جامعة محمد خيضـــر بسكـــرة
كلية الحقوق والعلوم السياسية
قسم الحقوق

تتبع الدليل الرقمي في جرائم المعلوماتية في التشريع الجزائري

مذكرة مكملة لنيل شهادة الماستر في الحقوق

تخصص: قانون جنائي

إعداد الطالبة:
مليكة سعيدان

اشراف الأستاذة :
وردة شرف الدين

الموسم الجامعي : 2017/2016

الإهداء

أهدي هذا العمل المتواضع إلى صغاري الكبار..

الذين ربيتهم ووصيتهم على التمسك بالإيمان و التسلح بحب العلم..

و لما ابتلاني الله بالمرض, وعجز الأطباء عن مداواتي..عالجوني بالإيمان و العلم.

و بفضل الله تعالى، و بتشجيعهم، و بصبرهم معي، أنجزت هذا البحث العلمي..

عسى أن يكون دافعا لهم لمواصلة اجتهادهم في سبيل طلب العلم، و تفوقهم الدائم مصداقا لقول نبينا و رسولنا الكريم عليه الصلاة و السلام:

﴿ اطلبوا العلم من المهد إلى اللحد. ﴾

إليكم صغاري الكبار:

أهدي عصارة فكري ، و ما تبقى في من جهد

- ❖ ملك سلسبيل : ملك روحي
- ❖ مارية تسنيم.: روح قلبي
- ❖ عبد الرحمن: قرة عيني

أحبكم

والدتكم..مليكة سعيدان

شكر و عرفان

﴿ قل هل يستوي الذين يعلمون و الذين لا يعلمون، إنما يتذكر أولو الألباب ﴾

الآية 9 :سورة الزمر

الحمد لله عدد خلقه و زنه عرشه و مداد كلماته...الحمد لله الذي رزقني نعمة العلم .. وإن تعدوا نعم الله فلا تحصوها...و إن ابتلاني بالمرض، فقد أمدني بالقوة لتحمل هذا الابتلاء..وسخر لي من عباده المِؤمنين ..من يساعدني في طلب العلم..

و أخص بالذكر الأستاذ الدكتور: **عبد الواحد شالة**، نائب رئيس جامعة محمد خيضر بسكرة.الذي منحني شهادة ميلاد جديدة. حين أمضى طلب تسجيلي بالجامعة.

وبذلك ساعدني مع صغاري ، الذين رافقوني إلى الجامعة للتسجيل، على قهر داء السرطان بدواء العلم. وأحمد الله أني لم أخيب ظنهم . فاجتهدت لأقدم هذا العمل بتوفيق من الله.

أقدم لك سيدي ، باسمي و باسم صغاري ، جزيل الشكر و العرفان. وفقك الله و أدامك منارة للعلم.

كما أتقدم بالشكر لأول أستاذة قابلتني بابتسامتها في أول حصة في الماستر.

وردة شرف الدين .و المشرفة على مذكرة التخرج..شكرا أستاذتي على توجيهاتك القيمة.أدامك الله مبتسمة و نشيطة.

كما أشكر كل من ساهم في اخراج هذا العمل، خاصة صديقتي الدكتورة: **دليلة الباح** التي تركت بيتها و أولادها وسكنت معي لتشرف على الولادة القيصرية ، كما تسميها، لهذا المولود في أسبوعه الأخير، و السيد فاتح صاحب مطبعة الفجر،الذي أصر على وضع اللمسات الأخيرة للمذكرة.

شكرا هاجر, سعاد, دلال ,زهور,رحمة,فضيلة,.بلبل.ماري.ميمو,و جدو.

شكرا للجميع.

مليكة سعيدان

يشهد العالم في عصرنا الحالي ثورة معلوماتية رهيبة متسارعة التطور، خاصة بعد اندماج تقنية الحوسبة مع تقنيات الإتصال و استعمالاتها الواسعة في جميع مناحي الحياة الاجتماعية و الاقتصادية ..و هذا نظرا للسرعة و الدقة التي توفرها ، والتي ساعدت كثيرا في التحكم في تجميع المعلومات و معالجتها و تخزينها و استرجاعها ثم نقلها و تبادلها بين الأفراد و الشركات و المؤسسات المختلفة داخل الدولة أو خارجها عن طريق شبكة الإتصال الدولية (الأنترنت) و التي بدورها اختصرت الزمان و المكان في عالم إفتراضي .

هذا التطور التكنولوجي المتسارع استفاد منه أيضا المجرمون ، الذين وجدوا في العالم الإفتراضي أرضية خصبة لتطوير أساليبهم الإجرامية. فظهرت جرائم المعلوماتية، وتنوعت مما جعل القائمين على التحري و التحقيق يجدون صعوبات و مشكلات قانونية لكشفها و إثباتها بالوسائل التقليدية. خاصة في مجال جمع الأدلة حيث ظهر نوع آخر من الأدلة الجنائية مرتبط بالعالم الإفتراضي أو البيئة الرقمية التي يولد ويعيش و يستخلص منها و هو الدليل الرقمي ، و الذي أثار في البداية جدلا فقهيا كبيرا حول مدى حجته و قبوله في الإثبات الجنائي بصفة عامة ، وفي جرائم المعلوماتية بصفة خاصة ، دفع بأغلب التشريعات إلى الإعتراف به و بقوته الثبوتية ، و هذا حسب نظام الإثبات المعتمد في كل دولة، و منها التشريع الجزائري الذي لم يكن في منأى عن خطورة هذا النوع من الجرائم المستحدثة ، التي تقتضي استحداث إجراءات جديدة، وأيضا أجهزة متخصصة في تتبع الدليل الرقمي لإثبات هذا النوع من الجرائم و مكافحتها .

و هو موضوع دراستنا **" تتبع الدليل الرقمي في جرائم المعلوماتية في التشريع الجزائري"** ، خاصة و أن الجزائر ، و إن تأخرت في الاستفادة من تكنولوجيات الحوسبة و الاتصال ، إلا أنها خطت في العشرية الأخيرة خطوات عملاقة في مجال رقمنة أغلب القطاعات الحيوية في البلاد نذكر منها عصرنة العدالة، الأرضية الرقمية لوزارة التربية الوطنية ....

هذا فضلا عن استعمالات الفرد و المؤسسات و الشركات للحواسيب المختلفة و المتطورة و الهواتف النقالة الذكية بأنواعها ، و استفادتهم من خدمات الإنترنت الكثيرة كالبريد الإلكتروني ، و مواقع التواصل الاجتماعي .

1- **أسباب اختيار الموضوع :**

أولا أسباب شخصية :

1- من الأسباب التي دفعتني لاختيار هذا الموضوع تتبع الدليل الرقمي في التشريع الجزائري، أني كنت ضحية في جريمة معلوماتية تعود تفاصيلها إلى تاريخ 2010/12/09م. (عيد ميلادي)، لما تلقيت رسالة تهديد و إساءة للرسول ﷺ و تشويه الإسلام الحنيف من طرف أحد المبشرين بالمسيحية. عن طريق رسالة الكترونية في الهاتف النقال . تقدمت على إثرها بشكوى ، تمت معاينة الهاتف النقال و بتسخيرة لمتعامل الهاتف النقال ، ثم التعرف على صاحب الرقم و معرفة عنوانه ، وتوبع بمحكمة بسكرة .

2- أيضا ما حفزني للبحث في هذا الموضوع ، هو ارتباطه بتقنية الحوسبة بتطورها المستمر و هذا يتناسب مع مجال دراستي السابقة و نيلي شهادة دراسات جامعية تطبيقية في الإعلام الآلي سنة 1995م ، فحاولت استغلال و توظيف معارفي و خبراتي في الإعلام الآلي ، في مجال تخصصي في القانون الجنائي عموما ، و الدليل الرقمي خصوصا ، وهذا ما سهل علي مهمة البحث في الخصائص الفنية و التقنية للدليل الرقمي .

3- و أهم سبب لاختيار هذا الموضوع، هو تكملة بحث سابق تضمنته مذكرة تخرجي في ليسانس علوم إدارية و قانونية (2011/2010) بعنوان : الجرائم المعلوماتية بين التشريع و الواقع .

ثانيا أسباب موضوعية :

من الأسباب الموضوعية التي دفعتنني للبحث في موضوع تتبع الدليل الرقمي، في التشريع الجزائري، قلة الدراسات في هذا المجال، خاصة الجزائرية. و هذا في اعتقادي يرجع إلى الدقة و الخصوصية التي يتميز بها لارتباطه بالتطور التكنولوجي و اعتماده على الجانب التقني و العلمي، وهو ما يصعب مهمة البحث فيه و تبادل كل جوانبه لكون أغلب الباحثين لا يتوفرون على المعرفة الكافية بمصطلحات تقنية الحوسبة و الإتصال (بحكم شعبة الدراسة).

هذا فضلا على أن الدليل الرقمي موضوع جديد مرتبط بجرائم مستحدثة نسبيا في مجتمعنا و هي جرائم المعلوماتية و أغلب الدراسات تناولتها من الجانب النظري أكثر من التطبيقي ، في الوقت الذي كان يجب التطرق إليه من كل الجوانب، ليتمكن الفرد من فهم كل ما يتعلق بالموضوع، ومن ثم وقاية نفسه و محيطه من سلبيات التكنولوجيا الجديدة و التي أصبحت تفرض علينا التعامل بمقتضاها، و لم يعد بالإمكان الاستغناء عنها.

و على هذا الأساس حاولت أن أقدم بحثا متخصصا نوعا ما ، أي دراسة أكثر عمقا و دقة في تفاصيل الموضوع مستغلة خبراتي المتواضعة في مجال تقنية الحاسوب و الإتصال عسى أن يكون مفيدا للقارئ و يقدم إضافة للمكتبة القانونية.

3- أهمية الدراسة :

تكمن أهمية الدراسة في الانتشار الواسع و المتزايد لجرائم المعلوماتية، و تعدد صورها و صعوبة اكتشافها و إثباتها بالأدلة الجنائية المعروفة و ظهور الدليل الرقمي كنوع جديد من الأدلة الجنائية لإثبات هذا النوع من الجرائم وما يتطلبه من قوانين موضوعية و إجرائية خاصة للبحث عنه واستخلاصه و تقديمه للعدالة للحكم على الجناة و ردعهم .

و بالتالي تكمن أهمية الموضوع في أهمية الدليل الرقمي في حد ذاته و مدى حجيته في إثبات جرائم المعلوماتية، بكشفها ومحاولة الحد منها. ما يفرض على المكلفين بذلك، أمنا و قضاء و تشريعا و حتى أفرادا ، اطلاعا واسعا . على ماهية الدليل الرقمي و آليات تتبعه .

و تكمن أهمية هذه الدراسة أيضا في ضرورة التحسيس بخطورة الجرائم المعلوماتية على أمن الأفراد و المؤسسات و الدولة، وبالتالي ضرورة الوقاية منها و التأهب لمكافحتها . و التعريف بهذه الظاهرة و بآليات إثباتها و قدرات أجهزة الدولة على ذلك خاصة في مجال تتبع الدليل الرقمي لإثبات هذه الجرائم .

وهذا من شانه طمأنة الضحايا و توعيتهم لتقديم شكاوي في حالة تعرضهم لاعتداءات من هذا النوع و هو التحدي الذي مازال في رأيي يعرقل الكشف عن جرائم المعلوماتية (إحجام الضحايا عن التبليغ) كما سنرى لاحقا .

3- إشكالية الدراسة :

موضوع دراستنا هو تتبع الدليل الرقمي في جرائم المعلوماتية يقودنا إلى طرح الإشكالية التالية :

- ما هي آليات تتبع الدليل الرقمي في جرائم المعلوماتية في التشريع الجزائري ؟

و هذه الإشكالية تفرض التساؤلات التالية :

- ما المقصود بالدليل الرقمي و ما هي خصائصه و تصنيفاته ؟
- ما مفهوم جرائم المعلوماتية كمحل للدليل الرقمي ؟
- ما مدى كفاية الإجراءات التقليدية في تتبع الدليل الرقمي ؟
- ما هي الإجراءات المستحدثة وما مدى نجاعتها في تتبع الدليل الرقمي ؟

4- الصعوبات التي يطرحها الموضوع :

إن موضوع الدليل الرقمي حديث نسبيا مثله مثل جرائم المعلوماتية في مجتمعنا الجزائري. و الصعوبة الأولى التي واجهتنا في إعداد هذه الدراسة هي ندرة المراجع الجزائرية التي تناولته إن لم نقل انعدامها، لأن المراجع الموجودة، تناولت جرائم المعلوماتية سطحيا، دون التعمق في تفاصيلها و طرح الجديد فيها. مما جعلنا نلجأ إلى البحث في النصوص القانونية المشيرة إليها و إلى الدليل الرقمي. لأن المشرع الجزائري لم ينص صراحة لكنه نظم أحكامه. (خاصة في القانون رقم 09-04 و المرسوم الرئاسي رقم 15-261 اللذين سنتطرق إلى دراستهما لاحقا) ، مما تطلب منا جهدا مضاعفا في البحث، يهون أمام أهمية الموضوع و النتائج التي توصلنا إليها. مستعينين بمراجع أجنبية في كثير من الأحيان، لتقريب الفهم أكثر، وتوضيح بعض الغموض.

و الصعوبة الثانية التي واجهتنا، هي عدم رد مصالح العدالة و الأمن و الدرك على طلباتنا للمساعدة في انجاز هذه الدراسة، و التي قدمناها منذ بداية البحث، و لم نتلقى الرد إلى غاية كتابة هذه السطور . وهذا في رأينا لا يخدم البحث العلمي ، و لا الهدف منه في مجال التحسيس بخطورة جرائم المعلوماتية و كيفية إثباتها من الناحية العملية، ولا سياسة الدولة المنادية بتقريب هذه القطاعات من المواطن.

و رغم ذلك سعينا إلى الوصول إلى المعلومات المطلوبة بطرقنا الخاصة، من خلال مواقع هذه القطاعات على الأنترنت و حوار مسجل بالإذاعة، و كذا حضور ملتقى حول الجرائم، المعلوماتية في جامعة محمد خيضر بسكرة و الاستفادة من المداخلات التي قدمها الباحثون و خاصة ضباط الدرك و الشرطة الوطنيين.

5- منهج الدراسة :

لقد لعبت طبيعة الموضوع دورا رئيسيا ومهما في اختيار منهج الدراسة المناسب إن لم نقل فرضت اتباعه ، وهو المنهج الوصفي الذي يهدف إلي التعرف على ظاهرة معينة كما وكيفا ، فيحدد أوصافها و خصائصها، و مقوماتها بحيث يسهل التعرف عليها فيما بعد و مقارنتها بباقي الظواهر الأخرى.و يظهر استعمال هذا المنهج في الفصل الأول.

كما فرضت الدراسة المنهج الاستقرائي التحليلي, باستقراء النصوص القانونية: الموضوعية و الإجرائية , التقليدية منها و المستحدثة في تتبع الدليل الرقمي، ثم تحليل هذه النصوص للوصول إلى النتائج المطلوبة، و هي مدى كفاية هذه النصوص في معالجة جرائم المعلوماتية و استخلاص الدليل الرقمي لإثباتها.و يغلب استعمال هذا المنهج في الفصل الثاني.

وقد حاولنا في هذه الدراسة مراعاة التسلسل المنطقي لعناصر الموضوع.

6- خطة الدراسة:

للإجابة عن الإشكالية الأساسية في الدراسة و الإشكاليات المتفرعة عنها قسمنا الدراسة إلى فصليين:

تناولنا في الفصل الأول ماهية الدليل الرقمي، وذلك في مبحثين،خصصنا المبحث الأول للحديث عن ماهية الجريمة المعلوماتية كمحل للدليل الرقمي و حجيته في إثبات جرائم المعلوماتية في التشريع الجزائري.

أما الفصل الثاني فتناولنا فيه إجراءات تتبع الدليل الرقمي في التشريع الجزائري ويتكون الفصل من مبحثين ، إذ تحدثنا في المبحث الأول عن الإجراءات التقليدية ، وفي المبحث الثاني على الإجراءات المستحدثة وكذا الأجهزة المتخصصة.

وفي آخر الدراسة توصلنا لعدد من النتائج أعقبناها بجملة من الاقتراحات تضمنتها خاتمة هذه الدراسة.

تقتضي دراسة الإجراءات تتبع الدليل الرقمي أن نتطرق أولا إلى ماهية الدليل الرقمي، ونظرا لارتباط الدليل الرقمي بجرائم المعلوماتية يقتضي الأمر التطرق قبلا إلى ماهية هذه الجرائم.

لذلك سنقسم هذا الفصل إلى مبحثين:

المبحث الأول : ماهية الجريمة المعلوماتية كمحل للدليل الرقمي.

المبحث الثاني: مفهوم الدليل الرقمي وحجيته في إثبات جرائم المعلوماتية.

المبحث الأول

الجريمة المعلوماتية كمحل للدليل الرقمي

جرت العادة في أي بحث علمي حين نخوض في ماهية موضوع معين فإننا نتطرق أولا إلى مفهومه، من حيث: تعريفه، خصائصه وأنواعه ثم محله.

لكن في هذا البحث نخرج عن هذه العادة ونتطرق إلى مفهوم الجريمة المعلوماتية قبل مفهوم الدليل الرقمي وذلك نظرا لخصوصية موضوع البحث في حد ذاته، ولأن تعريفات وخصائص وأنواع الدليل الرقمي يستمدها من تعريفات وخصائص وأنواع الجريمة المعلوماتية.

وبناءا على ذلك: قسمنا المبحث إلى مطلبين، نتناول في المطلب الأول: مفهوم الجريمة المعلوماتية. وفي المطلب الثاني نتناول تصنيفات الجريمة المعلوماتية في التشريع الجزائري.

المطلب الأول

مفهوم الجريمة المعلوماتية

لاشك في أن ظهور الجريمة المعلوماتية وتنوعها وتطورها مرتبط: بظهور والتطور وانتشار تكنولوجيات الإعلام والاتصال واستعمال التقنيات الحديثة في شتى المجالات كالتجارة الإلكترونية أو الرقمية، الاقتصاد الرقمي ،الحكومة الرقمية، العدالة الرقمية.....

وتعددت المفاهيم والمصطلحات الدالة على الظاهرة الإجرامية في مجال الحاسوب وشبكة الانترنت وذلك تبعا للتطور التاريخي لتقنية الحوسبة والاتصال والترابط بينهما.

فظهر في البداية مصطلح إساءة استخدام الحاسوب.....

تعددت المفاهيم والمصطلحات الدالة على الظاهرة الإجرامية في المجال الحاسوب وشبكة الإنترنت، وذلك تبعا للتطور التاريخي لتقنية الحوسبة والاتصال والترابط بينهما. فظهر في البداية مصطلح إساءة استخدام الحاسوب، احتيال الكمبيوتر، الجريمة المرتبطة بالكمبيوتر، الجرائم الحاسوبية.

وبعد ظهور شبكة الانترنت العملاقة ظهرت المصطلحات التالية: جرائم الانترنت، جرائم الكمبيوتر والانترنت، الإجرام ألمعلوماتي، الإجرام الافتراضي، الإجرام السيبيري، الغش ألمعلوماتي، جرائم الإلكترونية، الجرائم التقنية العالية، الجرائم المعلوماتية، وهناك مصطلح آخر: جرائم ذوي الياقات البيضاء كان قديما يطلق على الجرائم التي تنسب لأهل العلم.

ولا شك أن اصطلاح الجريمة المعلوماتية هو الأشمل والأدق للدلالة هذا النوع من الجرائم المتعلقة بالحاسوب والانترنت أو بغيرها من الوسائط الالكترونية الأخرى مثل الهاتف المحمول وذلك لاعتبارين: الأول أن المعلومة هي محور الفعل الإجرامي والذي يقع على المضمون ألمعلوماتي الذي يترجم إلى أرقام (0.1) والثاني ترابط تقنية الحوسبة والاتصال التي تخزن وتعالج وتنقل تلك المعلومات.

وعلى هذا الأساس سوف نعتمد هذا الاصطلاح في دراستنا هذه والملاحظ أنه أيضا الأكثر شيوعا واستعمالا في أغلب الدول الأوروبية والعربية وحتى في الجزائر.

وسنحاول في هذا المطلب الإحاطة بمفهوم بالجريمة المعلوماتية من خلال الفروع التالية.

الفرع الأول: تعريف الجريمة المعلوماتية

مصطلح الجريمة المعلوماتية مركب من مصطلحين: الجريمة والمعلوماتية. للوصول إلى تعريف الجريمة المعلوماتية، لابد من تعريف كل مصطلح على حدى..

أولا: تعريف الجريمة

الجريمة هي الفعل الذي يجرمه القانون، ويقر له جزءا جنائيا أو هي فعل أو امتناع يخالف قاعدة جنائية تحظر السلوك المكون لها، وترتب لمن يقع منه جزاءا جنائيا.

ويفضي هذا التعريف إلى القاعدة الشهيرة لا جريمة ولا عقوبة إلا بنص[1]

ثانيا: تعريف المعلومة

عرفها المشرع الفرنسي وفقا للقانون 82/ 652. الصادرة 26 جويلية سنة 1982: على أنها صورة أو مستندات أو معطيات أو خطابات أيا كانت طبيعتها.

ثالثا: تعريف المعلوماتية

هي المعالجة الآلية للمعلومات، وهي ترجمة من اللغة الفرنسية لكلمة Informatique وتعني تكنولوجيا ومعالجة و إرسال المعلومات بواسطة الكمبيوتر.

وقد استعمل هذا المصطلح لأول مرة: ميخالوف Mikhalov مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفيتي وسماه بعلم المعلومات العلمية [2]

[1] . منصور رحماني: الوجيز في القانون الجنائي العام ، دار العلوم للنشر والتوزيع. ص83.

[2] خثير مسعود: الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر2010، ص19.

رابعا: تعريف الجريمة المعلوماتية

مثلما تباينت المصطلحات الدالة على الجريمة المعلوماتية تباينت أيضا تعريفاتها.وبالتالي لا يوجد تعريف قانوني موحد للجريمة المعلوماتية.

إن غياب تعريف قانوني دقيق لهذا المصطلح وترك الأمر للفقهاء لإعطاء مفاهيم وتصورات مختلفة جعل الأمر أكثر تعقيدا، مما يشكل عائقا أمام رجال القانون لبحث وفهم هذه الجريمة ومن ثم إثباتها ومكافحتها.[1]

وهكذا ظهرت تعريفات فقهية مختلفة حسب الزاوية التي ينظر منها للجريمة المعلوماتية، منها الضيقة ومنها الموسعة وهذا ما سنتطرق إليه.

1- التعريفات الضيقة للجريمة المعلوماتية:

أيضا اختلف الفقه في تعريف الجريمة المعلوماتية من وجهة نظر ضيقة، فمنهم من اعتمد معيار الوسيلة المستعملة ومنهم من اعتمد المعيار الشخصي والمتمثل في توافر المعرفة بتقنية الحاسب، ومنهم من اعتمد المعيار الموضوعي لكون الجريمة المعلوماتية موضوعها المال المعلوماتي المعنوي.[2]

وعلى هذا الأساس سنورد التعريفات التالية

أ- معيار الوسيلة:

يعرف الفقيه Merwe الجريمة المعلوماتية على أنها: الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي.[3]

([1]). غنية باطلي: الجريمة الاكترونية، منشورات الدار الجزائرية، 2015،، ص13.
([2]) المرجع نفسه، ص 14.
([3]) د. أمين الشوابكة: جرائم الحاسوب والانترنت، دار الثقافة عمان، الاصدار الثالث، 2009، ص8.

ب- المعيار الشخصي:

عرفها الفقيه David Thompson: هي جرائم يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب [1].

وقيل أيضا بأنها الأفعال التي يرتكبها شخص على دراية بتقنية المعلومات. وقيل أنها الأنشطة أو الأفعال الغير المشروعة التي يتطلب ارتكابها أو متابعة فاعلها والتحقيق فيها دراية بنظم المعلومات.[2]

ج- المعيار الموضوعي:

لا ينظر هنا إلى شخص الفاعل أو الوسيلة المستخدمة وإنما إلى موضوع الجريمة المعلوماتية الذي هو المال ألمعلوماتي المعنوي.

فقيل بأنها: نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك يتم تحويلها عن طريقه [3].

أو هي الجرائم التي ترتكب على الأنظمة الإلكترونية والشبكات المعلوماتية[4]. كالقرصنة والاستعمال غير المشروع للأنظمة المعلوماتية، فقد تقع على حق الملكية الفكرية أو حرمة الحياة الخاصة أو سلامة الشرف والاعتبار.

([1]) . غنية باطلي: مرجع سابق، ص17.
([2]) أمين فرج يوسف: الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية،2009، ص216.
([3]) محمد أمين الشوائكة: مرجع سابق، ص8.
([4]) د. غنية باطلي: مرجع سابق ،ص17.

2ـــ التعريفات الموسعة للجريمة المعلوماتية:

نظرا لقصور التعريفات الضيقة للجريمة المعلوماتية فقد ظهرت تعريفات أخرى موسعة، أكثر شمولية وتعبيرا عن هذا النوع المستحدث من الجرائم، باستعمال أكثر من معيار و فيما يلي سنورد أهم التعريفات :

أ- تعريف المجلس الأوروبي:

أقر المجلس الأوروبي في تقرير الجرائم المتعلقة بالحاسوب بقيام الجريمة المعلوماتية في كل حالة يتم فيها تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال انجاز البيانات أو معالجتها، وتبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية لشخص أخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر. [1]

ب- تعريف مؤتمر الأمم المتحدة:

تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، تعريفا موسعا للجريمة المعلوماتية جاء فيه:" أنها أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، ونشمل ذلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية". [2]

نلاحظ بأن هذا التعريف حاول الإحاطة بكل أنواع الجرائم التي يمكن إن ترتكب في بيئة الكترونية. وهو ما تبناه المشرع الجزائري كما سنرى.

---

[1] نهلا عبد القادر المومني : الجرائم المعلوماتية ، دار الثقافة النشر و التوزيع، االأردن 2008، ص 49..

[2] مؤتر الأمم المتحدة العاشر الذي عقد في الفترة مابين 10-17 أفريل 2000 فينا.

ج- تعريف المشرع الجزائري:

لم يرد مصطلح الجريمة المعلوماتية في التشريع الجزائري بل استعمل في البداية مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات وذلك من خلال قانون رقم 04-15. [1] المتضمن تعديل قانون العقوبات والذي يدل فقط على الجرائم التي يكون النظام المعلوماتي محلا لها وأمام اتساع رقعة الاعتداءات الأخرى وتنوعها وعدم كفاية القانون السابق لتجريمها، فقد تدارك المشرع هذا الفراغ التشريعي وظهر مصطلح: الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال من خلال قانون رقم 09-04 [2] حيث جاء التعريف الموسع التالي في المادة 02/ف1: "يقصد في مفهوم هذا القانون بما يلي: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية."

وهنا المشرع الجزائري تبنى التعريف الموسع للجريمة المعلوماتية فهي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أي التي يكون المنظومة المعلوماتية محلا لها، تشمل الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها، أو مسهلة لها، ويدخل فيها إلى جانب الحاسوب : الهاتف المحمول وكل وسيلة الكترونية جديدة أخرى، لأنه يتشابه معه في مكوناته وإمكانياته،، بل يزيد عنه أنه سهل الاستعمال.

---

[1] قانون رقم 04- 15 المؤرخ في 10/ 2004/11 التضمن تعديل قانون العقوبات القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

[2] .قانون رقم 09- 04 مؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ج ر عدد47 صادرة بتاريخ 16 أوت 2009.

