التي تشمل :

1 - عائشة بن قارة مصطفى ، المرجع السابق ، ص154.

2 - المادة 02 من القانون 04-09 ، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، المرجع السابق.

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة .
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية و كذا تاريخ و وقت و مدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها.¹

1 - المادة 11 من القانون 04-09 ، المتعلق بالوقاية من الجرائم المتصلة بجرائم تكنولوجيا الإعلام و الاتصال و مكافحتها ، المرجع السابق.

ومن خلال هذا الفصل الثاني تناولنا الإجراءات القانونية الخاصة بالدليل التقني خاصة تلك المستحدثة من قبل المشرع الجنائي نظرا للخصوصية التي يتميز بها الدليل التقني عن غيره من الأدلة في الجرائم التقليدية .

كما بينا من خلال هذا الفصل أيضا أن الدليل التقني بالرغم من إقرار إجراءات مستحدثة لاستخلاصه ، إلا أنه يخضع للإجراءات التقليدية كالمعاينة و التفتيش ... الخ ، مما يعني الدليل التقني يخضع للإجراءات التقليدية و الحديثة معا .

في ذات الشأن ، تطرقنا إلى إبراز حجية و مكانة الدليل التقني في الإثبات الجنائي، والشروط التي تتطلبها الأدلة وفق ما أقره المشرع الجنائي .

الختمة

الخاتمة

إن التطور التكنولوجي لتقنية المعلومات أثر بشكل مباشر على خصوصية الأفراد عامة ، و الدولة خاصة ، لاسيما أن هذه التقنيات أصبحت تستعمل كوسيلة لارتكاب الجريمة تارة ، و كموضوع للجريمة تارة أخرى ، مما أدى إلى اختلاف طبيعة الدليل من مادي ملموس إلى معنوي غير ملموس ، ما نتج عنه ظهور طائفة جديدة من الأدلة تتفق و طبيعة البيئة التي ارتكبت فيها الجريمة ، و هي الأدلة التقنية التي ظهرت مع ظهور المجتمع المعلوماتي الذي ولدت فيه الجريمة المعلوماتية .

و من خلال ما سبق فإن الاستعانة بالدليل التقني كوسيلة إثبات لهذا النوع من الجرائم يقتضي أن يتم الحصول عليه وفق الإجراءات التي أقرها المشرع ، و من قبل أشخاص مؤهلين فنيا و علميا محددين بموجب القانون ، مما يضيف عليه طابع المشروعية حتى تكون له حجية و يقينية من حيث قوته الإثباتية، شأنه في ذلك شأن الأدلة الأخرى ، و يحوز للقاضي الجنائي الاستناد عليه في أحكامه .

فتقديم الدليل التقني إلى المحكمة سليما يعطي للقاضي الجنائي الصلاحية المطلقة في تقدير هذا الدليل ، و يدخل ضمن السلطة التقديرية للقاضي ، إذ لا يمكن استبعاده إلا بدليل أقوى منه يولد لدى القاضي قناعة أكبر من تلك التي يولدها الدليل التقني .

و في كل الأحوال فإن الأخذ بالدليل التقني يعود إلى قناعة القاضي بهذا الدليل ، و له في ذلك التأكد من صحة إجراءات الحصول عليه لتأكيد مشروعيته ، و نظرا للطابع الفني الذي يميز الدليل التقني فقد خول القانون للقاضي الجنائي الاستعانة بالخبراء و الفنيين لإبداء آرائهم في الدليل التقني المطروح في الدعوى ، التي تكون آراء ذات طابع قضائي .

و عليه ، وجب على هيئات التحقيق المختصة استخلاص الدليل التقني طبقا لمبادئ المشروعية الإجرائية و القانونية التي تضمن صحة و دقة ذلك الاستخلاص ، فإذا تم استخلاصه وفق ذلك فإن الدليل التقني سيكتسب حتما طابع مشروعا .

