جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم : القانون الخاص

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

وسائل وأساليب التحري في مجال مكافحة الجرائم الإلكترونية

ميدان الحقوق و العلوم السياسية

الشعبة: الحقوق

التخصص: القانون القضائي

من إعداد الطالب :

– بن حريقة محمد الامين

تحت إشراف الأستاذ :

–بوسحبة جيلالي

أعضاء لجنة المناقشة

الأستاذ .....زواتين خالد.....رئيسا

الأستاذ .....بوسحبة جيلالي..... مشرفا مقررا

الأستاذ.....بن عوالى على.....مناقشا

السنة الجامعية: 2020/2019

نوقشت يوم:**2020/11/25**

الإهداء

أهدي هذا العمل إلى أعز ما يملك الإنسان في هذه الدنيا إلى ثمرة نجاحي إلى من أوصى بهما الله سبحانه وتعالى :

" وبالوالدين إحسانا "

إلى الشمعة التي تحترق من أجل أن تضئ أيامي إلى من ذاقت مرارة الحياة وحلوها، إلى قرة عيني وسبب نجاحي وتوفيقي في دراستي إلى

"أمي "

أطل الله في عمرها

إلى الذي أحسن تربيتي وتعليمي وكان مصدر عوني ونور قلبي وجلاء حزني ورمز عطائي ووجهني نحو الصلاح والفلاح إلى

"أبي "

رحمه الله

إلى أخواتي وجميع أفراد عائلتي

إلى أستاذي " **بوسحبة جيلالي** " و جميع الأساتذة الأجلاء الذين أضاءوا طريقي بالعلم

وإلى كل أصدقاء الدراسة و العمل ومن كانوا برفقتي أثناء إنجاز هذا البحث إلي كل هؤلاء وغيرهم ممن تجاوزهم قلمي ولن يتجاوزهم قلبي أهدي ثمرة جهدي المتواضع

شكر وتقدير

- الحمد لله على توفيقه وإحسانه، والحمد لله على فضله وإنعامه، والحمد لله على جوده وإكرامه، الحمد لله حمدا يوافي نعمه ويكافئ مزيده

أشكر الله عز وجل الذي أمدني بعونه ووهبني من فضله ومكنني من إنجاز هذا العمل ولا يسعني إلا أن أتقدم بشكري الجزيل إلى كل من ساهم في تكويني وأخص بالذكر أستاذي الفاضل **" بوسحبة جيلالي "**

الذي تكرم بإشرافه على هذه المذكرة ولم يبخل علي بنصائحه الموجهة لخدمتي

فكان لي نعم الموجه والمرشد

كما لا يفوتني ان أشكر أعضاء لجنة المناقشة المحترمين الذين تشرفت لمعرفتهم وتقييمهم لمجهوداتي

كما أشكر كل من قدم لي يد العون والمساعدة ماديا أو معنويا من قريب أو بعيد

إلى كل هؤلاء أتوجه بعظيم الامتنان وجزيل الشكر المشفع بأصدق الدعوات.

مقدمة

إن أهم ما يُميز العصر الحالي عن غيره من العصور هو ما نشهده اليوم من تطور مثير في المجالات التكنولوجية، الأمر الذي انعكس على مجمل مجالات الحياة، بحيث نستطيع القول بثقة بأنه لم يُعد هناك شأن يتصل بالحياة الانسانية إلا ناله نصيب من هذا التطور التكنولوجي المثير الذي أحدث ثورة أدخلت البشرية في عصر جديد.

وعلى الرغم من الايجابيات العديدة التي أحدثتها تقنية الانترنت في تسهيل نقل وتبادل المعلومات، إلا إن هناك خشية متزايدة من تنامي الخروق والسلبيات والأعراض الجانبية لهذه الشبكة واستغلالها من قبل بعض الشركات والهيئات والعصابات والأفراد لارتكاب وتعميم أعمال وأفعال تتقاطع مع القوانين ومع الاعراف والأخلاق والآداب.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتجات النظام، وتكشف عن أهم التحديات القانونية التي تفرضها جرائم المساس بأنظمة الكومبيوتر على النظام المعلوماتي الجزائري بشكل خاص والعالمي بشكل عام، ولتحقيق هذا الهدف يحاول هذا البحث بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لشبكة الإنترنت، من هذا المنطلق، نتساءل ما هي أبرز الأنماط الإجرامية في مجال المساس بأنظمة الكومبيوتر والإنترنت؟،

إضافة إلى ما سبق، تتميز الجريمة الإلكترونية بصعوبة اكتشافها وإثباتها بسبب ارتكابها بطريقة تقنية كثيرة التعقيد وسهولة تدمير ومحو المعلومات الخاصة بارتكابها وأنها أيضا ذات طبيعة دولية متعدية الحدود حيث تتجاوز الفواصل الجغرافية لعدة دول، فمثلا الدراسة التي قامت بها شركة (Symantec) وهي شركة مختصة في حماية الأنظمة والبرامج الإلكترونية سنة 2010، بينت فيها أن الاعتداءات على الأنظمة الإلكترونية وإصلاحها سنويا يسبب خسارة مالية قدرها 114 مليار دولار في العالم وأن هذه الاعتداءات مست 431 مليون شخص."

ولعل خصوصية الجريمة الاكترونية ، أبرزت مشكلة المكافحة الإجرائية للجريمة الإلكترونية خاصة من ناحية كيفية جمع الأدلة الإلكترونية ومدى حجيتها، وحتى تتوفر في الدليل الإلكتروني المشروعية التي تشترطها القوانين في كافة التشريعات.

والمشرع الجزائري، اقتداء بالمشرعين الذين سبقوه، سارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية، وذلك بتعديل بعض المواد في قانون الإجراءات الجزائية وإصدار قوانين خاصة وجديدة في مجال الإجراءات.

أهمية البحث:

تكمن أهمية البحث في مدى الخطورة التي تُشكلها الجرائم الالكترونية إذ إنها تطال الحق في الحصول على المعلومات وتمس حرمة الحياة الخاصة للأفراد وتُهدد الأمن الوطني وتُؤدي إلى فقدان الثقة بالتقنية وغيرها من مفاصل الحياة العامة المختلفة.

3مشكلة البحث:

تتمثل مشكلة البحث في مدى الصعوبة التي تُواجهها إجراءات التحقيق في هذا النوع من الجرائم والمتمثلة في اخفاء الجريمة وسهولة وسرعة محو أو تدمير أدلة ومعالم الجريمة والضخامة البالغة لكمية البيانات المراد فحصها على الشبكة، وتبرز كذلك صعوبات في مسائل جمع الأدلة من المعاينة والتفتيش والضبط وغيرها من الاجراءات، فضلاً عن الطابع العالمي الذي تمتاز به هذه الجرائم لكونها من الجرائم التي تتجاوز عنصري الزمان والمكان.