وكما سبق القول فان الهاتف المحمول والخلوي يتشابه إلى حد كبير مع إمكانيات الكمبيوتر مثل الرسائل الالكترونية والصور عن طريق تقنية البلوتوث ، أيضا الدخول إلى الانترنت ، فهو تقنية من تقنيات الحوسبة المتطورة من غير المعقول إخضاعها إلى قانون الاتصالات. [1]

الفرع الثاني:خصائص الجريمة المعلوماتية

تتخذ الجريمة المعلوماتية طابعا متميزا يجعلها تختلف عن الجرائم التقليدية مما يطرح تحديات كثيرة لمكافحتها و يرجع ذلك لارتباطها بتطور تكنولوجيا الإعلام و الاتصال من جهة ومن جهة أخرى لقصور القوانين الوطنية على مواكبتها و بالتالي تثور إشكالية صعوبة اكتشافها وصعوبة إثباتها وأخيرا صعوبة مكافحتها .

وفيما يلي سنحاول حصر خصائص الجريمة المعلوماتية منها ما يتعلق بالجريمة في حد ذاتها ومنها ما يتعلق بشخص الجاني.

أولا خصائص تتعلق بالجريمة في حد ذاتها:

1-**الجريمة المعلوماتية من الجرائم العابرة للحدود:** فهي ذات صبغة عالمية مما يجعل مسرحها هو كل العالم نظرا لوقوعها على شبكة الانترنت أي إنها لا تقع بمكان محدد كباقي الجرائم الجنائية [2] فقد تقع الجريمة في دولة. وتلحق ضررا بشخص في دولة أخرى، وبالتالي أي القوانين تطبق في ظل إقليمية القوانين وكذا الاختصاص القضائي.مما يقتضي تعاونا دوليا لمكافحة هذا النوع من الجرائم عن طريق المعاهدات والاتفاقيات الدولية، مثل اتفاقية بودابست سنة 2001 [3] و الاتفاقية العربية لمكافحة تقنية المعلومات .

---

[1] عائشة بن قارة مصطفى : حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن دار الجامعة الجديدة،2010 ص 31.

[2] غنية باطلى: مرجع سابق ، ص 49.

[3] اتفاقية بودابست الموقعة في 11/23/ المتعلقة بالجرائم المعلوماتية،مشار إليها عند ا.هلالي عبد الله احمد:اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها.الطبعة الأولى، القاهرة، 2007.

المحررة بالقاهرة بتاريخ2010/12/21 والتي صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-252 مؤرخ في 2014/09/08 [1] .

2-**صعوبة اكتشافها وإثباتها**: فهي لا تترك آثارا ظاهرة، فهي تستهدف البيانات المخزنة في نظم المعلومات التي هي مجرد أرقام و دلالات تتغير وتمحى من السجلات بسهولة.

وغالبا ما تكتشف بالصدفة، لأنها تتم في بيئة غير تقليدية، خارج الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب و الانترنت ويطلق عليها "البيئة الرقمية" تنعكس بدورها على طبيعة الدليل الذي تنتجه مما تجعله غير مرئي. [2] ويطرح مشكلات قانونية تتعلق بجمعه واستخلاصه، وتقديمه للقضاء مما اقتضى إجراءات خاصة لتتبع الدليل الرقمي وهذا ما سنتطرق إليه لاحقا بالتفصيل لأنه موضوع دراستنا.

كما أن المجني عليه يلعب دورا رئيسا في صعوبة اكتشاف وقوع الجريمة المعلوماتية، حيث تحرص أكثر الجهات التي تتعرض أنظمتها للانتهاك، على عدم الكشف حتى بين موظفيها عما تعرضت له، تجنبا للإضرار بسمعتها ومكانتها، وهز الثقة في كفاءتها [3].

ونفس الشيء ينطبق على الأفراد الذين تتعرض حساباتهم للقرصنة مثل الفيس بوك أو البريد الالكتروني.

وهنا يلعب الجانب التوعوي و التحسيسي دورا كبيرا حول خطورة وفداحة هذه الجرائم، وضرورة مكافحتها.بعدم الإحجام عن التبليغ عنها.

---

[1] جريدة رسمية .عدد 57، صادرة في 2014/09/28.
[2] عائشة بن قارة مصطفى: مرجع سابق. ص57.
[3] نهلة عبد القادر المومني: مرجع سابق.ص54.

ثانيا خصائص تتعلق بالجانى(المجرم المعلوماتى):

1-من حيث أسلوب ووسائل ارتكاب الجريمة:

إذا كان ارتباط الجريمة المعلوماتية بتكنولوجيا الإعلام والاتصال قد جعلها تتميز عن الجريمة التقليدية وكذلك هذا الارتباط جعل المجرم المعلوماتي يتميز عن المجرم التقليدي سواء من حيث وسائل ارتكاب الجريمة أو أسلوب ارتكابها فالمجرم المعلوماتي يعتمد غالبا على أسلوب التضليل و الخداع دون اللجوء إلى أسلوب العنف، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء[1].

لذلك يقال أنها جرائم ناعمة، لا تحتاج أدني مجهود عضلي، بل تعتمد على الدراسة الذهنية و التفكير العلمي المدروس القائم عن معرفة تقنية الحاسب[2] فضلا عن امتلاك و توافر وسائل هذه التقنية من حاسب إلي، أو هاتف محمول ذكي، أو أي وسيلة تقنية أخرى تستعمل في ارتباك الجريمة المعلوماتية وشبكة الانترنت.

2- من حيث هدف ارتكاب الجريمة:

الدافع إلى ارتكاب الجريمة المعلوماتية ليس إجراميا في كل الأحوال فقد يكون بدافع الفضول و الاطلاع، إثبات القدرة على قهر النظام وكسر الحاجز الأمني للأنظمة، وأحيانا أخرى يكون بدافع تحقيق الكسب المادي وبذلك يمكن حصر المجرم المعلوماتي في ثلاث طوائف.

ا-**المخترقون**:وتشمل هذه الطائفة نوعين: الهاكرز و الكراكز.

(1) أمير فرج يوسف، مرجع سابق.ص216.

(2) محمد أمين الرومي: جرائم الكمبيوتر و الانترنت. دار المطبوعات الجامعية . الإسكندرية.200 4.ص23.

01-الهاكرز أو المتطفلون:

المتطفل هو الشخص الذي يشعر بالفخر لمعرفته بأساليب عمل النظام أو الشبكات،حيث يسعى للدخول إليها بدون تصريح، وهؤلاء الأشخاص عادة لا يتسببون في أي أضرار مادية[1] وإنما ينطلقون من دوافع التحدي واثبات الذات، بكسر أمن نظم الشبكات[2].

02-الكراكرز، المخربون أو المقتحمون:

المخرب هو الشخص الذي يحاول الدخول على أنظمة الكمبيوتر دون تصريح، وهؤلاء الأشخاص عادة ما يتسببون في أضرار مادية عكس المتطفلين.

ب-المحترفون:

أهداف هذه الطائفة هي تحقيق الكسب المادي سواء لهم أو للجهات التي دفعتهم إلى ارتكاب جرائم الاعتداء على أنظمة الكمبيوتر إلى جانب أهداف سياسية وأخرى فكرية، يرتكبون جرائهم في الخفاء ويسعون لعدم كشفا، بحيث ينطبق على أفعالهم وصف الجريمة المنظمة.

ج-الحاقدون:

ينعدم عند هذه الطائفة هدف الكسب المادي ، أو التحدي لاختراق النظام الأمني للشبكة، و إنما تحركهم الرغبة في الانتقام و الثأر ، سواء من صاحب العمل إذا كانوا موظفين ، أو من أي مؤسسة مستهدفة من إجرامهم إذا كانوا غير موظفين فقد يكونوا مستخدمي نفس النظام و تربطهم علاقة به و يستخدمون في إجرامهم تقنية الفيروسات والبرامج المدمرة للنظم.

يعتبر الباحثون هذا التصنيف أفضل تصنيف للمجرم المعلوماتي الذي أورده: . David Icove Paul Serger .William Vomstouchفي مؤلفهم جرائم الكمبيوتر الصادر عام 1995.

(1) أمير فرج يوسف، مرجع سابق.ص68 .
(2) المرجع نفسه ص68.

المطلب الثاني:

تصنيفات جرائم المعلوماتية

تعددت وتنوعت جرائم المعلوماتية، وذلك حسب تطورها عبر الزمن، و المرتبط أساسا بتطور تقنية الحوسبة و الاتصال وانتشار استعمالاتها في جمع الحالات:

ومثلما تباينت تعريفات جرائم المعلوماتية تباينت معها تصنيفاتها، سواء من طرف الفقهاء أو من المشرعين. وهذا ما سنتناوله في الفرعين التاليين.

الفرع الأول: التصنيفات الفقهية

يصنف الفقهاء و الدارسون الجرائم المعلوماتية ضمن فئات متعددة، تختلف حسب الأساس الذي يستند إليه التقسيم. فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب و أخرى ترتكب بواسطته،وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، و آخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وبصفة عامة تم تصنيف جرائم المعلوماتية بحسب دور الحاسوب وشبكة المعلومات فيه

فقد يكون الحاسوب(أو أي وسيلة تقنية مشابهة)، وشبكة المعلومات هدفا، وقد يكون وسيلة، وقد يكون بيئة لارتكاب هذه الجرائم وفي حالات قد يكون وسيلة و بيئة في وقت واحد، ورغم ذلك يبقى محل الجريمة دائما هو المعطيات باعتبارها مالا معنويا،إما بذاتها أو بما تمثله هذه المعطيات التي قد تكون مخزنة داخل النظام أو على احد وسائط التخزين أو تكون في طور النقل و التبادل ضمن وسائل الاتصال المندمجة مع نظام الحوسبة[1].

وبالتالي يستبعد الجرائم التي تقع على الحاسوب ككيان مادي مثلا سرقته أو سرقة أو إتلاف جزء منه، بحيث تدخل في الجرائم العادية وتطبق عليها النصوص الجنائية التقليدية، فهي ليست مستحدثة.

[1] وسيم حرب ورقة عمل مقدمة لأعمال الندوة الإقليمية حول جرائم المعلوماتية.2007 .

أولا: الحاسوب وشبكة المعلومات هدف للجريمة

قد يكون الحاسوب وشبكة المعلومات هدفا للجرائم المعلوماتية مثل:

ـ اختراق الأنظمة المعلوماتية.

-الدخول غير المشروع للمواقع بغية إتلاف وتدمير البيانات و المعطيات و المعلومات المخزنة.

-القرصنة المعلوماتية بالاستيلاء و الاستخدام غير المشروع لنظم التشغيل، و البرامج و البيانات المنقولة عبر النظم.

-الاعتداء على خصوصية الأشخاص، وذلك عن طريق التسلل ومعرفة بيانات مستخدمي شبكة الانترنت دون علمهم والاطلاع على كافة ما يحتويه جهاز الحاسوب من بيانات الأفراد الأمر الذي يستغله البعض من جرائم الابتزاز[1].

ثانيا:الحاسوب وشبكة المعلومات وسيلة للجريمة

في هذه الحالة، يلعب الحاسوب وشبكة المعلومات دورا لمسهل لارتكاب بعض الجرائم التقليدية مثل:

السرقة: أو الاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف و التزوير أو استخدام التقنية في الاستيلاء على أرقام بطاقات الائتمان إعادة استخدامها.

القتل:عن الدخول إلى البيانات المخزنة و التلاعب بها مثل البيانات الخاصة بالمرضى فتغيير البيانات: نتائج التحاليل المخبرية أو الوصفة الطبية يؤدي إلى تشخيص خاطئ للمرضى وبالتالي إعطاء المريض دواء لا يناسبه قد يؤدي إلى قتله.

(1) هدى قشقوش.جرائم الحاسب الآلي في التشريع المقارن.ط1،دار النهضة العربية،القاهرة،1992،ص10 .

- كذلك التلاعب بنظم التحكم بالطائرات و السفن قد يؤدي إلى تدميرها و بالتالي قتل ركابها.

- إلى غير ذلك من الأمثلة في هذا المجال يسهل القتل دون عنف أو تهديد.

ثالثا: الحاسوب وشبكة المعلومات بيئة للجريمة

يمكن أن يكون الحاسوب وشبكة المعلومات بيئة للجريمة، وذلك في حالة تخزين البرامج المقرصنة فيه، و المواقع الإباحية التي تنشر الصور و الأفلام الخليعة، وما تلعبه من دور في نشر الرذيلة وهدم الأخلاق.

كما تساهم في ترويج المحذرات و الأنشطة الأخرى غير المشروعة [1]. و كل هذا في نطاق واسع أمام سقوط الحدود الجغرافية في هذا النوع من الجرائم العابرة للحدود.

الفرع الثاني: التصنيفات التشريعية لجرائم المعلوماتية

نظرا لتزايد المخاطر الأمنية و الأضرار الجسيمة التي ألحقتها جرائم المعلوماتية سواء بالأفراد أو بالمؤسسات، وذلك طبعا راجع للاستعمال الواسع للحاسوب وتكنولوجيا الإعلام و الاتصال في جميع المجالات وفي جميع القطاعات. كثفت الدول جهودها لمواجهة هذا الخطر الداهم. وذلك بسن قوانين داخلية وتعديلها باستمرار للإحاطة بكل أصناف جرائم المعلوماتية فضلا عن المعاهدات و الاتفاقيات الدولية بغية عدم إفلات مرتكبي هذا النوع من الأفعال الإجرامية من العقاب، بسبب قصور النصوص التقليدية سواء من الجانب الموضوعي أو الإجرامي.

وسنتناول في هذا المقام كنموذج الأفعال المجرمة وفق اتفاقية بودابست ثم سنتناول الأفعال المجرمة وفق التشريع الجزائري ، وذلك حسب التسلسل الزمني للقوانين التي نصت عليها.

[1] هدى قشقوش.جرائم الحاسب الآلي في التشريع المقارن.ط1،دار النهضة العربية،القاهرة،1992،ص10 .

أولا: اتفاقية بودابست

أو الاتفاقية الأوروبية للجريمة المعلوماتية: وقعت هذه الاتفاقية في 2001/11/23، ودخلت حيز التنفيذ في الأول من جويلية 2004، و تعتبر بمثابة دعوة موجهة لكل دول العالم للتصدي لجرائم المعلوماتية، وجاءت نتيجة محاولات عديدة منذ الثمانينات.

وتتكون هذه الاتفاقية التي وضعها المجلس الأوروبي من ثماني و أربعين مادة[1]. وما يهمنا هنا المواد من 2 إلى 10و التي تعبر عن الأفعال التي تدخل في جرائم المعلوماتية.وهي:

- -الولوج غير القانوني(المادة 2).
- -الاعتراض غير القانوني(المادة 3).
- -الاعتداء على سلامة البيانات(المادة 4).
- -الاعتداء على سلامة النظام(المادة 5).
- -إساءة استخدام أجهزة الحاسب(المادة 6).
- -التزوير المعلوماتي(المادة 7).
- -الغش المعلوماتي(المادة 8).
- -الجرائم المتصلة بالمواد الإباحية الطفولية(المادة 9).
- -الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة(المادة 10).

(1) هلالي عبد الله احمد : مرجع سابق ،ص8 ،ص9.

ثانيا: وفق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

حررت هذه الاتفاقية بالقاهرة بتاريخ 2010/12/21 ووقعت من طرف وزراء الداخلية و العدل العرب، وقد صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-252 مؤرخ في 08سبتمبر سنة 2014[1].

وتهدف هذه الاتفاقية كما جاء في المادة الأولى منها إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطاء هذه الجرائم حفاظا على امن الدول العربية ومصالحها وسلامة مجتمعاتها وإفرادها.

وتضمنت هذه الاتفاقية الجوانب الموضوعية و الإجرامية لجرائم المعلوماتية.

حيث جاء في الفصل الثاني منها تحت عنوان: التجريم، المادة الخامسة، ضرورة التزام كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقا لتشريعاتها و أنظمتها الداخلية.

وبينت الاتفاقية الأفعال المجرمة في المواد من 6 إلى 19وهي:

- جريمة الدخول غير المشروع(المادة 6).
- جريمة الاعتراض غير المشروع(المادة 7).
- الاعتداء على سلامة البيانات(المادة 8).
- جريمة إساءة استخدام وسائل تقنية المعلومات(المادة 9).
- جريمة التزوير(المادة10).
- جريمة الاحتيال(المادة 11).
- جريمة الإباحية(المادة 12).
- المقامرة و الاستغلال الجنسي(المادة 13).
- جريمة الاعتداء على حرمة الحياة الخاصة(المادة 14).

[1] الجريدة الرسمية عدد 57، صادرة بتاريخ 2014/10/28 .

- الجرائم المتعلقة بالإرهاب و المرتكبة بواسطة تقنية ا لمعلومات(المادة 15).
- الجرائم المتعلقة بالجرائم المنظمة و المرتكبة بواسطة تقنية المعلومات(المادة 16).
- الجرائم المتعلقة بانتهاك حق المؤلف و الحقوق المجاورة(المادة 17).
- الاستعمال غير المشروع لأدوات الدفع الالكترونية(المادة 18).
- الشروع و الاشتراك في ارتكاب الجرائم المنصوص عليها في هذا الفصل (المادة 19).

ثالثا: وفق التشريع الجزائري

كانت الجريمة المعلوماتية في الجزائر مع بداية سنة 2000 مجرد حدث تتناوله وسائل الإعلام، بيد ان الحظر منذ بداية استخدام الإعلام الآلي وظهور مقاهي الانترنت وانتشارها والواسع في ربوع الوطن.

وقد تفشت ظاهرة الجريمة المعلوماتية في السنوات الأخيرة ليستخدم المجرمون كل الأساليب التقنية الحديثة في الإجرام مثل تزوير العملة الصعبة وغسيل الأموال وتزوير وثائق النقر عن طريق معالجتها بالسكانير والإعلام الآلي.

كما ظهرت حالات النصب والاحتيال عبر الانترنت واختراق المواقع الجزائرية، كما ظهر الإرهاب الدولي بإنشاء مواقع إرهابية استخدمت للتواصل فيما بينها لتجنيد الشباب. [1].

هذا ما دفع الجزائر للانتباه لهذه الظاهرة الإجرامية من خلال سن قوانين تجرم هذه الأفعال. في البداية كانت نصوص متفرقة في قوانين مختلفة. مثل قانون البريد والمواصلات، قانون المؤلف والحقوق الحيازة. وصولا إلى قانون خاص لمكافحة الجرائم الماسة لأنظمة المعالجة الآلية للمعطيات، وهو قانون رقم 04-15 المعدل والمتمم لقانون العقوبات، ويعد أول قانون : صنف جملة من جرائم المعلوماتية وعقوباتها، ثم تبعته قوانين أخرى وهذا ما سنتناوله فيما يلي:

[1] جريدة الخبر : اليومية جزائرية العدد 6302، الثلاثاء 12 مارس 2011.

1 - قانون رقم 2000-03. المؤرخ في 15 أوت 2000، الخاص بالقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية. [1].

- فتح أو تحويل تخريب البريد وانتهاك بأي طريقة لسرعة المراسلات الصادرة أو المرسلة و المستقبلة عن طريق المواصلات السلكية المساعدة في ارتكاب هذه الأفعال (م 127)
- انشاء او نشر او استعمال دون ترخيص من المرسل او المرسل اليه، مضمون المراسلات المرسلة عن طريق اللاسلكي الكهربائي او الاخبار برجودها (م137)
- تخريب او اتلاف بأي شكل كا الاجهزة او المنشآت او وحدات المواصلات السلكية واللاسلكية (م 138)

2- قانون رقم 03-05 مؤرخ في 19 جويلية سنة 2003 الخاص بحقوق المؤلف والحقوق الحيازة[2]**:**

هذا القانون نص المشرع الجزائري صراحة على اعتبار برامج الحاسوب من المصنفات المحمية، بموجب الحالة 4/أ.

واعتبر أي اعتداء على الحق المالي او الأدبي للمؤلف يشكل فعلا من أفعال التقليد، هي بحق المادة 151:

أ- الكشف غير المشروع للمصنف او المساس بسلامته

ب- استنساخ مصنف بأي أسلوب من الأساليب في شكل نسخ مقلدة

ج- استيراد او تصدير نسخ مقلدة من مصنف او أداء

د- بيع نسخ مقلدة لمصنف او أداء

ه- تأجير او وضع تحت رهن التداول لنسخ مقلدة لمصنف او أداء

[1] الجريدة الرسمية عدد 48، صادرة بتاريخ 08 أوت 2000 .

[2] الجريدة الرسمية عدد 44، صادرة بتاريخ23 جويلية 2003.

3- قانون رقم 04-15، مؤرخ في 2014/11/10:المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08-06-1966 "قانون العقوبات"

تضمن القسم السابع مقرر من الفصل الثالث: من الباب الثاني من الكتاب الثالث ، تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات "8 مواد من 394 مكرر الى 394 مكرر 7. حدد المشرع الجزائري في هذا القانون أصناف من الجرائم الماسة بالمعالجة الآلية للمعطيات وهي:

أ- حرية الدخول او البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات او محاولة ذلك (المادة 394 مكرر / فقرة 10)

ب- الدخول او البقاء المؤدي الى حدث او تغير لمعطيات المنظومة (المادة 394 مكرر/ فقرة 2)

ج- الدخول او البقاء المؤدي الى تخريب نظام استعمال المنظومة (المادة 394 مكرر/ فقرة 30)

د- جريمة إدخال معطيات في نظام المعالجة الآلية او إزالة المعطيات التي يتضمنها عن طريق الغش (المادة 394 مكرر 1)

ه- جريمة تصميم او بحث او تجميع او توفير او نشر او الاتجار في معطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية أخرى يمكن ان ترتكب بها جرائم منصوص عليها في هذا القسم عن طريق الغش (المادة 394 مكرر 2/ فقرة 2)

و- جريمة حيازة او انشاء او نشر او استعمال لأي غرض كالمعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر2/ فقرة 3)

ز- المشاركة في مجموعة او اتفاق بغرض الاعداد لجريمة او اكثر من الجرائم المنصوص عليها في هذا القسم. وكان هذا التغيير محسدا بفعل او عدة افعال مادية يعاقب عليها بالعقوبات المقررة للجريمة ذاتها (المادة 394 مكرر5)

ح- الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم، ويعاقب عليه بالعقوبات المفرزة للجنحة (المادة 394 مكرر 7), وتجدر الإشارة إلى انه يتضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجرائم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام (م 394 مكرر 3).

ونفس الشيء إذا كان الجاني شخصا معنويا، تضاعف غرامته إلى 5 مرات. الحد الأقصى الغرامة المقررة للشخص الطبيعي (المادة 394 مكرر 4).

العقوبة الأصلية المقررة لهذه الجرائم هي الحبس والغرامة معا، إلى جانب عقوبات تكميلية تتمثل في مصادرة أجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا جريمة من الجرائم م المعاقب عليها وفقا لهذا القسم علاوة على إعلان المحل او مكان الاستغلال اذا كانت الجريمة نفس ارتكبت يعلم مالكها. المادة 394 مكرر 6. [1].

وفي عام 2006، ادخل تعديل آخر على قانون العقوبات الجزائري بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، مس مواد القسم السابع المكرر (394 مكرر، 394 مكرر1، 394 مكرر 2)

حيث تم تشديد عقوبة الحبس والغرامة المقررة للأفعال المذكورة في هذه المواد.

يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى، وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم، حيث بلغ عدد مستخدمين

[1] أنظر مواد: 394 مكرر1، 394 مكرر2 من قانون 04- 15 الخاص بجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الانترنت في المجتمع الجزائري سنة 2000 حوالي 150 ألف مستخدم ليصل سنه 2007 الى 246000 مستخدم. [1].

وحسب آخر دراسة حول الانترنت وسندات التواصل الاجتماعي بالجزائر قامت بها الشركة المختصة (ايمار للبحوث والاستشارات)

في الفترة من 02 فيفري و 01 ماي 2017 جاء فيها ان 13مليون جزائري من البالغ سنهم 15 عاما وما فوق يتصفحون الانترنت يوميا وهذا يمثل نسبة 46% من هذه الشريحة من المجتمع

وتعتبر الشركة أن الانترنت هي وسيلة إعلام الشباب باعتبار ان السن عامل محدد للسلوك إزاء هذه الوسيلة الإعلامية بحيث ان 77% من الفئة 15-24 سنة، و 55% من فئة 25-34 سنة و 32% من فئة 35-44 سنة و21 % من فئة 45-54 سنة إضافة إلى 17% من فئة 55 سنة فما فوق يتصفحون يوميا الانترنت. [2]

4- قانون رقم 08-01 مؤرخ في 2008/01/23 المتمم للقانون رقم 83-11 مؤرخ في 02 جويلية 1983 والمتعلق بالتأمينات الاجتماعية [3]

الذي تم بموجبه تثبيت صفة المؤمن له اجتماعيا ببطاقة الكترونية (6 مكرر)

وتزويد كل من هيكل العلاج ومهنيي الصحة بمفتاح الكتروني وحزمة الأعمال التالية:

[1] عائشة بن قارة : مرجع سابق، ص 30

[2] موقع جريدة العاصمة نيوز مقال منشور في 16 أفريل 2007، أطلع عليه يوم 21/ 04/ 2017
www. elassima .news. com

[3] الجريدة الرسمية عدد 04، صادرة بتاريخ17 جانفي 2008 .

أ- استلام أو تسليم بهدف الاستعمال غير المشروع للبطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو لمهني الصحة. (م 930 مكرر 2)

ب- القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا او المفتاح الالكتروني لهيكل العلاج او لمهني الصحة.

ج- إعداد أو تعديل او نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول او باستعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا او في المفتاح الالكتروني لهيكل العلاج او لمهني الصحة (م 93 مكرر 3),

د- نسخ أو تضييع او حيازة او توزيع بطريقة غير مشروعة البطاقة الالكترونية للمؤمن له اجتماعيا او المفتاح الالكتروني لهيكل العلاج او لمهني الصحة. (مادة 93 مكرر 4).

5- قانون رقم 14 – 08 مؤرخ في 4 فيفري سنة 2014 معدل ومتمم للأمر 66-156 المؤرخ في 08 جوان 1966. [1]

والمتضمن قانون العقوبات في القسم السابع بعنوان انتهاك الآداب العامة جاء في المادة 33 مكرر 1، تجريم مايلي:

أ- تصوير قاصر لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية حقيقة أو غير حقيقية.

ب- تصوير الأعضاء الجنسية للقاصر لأغراض جنسية أساسا

ت- القيام بإنتاج او توزيع او نشر او ترويج او استيراد او تصدير او عرض او بيع او حيازة مواد إباحية متعلقة بالقصر.

6- قانون رقم 15-03 مؤرخ في أول فيفري 2015 المتعلق بعصرنة العدالة [2]**:**

[1] قانون العقوبات : أحسن بوسقيعة ، برتي للنشر، 2015..

[2] الجريدة الرسمية عدد 06، صادرة بتاريخ19 فيفري 2015 .

يهدف هذا القانون كما جاء في المادة الأولى منه إلى عصرنة سير قطاع العدالة من خلال:

- وضع منظومة معلوماتية مركزية لوزارة العدل للمعالجة الآلية للمعطيات تتعلق بنشاط وزارة العدل والمؤسسات التابعة لها وكذا الجهات القضائية للنظام القضائي العادي والنظام القضائي الإداري ومحكمة التنازع (م2)

- كما يمكن ان الوثائق والمحررات القضائية التي تسلمها مصالح وزارة العدل والمؤسسات التابعة لها والجهات القضائية بتوقيع الكتروني تكون صلته بالمحرر الأصلي مضمونه بواسطة وسيلة تحقق موثوقة (م4)
- ويتم إثبات العلاقة بين معطيات التحقق من التوقيع الالكتروني وصاحب التوقيع عن طريق شهادة الكترونية موصوفة تصدرها وزارة العدل (م6)
- بحيث تضمن وزارة العدل التصديق على التوقيع الالكتروني بواسطة ترتيب الكتروني مؤمن يضمن التعرف على هوية الشخص المرسل اليه وتاريخ صلاحية التوقيع والمعلومات التي يتضمنها (م7).