ولقد توصلنا من خلال دراسة الموضوع إلى أهم النتائج التالية :

- الدليل التقني يتم بواسطته إثبات الجرائم التي تقع على النظام المعلوماتي ، و من

الخاتمة

- خلاله أيضا يتم إثبات الجرائم التقليدية التي ترتكب بواسطته .
- الدليل التقني عبارة عن معلومات مخزنة في جهاز الحاسوب و ملحقاته ، أو متنقلة عبر شبكات الاتصال ، و التي يتم تجميعها و تحليلها باستعمال برامج و تطبيقات تكنولوجيا خاصة ، بهدف إثبات وقوع الجريمة و نسبتها إلى مرتكبها .
 - تتمتع الدليل التقني يتمتع بقيمة قاطعة باعتباره يندرج ضمن الأدلة العلمية ، حيث يمكن التأكد من مصداقيته من خلال إجراء اختبارات تمكن من التأكد من صحته.
 - أن الدليل التقني يخضع لضوابط و قيود لاستخلاصه محددة مسبقا من قبل المشرع الجنائي ، حتى يكفل من جهة حق الدولة في الحفاظ على أمنها و نظامها ، و من جهة أخرى حماية حق الفرد في سرية خصوصياته .
 - خضوع الدليل التقني للسلطة التقديرية للقاضي الجنائي شأنه شأن باقي الأدلة التقليدية.
 - استخلاص الدليل التقني يحتاج إلى مؤهلين علميا و فنيا في مجال تكنولوجيا المعلومات ، و هذا بالنظر إلى الخصائص التي تميزه أبرزها التطور السريع و المستمر لتكنولوجيا المعلومات .
 - الاستعانة بالدليل التقني من قبل القاضي الجنائي يحتاج إلى خبراء و فنيين في الغالب لرفع الغموض الذي يشوبه .
- على ضوء النتائج السابقة نطرح الاقتراحات التالية:
- ضرورة التكوين المستمر للمحققين و القضاة في هذا المجال للتمكن من التعامل مع الجرائم المعلوماتية ، حتى يتسنى لهم الوصول الحقيقة في هذا النوع من الجرائم .
 - تكثيف البحوث و الدراسات في مجال جرائم نظم المعلوماتية ، و توسيع نشرها على الكليات و مراكز تكوين المحققين و القضاة لمواكبة التطورات في هذا المجال .
 - الاستعانة بأحدث التقنيات المبتكرة في مجال مكافحة جرائم المعلوماتية و إتاحة الاستعمال المباشر لها من قبل سلطات التحقيق لمباشرة التحريات فور وقوع الجريمة .
 - توسيع التجريم في هذا المجال لسهولة ارتكاب هذا النوع من الجرائم.

قائمة المراجع

- 1- جميل صليبا ، المعجم الفلسفي للمصطلحات القانونية ، دار المناهج للنشر و التوزيع ، ط 1، الأردن، سنة 1990.
- 2- عبد العظيم وزير ، شرح قانون العقوبات القسن الخاص ، جرائم الاعتداء على الأموال ، دار النهضة العربية القاهرة ، سنة 1993.
- 3- هلاي عبد الله أحمد ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، دراسة مقارنة ، دار النهضة العربية القاهرة ، سنة 1993.
- 4- محمد مروان ، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري ، الجزء الأول ، ديوان المطبوعات الجامعية ، الجزائر ، سنة 1999.
- 5- علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب و الانترنت ، عالم الكتب الحديثة ، الأردن ، سنة 2004.
- 6- عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر و الانترنت ، الطبعة الأولى ، دار الفكر الجامعي ، القاهرة مصر ، سنة 2006.
- 7- كوثر أحمد خالد ، الإثبات الجنائي بالوسائل العلمية ، مكتب التفسير للنشر و الإعلان / أربيل ، الطبعة الأولى ، سنة 2007.
- 8- ياسر الأمير فاروق ، مراقبة الأحاديث الخاصة في الاجراءات الجزائية ، دار المطبوعات الجامعية ، الطبعة 1 ، مصر 2009.
- 9- مولود ديدان ، قانون الإجراءات الجزائية ، الأمر 11-02 ، دار بلقيس الجزائر ، سنة 2012.
- 10- شعبان محمود محمد الهواري ، أدلة الإثبات الجنائي ، دار الفكر و القانون ، الطبعة الأولى ، ليبيا ، سنة 2013.