أسباب إختيار البحث:

لا يخفى سبب اختياري لهذا البحث، وهو رغبتي في الوقوف على حقيقة التعامل مع الجريمة الإلكترونية من الناحية الإجرائية فالكثير من الدراسات التي عنيت بهذه الجرائم باتت تركز على الجانب الموضوعي فقط،

أهداف الدراسة:

ينبع الهدف من هذه الدراسة من محاولة المساهمة في وضع الخطوط العريضة للتعرف على طرق التحقيق في هذا النوع من الجرائم، ذلك أن جدة وحداثة الجرائم الإلكترونية وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها و كيفية التعامل معها وأسلوب التحقيق فيها، إذ لا شك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية.

إشكالية البحث: وما هي الوسائل وأساليب المتخذة من قبل المشرع الجزائري في مجال مكافحة جرائم الإلكترونية ؟.

وتفرعت إلى ما يلي :

- **ماهي الاليات التي تتبعها للكشف عن الجرائم الاكترونية**
- **ماهي وسائل اساليب البحث والتحري الخاصة في المتابعة الجرائم الاكترونية**

إذا كانت ظاهرة الإجرام المعلوماتي قد أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم و احترام مبدأ الشرعية والتفسير الضيق للنصوص الجنائية، فقد أثارت في نفس الوقت العديد من المشكلات في نطاق القانون الجزائي الإجرائي، وتبدأ المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها في كثير من الأحيان ببيانات المعالجة الكترونية وكيانات منطقية غير مادية، ومن ثم يصعب الكشف عن تلك الجرائم وإثباتها نظرا للسرعة والدقة العالية في تنفيذها وكذا إمكانية محوها وتمويه آثارها وإخفاء الأدلة المتحصلة منها عقد تنفيذها.

ولذلك فقد امتد تأثير التقنية الإلكترونية إلى الجانب الإجرائي من القانون الجزائي، ذلك أن نصوص هذا القانون إنما صيغت لتحكم الإجراءات المتعلقة بجرائم تقليدية، ترتكب في عالم

مادي وملموس يلعب فيه السلوك المادي الدور الأكبر والأهم على خلاف الجريمة الإلكترونية التي ترتكب

منهجية البحث:

سنتناول في هذا الموضوع وسائل واساليب البحث والتحري في الجرائم الالكترونية في نطاق التحقيق الجنائي محاولين قدر الامكان وضع اليد على بعض الحلول الناجعة لمكافحة هذه الظاهرة الإجرامية، مستندين في ذلك إلى عرض وتحليل النصوص القانونية المتعلقة بهذا المجال.

خطة البحث:

يقتضي إيفاء هذا الموضوع حقه تقسيمه هذه الموضوع الى فصلين اما عنوان الفصل الاول الإطار المفاهمي للجرائم الإلكترونية وطرق مكافحتها وسوف نقسم الفصل الى مبحثين، إذ سيكون عنوان المبحث الأول (ماهية الجريمة الإلكترونية) وفي المبحث الثاني إجراءات البحث و التحري للكشف عن الجرائم الإلكترونية

اما عنوان الفصل الثاني جاء خصوصية الجريمة الإلكترونية من الناحية الإجرائية

ويتضمن مبحثيتن، سيُخصص المبحث الأول المتابعة القضائية في الجريمة الإلكترونية والمبحث الثاني أساليب التحري والتحقيق و إثبات في الجريمة الإلكترونية وسوف ننهي البحث بخاتمة تتضمن أهم النتائج والتوصيات .

الفصل الأول
الإطار المفاهمي للجرائم الإلكترونية وطرق مكافحتها

تمهيد

إن موضوع الجريمة الإلكترونية يعتبر بحد ذاته موضوع الساعة ومشكل كل الدول العالم ولا سيما الجزائر، بإعتبار أن هذه الجريمة أصبحت تمس حقوق الأشخاص من خلال التعديّ عليهم بمختلف الطرق والأساليب، والحث والتحري في الجرائم الإلكترونية ومن خلال هذا الفصل سنحاول إستعراض في المبحث الأول ماهية الجريمة الإلكترونية الذي يتضمن مطلبين ، مطلب الأول تعريف الجريمة الإلكترونية و المطلب الثاني خصائص الجريمة الإلكترونية أما في المبحث الثاني فقد تطرقنا إلى أسس تصنيف الجريمة الإلكترونية و الذي يتضمن مطلبين المطلب الأول الإلكترونية وسيلة لإرتكاب الجرائم أما المطلب الثاني الإلكترونية هدفا من إرتكاب الجرائم .

المبحث الأول : ماهية الجريمة الإلكترونية

تعددت التعريفات الخاصة بالجريمة الإلكترونية وتباينت فيما بينها وتعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وسوف نحاول من خلال هذا المبحث تعريف الجريمة الإلكترونية لننتقل فيم بعد إلى خصائصها.

المطلب الأول : تعريف جريمة الإلكترونية

إختلاف النظم القانونية والثقافية بين الدول، وإنجر عنه تعريف للجريمة الإلكترونية تارة في المجال الضيق وتارة آخرى في المجال الموسع.

لذا سوف نتطرق إلى التعريف الفقهي الضيق لهذه الجريمة ثم التعريف الموسع.

الفرع الأول : التعريف الضيق للجريمة الإلكترونية

لا يوجد مصطلح قانوني موحد للدلالة على ظاهرة الإجرامية الناشئة في البيئة الكمبيوتر وفيما يعد بيئة الشبكات، بل تباينت هذه المصطلحات حيث رافق هذا التباين مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات[1] فظهرت عدة محاولات لتعريفها تعريفا ضيقا من بينها:

ماذهب إليه الفقيه (MERWE) حيث يرى أن الجريمة الإلكترونية (جريمة الحاسب) هي :

– الفعل الغير المشروع الذي يتورط في إرتكابه الحاسب الآلي وهي الفعل الإجرامي الذي يستخدم في إقترافه الحاسب الآلي كأداة رئيسة.[2]

– في أخرى ذهب (Tièdement) إلى أن الجريمة الإلكترونية تشمل أي جريمة ضد

[1] - عائشة بن قارة مصطفى، حجية الدليل الإليكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير كلية

[2] - MARWE VANDER ,computer crimes and other grimes against information Technology in south Africa ,"R.I.D.P",1993;p554.

المال، مرتبطة بإستخدام المعالجة الآلية للمعطيات [1].

– فيما ذهب الفقيه (Rosblat) إلى تعريفها بأنها كل نشاط غير مشروع موجه لنسخ أو تغيرات أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول طريقه.