وبموجب هذا القانون يتم تجريم:

أ- الاستعمال بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع الكتروني يتعلق بتوقيع شخص آخر (م 17)

ب- مواصلة الاستعمال لشهادة الكترونية رغم العلم بانتهاء مدة صلاحياتها أو إلغائها (م 18)

7- قانون رقم 15-04 مؤرخ في 1 فيفري 2015 المتعلق بالتوقيع والتصديق الالكتروني: [1]

[1] الجريدة الرسمية العدد 06، صادرة بتاريخ10 فيفري 2015.

يهدف هذا القانون كما جاء في مادته الأولى الى تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني.

ويعرف التوقيع الالكتروني في المادة الثالثة بأنه بيانات في شكل الكتروني مرفقة او مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق.

أما شهادة التصديق الالكتروني فهي وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع.

وعلى هذا الأساس تم تجريم الأفعال التالية:

أ- الإدلاء بإقرارات للحصول على شهادة تصديق الكتروني موصوفة (م 66)

ب- حيازة ان إنشاء او استعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير.

ت- قيام الشخص المكلف بالتدقيق يكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق.

ث- استعمال شهادة للتصديق الالكتروني الموصوفة لغير الأغراض التي منحت من اجلها.

في نهاية هذا المبحث نكون قد سلطنا الضوء على مفهوم الجريمة المعلوماتية باعتبارها مجالا للدليل الرقمي بتعريفاتها المختلفة، الضيقة منها والموسعة وعرضنا أهم خصائصها التي تميزها عن باقي الجرائم التقليدية

لنصل في الأخير أي أهم أنواعها بذكر تصنيفاتها المختلفة، الفقهية ، والتشريعية مركزين على التشريع الجزائري مجال بدراستنا لنلخص بالقول إن الجريمة المعلوماتية ، تقاوم التعريف ، تكسر الحدود الجغرافية للدول وتتمرد على النصوص القانونية التقليدية لتفرض إحكاما موضوعية وإجرائية مستحدثة، حداثة

الجريمة خاصة في مجال استخلاص الدليل الرقمي، لإثباتها ولنسبتها إلى الفاعل الذي هو الأخر مميز عن المجرم التقليدي.

وقبل النظر لهذه الإجراءات الخاصة، رأينا من الضروري التعرف على مفهوم الدليل الرقمي. وحجته في إثبات هذا النوع من الجرائم وهذا ما سنراه في المبحث الثاني

المبحث الثاني

مفهوم الدليل الرقمي و حجيته في اثبات جرائم المعلوماتية

عرفنا أن الجريمة المعلوماتية ذات طبيعة خاصة ولها مسرح جريمة يختلف عن مسرح الجريمة التقليدية وإنها تتم في بيئة رقمية على الحاسوب و الانترنت مما يصعب إثباتها بالوسائل التقليدية بل يقتضي دليلا من نفس طبيعتها الخاصة أطلق عليه **الدليل رقمي** و يعود هذا المصطلح إلى استخدام النظام الرقمي الثنائي المتمثل في (0,1) ، وهي الصيغة التي تسجل بها كل البيانات داخل الحاسوب هذه البيانات التي يقع الاعتداء عليها ، سواء كانت في شكل حروف ، أرقام، رموز ، أصوات ، صور ، تحول إلى نظام ثنائي (0،1) يفهمه الحاسوب هذه الطبيعة الخاصة للدليل الرقمي تطرح إشكاليات قانونية في جمعه و استخلاصه لإثبات جرائم المعلوماتية.

ونتناول في هذا المبحث مفهوم الدليل الرقمي و تعريفاته المختلفة، خصائصه التي نميزه عن باقي الأدلة الجنائية ، أنواعه المختلفة في المطلب الأول

وحجيته في إثبات جرائم المعلوماتية في المطلب الثاني.

المطلب الأول

مفهوم الدليل الرقمي

ارتبط ظهور الدليل الجنائي الرقمي بظهور الجريمة المعلوماتية، وهو بذلك يلعب دورا كبيرا في إثباتها و نسبتها إلى الفاعل . لقصور الأدلة الجنائية التي تعارف عليها الفقه و القضاء في إثبات هذا النوع من الجرائم وملاحقة مرتكبيها .

سنتعرف في هذا المطلب على مفهوم الدليل الرقمي من خلال التطرق إلى تعريفاته المختلفة . وخصائصه التي تميزه عن الباقي الأدلة الجنائية . وكذا تصنيفاته أو أنواعه. لتصل إلى تحديد موقعه من بين تصفيات الأدلة الجنائية المعروفة. أو انفراده بصنف مميز.

الفرع الأول : تعريفات الدليل الرقمي

قلنا أن الدليل الرقمي يستمد خصوصيته من خصوصية الجرائم المعلوماتية باعتبارها محلا له لذلك فقد تباينت تعريفاته هو أيضا . وستناول فيما يلي أهم ما ورد من تعريفات بشأنه وقبل ذلك سنتطرق إلى تعريف الدليل الجنائي بصفة عامة.

أولا التعريف الدليل الجنائي :

سنعرف الدليل لغة و اصطلاحا ثم نعرف الدليل الجنائي

1_ التعريف اللغوي للدليل :

يعريف الدليل لغة بأنه مرشد وما يتم به الإرشاد والدليل هو الدال أيضا والجمع الأدلة و دلالات . [1]

2_ **التعريف الاصطلاحي للدليل** : عرفه بعض الفقهاء بأنه وسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها ، والمقصود بالحقيقة في هذا السياق ، كل ما يتعلق بالوقائع المعروضة على القاضي لإعمال حكم القانون عليها [2]

3 تعريف الدليل الجنائي :

بناء على ما نقدم يمكن تعريف الدليل الجنائي ذاته : معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية لإثبات صحة افتراض ارتكاب الشخص للجريمة وذلك لرفع ارخص درجة اليقين والاقتناع لدى القاضي في واقعة محل الخلاف

للإشارة فان أغلب التشريعات ، ومنها التشريع الجزائري، لم تضع تعريفا للدليل الجنائي وتركت المسألة للفقهاء ،بأنها باستثناء عدد قليل من التشريعات على غرار التشريع السوفيتي الذي عرف الأدلة فإنها : المعلومات التي على ضوئها يحدد المحقق أو المحكمة طبقا للطرف المتضرر قانونا توافر تخلف فعل خطر اجتماعيا ، وتاثيم الشخص الذي ارتكب الفعل .

ثانيا تصنيفات الدليل الجنائي:

سنتناول فيما يلي : تصنيفات الدليل من حيث المصدر لما لها علاقة بموضوع دراستنا ، ولنعرف من خلالها موقع الدليل الرقمي .

---

[1] جميل صليبا : المعجم الفلسفي ، دار الكاتب اللبناني بيروت الطبعة1 ،1970، ص 23

[2] أحمد فتحي سرور : الوسيط في قانون إجراءات الجنائية دار النهضة العربية القاهرة، الطبعة 2، 1981.ص418

1- **الدليل المادي** : هو الدليل الذي يكون مصدره مصدر العناصر المادية، ويدل مباشرة على الواقعة المراد إثباتها أي يمكن رؤيته ولمسه لوجود الشيء المسروق في حيازة الجاني أو اثأر أقدام أو بصمات يعثر عليها في في محل الحادث وقد حظي هذا النوع من الأدلة بالدراسة من قبل العديد من الفقهاء والباحثين خاصة انه يرتبط بشكل مباشر بالوسائل العلمية في المجال كشف الجريمة

2- **الدليل القانوني** : هو حدده المشرع بحيث لا يمكن الإثبات بغيره ، وهو الأصل في المواد في المواد المدينة أما في المواد الجنائية فان الأدلة غير إذ يجوز إثبات الجرائم بأي طريق من طرف الإثبات ماعدد أحوال التي تنص فيها القانون على غير ذلك ، القاضي ان يصدر حكمه تبعا لإقناعه الخاص أي يبني قراره الأعلى الأدلة المقدمة له المرافعات والتي حصلت المناقشة أمامه " المادة 212 من قانون الإجراءات الجزائية الجزائري"

ويقصد بالأحوال التي ينص عليها القانون الاستثناءات الواردة على مبدأ حرية الإثبات حددها المشرع مثل: إثبات جريمة حمل السلاح دون ترخيص، يكون بحيازة السلاح. و إثبات السياقة في حالة سكر يكون فقط بالفحوص الطبية ولو كان الجاني معترفا بذلك .

وكذلك الحال في إثبات المسائل غير الجنائية كالمسائل الفرعية التي تطرح بصفة عرضية أثناء سير الدعوى سواء كانت مدينة أو تجارية أو إدارية أو شخصية. هنا تطبق وسائل الإثبات الخاصة بكل قانون.

3- **الدليل العلمي او الفني :**

هو الدليل الذي يكون مصدره رأي علمي حول تقدير مادي ، كالخبرة التي تتمثل في تقارير فنية مختصة تصدر عن الخبر رأيه العلمي في وقائع معينة. ومن أمثلة الأدلة التي يلجأ إليها القاضي للخبراء، اختبارات الحمض النووي بصمات الأصابع.

4- **الدليل القولي** :

وهو الدليل الذي يكون مصدره أشخاصا أدركوا معلومات مفيدة للإثبات بإحدى حواسهم وتتمثل في الإعتراف، وأقوال الشهود.

من خلال ما تقدم من تصنيفات للدليل الجنائي يطرح التساؤل التالي : في أي صنف يقع الدليل الرقمي، أم أنه صنف مميز يضاف إلى الأصناف المذكورة الأخرى ؟ و سنعرف الإجابة من خلال تعريفه و عرض خصائصه و تقسيماته وهذا ما سنتناوله فيما يلي :

ثالثا: تعريف الدليل الرقمي

المشرع الجزائري لم يعرف الدليل الرقمي ، ولم يرد هذا المصطلح تعريفه سواء في القانون 04- 15 المتعلق بالجرائم المالية بأنظمة المعالجة الآلية المعطيات، أو قانون 09 - 04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها أين أورد تعريف بعض المصطلحات المتعلقة بجرائم المعلوماتية. أو المرسوم الرئاسي رقم 15/ 261 المتعلق بتنظيم الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام و الاتصال، وإنما اعترف المشرع بالكتابة الالكترونية كوسيلة إثبات في المادة المدنية في إعادة 323 مكرر 1 « يعتبر الإثبات بالكتابة في الشكل

الالكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها و أن تكون معدة و محفوظة في ظروف تضمن سلامتها . »[1]

وعرف قبل ذلك في المادة 323 مكرر من نفس القانون المقصود بالكتابة « ينتج الإثبات بالكتابة من تسلل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مهما كانت الوسيلة التي تتضمنها ، وكذا طرق إرسالها . »[2] وهذا يتوافق مع تعريف البيانات الذي سبق الإشارة إليه في هذا البحث.

و الدليل الرقمي شأنه شأن الجريمة المعلوماتية التي يستمد منها أغلب خصائصه بما فيها التعريف الذي يتباين هو الآخر وفيما يلي سنورد بعض التعريفات :

1- لقد عرف الأستاذ كيسي الأدلة الجنائية الرقمية بأنها « تشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت أو توجد علاقة بين الجريمة و الجاني أو بين الجريمة و المتضرر منها، و البيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات، بما فيها النصوص المكتوبة ، الرسومات ، الخرائط، الصوت و الصورة . »[3]

2- أما المنظمة العالمية لدليل الحاسوب IOCE فقد عرفته في مارس سنة 2000 بأنه : المعلومات المخزنة أو المنقولة و التي يمكن الاعتماد عليها أمام المحكمة محددة الجهة التي يقدم اليها الدليل و هي المحكمة ، و تجاهلت الصيغة التي يتم بها

(1) الجريدة الرسمية ، عدد 44 بتاريخ 26 جوان 2005 .
(2) قانون رقم 05- 01 المؤرخ في 20 جوان 2005، المعدل المنتظم للامر رقم 75-58 التضمن القانون المدني
(3) مشار إليه عند : عائشة بن قارة مصطفى مرجع سابق 54..

تخزين المعلومات ، و تداركته في تعريف آخر في سنة 2001: «المعلومات ذات القيمة المحتملة المخزنة أو المنقولة في صورة رقمية. »[1]

3- و عرفته الدكتورة عائشة بن قارة مصطفى بأنه « معلومات مخزنة في أجهزة الحاسوب و ملحقاتها - من دسكات و أقراص مرنة و غيرها من وسائل تقنية المعلومات كالطابعات و الفاكس - أو متنقلة عبر شبكات الإتصال و التي يتم تجميعها و تحليلها و استخدام برامج و تطبيقات و تكنولوجيا خاصة بهدف إثبات وقوع الجريمة نسبتا إلى مرتكبيها »[2]

وسنرى فيما يلي أهم الخصائص التي تميز الدليل الرقمي

الفرع الثاني : خصائص الدليل الرقمي

مما لاشك فيه أن الدليل الرقمي يستمد خصائصه من البيئة التي يولد فيها ، وهي البيئة الرقمية التي تكون فيها البيانات على شكل نبضات مغناطيسية أو كهربائية يتطلب استخلاصه و تحليله باستخدام برامج و تطبيقات و تكنولوجيات خاصة ، وتفرض على المكلفين بذلك معرفة بهذه التكنولوجيات لضمان تقديمه إلى القضاء كوسيلة إثبات في جرائم المعلوماتية و سنحاول في هذا الفرع التعرف على أهم خصائص الدليل الرقمي .

أولا: علمي

يستمد الدليل الرقمي هذه الخاصية لكونه لا يمكن استخلاصه إلا باستخدام طرق علمية، ويتم حفظه على أسس علمية ، لذلك فإن ما ينطبق على الدليل العلمي ينطبق

[1] د محمد مرسي : التحقيق الجنائي في الجرائم الالكترونية ، مابع الشرطة القاهرة 2009 ص 213
[2] مشار إليه عند : عائشة بن قارة مصطفى مرجع سابق 61..

على الدليل الرقمي فهو يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة، وفقا لقاعدة في القانون المعارض التي مفادها أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة. و يستبعد تعارض الدليل العلمي مع القواعد العلمية السليمة، و لأن الدليل العلمي من نفس الطبيعة فلا يجب أن يخرج عما وصل إليه العلم الرقمي . [1]

ثانيا: تقني

يستمد الدليل الرقمي هذه الخاصية من البيئة التي يتكون فيها ، وهي البيئة الرقمية أو التقنية التي تكون فيها البيانات على شكل نبضات الكترونية يتطلب إدراكها و الإطلاع عليها استخدام أجهزة و الاستعانة ببرامج خاصة بحيث يفرض التعامل معه معرفة تتوافق مع طبيعة التقنية المتطورة باستمرار.

ثالثا: صعب التخلص منه .

يتميز الدليل الرقمي عن باقي الأدلة التقليدية لكونه يصعب التخلص منه. فإذا كانت الأدلة التقليدية يمكن التخلص منها بسهولة : كحرق الأوراق، مسح البصمة ، أو حتى قتل الشهود حتى لا يدلوا بشهادتهم فإن الأمر يختلف بالنسبة للدليل الرقمي فإنه من غير الممكن فعل ذلك ، وإن حاول الجاني إخفاء جريمته أو محو الدليل ، حيث يمكن استرجاع الدليل بعد محوه و إصلاحه بعد إتلافه و إظهاره بعد إخفائه، لأن هناك بفضل التطور العلمي و التكنولوجي، برامج حاسوبية وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها [2]

و أيضا يمكنها تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله وذلك لإمكانية مقارنته مع الأصل (باستعمال الخوارزميات) ، كما نشاط الجاني لمحوالدليل يسجل

---

[1] عمر محمد أبو بكر بن يونس الإجراءات الجبائية عبر الانترنت، بدون در النشر ، 2006، مشار إليه عند : عائشة بن قارة مصطفى مرجع سابق 62..

[2] عائشة بن قارة مصطفى، مرجع سابق، 62..

كدليل، أيضا حيث أن نسخة من هذا الفعل يتم تسجيلها في الحاسوب ويمكن استخلاصها لاحقا لاستخدامها كدليل إدانة ضده. [1]

رابعا : قابلية النسخ

يتميز الدليل الرقمي عن الأدلة التقليدية بقابليته للنسخ ، بحيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية. [2] بالإضافة إلى أن طريقة نسخ الدليل الرقمي من أجهزة الحاسوب تقلل أو تعدم تقريبا مخاطر إتلاف الدليل الأصلي ، حيث تتطابق طريقة نسخه مع طريقة الإنشاء. [3]

خامسا : خصائص أخرى.

- ـ الاتساع العالمي لمسرح الجريمة ، يمكن مستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية، و بمناطق مختلفة من العالم، مما يسهم في الاستدلال على الجناة أو أفعالهم بسرعة أقل نسبيا.
- امتيازه بالسعة التخزينية العالية ، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور ، دسك صغير يمكنه تخزين مكتبة صغيرة .
- يمكن من خلال دليل رقمي دراسة المعلومات عن الجاني وتحلليها في ذات الوقت ، فالدليل الرقمي يمكنه أن يسجل تحركات الفرد ، كما أنه يسجل عاداته و سلوكياته و بعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي[4]

---

(1) محمد مرسي، مرجع سابق، 62..
(2) عائشة بن قارة مصطفى مرجع سابق 64..
(3) محمد مرسي، مرجع سابق، 62..
(4) محمد مرسي مرجع سابق ص 218.

- إلي جانب تميزه بالتنوع و التطور بتنوع الجرائم و تطور تكنولوجيات الإعلام و الإتصال.

بعد أن عرضنا أهم الخصائص التي تمييز الدليل الرقمي في هذا الفرع سنتناول في الفرع الآتي: أنوع الدليل الرقمي

الفرع الثالث: تقسيمات الدليل الرقمي

عرفنا الدليل الرقمي بأنه معلومات مخزنة أو منقولة بصيغة رقمية، يعتمد عليها في التحقيقات، وأمام المحكمة للإدانة أو البراءة. وعرفنا أهم الخصائص التي تميز الدليل الرقمي فهو علمي، تقني قابل للنسخ، ويصعب التخلص منه.

كما سبق و تطرقنا إلى تصنيفات الدليل الجنائي من حيث المصدر: مادي قانوني، فني، قولي، وطرحنا تساؤل حول موقع الدليل الرقمي من هذه التصنيفات.

وللإجابة على هذا التساؤل نشير إلى الجدل الفقهي الذي ثار حول هذا الموضوع، بحيث ظهر اتجاهان اثنان:

الاتجاه الأول: يرى أنصاره أن الأدلة الجنائية الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان،إذا ما كانت مطبوعات مستخرجة من الحاسوب. فالأدلة الرقمية في منظور هذا الاتجاه لا تختلف من حيث المفهوم و القيمة عن آثار الأسلحة وبصمات الأصابع و البصمة الوراثية ADN. وغيرها من الأدلة العلمية [1].

الاتجاه الثاني: يرى أنصاره بأن الأدلة الرقمية نوع متميز من أنواع الإثبات ولها من المواصفات ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية الأربعة (القانونية، الفنية،

(1) أحمد ابو القاسم: الدليل المادي ودوره في الإثبات في الفقه الجنائي الإسلامي، دار النهضة العربية،1991، ص17 ..
(2). مشار اليه عند عائشة بن قارة مصطفى،ص68.

القولية والمادية). وهذا هو الرأي المرجح[1]. لأن الأدلة الرقمية كما رأينا تتمتع بخصائص جعلتها متميزة عن غيرها من الأدلة الجنائية التي سبق ذكرها.

وهذه الخصائص مستمدة من جرائم المعلوماتية التي هي محل هذه الأدلة الرقمية. وتتميزها بمسرح الجريمة، والبيئة الخاصة التي ترتكب فيها هذه الجريمة، وأيضا بالإجراءات الخاصة لجمع و تحليل وتقديم الأدلة الرقمية، وحتى تميز القائمين على ذلك بكفاءات علمية وتقنية تتماشى مع تطور تكنولوجيات الإعلام و الإتصال، و الدليل الرقمي بدوره يتميز بالتنوع فلا يأتي على صورة واحدة، وظهرت تقسيمات كثيرة،وفيما يلي نستعرض أهم تقسيمات الدليل الرقمي:

أولا: التقسيمات الفقهية

نظرا لتنوع الدليل الرقمي، وتعدد صوره، وأيضا تطوره المرتبط بالبيئة التي يعيش فيها، فقد اختلف الفقهاء في وضع تقسيم واضح وموحد لهذا النوع من الأدلة، فبعضهم قسمه بحسب مكوناته، والبعض قسمه بحسب مكان تواجده، والبعض الآخر حسب التقسيم الفقهي لجرائم المعلوماتية وهذا الأخير الذي سنتناوله فيما يلي:

أ- الأدلة الرقمية الخاصة بجهاز الحاسوب وشبكاته.

ب- الأدلة الرقمية الخاصة بالأنترنت.

(3) عائشة بن قارة مصطفى، مرجع سابق،ص69 .

ج- الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات من أجهزة الشبكة العالمية للمعلومات.

د- الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات [1]

الملاحظ أن هذه التقسيمات لا تتناسب مع مفهوم التقنية الحديثة لأنها تناولت الدليل الرقمي الخاص بجهاز الحاسوب وشبكاته فقط ولم تتناول كل ما يتعلق بالدليل الرقمي،

كما أنها ميزت بين شبكات الحاسوب و الأنترنت وبروتوكول تبادل المعلومات و الشبكة العالمية التي هي في الأصل واحد[2]

ثانيا: التقسيمات التشريعية:

على المستوى التشريعي لا توجد تقسيمات موحدة بين كل الدول، نظرا لاختلاف جرائم المعلوماتية وبالتالي اختلاف الأدلة الرقمية تبعا لذلك. إلا أننا سنورد تقسيمات المشرع الأمريكي باعتباره السباق في الإهتمام بالأدلة الرقمية بدليل إنشاء المنظمة الدولية لأدلة الحاسوب ICOE التي سبق الإشارة إليها.

حيث قامت وزارة العدل الأمريكية للدليل الرقمي سنة 2002 بتقسيمه إلى ثلاث مجموعات [3]

- السجلات المحفوظة في الحاسوب.
- السجلات التي تم إنشاؤها في الحاسوب.
- السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب.

---

[3] عائشة بن قارة مصطفى، مرجع سابق،ص 73 .

[4]ممدوح عبد الحميد عبد المطلب: البحث العلمي و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الأنترنت، دار الكتب القانونية، مصر،2006،ص88 .

[3] عبد الناصر محمد فرغلي ومحمد عبيد سيف المسماري: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية. بحث مقدم إلى المؤتمر العربي الأول لعلم الأدلة الجنائية و الطب الشرعي، الرياض12-14 نوفمبر 2007،ص[14] .

1- السجلات المحفوظة في الحاسوب او المخزنة:

وهي الوثائق المكتوبة المحفوظة مثل البريد الالكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الأنترنت [1]. و البريد الإلكتروني يتم بواسطة تبادل الرسائل و الملفات و الرسوم و الصور و البرامج وغيرها. عن طريق إرسالها من المرسل إلى شخص أو أكثر، وهذا باستعمال البريد الإلكتروني [2] للمرسل إليه، فهو عبارة عن صندوق تتواجد فيه كل الرسائل المرسلة إلى صاحب البريد الذي سبق له إرسالها، والملغاة وغيرها من الأمور التي يحتوي عليها البريد الإلكتروني.

2- السجلات المنشاة بواسطة الحاسوب أو المتوالدة:

وتسمى بالبصمة الإلكترونية، تضبطها التقنية أليا دون تدخل الفرد،يترك الجاني أثره دون أن يرغب في وجوده، إذ يقوم الحاسوب بتكوين مخرجات حركة البرامج. والذي يسيطر عليها تحديدا، ليس مستخدم الحاسوب أو الجاني. وإنما الحاسوب ذاته حين استقباله للبرمجيات التي تعمل على تشغيله [3]، مثل سجلات الهاتف، فواتير أجهزة السحب الآلي.

3- السجلات التي حفظ جزء منها بالإدخال، وجزء منها تم إنشاؤه بواسطة الحاسوب:

وهي نوع ثالث من السجلات يجمع بين تدخل الإنسان ومعالجة الحاسوب، كما لو أدخل متهم بيانات معينة وطلب من الحاسوب أن يقوم بمعالجتها توصلا إلى نتائج يسمح بها البرنامج المستخدم. كمن يتهرب من الضرائب فيقوم بتسجيل بيانات غير صحيحة عن دخله

---

[1] عائشة بن قارة مصطفى،مرجع سابق،ص74 .

[2] خالد ممدوح إبراهيم : حجية البريد الالكتروني في الإثبات ، دار الفكر الجامعي ، الطبعة الأولى ، مصر ، 2007، ص101- 102 .

[3] بحرية هارون : دور الدليل الرقمي في إثبات الجريمة المعلوماتية في التشريع الجزائري ، مدخلة في الملتقى الوطني حول الجريمة المعلوماتية، جامعة بسكرة .

وربحه طالبا من الحاسوب حساب الضريبة المستحقة [1]. ومن أمثلتها أوراق العمل المالية التي تحتوي على مدخلات ويتم معالجتها بإجراء عمليات حسابية.

الملاحظ على هذه التقسيمات أنها ليست شاملة للدليل الرقمي، بل اقتصرت على نوع محدد منه. وهي سجلات الحاسوب التي تحتوي على نص، بالرغم من أن الدليل الرقمي يشمل كافة البيانات الرقمية الممكن تداولها رقميا كالصور و الأصوات والرسوم وغيرها. كما أنها لم تراعي التطور المستمر للبيئة الرقمية التي يعيش فيها الدليل الرقمي، حيث يستخدم حاليا بروتوكولات الاتصالات TCP/IP في تحقيق جرائم المعلومات. وهي تعتبر احد الأدلة الرقمية الهامة جدا، لا تقبل الشك لدى الخبير، لأنها تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحدد الأجهزة التي أصابها الضرر من الفعل الإجرامي و تحديد نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة[2]. ويسمى IP.

بينما يخص بروتوكولات الاتصالات أو بروتوكولات تراسل الانترنت TCP/IP هما في الأصل بروتوكولان مسجلان في شبكة الانترنت، ويعملان معا بشكل متزامن:

- **بروتوكول الأنترنت Internet Protocol IP:** هو عنوان فريد لكل حاسوب يدخل شبكة الأنترنت ولا يمكن آن يدخل الشبكة جهازان بنفس العنوان في كل الكرة الأرضية، وهو يعادل البصمة الوراثية إذا ارتبط بالعنوان الفيزيائي Media Access Control وهو رقم فردي مخزن في كل بطاقة شبكة.

(1) شيماء عبد الغني محمد عطاء الله:الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة.2007،ص409 .
(2) عائشة بن قارة مصطفى،مرجع سابق،ص76 .

وهو عبارة عن رقم تسلسلي، مسؤول عن عنونة وترقيم و توجيه الرسائل الى عناوينها، بالإضافة إلى منح كل جهاز أو موقع على الشبكة رقما معينا، يطلق عليه اسم بريد الكتروني إذا تعلق بالبريد الالكتروني. ويطلق عليه اسم النطاق إذا تعلق بعنونة الواب(World Wide Web (WWW التي تساعد على تصفح المعلومات و استعراضها على شبكة الانترنت.