ثانيا : المقالات

1- اللواء د.محمد البشري ، الأدلة الجنائية الرقمية مفهومها و دورها في الإثبات،
المجلة العربية للدراسات الأمنية و التدريب ، المجلد 17 العدد 33 ، الإمارات
العربية المتحدة ، سنة 2002.

2- نور الهدى محمودي ، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية ، مجلة
الباحث للدراسات الأكاديمية ، العدد الحادي عشر ، جوان 2017.

3- أمحمد طارق الجملي، مجلة الحقوق، المجلد 12، العدد1، جامعة بنغازي ليبيا ،
دون سنة النشر .

ثالثا : رسائل الدكتوراه و مذكرات الماجستير و مذكرات الماستر

ا. أطروحات الدكتوراه

1- ملياني عبد الوهاب ، أمن المعلومات في بيئة الأعمال الالكترونية ، رسالة لنيل
شهادة الدكتوراه في القانون العام ، جامعة أبوبكر بلقايد تلمسان، السنة الجامعية
2016/2017.

2- عفاف خذيري ، الحماية الجنائية للمعطيات الرقمية ، أطروحة لنيل دكتوراه في
القانون الجنائي ، جامعة العربي تبسي تبسة ، السنة الجامعية 2017-2018 .

3- براهيم جمال ، التحقيق الجنائي في الجرائم الالكترونية ، أطروحة لنيل شهادة
الدكتوراه في العلوم تخصص القانون ، جامعة مولود معمري - تيزي وزو ، تاريخ
المناقشة 27-06-2018.

4- رابحي عزيزة ، الأسرار المعلوماتية و حمايتها الجزائية ، أطروحة مقدمة لنيل
شهادة الدكتوراه علوم في القانون الخاص ، جامعة أبوبكر بلقايد تلمسان ، السنة
الجامعية 2017-2018

قائمة المراجع

- 5- بن طالب ليندا، الدليل الالكتروني و دوره في الإثبات الجنائي (دراسة مقارنة) ، أطروحة لنيل شهادة الدكتوراه ، تخصص قانون ، جامعة مولود معمري تيزي وزو ، سنة 2019.
- II. رسائل الماجستير
- 1- فيصل مساعد العنزي ، أثر الإثبات بالوسائل التقنية الحديثة على حقوق الإنسان ، بحث مقدم استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2007.
- 2- عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في مجال الإثبات الجنائي دراسة مقارنة، رسالة مقدمة للحصول على درجة الماجستير في الحقوق ، كلية الحقوق جامعة الاسكندرية ، 2009.
- 3- ثنيان ناصر آل ثنيان ، إثبات الجريمة الالكترونية ، رسالة ماجستير ، تخصص السياسة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، السعودية ، سنة 2012.
- 4- محمد نافع فالح رشدان العدوانى ، حجية الدليل الالكتروني كوسيلة من وسائل الاثبات في المسائل الجزائية (دراسة مقارنة بين القانونين الكويتي و الأردني) ، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام ، جامعة الشرق الأوسط ، سنة 2015.
- 5- سعيداني نعيم ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، تخصص علوم جنائية.