– أو أنها كما جاء في التعريف (Dauid Tompson) هي الجرائم يكون متطلبا لإقترافها ان يتوافر لدى معرفة بتقنية الحاسب.[2]

– وعرف (Leslie dball) الجريمة المرتبطة بالحاسب بأنها فعل إجرامي يستخدم الحاسب في إرتكابه كأداة رئيسية .

– وعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية أنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج الإلكترونية دورا رئيسيا .

– والحقيقة ان هذه التعريفات كانت قاصرة على الإحاطة بأوجه ظاهرة الإجرام المعلوماتي ولذلك فقد أنتقدت كون أن هذه التعريفات ركزت على وسيلة إرتكاب الجريمة لذا فهي ليست جامعة ولا مانعة.

– ومن أفضل التعريفات التي تدور حول الوسيلة هو تعريفها بأنها : تلك الجرائم التي يكون قد وقع في مراحل إرتكابها بعض العمليات الفعلية داخل نظام الحاسب، أي أنها الجرائم التي يكون دور الحاسب فيها إيجابيا اكثر منه سلبيا.

– وإزاء هذه الإنتقادات، حول جانب من الفقه تعريف الجريمة المعلومات على النحو واسع لظاهرة الإجرام المعلوماتي.

---

[1] -Klaus Tiede man, Fraude et autres délits d’affaires commis a l’aide d’ordinateurs électroniques, Rev, drpén , crim, 1984, p 612.

[2] - هشام رستم، جرائم الحاسب كصورة من صور الجرائم الإقتصادية المستحدثة بحث مقدم إلى لجنة العلمية بمصر لمنع الجريمة الإلكترونية ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيط ، العدد 17 ، سنة 1995 ص 107 و 108.

الفرع الثاني : التعريف الموسع للجريمة الإلكترونية

وهو ما ذهب إليه الفقيهان (MICHEL & CREDO) من أسوء إستخدام الحاسب او الجريمة الحاسب تشمل: إستخدام الحاسب كأداة لإرتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج الغير المصرح به لحاسب المجني عليه أو بياناته كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذات أو المعدلات المتصلة به، وكذلك الإستخدام غير المشروع لبطاقات الإئتمان، وإنتهاك ماكينات الحساب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إليكترونية، وتزيف المكونات المادية والمعنوية للحاسب.

وتناول رأي من الفقه تعريف الجريمة الإلكترونية بأنها : عمل أو إمتناع يأتيه الإنسان أضرارا بمكونات الحاسب وشبكات الإتصال الخاصة به التي يحمها قانون العقوبات ويفرض له عقابا.

ويمتاز هذا التعريف بانه يحتوي على كل صور الإعتداء الإيجابية والسلبية التي تقع أضرار بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به.

أنه يتضمن الأثر الجنائي المترتب على العمل أو الإمتناع غير المشروعين ويتمثل في الجزاء الجنائي بكافة صوره وأنواعه.[1]

بعد عرضنا لتعريف الجريمة الإلكترونية نضيف : أن شبكة الإنترنيت بوصفها نتاج تطور النظم الإلكترونية كأداة للربط والإتصال بين مختلف شعوب العالم، تشكل أداة لإرتكاب الجريمة الإلكترونية أو محالا لها وذلك بإساءة إستخدامها أو إستغلالها على النحو غير

[1] - طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر ، الإسكندرية، مصر ، 2009، ص 157 و 158.

المشروع، ولذلك ينبغي على الجهات التشريعية مواجهتها بتشريعات حاسمة لمكافحتها وتقديم مرتكبيها للعدالة.[1]

المطلب الثاني : خصائص الجريمة الإلكترونية

الجريمة الإلكترونية إفراز ونتاج للتقنية المعلومات، وإتساع نطاق تطبيقها في المجتمع، مما يعطيها لونا او طابعا قانونيا خاصا، ويميزها مجموعة من الخصائص يمكن تجميعها حول العناصر الآتي ذكرها.

الفرع الأول : خصوصية الجريمة الإلكترونية

أولا : صعوبة إكتشاف لجريمة المعلوماتية

تتسم الجرائم الناشئة عن إستخدام الأنترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، ولأن الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة .

مثلا عند إرسال الفيروسات وسرقة الأموال ولبينات الخاصة او إتلافها والتجسيس وسرقة المكالمات وغيرها من الجرائم.[2]

كما أن وسيلة تنفيذها تتميز بالطابع الفني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى عدم الإبلاغ عنها في حالة إكتشافها لخشية المجني عليهم من فقدان عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة ثانية واحدة.[3]

ثانيا : صعوبة إثبات الجريمة الإلكترونية

[1] - جميل عبد الباقي الصغير، الأنترنيت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية ، القاهرة، مصر، 2001، ص 04.

[2] - محمد عبيد الكعبي، الجرائم الناشئة عن الإستعمال الغير المشروع للشبكة الانترنت، دار النهضة العربية، القاهرة ، مصر ، 2001، ص 32.

[3] - نهلا عبد القادر المومني الجرائم المعلوماتية، الطبعة 2 ، دار الثقافة للنشر والتوزيع، دون بلد نشر ، 2001، ص 54.

فالجريمة الإلكترونية في بيئة غير تقليدية حيث تقثع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب و الأنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ونظرا لما تطلبه هذه الجرائم من تقنية لإرتكابها فهي تستلزم أسلوب خاص التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحسين الجهاز الأمني والقضائي ضد هذه الظاهرة، حيث لم تعد قادرة القوانين التقليدية على مواكبة السرعة الهائلة في التكنولوجيا والتي أدت إلى ظهور جرائم لم تكن موجودة في السابق، وباتت القوانين التقليدية القائمة عاجزة عن مواجهتها[1] مما يشكل عائقا أساسيا أمام إثبات الجريمة المعلوماتية.

ثالثا : أسلوب إرتكاب الجريمة الإلكترونية

الجرائم الإليكترونية هي الجرائم هادئة، تحتاج إلى قدرة علمية في التعامل مع جهاز الحاسوب وشبكة المعلومات الدولية(الأنترنت) بما في ذلك بعض تقنيات إرتكاب هذه الجرائم كالإختراق سواء عن طريق إستعمال نظام التشغيل أو إستخدام البرامج أو عن طرق تشمل كلمات السر وجمعها، كما ظهرت تقنيات السلامي(salami te chnique) ، أو حصان طراودة في إرتكاب عملية الإختلاس المالي وغيرها من الأساليب المتطورة التي أفرزتها التكنولوجيا [2].