- **بروتوكول التحكم في النقلTCP:** يقوم بتجزئة الرسالة المراد إرسالها إلى رزم من المعلومات تحمل معلومات تعريفية حول المرسل و المرسل إليه، ثم يتم تجميعها عند العنوان المقصود[1].

بالنسبة للمشرع الجزائري فقد أورد في نص المادة 06 من القانون رقم 04/09 شكل الدليل الرقمي بحيث يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين الكترونية قابلة للحجز ،أي حافظ المشرع على البيئة التي يتواجد فيها الدليل الرقمي، ثم وسع من أشكال الدليل حين قرر إمكانية استعمال الوسائل التقنية لتشكيل وإعادة تشكيل المعطيات قصد جعلها قابلة للإستغلال لأغراض التحقيق، وفي هذه الحالة أعطى المشرع سلطة التحقيق حرية تشكيل الدليل شريطة عدم المساس بمحتوى المعطيات، تبقى مسالة قبول هذا الدليل ومدى حجيته في إثبات الجريمة تخضع للسلطة التقديرية للجهة القضائية [2].

وهذا ما سنتناوله في المطلب الثاني.

المطلب الثاني

حجية الدليل الرقمي في إثبات جرائم المعلوماتية في التشريع الجزائري

مما لا شك إن مسالة الإثبات الجنائي بالدليل الرقمي في جرائم المعلوماتية تختلف في الإثبات فيها عن الجرائم التقليدية، وهذا راجع للطبيعة الخاصة لهذه الجرائم وللدليل الرقمي

[1] عائشة بن قارة مصطفى،مرجع سابق،ص76 .
[2] بحرية هارون: مرجع سابق، ص7 .

المرتبط بها. سواء بالنسبة للقائمين على كشفه و جمعه استخلاصه من حيث ضرورة توافر دراية تقنية المعلومات و الإتصال، أو بالنسبة للقاضي الجنائي فيما يخص قبوله وتقديره. و مرد ذلك لكونهم تعودوا على التعامل مع دليل مرئي وملموس، وربما ثابت. عكس الدليل الرقمي الذي سبق وتعرفنا على خصائصه، فهو مرئي وغير ملموس وعبارة عن نبضات الكترونية، ويأخذ أشكالا مختلفة، ويتطور بتطور البيئة التي يعيش فيها.

وهذا ما أثار جدلا فقهيا حول حجية الدليل الرقمي في الإثبات الجنائي من حيث سلطة القاضي الجنائي في قبول هذا النوع المستحدث من الأدلة و في تقديره، و كذا الشروط التي يجب توافرها في الدليل الرقمي ليكون مقبولا في الإثبات الجنائي. وعليه سنتطرق في هذا المطلب إلى سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي في الفرع الأول، وشروط قبول الدليل الرقمي في الفرع الثاني، وهذا في التشريع الجزائري.

الفرع الأول:سلطة القاضي الجنائي في قبول الدليل الرقمي

قبل التطرق إلى سلطة القاضي الجنائي في قبول الدليل الرقمي، نعرف الإثبات الجنائي بأنه مجموع الوسائل المستعملة للوصول إلى إظهار الحقيقة وبعبارة أدق هو إقامة الدليل على وقوع الجريمة، وعلى نسبتها إلى المتهم. فالقاضي الجنائي أثناء نظره الدعوى،

يبحث في الأدلة المعروضة أمامه، والمطروحة للمناقشة، لكي يستخلص منها حكمه، سواء بالبراءة أو بالإدانة [1]. وتخضع سلطة القاضي في قبول الدليل إلى طبيعة نظام الإثبات السائد في الدولة، لذلك سنتطرق إلى تعريف نظم الإثبات المعروفة وهي النظام المقيد، الحر والمختلط. مركزين على النظام الذي يتبناه المشرع الجزائري، وهو النظام المختلط، وأساس قبول الدليل الرقمي فيه وضوابطه.

أولا: نظم الإثبات الجنائي

عرفنا أن مفهوم الإثبات الجنائي هو مجموعة الإجراءات التي تهدف للوصول إلى الحقيقة. سواء بما يتعلق بالأفعال المرتكبة أو فيما يتعلق بشخصية المتهم الذي يكون محل متابعة جنائية، ولهذا يتكلم الفقهاء عن نظام الإثبات بدل الإثبات: وهي عبارة تنطوي على جملة من الوسائل التي تتعلق كلها بوسائل الإثبات، طبيعة الوسائل المقدمة، قوتها الثبوتية، الدور الذي يقوم به أطراف الدعوى، وكذا دور القاضي في إدارة هذه الوسائل[2].

وقد عرفت البشرية نظما مختلفة للإثبات، باختلاف الزمان و المكان من جهة، ومن حيث الخصائص والأسس من جهة أخرى، ليعرف العصر الحديث ثلاث نظم رئيسية وهي: نظام الأدلة القانونية، نظام الأدلة المعنوية، النظام المختلط.

1-نظام الأدلة القانونية:

يطلق عليه نظام الإثبات المقيد أو القانوني، في هذا النظام يحدد المشرع طرقا معينة للإثبات مسبقا، يتقيد بها القاضي، الذي ليس له الحرية في اختيار الدليل الذي يطمئن إليه، وإنما عليه أن يحكم بالنتيجة التي يصل إليها، وفقا للقيمة المقدرة من المشرع لكل دليل، و

---

[1] سامي جلال فقي حسين: مرجع سابق.ص68 .

[2] انظر ا.محمد مروان: نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري د.م.ح. الجزء 1. الجزائر..1999

المقدمة من الخصوم في الدعوى، وهنا موقف القاضي سلبي، ولا يجوز له أن يكمل ما في أدلة الخصوم من نقص، ولا أن يقضي بعلمه الشخصي ولا بما توصل إليه من قناعة شخصية. كالمشرع الهولندي، والمشرع الألماني الذي يحدد على سبيل الحصر وسائل الإثبات التي يتعين على القاضي قبولها. [1].

2- نظام الأدلة المعنوية:

يطلق عليه أيضا نظام الإثبات المعنوي أو المطلق أو الحر، وهنا يكرس مبدأ حرية الإثبات. المشرع لا يحدد طرقا معينة للإثبات، ويترك فيها الإثبات حرا بحيث يجوز للأطراف تقديم أي دليل لإثبات دعواهم والسعي لإقناع القاضي. والقاضي أيضا حر في اختيار وسيلة الإثبات التي يراها مناسبة لإظهار الحقيقة، ودوره إيجابي في هذا النظام، بل هو ملزم بالبحث وتكملة الدليل الناقص للكشف عن الحقيقة و له أن يقدر القيمة الإقناعية لكل دليل. و منها سلطة القاضي في قبول جميع الأدلة، و هنا تكون جميع طرق الإثبات مقبولة، ما لم يستبعد المشرع بعضها صراحة ،و يتبنى هذا النظام: القانون الفرنسي ، القانون المصري و القانون الجزائري في المادة 212 من قانون الإجراءات الجزائية[2].

3-النظام المختلط:

[1] عائشة بن قارة مصطفى. مرجع سابق.ص182 .
[2] المرجع نفسه . ص182

هذا النظام وسطي بين النظامين و هو يقوم على الجمع بين اليقين القضائي و اليقين القانوني، ويسود في القوانين الأنجلوسكسونية، حيث تقيد من حرية الإثبات في مرحلة الفصل في مسالة الإدانة أو البراءة في مرحلة تحديد العقوبة فيسود مبدأ حرية الإثبات [1].

ثانيا: أساس قبول و تقدير الدليل الرقمي في التشريع الجزائري

من خلال عرض نظم الثبات الأساسية (و هي: القانوني ، الحر والمختلط). و الإشارة إلى تبني المشروع الجزائري لنظام الإثبات الحر الذي يكرس مبدأ حرية القاضي في الاقتناع بمعنى أن القاضي حر في تكوين عقيدته من أي دليل يراه يقينا و يقتنع به [2] . فإن الدليل الرقمي مثله مثل باقي الأدلة الأخرى التي تم ذكرها على سبيل المثال القانون. مقبول في الإثبات الجنائي بصفة عامة و الإثبات في جرائم المعلوماتية بصفة خاصة [3].

و يجد أساسه في هذا النظام السائد الذي يرتكز على أساسين هما: مبدأ حرية الإثبات و مبدأ الاقتناع الشخصي للقاضي و هذا بنص المادة 212 الفقرة 1 من قانون الإجراءات الجزائية: ((يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك , و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص)).

وأيضا المادة 307 من نفس القانون فيما يخص الاقتناع الخاص لتشكيلة المحكمة .

و كما سبق وأن ذكرنا أن المشرع الجزائري لم يذكر مصطلح الدليل الرقمي. و هو أيضا لم يخصص نصوصا صريحة تتناول كيفية قبول الدليل الرقمي. و هذا يحيلنا إلى طرق الإثبات العامة المطبقة في قبول الأدلة، و التي تخضع لمبدأ حرية الإثبات و السلطة التقديرية للقاضي المشار إليها آنفا.

---

[1] عائشة بن قارة مصطفى : مرجع سابق . ص182

[2] محمد مروان: مرجع سابق، ص93.

[3] عائشة بن قارة مصطفى، المرجع نفسه، ص188.

و مبدأ حرية الإثبات يجعل للقاضي الجنائي دورا ايجابيا في توفير، وقبول وتقدير الدليل الجنائي بما في ذلك الدليل الرقمي . ويتجلى الدور الايجابي للقاضي الجنائي في توفير الدليل الرقمي من خلال الرقمي من خلال البحث عن هذا الدليل باستعمال سلطته المخولة له قانونا فيستطيع أن يأمر القائم بتشغيل النظام بتقديم المعلومات الأزمة لاختراق النظام و الولوج إليه من خلال الإفصاح عن كلمات المرور السرية، و الشفرات الخاصة بتشغيل البرامج كما أن له سلطة الأمر بتفتيش نظم الحاسوب بجميع مكوناته المادية والمعنوية و شبكات الإتصال[1].

لتأتي الخطوة الثانية وهي قبول الدليل الرقمي، بعد البحث عن الدليل وتقديمه من قبل كل من سلطة الإدعاء والمتهم و القاضي، في حالة ما إذا تطلب الفصل في الدعو يتطلب تحقيق دليل بعينه، وذلك من أجل خلق اليقين المطلوب لدى القاضي الثاني كأساس لإصدار حكمه بالإدانة أو البراءة. وأول ما يتأكد منه القاضي الجنائي في مرحلة قبول الدليل هو مدى مشروعيته قبل قبول الدليل الرقمي [2].

وسنتناول فيما يلي ضوابط الدليل الرقمي :

الفرع الثاني: شروط قبول الدليل الرقمي

عرفنا أن القاضي الجنائي في ظل نظام الإثبات المعنوي أو الحر يتمتع بسلطة واسعة في قبول أو تقدير أي دليل يطمئن إليه. لكن هذه السلطة ليست مطلقة كما قد يبدو للوهلة الأولى، بل مقيدة بشروط: لتفادي سوء التصرف ولدعم حقوق الأطراف. يمكن ايجازها في ثلاث شروط: مشروعية الدليل الرقمي، وجوب مناقشته في الجلسة، ويقينية الدليل الرقمي.

وهذا ما سنتناوله فيما يلي :

[1] عائشة بن قارة مصطفى، مرجع سابق ،ص194.
[2] عائشة بن قارة مصطفى، المرجع نفسه ، ص195.

أولا: مشروعية الدليل الرقمي

لكي يقبل القاضي الجنائي الدليل الرقمي يجب أن يكون مشروعا، أي تم الحصول عليه بطرق مشروعة أي عن طريق إجراءات قانونية صحيحة. وبالتالي يستبعد القاضي الدليل الذي تم جمعه بإجراءات باطلة. فمشروعية الدليل تعتبر ضمانا للحرية الفردية، بل وللعدالة ذاتها[1].

الدليل الرقمي يخضع لإجراءات خاصة في جمعه تختلف عن إجراءات باقي الأدلة الأخرى. وهذه الخصوصية يستمدها من البيئة الرقمية التي يعيش فيها كما سبق الذكر. المشرع الجزائري نص على هذه الإجراءات الخاصة في القانون رقم 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها. والذي سنتطرق إليه بالتفصيل في الفصل الثاني.

وترتكز مشروعية الحصول على الدليل الرقمي في مشروعية إجراءات التفتيش للبحث عن هذا الدليل و ضبطه في الوسط الافتراضي. ومن هنا فانه لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم دليلا رقميا تم الحصول عليه من تفتيش لنظام معلوماتي باطل. وذلك إثر صدور إذن من جهة غير مختصة مثلا، أو لم تكن الجريمة المعلوماتية محل الإذن قد وقعت بعد [2].

طبعا هذا بالإضافة إلى ضرورة احترام القواعد العامة للإجراءات الجنائية. والمبادئ القانونية العامة بما فيها احترام قيم العدالة وأخلاقياتها، والنزاهة واحترام حقوق الدفاع.

(1) عائشة بن قارة مصطفى، مرجع سابق ، ص195.
(2) عائشة بن قارة مصطفى، المرجع نفسه ، ص244.

ثانيا: وجوب مناقشة الدليل الرقمي في الجلسة

يؤسس القاضي اقتناعه الشخصي من مشروعية الدليل و أيضا من وجوب مناقشة هذا الدليل في الجلسة، وتعني قاعدة وجوب مناقشة الدليل في المواد الجنائية أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى. ويعد مبدأ المواجهة من أطراف الدعوى من أهم المبادئ التي يجب أن يؤسس القاضي اقتناعه على ضوئها حيث يتطلب هذا المبدأ طرح الأدلة في الجلسة، وأن تتاح الفرصة أمام طرفي الدعوى الجنائية لمناقشة الأدلة المقدمة من كل منهما وتقييدها، ويرتبط هذا المبدأ بالمبدأ القانوني العام، المتمثل في ضرورة إحترام حقوق الدفاع [1].

ووجوب مناقشة الدليل في الجلسة يقتضي أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته. وهذا الشرط نص عليه المشرع الجزائري في المادة:212 الفقرة 2 من قانون الإجراءات الجزائية: " ولا يسوغ للقاضي أن يبني قراره على الأدلة المقدمة في معرض المرافعات، والتي حصلت المناقشة فيها حصريا أمامه." بالإضافة إلى مبادئ المحاكمة الجزائية الأخرى المتمثلة في مبدأ الشفوية بحسب المواد:353،304،300، من نفس القانون. مبدأ العلنية بحسب المواد:342،285، 355، 399 من نفس القانون.

ومبدأ الشفوية هو مبدأ أساسي في الإجراءات الجنائية تقتضيه أولى بديهيات العدالة، حيث يجعل القاضي غير مكتف في تقديره للأدلة سواء كانت تقليدية أو رقمية، على ما دون بمحاضر التحقيق، وإنما يتوجب عليه أن يسمع الشهود واعتراف المتهم بنفسه وما يدلي به الخبراء ويطرح جميع الأدلة الأخرى للمناقشة الشفوية. فلا يكون هناك وسيط بين الدليل و القاضي،وغاية ذلك حتى يتاح لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة

[1] سامي جلال فقي حسين: مرجع سابق، ص117 .

إزاءه ويبين موقفه منه، مما يفيد القاضي في تكوين قناعته من حصيلة هذه المناقشات الشفوية التي تجري أمامه في الجلسة[1].

ولا يختلف الأمر بالنسبة للدليل الرقمي، سواء كان على شكل بيانات معروضة على شاشة الحاسوب أو مدرجة في حاملات البيانات اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مستخرجة في شكل مطبوعات، كل ذلك سيكون محلا للمناقشة عند الأخذ به كأدلة إثبات أمام المحكمة [2].

ثالثا: يقينية الدليل الرقمي

رأينا أن أهم النتائج التي تترتب على مبدأ حرية القاضي في تكوين قناعته الذي اعتنقه المشرع الجزائري وهي حرية القاضي في تقدير الأدلة وموازنتها وفقا لما يمليه عليه وجدانه بما في الدليل الرقمي، ومن دون أن يخضع في ذلك لرقابة المحكمة العليا، إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم و اليقين ، دون الظن و الترجيح و الاحتمال من ناحية، وأن يكون متوائما مع مقتضيات العقل و المنطق من ناحية أخرى[3]..

وهذا ما سنتطرق إليه بالشرح فيما يلي.:

1 بلوغ الاقتناع القضائي درجة اليقين:

المقصود باليقين لغة: العلم وزوال الشك

أما اليقين اصطلاحا: عبارة على حالة ذهنية ، أو عقلية تؤكد وجود الحقيقة [4]..

---

[1] فاضل زيدان محمد: مرجع سابق، ص254.
[2] عائشة بن قارة مصطفى، مرجع سابق، ص271 .
[3] رشيد بوكر : الدليل الالكتروني مدى حجيته في القانون الجزائري مجلة العلوم الاقتصادية عدد2، مجلد 27، جامعة دمشق ،2011، ص 323- 324 .
[4] عائشة بن قارة مصطفى، مرجع سابق، ص217 .

تهدف الخصومة الجنائية إلى معرفة الحقيقة ،مما مما يقتضي أن يصدر حكم القاضي عن اقتناع يقيني بصحة ما ينتهي إليه ،لا بمجرد الظن و الاحتمال ،إذ أن الشك يفسر لصالح المتهم،أخذا بقاعدة أساسية أن الأصل في الإنسان البراءة و شرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستقي منها هذا اليقين تقليدية أو مستخدمة كالدليل الرقمي.[1].

والوصول إلى اليقين يتم عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي، من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات و احتمالات ذات درجة عالية من التأكيد، تستبعد إمكانية تطرق أي شك أو ريب ، اتجاه تلك المحصلة النهائية التي وصل إليها القاضي في حكمه. [2].

واقتناع القاضي يصل إلى الجزم و اليقين عن طريق نوعين من المعرفة :أولهما المعرفة الحسية التي تدركها الحواس ، وثانيها المعرفة العقلية التي يقوم بها القاضي عن طريقا التحليل و الاستنتاج من خلال الربط بين مخرجات الحاسوب ، و الملابسات التي أحاطت بها.

وهنا الجزم بوقوع جرائم المعلوماتية ونسبتها إلى المتهم تتطلب نوعا جديدا من المعرفة ، مرتبطا بخصوصية هذه الجرائم، وذلك حتى يتمكن القاضي من استبعاد حالة الشك التي قد يقع فيها. .[3].

[1] سامي جلال فقي حسين، مرجع سابق، ص 121 .
[2] سامي جلال فقي حسين، المرجع نفسه، ص121 .
[3] رشيدة بوكر، مرجع سابق، ص 325 .

2_ مواءمة الإقتناع القضائي مع مقتضيات العقل و المنطق:

ذكرنا سابقا أنه يلزم لصحة و سلامة إقتناع القاضي بالدليل الرقمي أن يكون مبنيا على الجزم واليقين. لكن هذا لا يكفي وحده بل يلزم أيضا أن يكون متوائما مع مقتضيات العقل والمنطق لتتمكن المحكمة العليا من بسط رقابتها على سلطة القاضي التقديرية .

و يلتزم القاضي بمقتضى هذا الشرط بأن يبني اقتناعه على عملية منطقية تقوم على الإستقراء و الإستنباط ينتهي في ختامها إلى نتيجة معينة. فالقاضي و إن كان حرا في أن يعتقد في قيمة الأدلة سواء التقليدية أم الرقمية المطروحة. و لكنه لا يملك التحكم في هذا الإعتقاد، فاليقين المطلوب عند الإقتناع هو اليقين القضائي الذي يصل إليه القاضي بناء على العقل و المنطق. وبمعنى آخر تكون الأدلة التي اعتمد عليها القاضي في حكمه بما في ذلك الدليل الرقمي مؤدية إلى ما رتبه عليها من نتائج من غير تنافر مع العقل و المنطق . .[1].

على ضوء ما تقدم يمكن القول إن حجية الدليل الرقمي في إثبات جرائم المعلوماتية في التشريع الجزائري لا تثير أي صعوبات وذلك يرجع إلى تبني مبدأ حرية الإثبات و مبدأ الإقتناع الشخصي للقاضي و الذي يسمح للقاضي بقبول أي دليل و يتمتع بسلطة واسعة في تقديره ، وهذا طبعا مع احترام مبدأ المشروعية و اليقينية ، وباقي المبادئ القانونية العامة الأخرى، لنصل أن الدليل الرقمي في التشريع الجزائري شأنه شأن الأدلة الأخرى يحوز على حجية في إثبات جرائم المعلوماتية و إن كان ينفرد بإجراءات خاصة، سنتطرق إليها في الفصل الثاني .

[1] رشيدة بوكر، مرجع سابق، ص 325 .

تطرقنا في الفصل الأول إلى ماهية الدليل الرقمي و تعرفنا على أهم خصائصه التي تميزه على باقي الأدلة الجنائية، والتي يستمدها من البيئة الرقمية التي يعيش فيها مما يجعل إجراءات استخلاصه و تقديمه للعدالة تتميز بالخصوصية هي الأخرى.

وهذا ما حذى بأغلب التشريعات بما فيها التشريع الجزائري إلى تعديل قوانينها و سن قوانين أخرى تتماشى مع هذا النوع المستحدث من الأدلة. وكما اشرنا فقد تدخل المشرع الجزائري بتعديل قانون العقوبات وقانون الإجراءات الجزائية نظرا لأن النصوص التقليدية لا تتلاءم في كثير من الأحيان مع متطلبات البيئة الرقمية اللامادية.

من الجانب الموضوعي قام بتجريم الأفعال التي تمس النظام المعلوماتي بما في ذلك شبكة المعلومات بموجب قانون 04-15 المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفي مرحلة لاحقة وسع من نطاق التحريم حيث بالإضافة إلى الأفعال الماسة بأنظمة المعالجة الآلية. للمعطيات يشمل أي جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو بنظام للاتصالات الالكترونية و هذا بموجب قانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام و الاتصال و مكافحتها. طبعا دون إغفال تجريم بعض الأفعال بموجب قوانين خاصة (سبق ذكرها).

ومن الجانب الإجرائي وضع المشرع الجزائري في 2006 قواعد إجرائية [1] خاصة بمتابعة هذا النوع من الجرائم من خلال استثناء الجرائم المعلوماتية من القواعد العامة و مواجهتها بقواعد خاصة منها تمديد الاختصاص المحلي لكل من رجال الضبطية ووكيل الجمهورية و قاضي التحقيق و تمديد مواعيد الحبس، كما خصها بإجراءات استدلال خاصة كاعتراض المراسلات ,و التسرب.....

[1] الجريدة الرسمية العدد 3 الصادر بتاريخ 18 أكتوبر 2015

وأكملها في 2009 بإجراءات أخرى خاصة في قانون 09-04 السابق ذكره, منها المراقبة الإلكترونية وتفتيش المنظومات المعلوماتية إلى إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها وصولا إلى سنة 2015 التي تم فيها إنشاء هذه الهيئة بموجب قانون 15-261 [1].

وعلى هذا الأساس سنتناول في المبحث الأول الإجراءات التقليدية في تتبع الدليل الرقمي وفي المبحث الثاني الإجراءات المستحدثة في تتبع الدليل الرقمي و الأجهزة المتخصصة.

[1] قانون رقم 60-22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم لامر 66-155 المتضمن قانون الاجراءات الجزائية: الجريدة الرسمية عدد 84-2006

المبحث الأول

الإجراءات التقليدية

إذا كانت الجهات المكلفة بالبحث، و التحري على الجريمة، و المجرمين متعودة على التعامل مع الجريمة بصورها التقليدية. و التي يمكن إدراكها بالحواس. لما يمكن أن يخلفه مرتكبوها من آثار مادية في مسرح الجريمة من بصمات أو آثار أقدام أو بقع أو محررات مزورة. فإن الأمر في جرائم المعلوماتية يختلف، لأنها لا تخلف آثار مادية محسوسة، و يطرح الحصول على الدليل فيها إشكالات [1] من حيث دور الإجراءات التقليدية، كالمعاينة و الضبط و التفتيش و سماع الشهود و ندب الخبراء.

و هذا ما سنتناوله في مطلبين، يحتوي المطلب الأول على الإجراءات المادية، و المطلب الثاني على الإجراءات الشخصية.

[1] ا.حابت أمال: الطابع الخصوصي للإجراءات الجزائية من شان الجرائم المعلوماتية من القانون الجزائري : الملتقى الوطني حول الجريمة المعلوماتية ,جامعة بسكرة 2015

المطلب الأول:

الإجراءات المادية

نقصد بالإجراءات المادية تلك الإجراءات التي تعطى نتائج مادية محسوسة، و هي المعاينة، التفتيشي و الضبط . وقد يزداد دورها في الجرائم التقليدية بينما يتضاءل في الجرائم المعلوماتية أو العكس ، وهذا ما سنتناوله بالتوضيح في الفروع التالية:

الفرع الأول: المعاينة

أولا: تعريف المعاينة

يقصد بالمعاينة إثبات حالة الأماكن و الأسماء و الأشخاص و كل ما يعتبر في كشف الحقيقة، و المعاينة بهذا المعنى تستلزم الانتقال إلى محل الواقعة أوالى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة [1]

و بأسلوب آخر المعاينة هي انتقال ضابط الشرطة القضائية إلى مكان و قوع الجريمة إذا تطلب الأمر ذلك، من أجل إثبات حالة الأماكن و معاينة مخلفات الجريمة، و ضبط الأشياء المتحصلة أو المتخلفة عنها، أو التي استعملت في تنفيذ الجريمة [2].

[1] عبد الفتاح بيومي حجازي الجوانب الإجرائية لإعمال التحقيق في الجرائم المعلوماتية, القاهرة الطبعة الأولى.2009ص85

[2] د.على شملال: المستحدث في قانون الإجراءات الجزائري , الكتاب الأول دار هومة للنشر و التوزيع 2016ص35

ثانيا: الأحكام العامة للمعاينة

المعاينة هي إجراء من إجراءات التحقيق تتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها. وفي غير حالات التلبس التي نص عليها القانون تقوم بها سلطة التحقيق بنفسها أو تنتدب لها ضابط شرطة قضائية، وتدون نتائجها في محضر، و تتبع في شأنها جميع القواعد التي تحكم إجراءات المحاكمة، من إخطار الخصوم بمكان المعاينة، و زمانها ليتمكنوا من الحضور أثناء إجرائها. كما يمكن للمحكمة إن تقوم بإجراء المعاينة إذا رأت في ذلك سبيلا في كشف الحقيقة سواء كان ذلك من تلقاء نفسها أو بناء على طلب الخصوم[1].

ثالثا: المعاينة في جرائم المعلوماتية

إذا كانت المعاينة في الجرائم التقليدية ذات أهمية كبيرة تتمثل في تصور كيفية وقوع الجريمة وظروف ملابسات ارتكابها وتوفير الأدلة المادية التي يمكن تجميعها عن طريق المعاينة. فإن هذه الأهمية تتضاءل في جرائم المعلوماتية. ويرجع ذلك لكون الجرائم التقليدية غالبا لها مسرح تجري عليه الأحداث التي تخلف آثارا مادية تترتب عليها الأدلة بينما مسرح جرائم المعلوماتية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة[2] وذلك للإعتبارات التالية :

- أن جرائم المعلوماتية قلما يتخلف عن ارتكابها آثار مادية.
- تردد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنية مما يفسح المجال لحدوث أو تغيير أو العبث بالآثار المادية، مما يدخل الشك على الدليل المستمد من المعاينة إن وجد.