III. مذكرات الماستر

- 1- معمش زهية و غانم نسيم ، الإثبات الجنائي في الجرائم المعلوماتية ، مذكرة لنيل شهادة الماستر في الحقوق ، جامعة باتنة ، السنة الجامعية 2012-2013.
- 2- ابتسام بغو ، إجراءات المتابعة الجزائية في الجريمة المعلوماتية ، مذكرة تكميلية لنيل شهادة الماستر تخصص قانون جنائي للأعمال ، جامعة العربي بن مهيدي أم البواقي ، السنة الجامعية 2015/2016.
- 3- علاوي محمد ، دور الأمن المعلوماتي في الحد من الجريمة المعلوماتية ، مذكرة لنيل شهادة الماستر في الحقوق ، تخصص قانون جنائي ، جامعة محمد خيضر بسكرة ، السنة الجامعية 2016-2017 .
- 4- يوسف جفال ، التحقيق في الجريمة الالكترونية ، مذكرة مقدمة لنيل شهادة الماستر تخصص قانون جنائي ، جامعة محمد بوضياف المسيلة ، السنة 2016-2017.
- 5- بشرى عواطة ، حجية الدليل الالكتروني في الإثبات الجنائي ، مذكرة مقدمة لنيل شهادة الماستر في قانون الأعمال ، جامعة 08 ماي 1945 قالمة ، السنة 2017-2018.
- 6- بن نعيم خالد أمين ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري ، مذكرة لنيل شهادة الماستر في الحقوق ، تخصص قانون جنائي ، جامعة عبد الحميد بن باديس مستغانم ، سنة 2019.
- 7- مقراش محمد بن علي ، حجية أدلة الإثبات أمام القاضي الجزائري ، مذكرة لنيل شهادة الماستر ، تخصص قانون قضائي ، جامعة عبد الحميد بن باديس مستغانم ، سنة 2019.
- 8- رزيق محمد ، إجراءات المعاينة ، التفتيش و الحجز داخل المنظومة المعلوماتية ، مذكرة ماستر في القانون العام ، جامعة ألكلي محند أولحاج ، البويرة ، الجزائر ، سنة 2018-2019.

قائمة المراجع

رابعاً : النصوص القانونية

أ- الدستور

1- القانون رقم 01-16 ، المؤرخ في 06 مارس 2016 ، المتضمن التعديل الدستوري ، الجريدة الرسمية العدد 14 .

ب- القوانين

- 1- قانون العقوبات الصادر بموجب الأمر رقم 66-156 المؤرخ في 08 جوان 1966 ، المتضمن قانون العقوبات ، الجريدة الرسمية العدد 49 ، لسنة 1966.
- 2- الامر رقم 66-155 ، المؤرخ في 08 جوان 1966 ، المتضمن قانون الاجراءات الجزائية الجزائي من قانون الإجراءات الجزائية الجزائي.
- 3- القانون 2000-03 ، المؤرخ في 05 أوت سنة 2000 ، المحدد للقواعد العامة المتعلقة بالبريد و بالمواصلات السلكية و اللاسلكية ، الجريدة الرسمية العدد 48.
- 4- القانون 06-22 ، المؤرخ في 20 ديسمبر 2006 ، المؤرخ في 20 ديسمبر 2006 ، المعدل و المتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 ، المتضمن قانون الاجراءات الجزائية الجزائي ، الجريدة الرسمية العدد 84.
- 5- القانون 08-01 ، المؤرخ في 23 جانفي 2008 ، المتمم للقانون رقم 83-11 المؤرخ في 02 جويلية 1983 ، المتعلق بالتأمينات الاجتماعية ، الجريدة الرسمية العدد 04.
- 6- القانون 09-04 ، المؤرخ في 05 أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، الجريدة الرسمية العدد 47 .
- 7- القانون 15-03 مؤرخ في 11 ربيع الثاني عام 1436 الموافق لـ أول فيفري 2015 ، المتعلق بعصرنة العدالة ، الجريدة الرسمية الجريدة الرسمية عدد 06.
- 8- القانون 18-04 ، المؤرخ في 10 ماي 2018 ، المحدد للقواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، الجريدة الرسمية العدد 27 .

قائمة المراجع

9- القانون 07-18 ، المؤرخ في 10 جوان 2018 ، المتعلق بحماية المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، الجريدة الرسمية العدد 34.