رابعا: التعاون والتواطؤ على الإضرار

وهو أكثر تكرارا في الجرائم الإلكترونية عنه في الأنماط الأخرى للجرائم الخاصة أو الجرائم أصحاب الياقات البيضاء، وهم دوي المناصب الرفيعة المستوى في الإدارات وغالبا ما يكون متضمنا فيها متخصص في الحسابات، يقوم بالجانب الفني في المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة (المجني عليها) لتغطية عملية التلاعب

[1] - محمد عبيد الكعبي،مرجع سابق، ص 40.
[2] - عائشة بن قارة مصطفى، مرجع سابق، ص 44.

وتحويل المكاسب إليه، كما أنها من عادة من يمارس التملص على الحسابات تبادل المعلومات بصفة منتظمة حول أنشطتهم.[1]

خامسا : أعراض النخبة

يعتقد بعض المختصصين في تقنية الحسابات والإلكترونية أن من مزايا مراكزهم الوظيفية ومهارتهم الفنية، إستخدام الحسابات وبرامجها لأغراض شخصية أو ممارسة بعض الهويات الرائدة في فلك هذه التقنية وهو ما يعبر عنه بأغراض النخبة، ومن شأن ذلك تمادي بعضهم إلى إستخدام نظم الحاسب بصورة غير مشروعة تصل إلى حدّ إرتكاب الجرائم الخطيرة.[2]

سادسا : الأضرار

تقع الجرائم الإلكترونية في نطاق تقنية نتقدمة يتزايد يوما بعد يوم إستخدامها في إدارة المعاملات الإقتصادية والمالية – الوطنية والدولية – الإعتماد عليها في تسيير معظم شؤون العامة لأكثر الحكومات بمانع ذلك الأمن والدفاع، ومن شأن ذلك أن يضفي أبعادا مسبوقة على الخسائر و الأضرار التي تنجم عن هذه الجرائم.

والأدل على ذلك من أم الخسائر المادية الناجمة عن هذه الجرائم تبلغ وفقا لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية (N.C.C.C.D) في نهاية القرن الماضي حوالي 500 مليون دولار في السنة.[3]

سابعا : الصفة الدولية للجريمة المعلوماتية

[1] - إبراهيم الدسوقي عطية، مرجع سابق، ص 169.

[2] - Jack Bologna, Corporate Fraud, hte Basic of prevention and Detction , Butter worth, 1984,p11.

[3] - WASIK Martin , computer crimes and other crimes against information tesnnology in the unit kingdom "R.I.D.P" , 1991,p19.

يمكن القول – ويحق– أن من أهم الخصائص التي تميز الجريمة الإلكترونية هي تخطيها للحدود الجغرافية، ومن ثم إكتسابها طبيعة دولية أو كما ذهب البعض أنها جريمة ذات طبيعة متعدية الحدود .

فمع ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحسابات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينهما آلاف الأميال، أدت إلى أن دول مختلفة قد تتأثر بالجريمة الإلكترونية المرتكبة في أن واحد.

وتظهر هذه المشكلة بصفة خاصة في مجال البنوك من خلال التوسع الكبير في إجراء المعاملات البنكية عبر الشبكات المعلومات الدولية ذلك أعطى بُعد دولي لجرائم الإحتيال المعلوماتي بصفة خاصة .

كما يمكن للجاني الذي يتواجد في دولة بالدخول إلى ذاكرة حاسب آلي موجود في دولة أخرى، للقيام بعمل إجرامي في نطاق الإلكترونية يضر بشخص آخر موجود في دولة ثالثة مثل جرائم النصب المعلوماتي .

ومن القضايا الهامة ذات البُعد الدولي للجرائم الإلكترونية نذكر قضية " نقص المناعة المكتسبة" (الإيدز) وتتلخص وقائعها انه عام 1989 قام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج، الذي يهدف في ظاهرة إعطاء بعض النصائح الخاصة بالمرضى نقص المناعة المكتسبة إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (من أمثلة حصان طراودة) وكان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي، عند العمل ثم تظهر بعد ذلك على الشاشة عبارة يقوم الفاعل من خلالها بطلب مبلغ من المال، يرسل على العنوان بدولة (بنما)حتى يتمكن المجني عليه من الحصول على المضاد للفيروس، وفي عام 1990 تم إلقاء القبض على المتهم ويدعى (جوزيف بوب) في ولاية (أوهايو) USA وطلب

بريطانيا تسليمها المتهم لمحاكمته أما القضاء الإنجليزي، وقد وافق القضاء الأمريكي على تسليم المتهم.

وتظهر أهمية هذه القضية من ناحيتين:

الأولى : أنها المرة الأولى التي يتم تسليم المتهم في جريمة معلوماتية.

الثانية : أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد فيروس.[1]

الفرع الثاني : سمات المجرم المعلوماتي

أولا : المعرفة والمهارة والذكاء

تعني المعرفة التعرف على كافة الظروف التي تحيط بالجريمة الميراد تنفيذها وإمكانيات نجاحها وإحتمالات فشلها، فالجناة عادة يمهدون لإرتكاب جرائمهم بالتعرف على كافة الظروف المحيطة، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم، وتُميز المعرفة بمفهومها السابق مجرمي المعلوماتية، حيث يستطيع المجرم المعلوماتي أن يُكون تصورا كاملا لجريمته ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة الإلكترونية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته[2].

ويتمتع مجرمي الأنترنت بقدر لا يستهان به من المهارات تقنيات الحاسوب والأنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين من المهارة لدى الفاعل الذي قد

[1] - نائلة عادل فريد قورة،، جرائم الحاسب الإقتصادية، دراسة نظرية تطبيقية، منشورات الحلبي القانونية القاهرة، مصر ، 2005، ص 48.

[2] - طارق إبراهيم الدسوقي عطية، مرجع سابق ، ص 176.

يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال التكنولوجيا المعلومات.[1]

ثانيا : الوسيلة

الوسيلة يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته، وفيما يتعلق بالمجرم المعلوماتي فإت الوسائل المتطلبة للتلاعب بالأنظمة الحاسب الآلية هي في أغلب الحالات تتميز نسبيا بالبساطةوالسهولة في الحصول عليها ، فالمجرم المعلوماتي يتميز بقدرته على الحصول على ما يحتاج إليه أو إبتكار الأساليب التي تقلل من الوسائل اللازمة لأتمام النشاط الإجرامي.

ثالث : السلطة

يقصد بالسلطة الحقوق أو مزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من إرتكاب جريمته، فالكثير من مجرمي الإلكترونية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة .

وقد تتمثل هذه السلطة في الشيفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات بفتح الملفات وقراءتها وموها أو تعديلها، وقد تكون السلطة التي يتمتع بها الجاني غير شرعية كما الحال في حالة إستخدام شيفرة الدخول الخاصة بشخص آخر.[2]

رابعا : التكيف الإجتماعي

حيث ينشأ بين مجموعة لها صفات مشتركة فمثلا جماعة صغار نوابغ الإلكترونية لاشك أنهم يتكيفون في أفكارهم فيما بينهم وتنشأ بالتالي بينهم صفات وروابط تساعدهم على

[1] - MASCALA Corinne , criminalité et contrat électronique, Travaux de l'association, CAPITANT Henir , journées National paris, 2000,p118.