[1] عائشة بن قارة مصطفى: مرجع سابق ص 80
[2] عبد الفتاح بيموي حجازي: مربع سابق ص 60

- إمكانية التلاعب بالبيانات من طرف الجاني عن بعد أو محوها عن طريق التدخل من خلال وحدة طرفية.
- يمكن للمحقق أو ضابط الشرطة القضائية أن يستعين بالخبراء للفحص أو إبداء الرأي الفني حتى يمنع أي تشكيك في صحة الدليل المستمد من جرائم المعلوماتية [1]

رابعا: كيفية المعاينة في جرائم المعلوماتية

المتعارف عليه عند العلم بوقوع أي جريمة ينتقل ضابط الشرطة القضائية إلى مسرح الجريمة لمعاينتها، و أول ما يتبادر إلى الذهن، أنه انتقال مادي، لكن الأمر يختلف بالنسبة لجرائم المعلوماتية. فقد يكون انتقالا ماديا إلى مسرح تقليدي يقع خارج بيئة الحاسوب و الأنترنت ، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، قد يترك فيه الجاني عدة آثار كالبصمات و بعض متعلقاته الشخصية، و هو أقرب ما يكون إلى مسرح أي جريمة تقليدية.

وقد يكون انتقالا إفتراضيا إلى المسرح الإفتراضي و عبر العالم الإفتراضي حيث يستطيع المحقق أو ضابط الشرطة القضائية القيام بالمعاينة من مكتبه بواسطة الحاسوب، كما يمكنه اللجوء إلى مزود الخدمة الذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة [2]

وقد يكون انتقالا ماديا و افتراضيا معا في كل الأحوال عند إجراء المعاينة إلى مسرح الجريمة المعلوماتية يجب مراعاة ما يلي :

1- الاستعانة بأهل الخبرة و مختصين في الحاسوب و الأنترنت وقد يكون ضباط أو محققون مدربون.

(1) د. عائشة بن قارة مصطفى: مرجع سابق ص 82

(2) عائشة بن قارة مصطفى: المرجع نفسه ص 84

2- تأمين التيار الكهربائي من الانقطاع المفاجئ لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة، من جراء غلق جهاز الحاسوب و بالتالي فقدان كافة العمليات التي كان يتم تشغليها، و اتصالات الشبكة، و أنظمة الملفات الثابتة. [1]

3- تحديد أجهزة الحاسوب الموجود في مكان المعاينة و ما قد يتصل بها من أجهزة طرفية و محتوياتها، و أوضاع المكان الذي توجد به بصفة عامة. و تصويرها و تصوير أجزائها الخلفية وملحقاتها الأخرى. [2] و في حالة وجود شبكة الإتصالات يجب البحث عن خادم الملف وذلك لأجل تعطيل الإتصالات لمنع تخريب الأدلة أو محوها.

4- وضع دراسة كافية على مكان المعاينة و مراقبة تحركات داخل مسرح الجريمة و رصد الاتصالات الهاتفية من و إلى مسرح الجريمة مع إبطال مفعول أجهزة الهاتف المتحرك التي قد تساعد عن طريق تقنية معينة في تدمير أدلة الجريمة المعلوماتية[3] .

5- ملاحظة الطريقة التي تم بها إعداد النظام و الآثار الرقمية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات و بوجه خاص السجلات الرقمية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في حوار.[4]

(1) ممدوح عبد الحميد عبد المطلب ، مرجع سابق ص 115 .
(2) د. عائشة من قارة مصطفى مرجع سابق ص 86
(3) عبد الفتاح حجازي مرجع السابق ص 62
(4) د. عائشة قارة مصطفى مرجع سابق ص 86

معرفة بروتوكولات الإتصال عبر الأنترنت وإن تعلقت الجريمة بهذه الشبكة والتي تعرف باختصار ب (ip) .

6- عبر نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسوب من مجالات القوى المغناطيسية, الممرات المغناطيسية , التي قد تتسبب في محو البيانات، ولن يتأتى ذلك إلا عن طريق خبراء الحاسوب.

7- ملاحظة و إثبات حالات التوصيلات و الكابلات المتصلة بكل مكونات النظام حتى يتمكن من تحليل البيانات و مقارنتها و الوصول منها إلى دليل عند عرض الأمر على القضاء. [1]

8- القيام بحفظ المستندات الخاصة بالإدخال و كذلك مخرجات الحاسوب ذات الصلة بالجريمة ورفع ما قد يوجد عليها من بصمات أو آثار مادية.

9- ربط الأقراص الحاسوبية التي ربما تحمل الأدلة مع جهاز يمنع الكتابة أو التسجيل عليها، مما ينتج للمحققين قراءة بياناتها دون تغييرها.

10- 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 [2].

---

[1] عبد الفتاح بيومي حجازي: مرج سابق ص 62

[2] د. عائشة بن قارة مصطفى: مرجع سابق ص 87

الفرع الثاني: التفتيـــش

أولا : تعريف التفتيش:

يعتبر التفتيش إجراء من إجراءات التحقيق الابتدائي إذا أمر به قاضي التحقيق بعد اتصاله بالدعوى، و إجراء استدلالي إذا أمر به وكيل الجمهورية خلال مرحلة جمع الاستدلالات. [1]ويكون بالانتقال إلى المحل المراد تفتيشه بهدف البحث عن أدلة تتعلق بجريمة وقعت فعلا تفيد في كشف الحقيقة عنها أو عن مرتكبيها.

و نظرا لارتباط هذا الإجراء بالمساس بحرمة المسكن و أسرار الأشخاص و حرماتهم فقد قيده المشرع الجزائري بشروط موضوعية و أخرى شكلية، طبقا لما جاء في دستور سنة 1996 المادة 47: " تضمن الدولة حرمة المسكن، ولا تفتيش إلا بمقتضى القانون و في إطار احترامه، لا تفتيش إلا بأمر مكتوب صادر عن السلطات القضائية المختصة."

وإن كان التفتيش لا يختلف في مدلوله القانوني سواء بالنسبة للجرائم التقليدية أو جرائم المعلوماتية، إلا أنه في هذه الأخيرة له طابع خاص من حيث محله و إجراءاته الخاصة، هذا ما سنتناوله فيما يلي:

ثانيا : الأحكام العامة للتفتيش

كما سبق و إن ذكرنا، نظرا لما يطوى عليه التفتيش من مساس بحرمة المساكن، و حريات الأشخاص فقد أحاطها المشرع الجزائري بضمانات، بحيث " لا يجوز تفتيش المساكن و معاينتها وضبط الأشياء المثبتة إلا برضاء صحيح من الشخص الذي ستتخذ لديه هذه الإجراءات، و يجب أن يكون هذا الرضا بتصريح مكتوب بخط صاحب الشأن فإذا كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص أخر يختاره بنفسه، و يذكر ذلك في

[1] علي شملال: مرجع سابق، ص 42

المحضر مع الإشارة صراحة إلى رضاه"، المادة 64 قانون الإجراءات الجزائية الجزائري [1].

و قبلها المادة 44 من نفس القانون، " لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء متعلقة بالأفعال الجنائية المرتكبة. لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل أو الشروع في التفتيش".

هذه الشروط الشكلية للتفتيش أما عن الشروط الموضوعية أن تكون الجريمة وقعت فعلا. و أن توصف بجناية أو جنحة، وأن يكون هناك اتهاما قائما ضد شخص معين بالذات، سواء كان صاحب المسكن موضوع التفتيش متهما أصليا أو شريكا أو محرضا حائزا على أشياء لها علاقة بالجريمة، أن يكون المنزل المراد تفتيشه معينا و محددا تحديدا كافيا و أن يكون الغرض من تفتيشه الحصول على أدلة أو أشياء تفيد في إظهار الحقيقة[2].

وهناك شروط أخرى مثل تحديد وقت التفتيش من 5 صباحا إلى 8 مساءا و حضور الشاهدين....الخ نظمتها مواد من 41 إلى 47 مكرر من نفس القانون المذكور مع بعض الاستثناءات في جرائم المعلوماتية سنتطرق إليها مع الأحكام الخاصة بالتفتيش فيما يلي:

[1] القانون رقم 06-22 المؤرخ في 2 فيفري 2006 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 8-6-1996 الجريدة الرسمية عدد 84: الصادرة بتاريخ 24-12-2006

[2] د. على شملال: مرجع سابق ص 43

ثالثا : التفتيش في جرائم المعلوماتية

نظرا لخطورة جرائم المعلوماتية, فقد استثناها المشرع الجزائري من الأحكام العامة للتفتيش، و من أجل استخلاص الدليل الرقمي الذي يثير تحديات بشأن الإطار القانوني الملائم، و يرجع ذلك إلى تقنية الحاسوب و الإتصال، التي تتطلب بدورها لإجراء التفتيش تقنيات خاصة للتعامل مع نظم المعلومات و شبكات الإتصال.

فقد لا يكون النظام محل التفتيش مملوكا للمشتبه به و ليس ثمة وسيلة ميسرة لمعرفة ذلك، كما أن ملفات الحاسوب قد تكون مخبأة أو محمية داخل نظام الشخص و قد تنقل حول العالم من نظام لآخر بثوان ،كما يسهل إتلافها، كما أن الدليل قد يكون داخل النظام أو قد يكون مخزنا مع وسائط أخرى، كالأقراص مثلا ، وقد يكون أصلا في جزء من الشبكة لا يرتبط بالمشتبه به مباشرة، لكنه يستخدم هذا الموقع لإخفاء الأدلة و الملفات، أيضا قد تكون البيانات التي تثبت حصول الفعل جزء من خادم نظام حاسوب خارج الحدود في دولة أخرى، و قد يكون نشاط الجاني مباشرا بالأساس من حاسوب آخر أو من حاسوب محمول يسهل عليه التخلص منه أو إنكار ملكيته.

ورغم ذلك يبقى محل الجريمة إنما هو المعطيات باعتبارها مالا معنويا أوبما تمثله هذه المعطيات التي قد تكون مخزنة داخل النظام أو في إحدى وسائل التخزين ، أو تكون في طور النقل والتبادل ضمن وسائل الإتصال المندمجة مع نظام الحوسبة.

وبهذا المعنى يرد التفتيش على محتويات الحاسوب المادية و المنطقية و على شبكات الإتصال و هذا ما سنتطرق إليه فيما يلي:

1- تفتيش المكونات المادية للحاسوب :

يتكون الحاسوب من مكونات مادية ملموسة قادرة على قبول البيانات بغرض معالجتها و إخراجها و تجميعها و استخراج النتائج منها، و من مكونات منطقية أو معنوية هي برامج التشغيل ، و برامج التطبيقات، و المكونات المادية : هي

- وحدات الإدخال: لوحة المفاتيح ، وحدة قراءة الاسطوانات المرنة أو الممغنطة، الفارة.....الخ
- وحدات الإخراج: شاشة العرض ، الطابعة، جهاز الرسم.
- وحدة المعالجة المركزية : و تقوم بالعمليات الحسابية و تخزينها و المقارنات المنطقية و الاحتفاظ بها [1]

لا تثار أي مشكلة في تفتيش هذه المكونات المادية للحاسوب لأنه يرد على الأشياء، وهو ما أكدته المادة 64 من قانون الإجراءات الجزائية، سواء كان الحاسوب و ملحقاته المادية موجود في أماكن خاصة أو عامة للمنزل أو محمول باليد أو مقهى الانترنت شرط أن تراعى فيه الضمانات و القيود القانونية . [2]

في الواقع أن تفتيش المكونات المادية بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية وقعت و يفيد في كشف الحقيقة عنها و عن مرتكبيها يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة .[3]

إلا إن المشرع الجزائري استثنى في تعديل القانون رقم 06-22 المذكور آنفا في المواد 45 الفقرة 03 و 47 الفقرة 2 و 64 الفقرة 3 من قانون الإجراءات الجزائية، تطبيق هذه الضمانات المتعلقة بالحرية الشخصية و حرمة المسكن فيما يخص جرائم المعلوماتية و يرجع السبب في ذلك إلى سهولة التلاعب بالأدلة و محوها و إتلافها بسرعة كبيرة .[4]

---

[1] خثيز مسعود: مرجع سابق ص 24

[2] د. ادريس قرفي,: تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية بين اتفاقية بودابست و التشريع الجزائري ، الملتقى الوطني حول الجريمة المعلوماتية، جامعة بسكرة 2015.

[3] د. عائشة بن قارة مصطفى:مرجع سابق ،ص 88

[4] د. قرفي ادريس: مرجع سابق .

حيث أجاز المشرع الجزائري التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار و الليل، بناء على اذن مسبق من وكيل الجمهورية، و استغنى عن حضور الأشخاص المحددين في المادة 45 الفقرة الأولى[1]

2- تفتيش المكونات المنطقية للحاسوب

بالإضافة إلى المكونات المادية للحاسوب التي سبق التطرق إليها، فإن الحاسوب يتكون من مكونات منطقية أو معنوية و بدونها يصبح الحاسوب جسدا لا روح فيه، و تتمثل في البرامج و تنقسم إلى قسمين:

- **برامج التشغيل:** تقوم بدور أساسي في تسيير الجهاز, فهي التي تحافظ على النظام داخل الجهاز الحاسب، كما إنها تخدم برامج التطبيقات عن طريق تحقيق أكبر إستفادة ممكنة من الحاسب. و تقوم برامج التشغيل بوظائف أهمها التحكم و السيطرة على مكونات الحاسوب، الربط من المستخدم و الجهاز من خلال معالجة اللغات حيث تختلف لغة الحاسوب عن لغات البشر [2]
- **برامج التطبيقات:** وهي تلك الأوامر التي يصدرها المستخدم للحاسوب و تكون على نوعين: البرامج الجاهزة و هي التي تنتجها الشركات المتخصصة مثل برامج word, Exel وغيرها، و البرامج المكتوبة و هي التي يقوم بكتابتها المستخدمون لحل مسائل معينة لا تتوفر بها برامج خاصة في الحاسوب. [3]

و قد أجاز المشرع الجزائري صراحة تفتيش النظم المعلوماتية بموجب نص المادة 05 من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام و الإتصال و مكافحتها حيث جاء فيها " يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية و في الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش و لو عن بعد إلى:

---

(1) د. عائشة بن قارة مصطفى:مرجع سابق ص 90
(2) خثير مسعود:مرجع سابق ص 30
(3) د. جلال فقي حسين: مرجع سابق ص 46

أ. منظومة معلوماتية او جزء منها و كذا المعطيات المعلوماتية المخزنة فيها

ب. منظومة تخزين معلوماتية [1] "

المعلومات المذكورة في المادة 04 هي :

- الوقاية الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الأمن الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- بمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2]

ويقصد بمنظومة معلوماتية كما نصت المادة 21 من نفس القانون أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة بيوم واحد منها أو أكثر بمعالجة آلية المعطيات تنفيذا لبرنامج معين.

أما المعطيات المعلوماتية فهي أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها .[3]

3- تفتيش الشبكات المعلوماتية المتصلة بالحاسوب

- الشبكة المعلوماتية هي اتصال جهازي بحاسوب أو أكثر ببعضها سلكيا أو لا سلكيا فان كانوا في نفس الموقع سميت شبكة محلية أما إذا كانوا متفرقين تسمى بعيدة المدى و مع ظهور الأنترنت أعطت الاتصال بعدا دوليا [4]

---

[1] د. قرفي ادريس:مرجع سابق

[2] المادة 04 من القانون رقم 09-04

[3] المادة 02 من القانون رقم 09-04 فقرة ب و ج

[4] د. ا قرفي دريس: مرجع سابق

و يقصد بالإنترنت شبكة الاتصالات الدولية ظهر هذا المصطلح عام 1982 ثم أعلن في سنة 1988 عن استخدام الأنترنت وسيلة أساسية للإتصالات. وهي عبارة عن شبكة ضخمة من الحواسيب المتصلة فيما بينها حول العالم، و التي يتم من خلالها، تبادل المعلومات .[1] وأصبحت تقدم خدمات كثيرة منها البريد الالكتروني و التخاطب عبر الدردشة و التحويل المالي بين البنوك و الشركات مختصرة المسافات و الوقت.

وتتطلب الأنترنت في عملها توافر جهاز حاسوب، كابلات ، خط هاتف ، برمجيات الأنترنت، و تسمى المتصفحات، وتقنية تدعى المودام و هو عبارة عن وحدة ربط تستخدم في إرسال البيانات عبر خطوط الهاتف و بروتوكول تراسل الأنترنت IP/TCP[2]

و يشمل بروتوكول التحكم في النقل TCP الذي يقوم بتجزئة الرسالة المراد إرسالها إلى رزم من المعلومات تحمل معلومات تعريفية حول المرسل و المرسل إليه ثم يتم تجميعها عند العنوان المقصود. و بروتوكول الأنترنت IP المسؤول عن عنونة و ترقيم و توجيه الرسائل إلى عناوينها المقصودة بالإضافة إلى منح كل جهاز أو موقع على الشبكة رقما معينا الذي قد يصل إلى 128 رقما.

هنا تثار إشكالية في إجراء التفتيش لاستخلاص الدليل الرقمي خاصة فيما يتعلق بالاختصاص نظرا لعالمية الشبكة المعلوماتية ، وهو ما عالجه المشرع الجزائري في القانون 09-04 فإذا ظهر أن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى يمكن الدخول إليها عن طريق المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها وذلك بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

(1) نهلاعبد القادر المومنية: مرجع سابق ص 35
(2) نهلاعبد القادر المومنية: مرجع نفسه ص 36

و إذا كانت هذه المنظومة واقعة خارج الإقليم الوطني يتم الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل . [1]

كما يمكن للسلطات المكلفة بالتفتيش 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 لانجاز مهمتها [2]

الفرع الثالث: الحجز

أولا : تعريف الحجز أو الضبط

هو إجراء من إجراءات التحقيق التي تهدف إلى وضع اليد على الأدلة المتحصلة من التفتيش، وتحريزها لمصلحة التحقيق.

ثانيا : الأحكام العامة للحجز

قد يكون الحجز نتيجة معاينة و قد يكون نتيجة تفتيش، و يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس أن يخطر وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية و يتخذ جميع التحريات اللازمة. و عليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي و أن يضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة .[3]

تغلق الأشياء أو المستندات المحجوزة و يختم عليها إذا أمكن ذلك ، فإذا تعذرت الكتابة فإنها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطا من الورق و يختم عليه بختمه. [4] وتطبق نفس الأحكام العامة للمعاينة والتفتيش على الحجز مثل المواقيت والإذن. ضمأن للحريات الشخصية.

---

[1] المادة 5 من القانون رقم 09-04

[2] المادة 5 من القانون رقم 09-04 الفقرة الاخيرة

[3] المادة 42 قانون الإجراءات الجزائية الجزائري

[4] المادة 45 من قانون الإجراءات الجزائية الجزائري 06-22

ثالثا: الحجز في جرائم المعلوماتية

إن الاستثناءات الواردة على المعاينة و التفتيش في جرائم المعلوماتية نفسها ترد على الحجز بموجب القانون 06- 22 المذكور آنفا . بحيث يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني ، في كل ساعة من ساعات النهار أو الليل، و ذلك بناء على إذن مسبق من وكيل الجمهورية.

كما يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا و في أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك. [1]

بالنسبة للمكونات المادية للحاسوب، لا يثير حجزها أي مشكلات بحيث تخضع للقواعد العامة للحجز. أما حجز المعطيات المعلوماتية فقد نظمها المشرع الجزائري من خلال القانون 09-04 وهناك نوعان من الحجز:

1- حجز المعطيات المعلوماتية عن طريق النسخ :

عندما تكتشف السلطة المختصة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و انه ليس من الضروري حجز كل المنظومة ،يتم نسخ المعطيات محل البحث، و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز و الوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. كما يجب في كل الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز استعمال الوسائل التقنية لتشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات [2]

و يتم ذلك باستخدام برامج متخصصة منها :

---

[1] المادة 67: من القانون 06-22

[2] المادة 6 من القانون رقم 09-04

- **برامج معادلة الملفات X Tre Pro Gold:** وهو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب ، و يستخدم لتقييم محتويات القرص الخاص بالمتهم أو الأقراص المرنة المضبوطة ,أو يستخدم لقراءة البرامج في صورتها الأصلية كما يمكن من البحث عن كلمات معينة أو عن إنشاء ملفات أو غيرها.
- **برنامج النسخ Lap Link :** هو برنامج يمكن تشغيله من قرص مرن و يسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم و نقلها إلى قرص أخر سواء على التوازي أو التوالي . و هو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم. [1]

2- <u>الحجز عن طريق منع الوصول الى المعطيات:</u>

إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 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 استعمال هذه المنظومة. ويتم ذلك باستخدام أساليب مختلفة منها : أسلوب تجميد التعامل بالحاسوب أو إحدى القطع المكونة له التي استخدمت في إرتكاب الجريمة ويتخذ هذا الأسلوب عدة مظاهر من أبرزها:

- نظام ضغط محتويات القرص الصلب.
- نقل تلك المحتويات إلى أقراص صلبة متعددة أو ممغنطة. [2]

[1] د. عائشة بن قارة مصطفى مرجع سابق ص 57
[2] المادة 7 من القانون رقم 09-04 مرجع سابق

و في كل الأحوال فأن إجراء حجز المعطيات المعلوماتية يجب بطريقة فنية حتى لا يكون تلك الأدلة عرضة للتلف و الإفساد، لذلك يتعين اتخاذ بعض الإجراءات الخاصة للمحافظة عليها و صيانتها من طرف أشخاص مؤهلين، كضبط الدعائم الأصلية للبيانات و عدم الاقتصار ضبط نسخها. وعدم تعريض الأقراص و الأشرطة الممغنطة لدرجة الحرارة العالية و لا إلى الرطوبة . [1]

[1] د.عائشة بن قارة مصطفلى : مرجع سابق ص 117

المطلب الثاني :

الإجراءات الشخصية

تكلمنا عن الإجراءات التقليدية المادية في تتبع الدليل الرقمي، و هي المعاينة و التفتيش و الحجز، وهي ذات طابع مادي توصل القائمين بها مباشرة بالدليل. و سنتكلم في هذا المطلب عن الإجراءات التقليدية الشخصية، و هي الشهادة و الخبرة لاعتبار تدخل الأشخاص، الشاهد و الخبير في هذه الإجراءات كوسطاء بين القائمين بها و الدليل.

الفرع الأول : الشهادة

أولا : تعريف الشهادة

الشهادة بشكل عام هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدراكه بحواسه بطريقة مباشرة أو غير مباشرة، و الشهادة هي إجراء من إجراءات التحقيق، و هي المعلومات التي تتعلق بالجريمة و بظروف ارتكابها التي يدلي بها الشاهد أمام سلطات التحقيق[1]

ثانيا : الأحكام العامة للشهادة

نظم المشرع الجزائري أحكام الشهادة في القسم السابع من قانون الإجراءات الجزائية الجزائري تحت عنوان سماع الشهود في المواد من 88 إلى 99. [2]

1- بحيث يستدعي قاضي التحقيق أمامه بواسطة أحد أعوان القوة العمومية، كل شخص يرى فائدة من سماع شهادته أو بواسطة كاتب عمومي، أو موصى عليه، كما يمكن لكل شخص يملك معلومات عن الجريمة أن يحضر طواعية لتقديم شهادته كما نصت المادة 88 من نفس القانون.

---

[1] ا.د. رضا هميسي:احكام الشاهد في الجريمة المعلوماتية و الملتقى الوطني حول الجريمة المعلوماتية جامعة محمد خيضر بسكرة 2015

[2] انظر:المواد من 88الى 99: القسم السابع قانون الإجراءات الجزائية الجزائري

2- يؤدي الشهود شهادتهم أمام قاضي التحقيق بمساعدة كاتب فرادى بغير حضور المتهم و يحرر محضر بأقوالهم. (المادة 90.)

3- و كل شخص استدعى لسماع شهادته ملزم بالحضور و حلف اليمين و أداء الشهادة مع مراعاة الأحكام القانونية المتعلقة بالسر المهني و إلا عوقب بغرامة من 200 إلى 2000 دج و نفس العقوبة تطبق عليه إذا حضر و امتنع عن الإدلاء بالشهادة (المادتان 89-97).

4- غير أنه يجوز للقاضي مناقشة الشاهد أو مواجهته شهود آخرين أو بالمتهم، و أن يجري بمشاركتهم كل الإجراءات و التجارب الخاصة بإعادة تمثيل الجريمة مما يراه لازما لإظهار الحقيقة [1].

تجدر الإشارة هنا إلى الجديد في الأمر، أن المشرع الجزائري وفر حماية لشهود و الخبراء و الضحايا وحتى أهاليهم، إذا كانت حياتهم أو سلامتهم الجسدية أو مصالحهم الأساسية معرضة لتهديد خطير بسبب المعلومات التي يمكنهم تقديمها و التي تكون ضرورية لإظهار الحقيقة.

و هذا بموجب الأمر رقم 15-02 المؤرخ في 23 جويلية 2015 المعدل لقانون الإجراءات الجزائية،حيث جاء الفصل السادس من هذا الأخير، تحت عنوان: "حماية الشهود و الخبراء و الضحايا" تضمن قواعد صارمة في هذا الأمر في المواد من 65 مكرر 19 إلى 65 مكرر 28.

[1] المادة 96:من قانون الإجراءات الجزائية الجزائري 2009

ثالثا: الشهادة في جرائم المعلوماتية

تختلف الشهادة في جرائم المعلوماتية عن مثيلتها في جرائم التقليدية. و مرد ذلك هو البيئة التي ترتكب فيها الجريمة و التي يوجد فيها مسرح الجريمة و هي بيئة افتراضية لا مادية عكس البيئة التي ترتكب فيها الجريمة في صورتها التقليدية و بالتالي فان شهودها غالبا ما يكونون من الأشخاص المحيطين بهذه البيئة [1]

و بأسلوب آخر لهم علاقة بالبيئة الافتراضية التي وقعت فيها الجريمة، و هم بذلك يتميزون بالخبرة و التخصص في تقنية الحاسوب و شبكات الإتصال، و يطلق على الشاهد في جرائم المعلوماتية، الشاهد المعلوماتي وله دور كبير في استخلاص الدليل الرقمي .

و سنرى فيما يلي الفرق بين الشاهد المعلوماتي و الشاهد التقليدي. و فئات الشاهد المعلوماتي.

1- الفرق بين الشاهد المعلوماتي و الشاهد التقليدي

بداية نشير إلى أن الأحكام العامة للشهادة تسري على كل من المعلوماتي و التقليدي و بالتالي تسري عليهما نفس الالتزامات، الفرق الموجود بينهما يكون في الصفة و فيما يقدمه كل واحد.

فالشاهد المعلوماتي تكون لديه خبرة و تخصص في تقنية الحاسوب و شبكات الاتصال، و هو اختلاف جوهري مما يجعل شهادته لا تتوقف على مجرد الإدلاء بما سمعه أو رآه أو لمسه كما هو الأمر بالنسبة للشاهد التقليدي، بل تعداه الى تقديم ما لديه من معلومات و خبرات لازمة للمساعدة في تتبع و استخلاص الدليل الرقمي .

[1] ا.د. رضا هميسي: مصدر سابق

مثل الولوج النظام المعالجة الآلية للمعطيات، من خلال الإفصاح عن كلمات المرور و الشفرات الخاصة بالبرامج المختلفة [1] .