ج- المراسيم

- 1- المرسوم الرئاسي رقم 04-183 ، المؤرخ في 26 جوان 2004 ، يتضمن احداث المعهد الوطني للأدلة الجنائية و علم الاجرام للدرك الوطني و تحديد قانونه الاساسي ، الجريدة الرسمية عدد 41.
- 2- المرسوم الرئاسي رقم 04-432 ، المؤرخ في 29 ديسمبر 2004 ، يتضمن انشاء المعهد الوطني للبحث في علم التحقيق الجنائي ، الجريدة الرسمية عدد 84.
- 3- المرسوم الرئاسي رقم 15-261 ، المؤرخ في 08 اكتوبر 2015 ، المحدد لتشكيلة و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، الجريدة الرسمية عدد 53.
- 4- مرسوم رئاسي رقم 20-05 ، المؤرخ في 20 جانفي 2020 ، المتعلق بوضع بمنظومة وطنية لأمن الأنظمة المعلوماتية ، الجريدة الرسمية عدد 04.

فهرس المحتويات

الصفحة	الفهرس
07-1	مقدمة
	الفصل الأول : الطبيعة القانونية للدليل التقني
09	المبحث الأول: الإطار المفاهيمي للدليل التقني .
09	المطلب الأول : مفهوم الدليل التقني
09	الفرع الأول : تعريف الدليل
10	الفرع الثاني : تعريف التقنية
11	الفرع الثالث : استخلاص تعريف للدليل التقني و تحديد مميزاته
15	المطلب الثاني : أنواع الأدلة التقنية و تقسيماتها
15	الفرع الأول - أنواع الدليل التقني
17	الفرع الثاني : تقسيمات الأدلة التقنية بحسب مكان وجودها
20	المطلب الثالث : محل الدليل التقني
20	الفرع الأول : تحديد محل الدليل التقني
21	الفرع الثاني : خصائص النظام المعلوماتي باعتباره محل الدليل التقني

فهرس المحتويات

23	الفرع الثالث: المواجهة التشريعية للإعتداء على النظام المعلوماتي
36	المبحث الثاني : المكانة الإجرائية للدليل التقني في الإثبات الجنائي
36	المطلب الأول : مفهوم الإثبات الجنائي و علاقته بالجرائم المعلوماتية
36	الفرع الأول : تعريف الإثبات .
37	الفرع الثاني: علاقة الإثبات بالجرائم المعلوماتية
38	الفرع الثالث: نظم الإثبات
45	الفرع الرابع : حجية الإثبات بالدليل التقني
48	المطلب الثاني: الأجهزة المكلفة بالحصول على الدليل التقني
48	الفرع الأول: الأجهزة العامة المكلفة بالحصول على الدليل التقني
53	الفرع الثاني : الأجهزة المتخصصة المكلفة بالحصول على الدليل التقني
57	الفرع الثالث : دور مزودي الخدمات في التحري عن الجرائم الماسة بالمعالجة الآلية للمعطيات
الفصل الثاني : الإجراءات الخاصة بالدليل التقني و حجيته في الإثبات	
61	المبحث الأول : القواعد الإجرائية التقليدية الكفيلة بالحصول على الدليل التقني
61	المطلب الأول: المعاينة و الخبرة

فهرس المحتويات

61	الفرع الأول : المعاينة
62	الفرع الثاني : الخبرة
70	المطلب الثاني : التفتيش و الشهادة
70	الفرع الأول : التفتيش
85	الفرع الثاني : الشهادة
87	المبحث الثاني: القواعد الإجرائية الحديثة للحصول على الدليل التقني
88	المطلب الأول: التسرب و اعتراض المرسلات
88	الفرع الأول : التسرب
90	الفرع الثاني : اعتراض المرسلات السلكية و اللاسلكية
92	المطلب الثاني : المراقبة الالكترونية و حفظ المعطيات
92	الفرع الأول : المراقبة الالكترونية
93	الفرع الثاني: حفظ المعطيات
98	الخاتمة
101	قائمة المراجع