[2] - طارق إبراهيم الدسوقي عطية، مرجع سابق ، ص177.

إرتكاب جرائمهم تتعدى تلك الروابط والصلات النطاق المحلي بحيث ينشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم، وتزداد خطورتهم الإجرامية إذا تزايد تكيفهم الإجتماعي مع وتافر الشخصية الإجرامية لديهم.[1]

خامسا : الباعث

وأخيرا يأتي الباعث وراء إرتكاب الجريمة، ولا يختلف باعث الجاني على إرتكاب الجريمة الإلكترونية في كثير من الحيان عن الباعث لإرتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء إرتكاب الجريمة المعلوماتية، ثم يأتي بعد مجرد الرغبة في فهو نظام الحاسب وتخطي حواجز الحماية حوله، وأخيرا الإنتقام من رب العمل أو أحد الزملاء[2].

ففي دراسة قديمة لإحدى المجالات المتخصص في الأمن المعلوماتي تعرض لها الفقه (PARKER) خلصا إلى أن 43% من حالات الإعتداء عاة نظم المعالجة الآلية المعلن عنها قد بوشرت بهدف إختلاس الأموال وأن 23% من أجل سرقة المعلومات وأن 19 % افعال الإتلاف وأن 15 % سرقة وقن الآلة، أي الإستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية.

أما فيما يتعلق بالرغبة في تحدي وقهر النظام فمن أشهر القضايا المتعلقة بهذه الحالة كان قد تعامل معها مكتب التحقيقات الفيدرالية، أطلق عليها إسم مجموعة الجحيم العالمي(GLOBAL HELL) تتلخص وقائعها في تمكين مجموعة من الأشخاص من إختراف مواقع البيت الأبيض والشركة الفديرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وقد أدين إثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة وقد

[1] - ايمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار النشر، دون بلد النشر، سنة 2004، ص 17.

[2] - D.B.PARKER, comibattre la criminalité informatique , edoros,1987,p142.

ظهرت من التحقيقات أن هذه المجموعات تهدف إلى مجرد الإختراق أكثر من التدمير او إلتقاط المعلومات الحساسة.

بالإضافة إلى الباعث آخر يدفع إرتكاب الجريمة الإلكترونية من قبيل ذلك أسباب تتعلق بالحياة المهنية، كالشعور بالحرمان من بعض الحقوق المهنية وخاصة ما يتعلق منها بالراتب ، ومن أمثلة ذلك قيام موظف فصل من الشركة التي كان يعمل بها وقبل يومين من تركه العمل قام ببرمجة كومبيوتر بالشركة زارعا نوعا من الفيروسات وبعد يومين حذفت المعلومات هامة في الشركة .[1]

الفرع الثالث : تصنيف المجرم المعلوماتي

أولا : المخترقون أو المتطفلون:

يتحد في هذا الإطار نوعين من المخترقين أو المتطفلين :

1- الهاركز (Les hackers)

يعرف الهاكرز بأنه الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي[2] ويقصد بهم الشباب البالغ المفتون بالمعلوماتية، والحسبات الآلية، أغلب هذه الطائفة هم من الطلبة والشباب حاصلين على المعرفة في مجال التقنية الإلكترونية والباعث الأساسي لهذهذ الطائفة عو الإستمتاع باللعب والمزاح بإستخدام هذه التقنية إثبات مهارتهم وقدراتهم بإكتشاف وإظهار مواطن الضعف غب الأنظمة المعلوماتية، دون أي إلحاق ضرر بها لديهم في المغامرة والتحري والرغبة في الإكتشاف.[3]

[1] - رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، وفي التشريع الجزائري المقارن، الطبعة الأولى ، منشورات الحلبي الحقوقية، بيروت ، لبنان، 2012، ص 95 و 96.

[2] - أسامة سمير حسين، الإحتيال الإليكتروني (الوجه القبيح للتكنولوجيا) ، الحنادرية للنشر والتوزيع ، الطبعة الأولى ، الأردن، 2011، ص 134.

[3] - عبد الفتاح البيومي الحجازي ، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر و الأنترنت، دار الفكر الجامعي ، الطبعة الأولى، الإسكندرية ، مصر ، 2006، ص 46.

2- الكراكز (Les crakers) :

ويعني ذلك المقتحم وتعرف هذه الطائفة بالمجرمين البالغين أو المخربين المهنين والكراكز تتراوح أعمارهم بين 25-45 عاما ومن أبرز سمات وخصائص أفراد هذه الطائفة، أنهم ذوي مكانة في المجتمع وأهنهم دائما ما يكونوا من المتخصصين في مجال التقنية الإليكترونية، أي أنهم يتمتعون بالمهارات، ومعارف فنية في مجال الأنظمة الإليكترونية أو الإلكترونية تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية المعلومات. [1]

ثانيا : مجرمو الكمبيوتر المحترفون:

تتميز هذه الطائفة بسعة للأنشطة التي تركب من قبل أفرادها، لذا فإن هذه الطائفة تعد الأخطر من بين مجرمي وللجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الكمبيوتر كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي. [2]

وتعتبر هذه الفئة أكثر خطورة من الصنف الأول للأضرار الكبيرة التي يُلحقوانها بضحاياهم وبإعتداءاتهم الإجرامية الخطيرة.

ثالثا: الحاقدون:

هذه الطائفة لا يغلب عليها توافر الأهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمين، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارتية وبنفس الوقت لا يسعون إلى مكاسب مادية او سياسية، إنما يحرك أنشطتهم الرغبة بالإنتقام والثأر كأثر لصاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها ولهذا فإنهم ينقسمون إما

[1] - محمد دباس الحميد، ماركو إبراهيم نينو، حماية الأنظمة المعلومات، دار حامد للنشر والتوزيع، الطبعة الأولى ، عمان ، 2007، ص 73.

[2] - جعفر حسين جاسم الطائي، جرائم تكنولوجيا المعلومات(رؤية جديدة للجريمة المعلوماتية)، دار البداية ،عمان، 2007، ص 162.

إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين أو على علاقة بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم. [1]

رابعا : الجماعات الإرهابية أو المتطرفون:

والتي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار إجتماعية أو سياسية أو دينية ويرغبون في فرض عذع المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويتركز نشاطهم بصفة عامة في إستخدام ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه .

ولقد بدأ إهتمام الجماعات الإرهابية، وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم، يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة الإلكترونية .