و لا يمكن هنا الخلط بين دور الشاهد و دور الخبير، فكل منهما يختلف عن الآخر في جرائم المعلوماتية، حيث أن الخبير يقوم بتقديم تقرير أو رأي أو نتائج نتوصل إليها من خلال تطبيق معايير علمية، و أصول فنية دقيقة، و هذا ما سنتطرق إليه لاحقا. [2]

2- فئات الشاهد المعلوماتي :

رأينا كيف يتميز الشاهد المعلوماتي عن مثيله التقليدي من حيث اتصاله بالبيئة الافتراضية التي يوجد فيها الدليل الرقمي، و خبرته في تقنية الحاسوب و شبكة الاتصال, مما يساعد المحققين في استخلاص الدليل الرقمي. و تنوع الدليل الرقمي ينعكس على الشاهد المعلوماتي الذي نجده في عدة فئات نذكر فيما يلي أهمها :

أ. عامل تشغيل الحاسوب:

هو الشخص المسؤول عن تشغيل الحاسوب و المعدات المتصلة به، و يجب أن تكون لديه خبرة كثيرة في استخدام الجهاز و مكوناته مثل و ضع القرص في وحدة الأقراص، و استخدام لوحة المفاتيح في إدخال البيانات ، و كذلك استخدام الطابعة و غيرها من الوسائط الالكترونية المستحدثة، و النقل منها إلى الحاسوب و العكس . [3]

(1) د. عبد الفتاح بيومي حجازي. مصدر سابق ص 227
(2) ا.د.رضا هميسي . مرجع سابق
(3) د. عبد الفتاح بيومي حجازي: مصدر سابق ص 223

ب. المحللون:

المحلل هو الشخص الذي يحلل الخطوات و يقوم بتجميع بيانات نظام معين و دراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة و استنتاج العلاقات الوظيفية من هذه الوحدات ، كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات و استنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسوب.

ج. المبرمجون أو مخططو البرامج:

و هم الأشخاص المتخصصون في كتابة أوامر البرامج، و حسب نوعية البرامج ينقسم هؤلاء إلى فئتين: مخططي برامج التطبيقات و مخططي برامج النظم.

يقوم مخططو برامج التطبيقات بالحصول على خصائص و مواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة و موثقة لتحقيق هذه المواصفات.

أما مخططو برامج النظم فيقومون باختيار و تعديل و تصحيح برامج نظام الحاسوب الداخلية، أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسوب بالبرامج و الأجزاء الداخلية التي تتحكم في وحدات الإدخال و الإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج .[1]

[1] د.عائشة بن قارة مصطفى: مرجع سابق ص 127

د. مقدمو الخدمات

عرفهم المشرع الجزائري في 2008 من القانون رقم 09-04 كما يلي:

أي كيان عام أو خاص يقدم لمستعملي خدماته, القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للإتصالات[1] . و أي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها .

و ألزم المشرع الجزائري مقدمي الخدمات بمساعدة السلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها و بوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة .[2]

و الملاحظ أن المشرع الجزائري ركز على مقدمي الخدمات فقط ، أي نوع واحد من الشهود في هذا القانون، مما يحيلنا إلى الأحكام العامة للشهادة بالنسبة لباقي الفئات من حيث التزام الشاهد لتقديم كل ما يمكنه تقديمه في سبيل الحصول على الدليل الرقمي و الاستعانة بأي شخص يمكنه ذلك.

و هناك تشريعات أخرى أضافت مهندس الصيانة للتأكد من سلامة الجهاز و ملاحقته و شبكات الاتصال و أيضا مديري النظم الذين تكل إليهم أعمال الإدارة في النظم المعلوماتية.

[1] الجريدة الرسمية : عدد 47 : أوت 2009

[2] المادة 10 من القانون رقم09-04.الجريدة الرسمية عدد 47 مؤرخة في 16 أوت 2009

الفرع الثاني : الخبرة

أولا: تعريف الخبرة

الخبرة هي وسائل الإثبات في المادة الجنائية، و هي إعطاء أو إدلاء أهل الفن أو علم معين. برأيهم في مسائل فنية تتعلق بتلك الفنون أو العلوم كتحديد ساعة أو لحظة وفاة أو سببها أو تحليل مادة معينة، و هي حالات فنية تعترض المحقق فلا يستطيع القطع فيها فيستعين بأهل الفن و العلم. [1]

أقرها المشرع الجزائري في القسم التاسع من قانون الإجراءات الجزائية في 14 مادة. من المادة 143 إلى المادة 165، حيث جاء في المادة 143من نفس القانون " لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة أو إما من تلقاء نفسها أو من الخصوم ".

ثانيا :الأحكام العامة للخبرة

نظم المشرع الجزائري الخبرة بأحكام نصت عليها المواد من 143الى 156 من قانون الإجراءات الجزائية كما سبق الذكر.

- يتم اختيار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة و تحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل في المادة 144، هذا عن الخبير المنتدب، و هناك الخبير الاستثنائي وهو شخص متخصص في مجال من المجالات الفنية غير مقيد في جدول الخبراء المعتمدين يقوم بانتدابه في مسالة محددة فقط، و يتعين لقبوله أن يحلف اليمين أمام الجهة القضائية أو القاضي الذي عينه بأن يقوم بأداء المهمة الموكولة إليه بالدقة و الأمانة المادة 431 من نفس القانون. [2]

---

[1] د.عبدالله اوهابية: شرح قانون الإجراءات الجزائية، دار هومة ، الطبعة الثانية.2011، ص 368 .

[2] ا. محمد مروان: مرجع سابق، ص 397 .

في حين يؤدي الخبير المقيد في الجدول اليمين مرة واحدة، هذه عن الخبير و تعيينه.

- أما سلطاته فيحدد قرار التعيين مهمته ، فلا يجوز تجاوز حدودها لأن الخبرة، يجب أن تقتصر على المسائل الفنية فلا يتعداها. [1] كما يجوز للخبير أثناء تأديته لمهامه الفنية سلطات معتبرة.

فبإمكانه تلقي أقوال غير المتهم كما له الحق في استجواب المتهم مع ضرورة مراعاة الأشكال التي قررها القانون لذلك. المادة (151الفقرة 3) .و القاعدة أن هذا الاستجواب يجري بواسطة قاضي التحقيق أو القاضي المعين من طرف المحكمة مع الحرص على أحكام المواد 115 و 116 من قانون الإجراءات الجزائية. [2]

يتولى الخبير مهمته تحت رقابة القاضي الذي عينه و يستجيب لطلبات الأطراف أثناء تنفيذ الخبرة كما في المادة 152. و يجب على الخبير تقديم تقرير نتائج الخبرة المكلف بها بمجرد الانتهاء منها في الميعاد المحدد لانجازها. و في حالة تقاعسه يتعرض لعقوبات تأديبية تصل إلى حد الشطب من الجدول، و في هذه الحالة عليه أن يقدم نتائج عمله و إعادة كل الوثائق التى عهد بها إليه خلال 24 ساعة، و هذا ما نصت عليه المادة 153. [3]

و تجدر الإشارة إلى أن تقرير الخبرة لا يلزم القاضي, و لهذا الأخير مطلق الحرية في تقريره, فله أن يأخذ بنتائج الخبرة أو استبعادها كما يشاء و له كذلك أن يأمر بإجراء خبرة تكميلية أو القيام بخبرة مضادة أو مقابلة لا سيما إذا تعارض تقرير الخبرة مع شهادة أحد الشهود . [4]

[1] المادة 146 من القانون الاجراءات الجزائية
[2] ا. محمد مروان,مرجع سابق ص 398
[3] محمد اوهايبية,مرجع سابق ص 370
[4] محمد مروان,مرجع سابق ص404

ثالثا : الخبرة في جرائم المعلوماتية

تلعب الخبرة دورا كبيرا في الجرائم التقليدية, و يزداد هذا الدور أهمية في جرائم المعلوماتية، في سبيل استخلاص الدليل الرقمي، نظرا لما يتميز به الدليل الرقمي كما رأينا من خصائص (تقني و علمي)، يقتضي التعامل معه معرفة علمية، و خبرة تقنية متخصصة في تقنية الحاسوب و تكنولوجيات الاتصال لا يمكن للقضاة الإلمام بها جميعا و يطلق عليها الخبرة التقنية ، لذلك يلجأ القضاة إلى خبراء في هذا المجال، و تسري على الخبرة التقنية نفس الأحكام العامة المنظمة للخبرة القضائية في الجرائم التقليدية، بالإضافة إلى الجوانب الفنية التي تحكم عمل الخبير التقني.

و سنتناول في البداية المسائل التي يستعان بها بالخبرة التقنية ثم نتطرق إلى خطوات استخلاص الدليل الرقمي.

1- المسائل التي تتطلب الخبرة التقنية:

- وصف تركيب الحاسوب و صناعته و طرازه وفق نظام التشغيل و أهم الأنظمة التي يستخدمها بالإضافة إلى ملحقاته و كلمات المرور و نظام التشفير.
- وصف طبيعة الحاسوب أو الشبكة، و نمط وسائل الاتصالات و تردد موجات البث و أمكنة اختزانها.
- وصف الوضع المحتمل لأدلة الإثبات و الهيئة التي تكون عليها . [1]
- القيام عند الإقتضاء بعزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق الضرر بالأجهزة .
- كيفية نقل أدلة الإثبات إلى أوعية ملائمة بغير أن يصيبها التلف .
- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا أمكن إلى أوعية ورقية بحيث يتاح للقاضي مطالعتها و فهمها مع إثبات أن المسطور على الورق مطابق لذلك المسجل على الحاسوب أو النظام أو الشبكة أو مثبتا عليها. [1]

[1] عائشة بن قارة مصطفى مرجع سابق ص 147

-

2- خطوات استخلاص الدليل الرقمي:

أ. خطوات ما قبل التشخيص و الفحص:

- التأكد من مطابقة محتويات إحراز المحجوزات لما هو مدون عليها .
- التأكد من صلاحية وحدات نظام التشغيل .
- تسجيل بيانات الوحدات المكونة المحجوزة كالتنوع و الطراز و الرقم المسلسل.

ب.خطوات التشغيل و الفحص :

- استكمال تشغيل باقي بيانات الوحدات من خلال قراءات الجهاز .
- عمل نتيجة من كل وسائط التخزين المحجوزة، خاصة القرص الصلب لإجراء عملية الفحص المبدئي على هذه النسخة كحماية الأصل من أي فقد أو تلف أو تدمير، سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برامجية.
- تحديد أنواع و أسماء المجموعات البرامجية ، و برامج النظام، و برامج التطبيقات، و برامج الاتصالات ، و ما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة، برامج إنشاء و معالجة الصور في جرائم دعارة الأطفال مثلا.
- إظهار الملفات المخبأة و النصوص المخفية داخل الصور.
- استرجاع الملفات التي محوها من الأصل و ذلك باستخدام برامج استعادة البيانات، و كذلك بالنسبة للملفات المعطلة أو التالفة، و استخدام خوارزميات للتأكد من سلامة الدليل من العبث، و بعد ذلك تخزن هذه الملفات أو البيانات و يعمل لها نسخ طبق الأصل أخرى من الأسطوانة أو القرص أو المحتوي لها لفحصها عن طريق تطبيق الخطوات السالفة الذكر.
- يتم إعداد قائمة يجرد فيها الخبير كل الأدلة الرقمية التي تم الحصول عليها في القرص الخاص بها مع إجراء مراجعة لكل صورة محتفظ بها في القرص في حاسوب آخر للتأكد من سلامة القائمة. [2]

---

(1) د. عبد الفتاح بيومي حجازي , مرجع سابق ص 135

(2) د. عائشة بن قارة مصطفى : مرجع سابق ص 149

- تحويل الدليل الرقمي إلى هيئة مادية و ذلك عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صورا أو نصوصا ، أو وضعها في أي وعاء آخر حسب نوعية البيانات و المعلومات المكونة للدليل. [1]
- فحص كل من الدليل الرقمي في شكله المادي' و الدليل المادي المحجوز و تحديد مدى توافقهما، كما يكسب الدليل الموثوقية و اليقينية اللتان تؤديان إلى قبوله لدى جهة التحقيق و الحكم .

ج ـ خطوة إعداد التقرير:

- في هذه المرحلة يتم إعداد التقرير بحيث يدون فيه جميع إجراءات البحث، و إذا كانت هناك ملاحق إيضاحية مصورة أو مسجلة ثم تسلم إلى جهة الحكم و القضاء.

3 ـ أدوات إستخلاص الأدلة الرقمية:

عادة ما توجد الأدلة الرقمية في مخرجات الطابعة و التقارير و الرسوم و في أجهزتها و ملحقاتها، و في الأقراص الصلبة و المرنة و أشرطة تخزين المعلومات، و في أجهزة المودام و البرامج و أجهزة التصوير و مواقع الواب و البريد الالكتروني, و لذلك نستخدم عدة طرق و أدوات لجمع الأدلة الرسمية منها :

أ. برنامج إذن التفتيش:

و هو برنامج قاعدة بيانات يسمح بإدخال كل البيانات الهاتفية الهامة المطلوبة لترقيم الأدلة و تسجيل البيانات منها ، و يمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة و البحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد طرق ضبط هذا الدليل.

[1] د. عائشة بن قارة مصطفى: مرجع سابق ص 149

ب.قرص بدء تشغيل الحاسوب :

و هو قرص يمكن المحقق من تشغيل الحاسوب إذا كان النظام التشغيل فيه محميا بكلمة مرور، و يجب أن يكون القرص مزودا ببرنامج مضاعفة المساحة، فربما كان المهتم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب .[1]

ت.برنامج معالجة الملفات :

وهو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة ، أو على القرص الصلب. و يستخدم لتقييم محتويات القرص الصلب. و يستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المحجوزة، أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

ث. **برنامج اتصالات** :

وهو برنامج يستطيع ربط جهاز المحقق بجهاز حاسوب المتهم لنقل ما به من معلومات و حفظها في جهاز نسخ معلومات ثم إلى القرص الصلب.[2]

[1] مصطفى محمد مرسي : مرجع سابق ص 219
[2] مصطفى محمد مرسي : مرجع نفسه ص 220

المبحث الثاني:

الإجراءات المستحدثة في تتبع الدليل الرقمي و الأجهزة المخصصة

تطرقنا في المبحث الأول إلى مجموعة الإجراءات التقليدية المتبعة في الحصول على الدليل الرقمي ، وهي المعاينة ، التفتيش ، الحجز ، الخبرة ، و الشهادة و رأينا كيف أن هذه الإجراءات لا تختلف في مدلولها القانوني في الجرائم التقليدية . غير أنها تختلف من حيث إنها تقتضي بعض الشروط لتتماشى مع طبيعة الدليل الرقمي الذي يفرض أسلوبا خاصا في التعامل معه.

كاشتراط المعرفة و الدراية بتقنية الحاسوب و الاتصال لإجراء المعاينة وكذا الخبرة التقنية اللازمة في التفتيش، وتميز الشاهد المعلوماتي بارتباطه بمسرح الجريمة، و تمديد الاختصاص للمحققين و القضاة و النواب . إلا أن هذه الإجراءات تبدو غير كافية أمام تنوع الدليل الرقمي وتنامي جرائم المعلوماتية العابرة للحدود و خطورتها على الأمن الدولي و الوطني .

وهذا ما حذى بالتشريعات بما فيها المشرع الجزائري إلى خلق قواعد قانونية إجرائية حديثة تعتمد بدورها على تقنية الحوسبة و الاتصال، لتجميع واستخلاص الدليل الرقمي، من خلال تسيير الإجراءات التقليدية أو خلق إجراءات مستحدثة قائمة بذاتها تستدعي هي الأخرى أجهزة متخصصة سواء على المستوى الوطني أو الدولي للكشف عن جرائم المعلوماتية و استخلاص الدليل الرقمي أو الوقاية منها.

لذلك سنتناول في المطلب الأول الإجراءات المستحدثة وهي : التسرب ، اعتراض المراسلات ، التي جاء بها القانون رقم 06 -22 . ومراقبة الاتصالات الالكترونية التي تضمن أحكامها القانون رقم 09 -04 . وفي المطلب الثالث نتكلم عن الأجهزة المتخصصة في تتبع الدليل الرقمي على المستوى الدولي و الوطني .

المطلب الأول :

الإجراءات المستحدثة في تتبع الدليل الرقمي

كما سبق وأن ذكرنا أن المشرع الجزائري جرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04 – 15 السالف الذكر، و لقصور الإجراءات التقليدية في إثبات هذه الجرائم أعقبه بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 06 – 22 .

مضيفا إجراءات جديدة لها دور كبير في كشف هذه الجرائم و إثباتها. وهي اعتراض المراسلات و تسجيل الأصوات و التقاط الصور في الفصل الرابع ، و التسرب في الفصل الخامس . ومع التوسع في مفهوم جرائم المعلوماتية لتشمل كل ما له علاقة بتقنية الحاسوب والاتصال . أضاف المشرع الجزائري المراقبة الالكترونية ووضح أحكامها بموجب القانون رقم 04- 09 ، كإجراء وقائي، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

هذه الإجراءات المستحدثة سنتطرق إليها فيما يلي :

الفرع الأول : التسرب

أولا : تعريف التسرب

عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 حيث جاء فيها : يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم في ارتكابهم جناية أو جنحة بايهامهم أنه فاعل معهم أو شريك أو خاف .

ثانيا : أحكام التسرب

نظم القانون التسرب في الفصل الرابع ، المواد من 65 مكرر 11 إلى 65 مكرر 18 [1] وضمنه الأحكام التالية :

1- أن يصدر الإذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية المختص وتحت رقابته، مكتوبا ، ومسببا لمدة أقصاها أربعة (04) أشهر قابلة للتجديد مرة واحدة لنفس الفترة حسب مقتضيات التحقيق و إلا كان باطلا ، ويجوز لوكيل الجمهورية في وقت يراه مناسبا وقف عملية التسرب [2] .

2- أن يتضمن الإذن الممنوح الجريمة التي تبرر عملية التسرب ، ويذكر فيه هوية ضابط الشرطة القضائية التي تتم عملية التسرب تحت مسؤوليته أو عون الشرطة القضائية باعتباره مساعدا له .

3- يجوز للضابط أو الأعوان الذي يعملون معه في عملية التسرب استعمال هوية مستعارة ولا يجوز بأي حال من الأحوال إظهار هويته الحقيقية لأي منهم في أي مرحلة من مراحل الإجراءات .

4- أن يستعمل وسائل الحيلة و التستر بغرض ضبط الفاعلين و المساهمين معهم. على ألا ترقى لمرتبة التحريض على ارتكاب جريمة طبقا للمادة 265 مكرر 12 في فقرتها 2 ، ومن الوسائل المستعملة :

ا - اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

ب – استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي ، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[3]

---

[1] عبد الله أوهايبية : مرجع سابق ص 181

[2] أنظر المواد من 65 مكرر 11 إلى 65 مكرر 18 ، من قانون الإجراءات الجزائية الجزائري.

[3] عبد الله أوهايبية : مرجع سابق ص 282.

5 - يحرر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب و كذا الأشخاص طبقا للمادة 65 مكرر 19 . [1]

6 – يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية . [2]

وحماية للمتسرب من الخطر ، وتفاديا لفشل عملية التسرب ، حظر المشرع الكشف عن هوية المتسرب الحقيقية في أي مرحلة من مراحل الإجراءات ، محددا العقوبة على من يقوم بذلك بالحبس من سنتين إلى خمس سنوات و بغرامة من 50.000 دج إلى 20.000 دج . كما نصت المادة 65 مكرر 12 .

هذا إلى جانب حماية الشهود و الضباط وحتى أهاليهم بموجب الأمر رقم 15 – 02. و أحاطه بقواعد صارمة وردت في الفصل السادس من قانون الإجراءات الجزائية تحت عنوان : حماية الشهود و الخبراء و الضحايا .

الفرع الثاني : اعتراض المراسلات و تسجيل الأصوات و التقاط الصور .

أولا : تعريف اعتراض المراسلات :

لم يعرف المشرع الجزائري الاعتراض ، و إنما نظمه في الفصل الرابع من قانون الإجراءات الجزائية بموجب القانون 06 – 22 المؤرخ في 20- 11 - 2006 لذلك سنورد تعريف المشرع الأمريكي: بأنه الحصول على محتويات الاتصال اللاسلكي أو الالكتروني أو الشفوي، وذلك باستعمال أي وسيلة الكترونية أو ميكانيكية أو أي وسيلة أخرى. [3]

(1) الماد ة من 65 مكرر13 ، من قانون الإجراءات الجزائية الجزائري.
(2) الماد ة من 65 مكرر18 ، من قانون الإجراءات الجزائية الجزائري
(3) حابت آمال : مرجع سابق.

ثانيا : أحكام اعتراض المراسلات و تسجيل الأصوات و التقاط الصور.

وردت هذه الأحكام في المواد 65 من مكرر 5 إلى 65 مكرر 10 .

1- كما جاء في المادة 65 مكرر فإن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من بين الجرائم التي تقتضي فيها ضرورات التحري فيها و لتحقيق القيام بهذا الإجراء مثله مثل التسرب .

بحيث يجوز لوكيل الجمهورية المختص و قاضي التحقيق أن يأذن بما يلي :

ا – اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية

ب – وضع الترتيبات التقنية التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية ، و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص ، وهذا يتم ولو خارج المواعيد المحددة في المادة 47 من قانون الإجراءات الجزائية في كل ساعة من ساعات النهار و الليل. و يعتبر علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

2 - يتضمن الإذن المذكور كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها و الأماكن المقصودة سكنية أو غيرها و الجريمة التي تبرر اللجوء إلى هذا الإجراء.

ويسلم الإذن مكتوبا لمدة أقصاها أربعة (4 أشهر) قابلة للتجديد حسب مقتضيات التحري أو التحقيق. [1]

3 – و في سبيل تحقيق الهدف المرجو من هذا الإجراء و هو كشف الجريمة و الحصول على دليل إثباتها أجاز المشرع لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له ، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر لكل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة

[1] ا الماد ة من 65 مكرر7 ، من قانون الإجراءات الجزائية الجزائري.

مكلفة بالمواصلات السلكية و اللاسلكية للتكفل بالجوانب التقنية لهذاالإجراء (المادة 65مكرر 8)

4-يتعين على الضابط القائم بهذه المهمة تحرير محضر بالعمليات التي تمت طبقا للمادة 65 مكرر5 ,من إعتراض و تسجيل المراسلات و على الترتيبات التقنية و التقاط الصور و التسجيل الصوتي أو السمعي البصري و أن يتضمن المحضر تاريخ و ساعة بداية و نهاية العمليات [1]

كما يجب على الضابط أن يصف أو ينسخ المراسلات أو الصور أو المحادثات المسجلة و المفيدة في إظهار الحقيقة في محضر يودع بالملف. بالنسبة للمكالمات الأجنبية تنسخ و تترجم عند الاقتضاء بمساعدة مترجم، يسخر لهذا الغرض كما تنص المادة 65 مكرر من نفس القانون.

الفرع الثالث: مراقبة الاتصالات الالكترونية

أولا: تعريف مراقبة الاتصالات الالكترونية

تأتي مراقبة الاتصالات الالكترونية كإجراء وقائي مستحدث يكمل إجراء اعتراض المراسلات، للوقاية من جرائم المعلوماتية ويسمح به بشروط معينة، و يتم بوضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية، و تجميع وتسجيل محتواها في حينها، و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية ؛ وهذا مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات. [2]

وقد عرف المشرع الجزائري الاتصالات الاكترونية في القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها في المادة 2 الفقرة 9 ، بأنها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية .

(1) عبد الله أوهايبية : مرجع سابق ص280 .

(2) المادة 3 من قانون رقم 09- 04 المؤرخ في 16 أوت 2009.

وعرفها في المرسوم الرئاسي رقم 15- 261 المؤرخ في 8 أكتوبر 2015 : بأنها كل تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة الكترونية . بما في ذلك وسائل الهاتف الثابت و النقال .[1]

و الملاحظ أن التعريف الثاني هو الأشمل من الأول، و الأكثر مواكبة للتطور التكنولوجي في وسائل الاتصال بما في ذلك الهاتف الثابت و النقال الذي أصبح يقدم خدمات كثيرة مشابهة للحاسوب كالاتصال بالانترنت و تصفح المواقع المختلفة ، و الاتصال عبر الفايبر، و الواتساب وغيرها..... و بالتالي يمكن أن يكون وسيلة أو بيئة لجرائم المعلوماتية.

ثانيا : الحالات التي يسمح بها بالمراقبة الالكترونية

أجاز المشرع الجزائري القيام بالمراقبة الالكترونية لتجميع و تسجيل محتواها في حينها ، كدليل رقمي لإثبات الجرائم في الحالات التالية :

1- للوقاية من الأفعال الموصوفة بجرائم الإرهاب و التخريب أو الجرائم الماسة بأمن الدولة.
2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
3- لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى النتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإكترونية.
4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[2]

[1] الجريدة الرسمية العدد53 المؤرخة في8 أكتوبر 2015..
[2] ا الماد ة من 65 مكرر7 ، من قانون الإجراءات الجزائية الجزائري. السابق الذكر.

ثالثا : إحكام المراقبة الالكترونية

كما رأينا أجاز المشرع الجزائري المراقبة الالكترونية في حالات خاصة ، تفرضها مقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية.ولم يعممها على كل الجرائم لما فيها من مساس لحرمة الحياة الخاصة للأفراد تخص سرية المراسلات و الاتصالات المضمونة دستوريا ، و المحمية قانونا ، لذلك أخضعها المشرع لأحكام خاصة :

1- لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة. و عندما يتعلق الأمر بالوقاية من الأفعال الموصوفة بالجرائم الإرهابية و التخريب و الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر .

2- الضباط المختصون بهذا الإجراء في جرائم الإرهاب و التخريب و الماسة بأمن الدولة هم المنتمون للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و يسلم الإذن، مدته 6 أشهر قابلة للتجديد ، و ذلك على أساس تقرير يبين الترتيبات التقنية المستعملة و الأغراض الموجهة لها ، أما الجرائم الأخرى تخضع للأحكام المنصوص عليها في قانون الإجراءات الجزائية . [1]

3- يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ، و التي يطلق عليها البيانات المتحركة .

4- التزام مقدمي الخدمات بحفظ المعطيات المتعلقة بالسير ووضعها تحت تصرف السلطات المكلفة بالتحريات القضائية و تشمل :

ا - المعطيات التي تسمح بالتعرف على مستعملي الخدمة .

[1] حابت آمال : مرجع سابق.

ب - المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال .

ج - الخصائص التقنية و كذلك تاريخ ووقت و مدة كل اتصال.

د - المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها .

ه - .المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال ، و كذا عناوين المواقع المطلع عليها .

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، و كذلك التي تسمح بالتعرف على مصدر الاتصال و تحديد مكانه. و يحدد مدة حفظ المعطيات المحددة بسنة واحدة من تاريخ التسجيل.

وفي حالة عرقلة سير التحريات يعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات و غرامة مالية من 50.000 دج إلى 500.000 دج و يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات .

5 - يتعين على مقدمي خدمات الأنترنت ؛ التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة ما مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن .

مع وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام و الآداب العامة ، و إخبار المشتركين لديهم بوجودها . [1]

[1] أنظر المادتين 10، 11 من القانون رقم 09- 04.

المطلب الثاني:
الأجهزة المتخصصة في تتبع الدليل الرقمي

نتيجة لخصوصية الدليل الرقمي، و لجرائم المعلوماتية العابرة للحدود الجغرافية للدول، وأمام تنامي ظاهرتها و خطورتها على الأمن الداخلي و الدولي. لجأت أغلب التشريعات و منها التشريع الجزائري، إلى استحداث أجهزة متخصصة للتسهيل و الإسراع بتجميع الأدلة الرقمية في سبيل مكافحة هذا النوع من الإجرام سواء على المستوى الداخلي أو الدولي في إطار التبادل القضائي بين الدول.