فإعتماد المؤسسات المختلفة داخل الدول على أنظمة الحسابات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في اغلب الأحوال، قد جعل من هذه الأنظمة هدفا جذبا لتلك الجماعات، حيث لا تزال المثلة في هذا المجال قليلة وإن كان متوقعا تزايدها مستقبلا، ومن أمثلة الشهيرة في هذا الخصوص قيان إحدى الجماعات الإرهابية المعروفة في أوروبا بإسم « The Red Brigades » يتدمر ما يزيد عن 60 مركزا للمحاسبات الآلية خلال الثمانينات لتلفت الأنظار إلى أفكارها ومعتقداتها [2].

خامسا : صغار السن:

[1] - نسرين عبد الحميد نبيه، الجريمة الإلكترونية والمجرم المعلوماتي، منشأة المعارف للنشر والتوزيع ، الأردن، دون سنة ، ص 42.

[2] - طارق إبراهيم الدسوقي عطية ، مرجع سابق، ص 181.

أو كما يسمون (صغار نوابع المعلوماتية) هم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية، وقد أثارت هذه الفئة جدلا واسعا في مجال الفقهي ففي حين كثر الحديث عن مخاطر هذه الطائفة، رأى جانب من الفقه أنه من أحسن عدم تصنيف هؤلاء ضمن دائرة الإجرامهم بحساب أن لديهم ميلا للمغامرة والرغبة في البحث والإستكشاف.[1]

المبحث الثاني : إجراءات البحث و التحري للكشف عن الجرائم المعلوماتية

في مجال المكافحة الإجرائية للجريمة المعلوماتية، يتعين الإشارة إلى الدور الذي تلعبه الشرطة القضائية كأداة رئيسية لصيانة أمن المجتمع وحمايته من الجرائم بصفة عامة والجرائم الإلكترونية بصفة خاصة، حيث نظرا لطبيعة هذه الأخيرة الخاصة وكيان بيئتها غير المحسوس؛ تظهر صعوبة دور الشرطة في الكشف عنها ومتابعة مرتكبيها، الأمر الذي أدى بالدول السباقة في مكافحة الإجرام المعلوماتي إلى إيجاد وحدات من الشرطة متخصصة بالعمل في هذا المجال، تكون مزودة بالخبراء المدربين وتنظيم دورات لهم للتخصص في مجال مكافحة الجريمة المعلوماتية، وذلك بتلقينهم المعلومات الخاصة بتقنية الحاسوبات والجوانب الفنية لها حتى تسهل عليهم عملية الكشف عن الجرائم ومنع وقوعها بإحكام الرقابة على المحلات العامة كنوادي الأنترنت ...الخ، والتي تعد المجال الخصب لاقتراف جرائم الإلكترونية [2] وكمثال على هذه الوحدات المتخصصة: الوحدة المركزية لمكافحة الجريمة المرتبطة بتكنولوجيا المعلومات والاتصالات المنشأة بموجب مرسوم صادر عن وزارة الداخلية الفرنسية (OCLCTIC) في ماي 2000 والتي تم ضمها لمديرية الشرطة القضائية، مهمتها العمل بالتعاون مع وحدات التحقيق في جرائم الغش في تكنولوجيا المعلومات ، وعليه سوف نبرز هذه الإجراءات فيما يلي:

المطلب الأول :معاينة مسرح جرائم المساس بأنظمة المعالجة الألية للمعطيات

[1] - رشيدة بوكر، مرجع سابق، 97.

2- طارق الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، مصر ، 2009، ص 422.

عند التكلم عن المكافحة الإجرائية للجريمة المعلوماتية، أول ما يجب دراسته هو معاينة مسرح الجريمة المعلوماتية: ويقصد بهذه الأخيرة رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة[1] أو هي إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة وهي تتطلب أن ينتقل مأمور الضبط القضائي إلى مكان ما لمباشرتها لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء."

وهي إجراء جائز في كافة الجرائم، إلا أن غالبية التشريعات بما فيها التشريع الجزائري في المادة 61 من قانون الإجراءات الجزائية الجزائري[2]، تقصرها على الجنايات والجنح الهامة، بحيث تعد إجراء وجوبيا في الجنايات وجوازيا في الجنح، وهي قد تتم في مكان عام أو مكان خاص، فإذا كانت في مكان عام؛ فمأمور الضبط القضائي لا يحتاج إلى إذن أو ندب سلطة تحقيق بإجرائها، أما إذا كانت بمكان خاص؛ فلابد لصحتها، إما رضا حائز المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها.

والهدف من إجراء المعاينة هو ضبط ما استعمل في ارتكاب الجريمة أو نتج عنها، ووضع الأختام في الأماكن التي أجريت فيها المعاينة، إذا وجدت آثار أو أشياء تفيد في الكشف عن الجريمة، كما يجوز لمأمور الضبط القضائي أن يعين حراسا على هذه الأماكن مع ضرورة إخطار النيابة العامة بهذه الإجراءات.

ولمعاينة مسرح الجرائم المعلوماتية، يجب التفرقة بين حالتين:

أ- معاينة الجرائم الواقعة على المكونات المادية للحاسوب :(Hardware) كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لمأمور الضبط القضائي معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

1- محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، مصر، 2008، ص 123

2 - المادة 61 من قانون الإجراءات الجزائية الجزائري

ب- معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها :(Software) كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات، تتلخص فيما يلي:

* قلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.

* الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغييرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المستقى من المعاينة.

ولنجاح المعاينة في الجرائم الإلكترونية يوصي الخبراء بوجوب إتباع ومراعاة قواعد وإرشادات فنية أبرزها ما يلي:

* القيام بتصوير الحاسوب وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة مع التركيز على تصوير أجزائه الخلفية وملحقاته، ومراعاة تسجيل الزمان والتاريخ والمكان الذي التقطت فيه كل صورة.

* يجب ملاحظة واثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للحاسوب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.

* عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.

* وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.

* ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.

* إبعاد الموظفين عن أجهزة الحاسب الآلي وكذلك عن الأماكن التي توجد بها أجهزة أخرى.

* التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.

- القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.
- يجب أن تقتصر مباشرة عملية المعاينة على مأموري الضبط وفئة الباحثين، ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسوب واسترجاع المعلومات، وممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم، والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة، ففي فرنسا مثلا، يقوم فريق مكون من 13 شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إلى وكلاء النيابة والمحققين، وهم قد تلقوا تدريب متخصص إلى جانب اختصاصهم الأساسي في مجال التكنولوجيا الحديثة، وهم يقومون بمرافقة المحققين أثناء التفتيش، حيث يقومون بفحص كل جهاز وينقلون نسخة من الاسطوانة الصلبة وبيانات البريد الالكتروني ثم يقومون بتحرير تقرير يرسل إلى القاضي الذي يتولى التحقيق[1] .

أما عن المعدات والبرامج، فهم يستخدمون برامج تستطيع استعادة المعلومات من على الأسطوانة الصلبة ن كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة ومن المهم هنا أن يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حدى بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها، ومن قام برفعه وتحريزه وكيف ومتى تم ذلك[2] .

1- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012، ص 131.

2- يمثل الحاسوب الآلي المحل الرئيسي للتفتيش في نظم المعلوماتية، وينصب التفتيش على المكونات المادية: وهي مجموعة من الوحدات لكل منها وظيفة محددة وتتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، وتسمى بمعدات الحاسوب وهي: وحدات الإدخال، وحدة الذاكرة الرئيسية، وحدة ذاكرة القراءة، وحدة الحاسوب والمنطق، الشاشة، وحدة التحكم، وحدة الذاكرة المساعدة، وحدة الإخراج، الطابعة.

- طارق الدسوقي عطية، المرجع السابق، ص 441.

الفرع الأول :إجراءات تفتيش النظم الإلكترونية وضبطها

إن الهدف من التفتيش هو ضبط الأدلة المادية للكشف عن الجريمة، فكل ما يضبطه مأمور الضبط القضائي بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن يعد أيضا إجراء من إجراءات التحقيق في الجرائم المعلوماتية؛ بوضع اليد على الشيء وحبسه والمحافظة عليه، للحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينةوهو ما سنبرزه فيما يلي:

أولا: تفتيش نظم المعلوماتية

عملية تفتيش تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

الحالة الأولى :في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

الحالة الثانية :إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن، ففي ألمانيا يرى الفقه[1] أنه يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر تطبيقا لمقتضيات القسم 103 من قانون الإجراءات الجزائية الألماني، وذلك عندما يكون مكان تخزين البيانات الفعلي خارج المكان الذي يتم فيه التفتيش.

1- طرشي نورة، المرجع السابق، ص 115.

إذن لتفتيش الحاسوبات الآلية ذات نهاية طرفية في دولة أجنبية، نصت بعض التشريعات على طريقة ثانية كإجراء للتحقيق في الجريمة الإلكترونية وهذه الطريقة هي: التنصت والمراقبة الالكترونية لشبكات الحاسوب ويقصد بهذه الطريقة –التنصت– مراقبة المحادثات التلفونية وتسجيلها بالنسبة للأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويعتقد بفائدة محادثته في الكشف عن الجريمة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها.

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

الحالة الثالثة :إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوبات الآلية المحمولة) في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة ...الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات، وقد اتفقت بعض التشريعات، كالتشريع الجنائي الكندي في المادة 487 التي أجازت إصدار أمر قضائي لتفتيش وضبط أي شيء يؤدي للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها، ونصت صراحة على إمكانية تفتيش مكونات الحاسوبات المادية للكشف عن الجريمة الإلكترونية باتخاذ أي إجراء أو القيام بأي فعل لازم لجمع الأدلة والحفاظ عليها[1].

ثانيا : :تفتيش نظم الحاسوب المنطقية أو المعنوية :

يعرف الكيان المنطقي للحاسوب بأنه: "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات[2].

1– طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 385.

2– عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية،بيروت ، لبنان ، 2007. ص 45

وهو يشتمل على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي كالبرامج ونظم التشغيل وقواعد البيانات ... الخ، لقد ثار الخلاف في التشريع المقارن في مسألة ضبط وتفتيش المكونات المعنوية أو المنطقية للحاسوب، فتعددت الآراء في هذا الشأن؛ فذهب رأي إلى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في الكشف عن الحقيقة، فإن هذا المفهوم يجب أن يمتد ليشمل البيانات الالكترونية، كالقانون الإجرائي اليوناني في نص المادة 251 التي تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، تفسيرا لعبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة آليا أو الكترونيا، بما فيها ضبط البيانات المخزنة في حاملات البيانات المادية، أو في الذاكرة الداخلية وذلك بإعطاء المحقق أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل للمحاكمة الجنائية، على أساس إنها كيانات يمكن قياسها بما انها نبضات أو ذبذبات الكترونية قابلة لان تسجل وتخزن على وسائط معينة يمكن قياسها[1] .

وقد حذا المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري حذو التشريعات السابقة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك."

هناك بعض الحالات الخاصة يفرض التساؤل عن كيفيات التعامل معها قانونيا في إجراءات ضبط المعلوماتية، والتي سنرى كيف تصدت لها القوانين المقارنة، بالحل كالتالي:

1 – مدى جواز الاطلاع على المحتويات المعلوماتية:

يطرح في مجال التفتيش والضبط المعلوماتي في الجريمة الإلكترونية إشكال جواز أو عدم جواز اطلاع مأمور الضبط القضائي على المحتويات المعلوماتية، فجرى العمل في ألمانيا على أن سلطة الاطلاع على مطبوعات الحاسوب وحاملات البيانات تقتصر على المدعى

1– هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة،مصر ،2000، ص 52.

العام فقط، ولا يكون لضباط الشرطة الحق في قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى البيانات المخزونة دون إذن من الشخص الذي له الحق في نقل هذه البيانات، لكن كل ما يمكنهم هو مجرد فحص حاملات البيانات دون استخدام أي مساعدات فنية تطبيقا لما جاء في القسم 110 من قانون الإجراءات الألماني[1] .

2 – حق المتهم في الصمت:

يقصد بالحق في الصمت أن للشخص المتهم في جريمة ما مطلق الحرية في الكلام أو عدمه أو عدم الإجابة على الأسئلة الموجهة إليه من قبل مأمور الضبط القضائي أو الموظف القائم بالتحقيق معه، لأنه غير ملزم بالكلام كما يجب أن يراعى أن رفضه الإجابة وصمته، لا يجوز أن يؤخذان كقرينة ضده[2] وذلك تطبيقا للقاعدة الإجرائية العامة التي مفادها: "عدم إجبار الشخص على الكلام أمام أي جهة أو سلطة كحق من حقوق الإنسان"، والتي أوصى بها كل من المؤتمر الدولي السادس لقانون العقوبات المنعقد في روما سنة 1953، والمؤتمر الدولي الذي نظمته اللجنة الدولية لرجال القانون في أثينا في جوان لعام 1955، كما حرصت معظم التشريعات الجنائية على النص صراحة على هذا الحق كالقانون الفرنسي في المادة 114 قانون إجراءات جزائية التي تلزم قاضي التحقيق أن ينبه المتهم عند حضوره أمامه لأول مرة إلى أنه حر في عدم الإدلاء بأي إقرار، ويثبت ذلك التنبيه في محضر التحقيق، ومثلما فعل المشرع الجزائري في المادة 100 من قانون الإجراءات الجزائية.