نجد على المستوى الدولي أجهزة كثيرة أهمها جهاز الشرطة الدولية- الأنتربول - و شبكة الطوارئ الدولية التي أنشئت بموجب اتفاقية بودابست. و على المستوى الداخلي نجد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها التي أنشئت بموجب القانون رقم 09-04 ، وحدد تشكيلتها و تنظيمها و كيفيات سيرها المرسوم الرئاسي رقم 15-261 ، طبعا إلى جانب مخابر أخرى لاستخلاص الدليل الرقمي على مستوى جهاز الأمن و جهاز الدرك الوطني، وهذا ما سنتطرق إليه فيما يلي:

الفرع الأول : على المستوى الدولي و العربي

أولا: الأنتربول

الأنتربول أو الشرطة الدولية، هو جهاز يضم 188 دولة عضو منها الجزائر، و توجد مكاتب الأنتربول في الجزائر. - يجمع الأنتربول المعلومات عن جرائم المعلوماتية و يحفظها و يحللها و يتبادلها مع جميع بلدانه الأعضاء عبر منظومة الأنتربول العالمية للإتصالات.

- ينظم الأنتربول مرة كل عامين مؤتمرا دولي بشأن الإجرام المعلوماتي يدرس فيه ما يلي:

1. تيسير التعاون الدولي بين البلدان الأعضاء من خلال إعداد لائحة بأسماء ضباط اتصال ميسرين على مدار الساعة للمساعدة في التحقيقات بشأن الإجرام المعلوماتي.

2. زيادة تبادل المعلومات بين البلدان الأعضاء و بيان الأساليب الجرمية المتبعة في الإجرام المعلوماتي عن طريق حلقات العمل الإقليمية.

3. مساعدة الدول الأعضاء في التحقيق في الهجمات و غيرها من الجرائم المعلوماتية عبر تيسير خدمات في مجال التحقيق و قواعد البيانات.

4 - إبرام شراكات إستراتيجية مع منظمات دولية أخرى و هيئات القطاع الخاص... [1]

ثانيا: شبكة الطوارئ الدولية وفق إتفاقية بودابست

أنشئت بموجب إتفاقية بوداست التي سبق الإشارة إليها بنص المادة 35: يطلق عليها شبكة 7/24 ، و هي شبكة طوارئ دائمة لتفعيل المساعدة المتبادلة، تعمل على مدى 24 ساعة وبمعدل 7 أيام في الأسبوع بغرض التأكد من توفير المساعدة الفورية لإجراء التحقيقات المتعلقة بالجرائم الجنائية المرتبطة بنظم و بيانات معلوماتية أو لتجميع أدلة تثبيت ذات شكل إلكتروني لجريمة جنائية.... [2]

و يطلق عليها أيضا شبكة الثمانية، لأن أصل الفكرة يرجع إلى قرار الدول الثمانية الكبار إقامته نقطة مراقبة دائمة للأنترنت تعمل 24 ساعة على 24 ساعة تقوم بإعطاء إنذار بمجرد تسرب أحد القراصنة إلى الشبكة، و بمجرد إطلاق صفارة الإنذار تتحرك على الفور نخبة من خيرة الأخصائيين في عالم الأنترنت لتحديد مكان المشتبه فيه بإتباع أثره الإلكتروني، وفقا لمجال نشاطه الإجرامي .[3]

وجاء في نص المادة 35 من اتفاقية بودابست:

1. يجب على كل طرف أن يجد نقطة اتصال العمل على مدار 24 ساعة يوميا، و بمعدل 7 أيام في الأسبوع لغرض التأكد من توفير المساعدة الفورية، من أجل إجراء التحقيقات المتعلقة بالجرائم الجنائية المرتبطة بنظم و بيانات معلوماتية، أو لتجميع أدلة ذات شكل إلكتروني لجريمة جنائية وهذه المساعدة يجب أن تكون مشتملة على تسهيل ، أو إذا كان مسموحا وفقا للقانون الداخلي أو التطبيق العملي للقيام المباشر بالإجراءات التالية:

---

(1) نشره اعلامية للانتربول ، موقع الانتربول اطلع عليه يوم 07/ 04/ 2017.

(2) أ د هلالي عبد الله أحمد : مرجع سابق ، ص19.

(3) ادريس فرض : مرجع سابق ، ص19.

- تقديم المنشورات التقنية.
- التحفظ على البيانات وفقا للمادتين 29-30.
- تجميع أدلة و تقديم معلومات ذات طابع قانوني، وتحديد أماكن المشتبه فيهم.

2. . يجب أن تكون نقطة الاتصال الخاصة بطرف ما لديها القدرة على إجراء الاتصالات مع نقطة اتصال لطرف آخر على وجه السرعة.

- . إذا كانت نقطة الاتصال المحددة بواسطة طرف ما لا تعتمد على سلطة أو سلطات هذا الطرف المسؤولة عن المساعدة الدولية، أو تبادل تسليم المجرمين، فإنه يجب عليه أن تكون قادرة على التعاون مع هذه السلطة أو السلطات على وجه السرعة.

3- يجب على كل طرف أن يكون لديه طاقم مدرب و مزود بالأجهزة التي تسهل عملية تشغيل الشبكة. و الملاحظ أن أغلب الدول استندت في قوانينها الداخلية على اتفاقية بودابست وإن لم تكن طرفا فيها، مثل الجزائر التى أنشأت لهذا الغرض الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، و التي سنتطرق إليها لاحقا. و أيضا نفس الفكرة استمدتها الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 2010/12/21 التي نصت على إنشاء جهاز متخصص سنتطرق إليه فيما يلي:

ثالثا: جهاز متخصص وفق إتفاقية القاهرة

تم على مستوى جامعة الدول العربية التوقيع على الإتفاقة العربية لمكافحة جرائم تقنية المعلومات بتاريخ 2010/12/21 بالقاهرة، و صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 16-252 السالف الذكر المؤرخ في 2014/09/28 [1].

حيث نصت بموجب المادة 42 على إنشاء جهاز متخصص من أجل تعزيز التعاون ، و المساعدة الثنائية بين الدول الأطراف بخصوص الجمع الفوري لمعلومات تتبع المستخدمين أيضا فيما يخص الجمع الفوري لمحتوى اتصالات معينة تبث بواسطة تقنية المعلومات، حيث جاء في المادة 42:

[1] الجريدة الرسمية العدد 57 المؤرخة في 28/ 09/ 2014.

1. تكفل كل دولة طرف وفقا للمبادئ الأساسية لنظامها القانوني وجود جهاز متخصص و متفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الإلكتروني في جريمة معينة، و يجب أن تشمل مثل هذه المساعدة، تسهيل و تنفيذ:

أ. توفير المشورة التقنية.

ب. حفظ المعلومات إستنادا للمادتين السابعة و الثلاثين و الثامنة و الثلاثين .

ت. جمع الأدلة وإعطاء المعلومات القانونية و تحديد مكان المشبوهين.

2. أ- يجب أن يكون لدى ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة.

.ب - إذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزء من سلطات تلك الدولة الطرف المسؤولة على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة.

3- على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز المذكور أعلاه [1]

و الملاحظ على نحو هذه المادة أنه متوافق مع ما جاء في المادة 35 من إتفاقية بودابست. الفرق أن الأولى نصت على جهاز متخصص في الدول الأعضاء في الجامعة العربية. و الثانية نصت على شبكة طوارئ دولية لأن إتفاقية بودابست مفتوحة لكل دول العالم، وكلتا المادتين لم تحدد هذا الجهاز إن كان تابعا للشرطة أو الدرك أو إداري أو مستقل.

الفرع الثاني : على المستوى الوطني

أولا: جهاز الدرك الوطني ، المعهد الوطني للأدلة الجنائية و علم الاجرام

يوجد المعهد الوطني للأدلة الجنائية و علم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني [1] و يتكون من إحدى عشرة (11) دائرة متخصصة في مجالات مختلفة تضمن إنجاز:

[1] أنظر المادة 42 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الجريدة الرسمية العدد 57 المؤرخة في 2014/09/28.

- الخبرة
- التكوين و التعليم
- تقديم المساعدات.
- البحوث، الدراسات و التحاليل في علم الجريمة.

و من بين هذه الدوائر:_**دائرة الإعلام الآلي و الإكتروني** التي لها علاقة بموضوع دراستنا سنتعرف على مهامها وتنظيمها من خلال البطاقة التقنية التالية:

1 - مهام دائرة الاعلام الآلي و الإلكترونيك:

تقوم دائرة الاعلام الآلي و الإلكترونيك بالمهام التالية:

- معالجة تحليل و تقديم كل دليل رقمي و تماثلي للعدالة.
- تقديم المساعدة التقنية للمحققين في التحقيقات المعقدة التجهيزات.

- السهر على تأمين اليقظة التكنولوجية من أجل تحسين المعارف، التقنيات و الطرق المستعملة في مختلف الخبرات العلمية.

2- تنظيم دائرة الإعلام الآلي و الإلكترونيك:

لإنجاز المهام المنوطة بها تنقسم دائرة الإعلام و الإلكترونيك إلى ثلاثة مخابر و ذلك حسب نوع المعلومات (سمعية، بصرية، إعلام آلي)و هي:

- مخبر الإعلام الآلي
- مخبر الفيديو
- مخبر الصوت

فيما يلي سنتعرف على مهام كل مخبر و تجهيزاته و قاعاته

(1) مسار التحقيقات الجنائية، في مجال الجريمة المعلوماتية ، عرض مقدم من طرف ضابط المعهد الوطني ، للأدلة الجنائية و علم الإجرام ، الملتقى الوطني حول الجريمة المعلوماتية من الوقاية و المكافحة ، جامعة بسكرة يومي 16-17 نوفمبر 2015.

أ ـ مخبر الإعلام الآلي:

01 ـ المهام:

- تحليل و معالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش).
- تحديد التزوير الرقمي للبطاقات البنكية.

02- **التجهيزات:**

- محطة ثابتة و حمولة لإجراء خبرات الإعلام الآلي.
- جهاز إقتناء معلومات الهواتف و الحواسب.
- محطة ترميم و تصليح الأجهزة و الحوامل المعطلة.
- الخبرات الإعلامية(خبرات الإعلام الآلي و التجهيزات البنائية).

03- القاعات:

]يحتوى مخبر الإعلام الآلي على 07 قاعات وهي:

- مكتب التوجيه
- فصيلة الأنظمة المشحونة
- فصيلة تحليل المعطيات
- فصيلة الهواتف
- فصيلة اقتناء المعطيات
- قاعة موزع
- قاعة تخزين

ب ـ مخبر الفيديو:

01- المهام:

- إعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد.
- تحسين نوعية الصورة (فيديو، صور) بمختلف التقنيات.
- مقارنة الأوجه و شرعية الصور و الفيديو.
- السهر على تأمين اليقظة التكنولوجية من أجل تحسين المعارف، التقنيات و الطرق المستعملة في مختلف الخبرات العلمية.

02- التجهيزات:

- مجموعة أجهزة لقراءة مختلف حوامل الفيديو الرقمية و الممغنطة.
- جهاز فيديو بوكس.
- حبكات إعلامية (كونيتك ستديو ، ماكس ثلاثة أبعاد).
- موزع لحفظ شرائح الفيديو.

03- القاعات:

يحتوي مخبر الفيديو على أربع قاعات:

- قاعتان للتحليل
- قاعة تخزين
- قاعة موزع

ج ـ مخبر الصوت :

01- المهام:

- تحسين نوعية إشارة الصوت بنزع التشويش و تعديل السرعة.
- معرفة و تحديد المتكلم.
- تحديد شرعية التسجيلات.

02- التجهيزات

- أجهزة الإزدواجية و السماع.
- حيكات إعلامية (معالجة و تحسين التسجيلات الصوتية، نسخ الأقراص المضغوطة
- أجهزة التصليح و التغيير.

03- القاعات:

يحتوي مخبر الصوت على خمس قاعات.

- ثلاث قاعات للتحليل.
- قاعة تخزين.
- قاعة موزع.

كانت هذه بطاقة تقنية لدائرة الإعلام الآلي و الإلكترونيك التابعة للمعهد الوطني للأدلة الجنائية و علم الإجرام ببوشاوي (الجزائر العاصمة) عرفنا فيها مهام و تجهيزات مخابر هذه الدائرة اللازمة لإستخلاص الدليل الرقمي في جرائم المعلوماتية. على المستوى المركزي.

و بالإضافة إلى **المعهد الوطني للأدلة الجنائية و علم الإجرام**، يوجد **مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية و مكافحتها** ببئر مراد رايس، و التابع لمديرية الأمن العمومي للدرك الوطني (CPLCIC).

و هذا المركز هو الذي يتم التعامل معه من طرف مجموعة الدرك الوطني لولاية بسكرة في حالات جرائم المعلوماتية و استخلاص الدليل الرقمي بالخصوص. و هذا حسب تصريح رئيس مكتب الشرطة القضائية بالمجموعة [1].

حيث توجد 29 فرقة للدرك الوطني موزعة على كامل تراب ولاية بسكرة (باستثناء 3 بلديات هي: مخادمة، بوشقرون، عين زعطوط)، لتسهيل تقديم الشكاوى من المواطنين ومهام الفرقة حسب نفس التصريح: شرطة، إدارية، عسكرية و قضائية. و عن الإجراءات يقول رئس مكتب الشرطة القضائية بمجموعة الدرك الوطني لولاية بسكرة.

[1] لقاء تم يوم 20 مارس 2017، لمعرفة الواقع العملي لكيفية التعامل مع جرائم المعلوماتية ، و بالخصوص الدليل الرقمي.

- عندما توصل الفرقة بجريمة يتم الاتصال بوكيل الجمهورية و بالمسؤولين في المجموعة للإعلام.
- وحسب نوع و حجم الجريمة يتم معالجتها على مستوى الفرقة أو من طرف فصيلة الأبحاث.
- في البداية سماع القضية في دفتر التصريحات.
- تحرير محضر يرسل إلى وكيل الجمهورية الذي قد يطلب تقريرا إخباريا(في حالة جريمة هامة.)
- بالنسبة للمعاينة يتم تجميد مسرح الجريمة من طرف فصيلة الشرطة العلمية.
- بالنسبة للتفتيش أو مراقبة الموقع يكون بطلب ترخيص من وكيل الجمهورية.

كما يرسل إذن متابعة إلى رئيس المركز فيه ملخص القضية، و يحدد فيه الهدف من المتابعة، و الذي يعطي بروتوكول الأنترنت (Ip).

- وحسب طلب مركز رئيس الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية و على دقتها يتم حجز و تشميع الموجودات مثل القرص الصلب، و كل ما يتعلق بالجريمة محل المتابعة، و يتم إرسالها إلى المركز لتحليلها و استخلاص الدليل الرقمي منها لإثبات الجريمة.

و هذه بعض **الإحصائيات على المستوى الوطني:**

عالج مركز الوقاية من الجرائم و مكافحتها 500 قضية تتعلق بالجريمة الإلكترونية خلال سنة 2016، مقابل 240 قضية في سنة 2015 ، ويتعلق بالمساس و الإعتداء على الحياة الخاصة للأشخاص. وهذا حسب ما ذكره عقيد مختص بالجانب القانوني للجريمة المعلوماتية بالمركز، و هذا على هامش أشغال ندوة وطنية حول الجريمة المعلوماتية و أمن المنظمة بجامعة محمد بوضياف للعلوم و التكنولوجيا بوهران [1].

و نلاحظ هنا تزايد عدد هذا النوع من الجرائم إلى أكثر من الضعف من سنة 2016 و 2015 ، من 240 إلى 500 قضية، وهي في تزايد مستمر و دائم مما يقتضي تكثيف الجهود لمكافحتها.

[1]. مقال منشور لجريدة الشروق الالكترونية :بتاريخ 07 / 12/ 2016 على الموقع WWW.Echer com اطلع عليه يوم 2017 /07/14

ثانيا: جهاز الشرطة، المخبر المركزي للشرطة العلمية.

- أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة.ومخبرين جهويين في كل من قسنطينة ووهران.
- تم خلال سنة 2007 تدعم هذه المخابر بأقسام متخصصة في الأدلة الرقمية، تكمن مهامها في استغلال الأجهزة الإلكترونية التي يشتبه استعمالها في ارتكاب الجرائم بهدف استخلاص الأدلة الرقمية [1].
- و على المستوى الولائي توجد فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر.
- و في ولاية بسكرة توجد **فرقة مكافحة الجرائم المعلوماتية** بالمصلحة الولائية للشرطة القضائية بمديرية الأمن الولائي لولاية بسكرة، تقربنا لمعرفة الواقع العملي للتعامل مع جرائم المعلوماتية و كيفية متابعتها و استخلاص الدليل الرقمي منها و كذا طلب إحصائيات، و كان لقاؤنا مع المكلف بالإعلام الذي أحجم عن الإجابة و اكتفى بتقديم طلب للمركزية في انتظار الرد بالتصريح بالإجابة . .....؟؟؟؟

و في غياب الرد إلى غاية كتابة هذه السطور لجأنا إلى حوار سجلناه من إذاعة الجزائر الجهوية من بسكرة حول جرائم المعلوماتية مع نفس ضباط الشرطة [2].
وجمعنا المعلومات التالية:

1- في سؤال عن **كيفية اكتشاف الجريمة المعلوماتية** ؟ أو طريقة العلم بالجريمة ؟

إجابة رئيس الفرقة: عندنا عناصر متخصصة تراقب مختلف مواقع التواصل الاجتماعي و مواقع الأنترنت الأخرى، وأيضا المصلحة المركزية تقوم بالمراقبة المستمرة و الدائمة، و تبلغنا إذا كانت في إدارة إختصاصنا، و تكون معالجة القضايا عن طريق التنسيق مع النيابة العامة بمحكمة بسكرة، وأيضا عن طريق التبليغ من طرف المواطنين عن طريق الإنترنيت. و المديرية العامة للأمن الوطني وضعت حيز الاستغلال تطبيقا يعمل من الموقع المعروف Playstore اسمه ألو شرطة Allo chorta، يوفر التبليغ الآني و السريع لأي

(1). لقاء تم يوم 20 مارس 2017، لمعرفة الواقع العملي لكيفية التعامل مع جرائم المعلوماتية ، و بالخصوص الدليل الرقمي.
(2). حصة حوار مفتوح : إذاعة الجزائر الجهوية من بسكرة ، تاريخ البث : 22مارس 2017.

معلومة ، إذا تقدم مباشرة لأقرب مركز أمن من أجل تسهيل الإجراءات في إطار الشرطة الجوارية.

وأعطى رئيس الفرقة مثالا على مواطنة تقدمت شخصيا إلى الفرقة من أجل التبليغ عن صفحة في مواقع التواصل الاجتماعي الفيسبوك تقوم بالترويج لحبوب الإجهاض، ثم الإشهار لها على أنها حبوب تنظم الحمل وهي في الحقيقة للإجهاض ، و تم بيعها بمبالغ خيالية (10000 دج) . و بناء على هذا التبليغ قمنا بالتحقيق و تم توقيف الفاعلين و تقديمهم أمام العدالة و إيداعهم السجن.

2- في سؤال عن **نوع القضايا المعالجة** ذكرالمساس بحرية الحياة الخاصة، و منها :

- انتحال شخصية الغير في الفيسبوك عن طريق إنشاء صفحات على مواقع التواصل الاجتماعي تحمل نفس المعلومات الشخصية عن الشخص المراد انتحال شخصيته لإيهام الناس أنه هو نفسه هذا الشخص بهدف استغلالهم و ابتزازهم.
- أيضا نشر صور، مقاطع فيديو للأشخاص دون إذنهم.

و الدخول عن طريق الغش لمنظومة المعالجة الآلية للمعطيات، أو ما يعرف بالقرصنة سواء البريد الإلكتروني أو الفيسبوك أو غيرها من مواقع التواصل الاجتماعي.، نشر الإباحية، قضايا النصب و الإحتيال عبر مواقع التواصل الاجتماعي.، جرائم الإفادة بالجرائم الإرهابية.

و **الجرائم العقائدية**: منها : قضايا تمس بالعقيدة الإسلامية ، و قضايا تمس المنهج الوسطي للإسلام، وقضايا التشهير بالمسيحية أو بالديانات الأخرى حتى الديانات الوثنية.

وأحصى 5 قضايا في سنة 2016 من هذا النوع، و في ثلاثة أشهر الأولى من سنة 2017 ثلاث قضايا التشهير بالمسيحية، العقيدة الأحمدية، وقضايا أخرى تمس العقيدة الإسلامية (قيد التحقيق).

3- وعن **الإحصائيات على مستوى الولاية:**

يقول رئيس الفرقة أن كل القضايا تمت معالجتها ، و لا توجد قضية ضد مجهول و أعطى الإحصائيات التالية على مستوى الفرقة:

2015 ⟸ 15 قضية

2016 ⟸ 52 قضية

2017 ⟸ في الشهرين الأولين أكثر من 15 قضية

و الملاحظ أنها في تزايد مع الأخذ بعين الإعتبار أن أغلب الضحايا يلتزمون الصمت بعدم التبليغ. ما يجعل من مهمة التحسين و النوعية أكثر من ضرورة لتسهيل اكتشاف هذه الجرائم و ردع الفاعلين، لأن جرائم المعلوماتية تعتبر أخطر الجرائم لما تسببه من أضرار اجتماعية، فهي تؤثر على القيم الاجتماعية في الأسرة من خلال الإستخدام السلبي للأنترنت. كما أضاف المكلف بالإعلام بالفرقة.

أما **الإحصائيات على المستوى الوطني** فتحصلنا عليها من موقع الشرطة الجزائرية مع الأنترنت محتواها في الجدول التالي:

ولتبيان تنامي ظاهرة جرائم المعلوماتية نورد فيما يلي إحصاءات لهذه الجرائم، سجلتها مصالح المديرية العامة للأمن الوطني المتخصصة في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال خلال الـ 08 أشهر الأولى من سنة 2016 حيث بلغ عددها 567 تورط فيها 543 شخصا، تمت معالجة 385 جريمة [1].

[1]. إحصائيات نشرت بتاريخ 2/12/ 2016 بموقع الشرطة الجزائرية ccp-djs@algeriepolice.dz اطلع عليه يوم 23/03/ 2017

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الأنترنيت	430	289	365	68%
جرائم الإعتداء على سلامة الأنظمة المعلوماتية	57	31	39	55%
جرائم الإحتيال عبر الأنترنيت	25	17	32	68%
جرائم التحريض و التطرف عبر الأنترنيت	14	14	31	100%
الجرائم المخلة بالحياء	12	08	22	67%
جرائم بيع السلع المحظورة عبر الأنترنيت	06	05	15	84%
جرائم مختلفة (نسخ البرامج دون حق القرصنة)	23	21	39	92%
المجموع	567	385	543	68%

ثالثا : جهاز الإدارة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام و الاتصال و مكافحتها

هذه الهيئة هي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي مقرها الجزائر العاصمة لدى وزير العدل. أنشئت تطبيقا لنص المادة 13 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها [1] و بموجب المرسوم الرئاسي رقم..15-261 المؤرخ في 8 أكتوبر 2015 [2] الذي يحدد تشكيلها و تنظيمها و كيفيات سيرها .

[1] الجريدة الرسمية العدد 47 المؤرخة في16 أوت 2009.
[2] الجريدة الرسمية العدد 53 المؤرخة في 8 أكتوبر 2015.

2 - مهام الهيئة :

حسب نص المادة 14 من القانون السالف الذكر تكلف الهيئة بالمهام التالية:

أ- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

ب-مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية.

ت-تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تحديد مكان تواجدهم[1]

ث-ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و المساس بأمن الدولة تحت سلطة القاضي المختص و باستثناء أي هيئات وطنية أخرى.

ج- تجميع و تسهيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل استعمالها في الإجراءات القضائية.

د- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام و الاتصال .

ج- تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

هذا و الهيئة مكلفة أيضا بالمساهمة في تحديث المعايير القانونية في مجال تخصصها و باقتراح الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها. [2]

[1]. أنظر المادة 14 من القانون رقم : 09- 04

[2]. المادة 4 من المرسوم الرئاسي رقم 15- 261

3- تشكيلة الهيئة:

وفق نص المادة 6 من المرسوم الرئاسي رقم 15-261 فإن الهيئة تضم :

- لجنة مديرة.
- مديرية عامة .
- مديرية عامة للمراقبة الوقائية و اليقظة الالكترونية.
- مديرية التنسيق التقني.
- مركز للعمليات التقنية.
- ملحقات جهوية.

ونص المرسوم الرئاسي على تزويد الهيئة بقضاة وضباط و أعوان الشرطة القضائية من المصالح العسكرية للاستعلام و الأمن، و الدرك الوطني و الأمن الوطني، يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل و الدفاع الوطني و الداخلية.

وأيضا لمستخدمي الدعم التقني و الإداري على أن يتم جلبهم من ضمن مستخدمي المصالح العسكرية للاستعلام و الأمن، و الدرك الوطني، و الأمن الوطني. كما يمكن أن تستعين الهيئة بأي خبير أو أي شخص يمكن أن يعينها في أعمالها [1] . ومن صلاحيات الهيئة أنها مؤهلة لكي تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لانجاز المهام المسندة إليها. ونظرا لأهمية اللجنة المديرة، وكذا مديرية المراقبة الوقائية و اليقظة سنتكلم عنهما فيما يلي:

أ- اللجنة المديرة:

من مهام هذه اللجنة توجيه عمل الهيئة و الإشراف عليه ومراقبته، و كذلك ضبط برنامج عمل الهيئة و تحديد شروط و كيفيات تنفيذه. ونظرا لأهمية هذه الهيئة أوكل المشرع رئاستها إلى الوزير المكلف بالعدل ومن أعضائها:

[1] المادتان 18 و19 من المرسوم الرئاسي رقم 15- 261.

-الوزير المكلف بالداخلية.

-الوزير المكلف بالبريد و تكنولوجيات الإعلام و الاتصال.

بالإضافة إلى قائد الدرك الوطني ، المدير العام للأمن الوطني، كما تضم ممثل عن كل من رئاسة الجمهورية ووزراء الدفاع الوطني و قاضيان من المحكمة العليا.[1]

ب-مديرية المراقبة الوقائية و اليقظة الإلكترونية :

من أهم مهامها :

1. تنفيذ عمليات المراقبة للاتصالات الالكترونية من اجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال بناء على رخصة مكتوبة من السلطة القضائية و تحت مراقبتها.
2. جمع و مركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المعلوماتية.
3. وضع مركز العمليات التقنية و الملحقات الجهوية قيد الخدمة و السهر على حسن سيرها.[2]

كما تقوم المديرية بتنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة و جمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، و أيضا تنفيذ توجيهات اللجنة المديرة.

مما تقدم نستشف إدراك المشرع الجزائري لخطورة جرائم المعلوماتية، و ضرورة مكافحتها من خلال سن قواعد موضوعية و أخرى إجرائية تواكب التطور التكنولوجي من أجل الكشف عن هذه الجرائم، و إنشاء أجهزة متخصصة في جمع و استخلاص الدليل الرقمي. على غرار الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، التي يرأسها وزير العدل و تضم من بين

[1]. المادتان 20 من المرسوم الرئاسي رقم 15- 261

[2]. المادتان 11 من المرسوم الرئاسي رقم 15- 261

أعضائها وزير الداخلية ووزير البريد وتكنولوجيات الإعلام والاتصال . ومن تشكيلتها مديرية المراقبة و الوقاية و اليقظة الالكترونية.

وتبقى اليقظة الالكترونية هي المطلوبة في التصدي للجرائم المعلوماتية.

الفرع الثالث :أشهر الجرائم المعلوماتية

أولا: قضايا في الجزائر

1- الحرب الالكترونية بين مصر و الجزائر:

تعد الحرب الالكترونية بين مصر و الجزائر من أشهر القضايا التي ظهرت في 2009 على اثر مباريات كرة القدم عندما تأهل الفريق الوطني على حساب الفريق المصري في تصفيات كأس العالم.

كانت البداية عندما تعرضت منتديات الشروق اليومي لهجوم من قراصنة مصريين وكشف الهاكرز، و تحول الصراع الكروي بين الجزائر و مصر إلى حرب مفتوحة على الشبكة العنكبوتية، من خلال استهداف المواقع الجزائرية، موجهين تحذير لنظرائهم الجزائريين ، ردا على اختراق موقعي وزارتي الإعلام و الإنتاج المصريين. حيث قام أحد الهاكرز الجزائريين باختراق موقع الرئاسة المصرية، بعدما قام في البداية بتعطيل موقع صحيفة الأهرام المصرية . [1]

2- قضية بنك التنمية المحلية بسكرة:

وقعت قضية بنك التنمية المحلية بسكرة في سنة 2010 حول اختلاس أموال عمومية، و التزوير، و استعمال المزور، و إدخال معطيات في نظام المعالجة الآلية ، بإزالة و تعديل عن طريق الغش و النصب و الاحتيال. [2] وقد نتج عنه سحب أموال من حساب سيدة متوفية.

[1] جريدة الشروق الجزائرية: العدد 2725 صادرة بتاريخ 29/ 11/ 2009

[2] قرارصادر عن غرفة الاتهام: مجلس قضاء بسكرة، رقم الجدول 00469 / 10، رقم الفهرس 00465 / 10 تاريخ القرار 19 / 07/ 2010 .

3 ـ قضية تهديد عن طريق SMS :

وقعت قضية تهديد و الإساءة إلى الإسلام ، و الرسول صلى الله عليه و سلم،عن طريق الرسالة الالكترونية SMS بالهاتف النقال تعو د تفاصيلها الى 09/ 12/ 2010 . [1] وقد سبق الإشارة إليها في الأسباب الشخصية لاختيار الموضوع.

3 ـ قضية قرصنة الحساب :

تفاصيل هذه القضية جرت في هذه السنة (2017) حيث قام شاب بقرصنة حساب فيسبوك لفتاة و نسخ صورها التي كانت تتبادلها بين أصدقائها ضمن الدردشة الخاصة ، و استعمالها في ابتزاز هذه الفتاة و تهديدها بنشرها إن لم تخضع لطلباته. [2]

ثانيا: قضايا دولية :

نذكر هنا أول هجوم فيروسي وكان في سنة 1988 ، و آخر هجوم فيروسي في 12 ماي 2017 .

و في البداية نعرف الفيروس و هو عبارة عن برنامج حاسوب مثل أي برنامج تطبيقي ، و لكن يتم بواسطة أحد المخربين بهدف محدد وهو إحداث أكبر تلف ممكن بنظام الحاسوب ، و من أهم خصائص الفيروسات ، الاختفاء و التدمير ، الاختراق، العدوى. [3]

1- دودة موريس (Worm Moris) :

كان أول هجوم فيروسي في سنة 1988، ويدعى هذا الفيروس باسم (Worm_ Moris) أي دودة موريس نسبة إلى صاحبها كان روبرت تابان موريس وهو مدرس في معهد ماسا تشوستش للتكنولوجيا أول من اخترع دودة الأنترنت [4] .

دودة موريس تم إرسالها أول مرة من حواسيب معهد التكنولوجيا بجامعة ماسا تشوستش ، قامت الدودة بنسخ نفسها على آلاف الحواسيب في عدد من الساعات، كما تسببت

---

[1] حكم صادر عن محكمة بسكرة، قسم الجنح، رقم الجدول: 01721 / 11، رقم الفهرس: 1936 / 11 بتاريخ 03/14/ 2011 .

[2] المصدر :أمن ولاية بسكرة، فرقة المعالجة الجريمة المعلوماتية، حوار مفتوح إذاعة الجزائر الجهوية ـ بسكرة ـ

[3] أمير فرج يوسف: مرجع سابق، ص 14.

[4] أمال قارة: الحماية الجزائية المعلوماتية في التشريع الجزائرى، دار هومة، الجزائر، 2007، ص 10.

بخسائر كبيرة بأنظمة الحاسوب و ماتحتويه من معلومات ، مما عجل في تحرك عدد كبير من المبرمجين لكي يوقفوا الهجوم الفظيع.

و استمرت عملية الإصلاح عددا من الأيام لتسوية الوضع نسبيا، وقدرت قيمة تصليح الحواسيب التي التقطت العدوى بـ 200 و 53 ألف دولار . و لما وجدت المحكمة موريس مخطئا حكمت عليه بالمراقبة لمدة 3 سنوات و 400 ساعة في خدمة المجتمع و 10050 دولار غرامة.

1- دودة الفدية (Ramson Ware) :

هو نوع من الفيروسات تصيب الأجهزة العاملة بنظام التشغيل الويندوز(XP) استهدف يوم الجمعة 12 ماي 2017 آلاف المؤسسات و الأفراد عبر العالم في أ كبر عملية قرصنة في التاريخ. قدرت عدد الضحايا بـ 200 ألف ضحية، أغلبها شركات في 150 بلدا على الأقل. وحسب تصريح مدير الشرطة الأوربية "**اليوروبول** " جاء فيه: " نقوم بعمليات للتصدي لنحو 200 هجوم معلوماتي سنويا ، و لكننا لم نر مثل هذا الهجوم من قبل."

و برنامج الفدية يستعمل ثغرة في نظام الويندوز ، ليقوم بمنع المستخدم من فتح برامجه، و يجبره على دفع مبلغ من المال قيمته 300 دولار لاستعادتها ، وتدفع الفدية بالعملة الافتراضية بيتكوين. [1]

كذلك يطالب القراصنة بدفع الفدية في غضون ثلاثة أيام و إلا فإن المبلغ سيزداد إلى الضعف، أما إذا لم يدفع الضحية بعد سبعة أيام فسيتم محو الملف. و لصد هذا الهجوم الالكتروني الرهيب ، يجرى خبراء المعلوماتية و المحققون تحقيقات مكثفة و عاجلة للبحث عن آثار القراصنة و كشفهم. وهذا يتطلب تعاونا دوليا فعالا وجادا، ويعبر هذا الهجوم عن خطورة جرائم المعلوماتية في كل أنحاء العالم.

[1] منشور على الموقع WWW.France24. com يوم 2017 /05/14 و اطلع عليه في نفس اليوم.

بعد نهاية هذه الدراسة المتواضعة حول تتبع الدليل الرقمي في جرائم المعلوماتية في التشريع الجزائري نأمل أن نكون قد وفقنا في الإجابة عن الإشكالية المطروحة، فيما يخص الآليات التي سخرها المشرع الجزائري لتتبع الدليل الرقمي من أجل إثبات جرائم المعلوماتية التي أفرزتها التكنولوجية الحديثة سواء لمكافحتها أو للوقاية منها.

فتناولنا الموضوع في فصلين تكلمنا في الفصل الأول عن ماهية الدليل الرقمي، و أجبنا عن التساؤلات الفرعية حول المقصود بدليل الرقمي ، خصائصه، أنواعه . و كذلك المقصود بالجريمة المعلوماتية باعتبارها محلا لهذا الدليل بتعريفاتها المختلفة الضيقة منها و الموسعة وتصنيفاتها المختلفة.

وتكلمنا في الفصل الثاني عن الإجراءات التقليدية و مدى نجاعتها في مكافحتها جرائم المعلوماتية، لنصل في الأخير إلى جملة من النتائج دعمناها بجملة من المقترحات. ومن أهم النتائج التي توصلنا إليها من خلال هذه الدراسة:

1. المشرع الجزائري يتبنى التعريف الموسع لجرائم المعلوماتية ، و يطلق عليها الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال في القانون رقم 09- 04 وهي تشمل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي ورد ذكرها في قانون رقم 04- 15 بالإضافة إلى أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية، بالإضافة إلى نصوص خاصة أخرى.
2. الدليل الرقمي نوع آخر من الأدلة الجنائية له حجيته وقوته الثبوتية ، و يتميز بخصائص يستمدها من البيئة الرقمية التي يولد فيها ويستخلص منها، و بالتالي يقتضى التعامل معه دراية بتقنية الحاسوب و الأنترنت و إجراءات خاصة لتتبعه.

3. تجدر الإشارة أن بعض الفقهاء يرون بأن قبول الدليل الرقمي يخضع للسلطة التقديرية للقاضي وفق مبدأ حرية الإثبات أي يمكن له رفضه و عدم الأخذ به ، مثل سائر الأدلة التقليدية.

لكن البعض الأخر ينظر إلى خصوصية هذا الدليل التي تجعله يتفوق عن باقي الأدلة من الناحية الفنية، و هذا ما يجعله يتميز بحجية علمية قاطعة،لا حرية القاضي في مناقشتها، لكونها حقائق علمية ، وإنما تكون له الحرية في تقدير الملابسات المحيطة بالدليل الرقمي، من حيث ظروف وطرق جمعه و استخلاصه وهذا هو الإتجاه المقبول في رأينا.

4. المشرع الجزائري لم يعرف الدليل الرقمي، ولم يستعمل هذا المصطلح، ولكنه أشار إليه ونظم أحكامه، وللقاضي الجنائي سلطة في قبول و تقدير الدليل الرقمي وفق نظام الإثبات الحر و مبدأ الإقناع الشخصي الذي يتبناهما المشرع الجزائري طبقا للمادة 212 من قانون الإجراءات الجزائية بشرط مشروعية الدليل و أن يكون يقينيا و تمت مناقشته في الجلسة .

5. المشرع الجزائري يسعى لمكافحة جرائم المعلوماتية التي هي في تزايد مستمر بسب التطور المتسارع لتكنولوجيات الإعلام و الاتصال، من خلال المواكبة التشريعية بسن قوانين موضوعية و إجرائية جديدة، أو تعديل القوانين الموجودة لتتماشى مع خصوصية هذه الجرائم و خصوصية الدليل الرقمي لإثباتها ، و أيضا من خلال الاتفاقيات و الملتقيات ذات الصلة بالموضوع، آخرها احتضان الجزائر للإجتماع الأول للتعاون الشرطي الإفريقي أفريبول (Afripole) ، أيام 14- 15- 16 ماي 2017 بالفندق الأوراسي بالجزائر العاصمة. تحت شعار من أجل قارة افريقية أكثر أمنا ، بحضور ممثل عن الأنتربول، و رئيس مفوضية الإتحاد الإفريقي و بمشاركة قادة الشرطة و الأمن لحوالي 40 دولة افريقية .

6. التحديات التي كانت تطرحها الجريمة المعلوماتية، و كذا المشاكل التي تعرقل استخلاص الدليل الرقمي، لم تطرح بالحدة التي كانت عليها، بسبب مواكبة المشرع للتطور التكنولوجي ، وتطور و تنوع هذه الجرائم. بالنسبة للتحديات الإجرائية تغلب عليها المشرع بتعديل القوانين الموجودة ، أو سن قوانين جديدة كتمديد اختصاص ضباط الشرطة القضائية و القضاة و النواب و استحداث قواعد إجرائية جديدة تتماشى مع خصوصية الدليل الرقمي.

أما التحديات الموضوعية التي أثارها بعض الفقهاء من حيث تكاليفها المرتفعة، فهي تتضاءل بالنظر إلى حجم الخسائر الفادحة التى تسببها جرائم المعلوماتية. و المشكل الوحيد الذي مازال يطرحه هذا النوع من الجرائم هو عدم الإبلاغ من طرف الضحايا خاصة، مما يصعب اكتشافها و إثباتها .

و صعوبة تتبع الدليل الرقمي لم يعد تطرح أمام الإجراءات المستحدثة من اعتراض المراسلات و المراقبة الإلكترونية، و أيضا استحدث الأجهزة المتخصصة في ذلك، مثل مخبر الأدلة الجنائية و علم الإجرام، و الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.

6 ـ بالنسبة للإجراءات المستحدثة أثيرت مشكلة مساسها بحرمة الحياة الخاصة للأفراد ، لكن المشرع الجزائري أحاطها ببعض الضمانات، موازنا بين حق الفرد في حرمة حياته الخاصة المقررة دستوريا، وحق المجتمع في ردع الجناة، و حصر تطبيق الإجراءات الخاصة مثل مراقبة الإتصالات الإلكترونية في جرائم محددة.

7 ـ أغلب دول العالم بما فيها الجزائر في تأهب دائم للتصدى لجرائم المعلوماتية و يظهر ذلك جليا من خلال الملتقيات و المؤتمرات أو الاتفاقيات الثنائية و الإقليمية و العربية و الدولية المكثفة و المتواصلة، حرصا من هذه الدول على بحث آليات مكافحة هذا النوع من الجرائم والسبل الكفيلة للوقاية منها. و على وجه الخصوص

تبادل الخبرات التقنية في كيفية استخلاص الدليل الرقمي بأحدث الوسائل لضمان سلامة و تقديمه للعدالة .

وبناء على هذه النتائج التي توصلنا إليها في نهاية هذه الدراسة يمكننا طرح بعض المقترحات:

1. نظرا لوجود نصوص جرائم المعلوماتية في قوانين خاصة متفرقة مما يصعب ،على القائمين على معالجتها، الرجوع إليها، نقترح جمعها في قانون واحد، مع ضبط المفاهيم و توحيدها و تحديد المصطلحات بدقة، سواء فيما يخص الجرائم أو الدليل الرقمي، ووضع التعريفات المناسبة لكل مصطلح و توضيح الإجراءات.
2. توسيع دائرة المراقبة الالكترونية لتشمل كل الجرائم ، بحيث لا تقتصر فقط على تلك التي جاءت على سبيل الحصر مثل جرائم الإرهاب و التخريب و المساس بأمن الدولة.
3. ضرورة النص على إلزام الشاهد المعلوماتي بالإبلاغ عن أي جريمة يكتشفها و تقديم كل المعلومات الضرورية إلى سلطات البحث و التحري للحصول على الدليل الرقمي.
4. تعزيز سبل التعاون الدولي في سبيل مكافحة جرائم المعلوماتية من خلال انضمام الجزائر إلى الاتفاقيات و المعاهدات الدولية، خاصة معاهدة بوادبست.
5. تكثيف الدورات التكوينية المتخصصة لرجال الشرطة و الدرك و القضاء، حول إجراءات لاستخلاص الدليل الرقمي وكيفية التعامل معه، لضمان مكافحة جرائم المعلوماتية.
6. الإسراع بتفعيل دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، وتنصيب ملحقاتها الجهوية .
7. تدريس مقياس الجرائم المعلوماتية، مع التركيز على إجراءات التحري و التحقيق فيها، في كليات الحقوق، و معاهد القضاء الشرطة و الدرك.

8. نشر ثقافة الأمن المعلوماتي، و تحصين مؤسسات الدولة والشركات، ببرامج أمنية معلوماتية، من تصميم كفاءات جزائرية .
9. الإستعانة بالقراصنة الجزائريين، لتأمين النظم المعلوماتية ، و الإستفادة من خبراتهم في إجراءات التحري و التحقيق لاستخلاص الدليل الرقمي .
10. تشجيع البحوث الجامعية في مجال جرائم المعلوماتية .
11. تكثيف حملات التوعية و التحسيس بمخاطر جرائم المعلوماتية، و التعريف بقدرات الأجهزة المتخصصة على كشف الجريمة و إثباتها بالدليل الرقمي، بهدف دفع الضحايا إلى التبليغ عن الاعتداءات التي تطالهم.

I / المصادر

أولا : مصادر خارجية

1 – إتفاقية بودابست حول جرائم المعلوماتية . الموقعة بتاريخ: 23 /11 /2001 .

2 – الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة بالقاهرة بتاريخ: 21 / 09 /2010 .

ثانيا : مصادر داخلية

1 – دستور الجمهورية الجزائرية الديمقراطية الشعبية ، دار بلقيس ، 2016 .

2 – قانون العقوبات ، أحسن بوصقيعة ، برتي للنشر 2015 .

3 – قانون 2000 – 03 المؤرخ في 15 أوت 2000 يتعلق بالقواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية .

4 – قانون رقم 03 – 05 المؤرخ في 19 جويلية 2003 الخاص بحقوق المؤلف و الحقوق المجاورة .

5 – قانون رقم 08 – 01 المؤرخ في 23 جانفي 2008 المتمم للقانون رقم 83 – 11 المؤرخ في 02 جويلية 1983 المتعلق بالتأمينات الاجتماعية .

6- قانون رقم 14 – 08 المؤرخ في 4 فيفري 2014 المعدل و المتمم للأمر رقم 66 – 156 المؤرخ في 08 جوان 1966 . قانون العقوبات.

7 – قانون رقم 15 – 03 المؤرخ في 01 فيفري 2015 المتعلق بعصرنة العدالة .

8 – قانون رقم 15 – 04 المؤرخ في 01 فيفري 2015 المتعلق بالتوقيع و التصديق الإلكتروني .

9- قانون رقم 05 – 01 المؤرخ في 20 جوان 2005 المعدل و المتمم للأمر رقم 75 – 58 المتضمن القانون المدني .

10 – قانون رقم 06 – 22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للأمر 66 – 155 المتضمن قانون الإجراءات الجزائية .

11 – قانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 66 – 156 المؤرخ في 08 جوان 1966 قانون العقوبات .

12 – قانون رقم 09 – 04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

13 – المرسوم الرئاسي رقم 14 – 252 . المؤرخ في 08 ديسمبر 2014 المتعلق بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة بالقاهرة بتاريخ 12 سبتمبر 2010 .

14 – المرسوم الرئاسي رقم 15 – 2016 . المؤرخ في 08 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

15 – الأمر المتعلق رقم 15 – 02 المؤرخ في 23 جويلية 2015 المتضمن تعديل قانون الإجراءات الجزائية .

16 – قرار غرفة الاتهام ، مجلس قضاء بسكرة . رقم الجدول 00469 / 10 رقم الفهرس 00465 – 10 . تاريخ القرار : 19 / 07 / 2019 .

17 – حكم محكمة بسكرة . قسم الجنح ، 01721 – 11 . رقم الفهرس 1936 / 11 ، تاريخ الحكم : 14 / 03 /11 .

ثالثا : المعاجم

1- . جمال صليبا : المعجم الفلسفي ، دار الكتاب اللسان ، بيروت الطبعة الأولى ، 1970 .

II / المراجع

أولا : كتب متخصصة

1- آمال قارة : الحماية الجزائية للمعلوماتية في تشريع الجزائري، دار هومة ، الطبعة 2 ، الجزائر، 200

2- . أحمد ابو القاسم : الدليل المادي و دوره في الإثبات في الفقه الجنائي الإسلامي .دار النهضة العربية .1991 .

3- د . أمين الشوابكة ، جرائم الحاسوب و الانترنت ، دار الثقافة . عمان 2009 .

4- امير فرج يوسف : الجرائم المعلوماتية على شبكة الانترنت ، ديوان المطبوعات الجامعية ،القاهرة . 2009 .

5- خالد ممدوح إبراهيم : حجية البريد الالكتروني في الإثبات ، دار الفكر الجامعي ، الطبعة الأولى . مصر . 2007.

6- ختير مسعود : الحماية الجنائية لبرامج الكومبيوتر ، دار الهدى ، الجزائر. 2010.

7- سامي جلال فقي حسين : الأدلة المتحصلة من الحاسوب و حجيتها في الإثبات الجنائي (دراسة مقارنة) . دار شتات للنشر و البرمجيات ، دار الكتب القانونية ، مصر . 2010 .

8- شيماء عبد الغني محمد عطا الله : الحماية الجنائية للتعاملات الالكترونية .دار الجامعة الجديدة. 2007 .

9- عائشة بن قارة مصطفى : حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن ، دار الجامعة الجديدة . 2010 .

10- عبد الفتاح بيومي حجازي : الجوانب الإجرائية لأعمال التحقيق في الجرائم المعلوماتية. الطبعة الأولى ، القاهرة . 2009 .

11- غنية باطلي : الجريمة الالكترونية دراسة مقارنة . منشورات الدار الجزائرية .

12- فاضل زيدان محمد :سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة). الطبعة الأولى ، الإصدار الثاني . دار الثقافة للنشر و التوزيع . عمان الأردن 2006 .

13- محمد أمين الرومي جرائم الكومبيوتر و الانترنت . دار المطبوعات الجامعية، الإسكندرية ، 2004 .

14- محمد طارق عبد الرؤوف الحن : جريمة الاحتيال عبر الانترنت (الأحكام الموضوعية و الأحكام الجزائية) . الطبعة الاولى . منشورات الحلبي الحقوقية ، بيروت . لبنان 2011 .

15- محمد مرسي : التحقيق الجنائي في الجرائم الالكترونية . مطابع الشرطة . 2009 .

16- ممدوح عبد الحميد عبد المطلب : البحث و التحقيق الجنائي الرقمي في جرائم الكومبيوتر و الانترنت ، دار الكتب القانونية . مصر . 2008.

17- نهد عبد القادر المومني : الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع . الاردن .2008 .

18- هدى قشقوش: جرائم الحاسب الآلي في التشريع المقارن ، الطبعة الأولى . دار النهضة العربية . القاهرة . 1992 .

19- هلالي عبد اللاه احمد : اتفاقية بودابست لمكافحة جرائم المعلوماتية . معلقا عليها ، الطبعة الأولى . القاهرة 2007 .

ثانيا : كتب عامة

1 - احمد فتحي سرور : الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية . القاهرة . 1992 .

2 -. عبد الله اوهايبية : شرح قانون الإجراءات الجزائية ، الطبقة الثانية .دار هومة للنشر و التوزيع . 2011 .

3 -.علي شملال : المستحدث في قانون الإجراءات الجزائية الجزائري الكتاب الأول ، دار هومة للنشر و التوزيع . 2016 .

4 - . محمد مروان : نظام الإثبات في المواد الجنائية ، في القانون الوضعي الجزائري . ديوان المطبوعات الجامعية . 1999 .

5 - منصور دحماني : الوجيز في القانون الجنائي العام ، دار العلوم الجزائر . 2006 .

ثالثا : مقالات

1 -. إدريس قرين : تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية من اتفاقية بودابست و التشريع الجزائري الملتقى الوطني حول الجريمة المعلوماتية المنعقد بجامعة محمد خيضر بسكرة سنة 2015 .

2 - بحرية هارون : دور الدليل الرقمي في إثبات الجريمة المعلوماتية . الملتقى الوطني حول الجريمة المعلوماتية المنعقد بجامعة محمد خيضر بسكرة سنة 2015 .

3 - . حابت أمال : الطابع الخصوصي للإجراءات الجزائية في شان الجرائم المعلوماتية في القانون الجزائري . الملتقى الوطني حول الجريمة المعلوماتية المنعقد بجامعة محمد خيضر بسكرة سنة 2015 .

4 - . رضا هميسي : أحكام الشاهد في الجريمة المعلوماتية . الملتقى الوطني حول الجريمة المعلوماتية المنعقد بجامعة محمد خيضر بسكرة سنة 2015 .

5 - وسيم حرب : ورقة عمل مقدمة لأعمال الندوة الإقليمية حول جرائم المعلوماتية . 2007 .

6 - رشيدة بو بكر : الدليل الالكتروني ومدى حجيته في القانون الجزائري ، مجلة العلوم الاقتصادية و القانونية ، العدد الثاني ، المجلد 27 . جامعة دمشق . 2011 .

7 – عبد الناصر محمد حمو محمود فرغلي ، و محمد عبيد سيف سعيد المسماري : الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية ، بحيث مقدم إلى المؤتمر العربي الأول لعلم الأدلة الجنائية و الطب الشرعي ، المنعقد بالرياض في 132 _ 14 نوفمبر 2007 ، جامعة نايف العربية للعلوم الأمنية .

رابعا : لقاءات

1 - لقاء مع رئيس مكتب الشرطة القضائية لمجموعة الدرك الوطني لولاية بسكرة أجري بتاريخ 20 مارس 2017 .

2 - حصة حوار مفتوح : بثت بتاريخ 22 مارس 2017 . من إذاعة الجزائر الجهوية من بسكرة ، مع ضباط فرقة مكافحة الجريمة المعلوماتية .أمن ولاية بسكرة.

3 – لقاء مع رئيس خلية الاتصال و العلاقات العامة بأمن ولاية بسكرة اجري بتاريخ 06 افريل 2017 .

خامسا : مواقع الانترنت

1 – موقع الشرطة الجزائرية ccp – dgs@algerie.police.dz

2 – الموقع : www.france24.com

سادسا : الجرائد

1 – جريدة الشروق الجزائرية، العدد 2725 صادرة بتاريخ 10 / 11 / 2009 .

ملخص :

أمام تزايد جرائم المعلوماتية التي صاحبت تطور تقنية الحوسبة وشبكات الإتصال، ظهر الدليل الرقمي كنوع جديد يضاف إلى الأدلة الجنائية المعروفة الأخرى. ويتميز عنها بعدة خصائص يستمدها من البيئة الرقمية التي يولد فيها. هذا ما يجعل الإجراءات التقليدية لجمعه و استخلاصه غير كافية. نظرا لخصوصيته، يتطلب الدليل الرقمي خبرة تقنية و يفرض على سلطات التحري و التحقيق خبرة تقنية . لذلك و لضمان تتبع الدليل الرقمي، استحدث التشريع الجزائري إجراءات جديدة مثل مراقبة الإتصالات الإلكترونية. مع مراعاة ضرورة تحقيق توازن بين الحرية الشخصية للفرد و حق المجتمع في تتبع الجناة و معاقبتهم.

وحرصا من المشرع الجزائري على مكافحة الجرائم المعلوماتية وتسهيلا لتطبيق هذه الإجراءات استحدثت أجهزة متخصصة في ذلك من بينها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال المنشأة حديثا.

والملاحظ أن هذا النوع من الجرائم في تزايد دائم مواكبا التطور التكنولوجي مما يقتضي مضاعفة الجهود على جميع المستويات، مع التركيز على الجانب التحسيسي بمخاطر الاستعمال السيء للحواسيب ، الهواتف الذكية و الأنترنت ، و التأكيد على ضرورة التبليغ عن أي إساءة استعمال.

Résumé :

Devant la croissance des infractions informatiques qui accompagnent l'évolution de la technologie de l'informatique et les réseaux de la communication. La preuve numérique est apparue comme un nouveau type des preuves ajoutées à l' impot des autres connues . elle se caracterise par un certain nombre de propriétés dérivées de l' environnement numérique dans lequel elle est née .Ce qui rend les procédures pénales traditionnelles insuffisantes pour son extraction et sa collecte .Vu sa spécificité, la preuve numérique necessite une expérience téchnique et impose aux pouvoires d' investigation avoir une connaissance de la technologie. Pour faire face , et assurer le suivi de la preuve numérique, la législation algérienne a développé des nouvelles procédures , comme la surveillance des communications électroniques. en tenant compte la necessité de réaliser un équilibre entre la liberté personnelle de l'individu et le droit de la société à suivre et à punir les auteurs.

Dans l'intérêt du législateur algérien de combattre les infractions informatiques et à afin de faciliter l'application de ces procédures a mis au point des dispositifs spécialisés, y parmi , l' organisation national de la prévention des crimes liés aux technologies de l'information et de la communication.

Il est à noter que ce type de crimes sont dans une augmentation permanente en ligne avec le développement technologique, ce qui exige des éfforts redoublés à tous les niveaux, en mettant l'accent sur le côté sensibilisation concernant l' abus d'utilisation des ordinateurs, smartphones et internet, et la nécessité de signaler tout abus.