أما بالنسبة للشاهد المعلوماتي، نعلم أن الشهادة هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شهده أو سمعه أو أدركه بحواسه عن هذه الواقعة، كما يقصد بسماع الشهود السماح لغير أطراف الدعوى الجنائية بالإدلاء بما لديهم من معلومات أمام سلطات التحقيق، والشاهد المعلوماتي قد يكون شاهدا عاديا أو خبيرا في الدعوى القائمة، بالنسبة للشاهد العادي فهو ذلك الشخص الذي يقدم إلى القاضي معلومات حصل عليها بالملاحظة الحسية،

1– طرشي نورة، المرجع السابق، ص 120.

2– سامي صادق الملا، اعتراف المتهم، دار الفكر العربي، الطبعة الأولى،مصر ، 1998، ص 187 .

أما الخبير فهو ذلك الشخص المختص الذي يقدم إلى القاضي تقارير وآراء توصل إليها بتطبيق قوانين علمية وأصول فنية.

3 – مدى جواز إجبار المتهم والشاهد المعلوماتي على الإدلاء ببيانات

بالنسبة للمتهم المعلوماتي جرى العمل في الفقه والقانون في فرنسا حسب نص المادة 27 من ق اج ج الفرنسي التي نصت على أنه من غير الممكن إجراء تفتيش المساكن وضبط الأشياء التي يمكن أن تكون متعلقة بالجريمة إلا بموافقة صريحة للشخص المراد تفتيش منزله أو أشيائه كما بينت الفقرة الثانية من نفس المادة، بأن الموافقة يجب أن تكون صريحة لا ضمنية، وفي حالة رفض الموافقة الصريحة فإن ذلك يعني رفض ذوي الشأن، ولذلك تعد الإجراءات باطلة وعلى هذا لا يجوز قانونا إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات أو إلزامه بالكشف عن الشفرات أو كلمات السر خاصة بالدخول إلى هذه المعلومات أو إجباره على تقديم الأمر اللازم لوقف فيروس، تطبيقا لمبدأ عدم جواز إلزام الشخص بتقديم دليل ضد نفسه سواء عن طريق الشهادة أو غيرها من عناصر الإثبات، إلا أن ذلك لا يمنع من إجباره على تسليم الشفرة الخاصة بالحاسوب الآلي المخزنة فيه البيانات محل الجريمة[1] .

والشاهد المعلوماتي بنوعيه المذكورين سابقا يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، كما أنه يلتزم في بعض الدول الأوروبية بإجراء ما يسمى بإنعاش الذاكرة، بفحص الأماكن والمستندات التي توجد تحت سيطرته وذلك في كل من السويد وفنلندا والنرويج، أما في انجلترا فالقانون الانجليزي الصادر عام 1984 يعطي المحققين الحق في إلزام الغير بتمكين سلطات التحقيق الدخول إلى المعلومات المخزنة في الحاسوب الآلي أو الاطلاع عليها أو قراءتها، كما تسمح بعض التشريعات المقارنة في مجال التحقيق المعلوماتي الاستفادة من الشهود كخبراء أو كمساعدين للقضاء من تلقاء أنفسهم ودون حاجة لاستدعائهم[2] .

1- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، مصر ،2001، ص 106

2- محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، ط 8،مصر، 2008، ص. 68.

الفرع الثاني :القواعد الشكلية لتفتيش نظم المعلوماتية

تتلخص هذه القواعد كما يلي:

أ –**إجراء التفتيش بحضور أشخاص معينين بالقانون** :من بين هذه الأشخاص: المتهم والقائم بالتفتيش وشاهدين طبقا للمادة 45 من قانون الإجراءات الجزائية الجزائري، تنص على أن: أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية–القائم بالتفتيش–، وإذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته، غير أنه كاستثناء على هذه القواعد نص المشرع الجزائري في الفقرة الأخيرة من المادة45 من قانون الإجراءات الجزائية الجزائري، على أنه: "لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات".

ب –**إعداد محضر خاص بالتفتيش** :ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

ت –**إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده** :لهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي[1] .

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي:

1– طرشي نورة، المرجع السابق، 125.

– تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خدمة شبكة الانترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على أثار الجريمة.

– إبعاد المتهم عن مكان النظام إن كان قريبا منه.

– أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي.

– الدخول إلى الموقع ببطء، لكي لا يتم تشويه أو إتلاف الدليل.

– عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أو صعبة.

– يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها[1] .

وفي نطاق تفتيش نظم الحاسوب، نجد أن أغلب التشريعات الإجرائية لم تحدد مدة معينة لتنفيذ إجراء التفتيش ما عدا البعض منها كالتشريع الانجليزي الذي حدد مهلة الشهر الواحد من تاريخ إصدار الإذن كما أنها تختلف في الزمن الذي يجري فيه التفتيش أو تحديد المدة التي يجري فيها، غير أن الرأي الغالب في مجال تفتيش النظم الإلكترونية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم الإلكترونية هو ليلا، لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضا لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت، مثلما فعل المشرع الجزائري في الفقرة الثالثة من المادة 47 من ق إ ج ج[2] .

المطلب الثاني :إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية

تعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في الكشف أو في التحري عن الجرائم عموما، وفي سبيل كشفها عن هذه الجرائم، أعطاها القانون سلطة التحري عن الجرائم، كما منحهم قانون الوقاية من الفساد ومكافحته وكذا قانون الإجراءات الجزائية الجديد أساليب جديدة للتحري، أسماها "أساليب التحري الخاصة"، كما أضافت التأكيد على اعتبار جرائم

1– عفيفي كامل عفيفي، المرجع السابق، ص 65.

2– طرشي نورة، المرجع السابق، ص 126.

المساس بأنظمة المعالجة الآلية للمعطيات من الجرائم التي قرر المشرع صراحة وبنص صريح إمكانية إتباع إجراءات التحري الخاصة في الكشف عنها ومكافحتها، نص المادة 04 من القانون 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، التي قررت الفقرة الثانية منها أنه: " في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني."

أول خطوة في الكشف عن جرائم الإعلام الآلي على مستوى الضبطية القضائية هي مرحلة التحري، حيث يقصد بالتحري في مجال الضبط القضائي، البحث عن الجرائم المرتكبة والتحقق من صحة الوقائع المبلغة لضباط الشرطة القضائية، وجمع القرائن التي تفيد في حصول الواقعة أو نفي وقوعها[1].لذلك فإن رجال الضبطية القضائية إذا أخطروا بجريمة من الجرائم، فإنهم يقومون بالإجراءات الأولية وهذه الإجراءات مرتبطة بالبحث والتحري والذي يعد كمرحلة تمهيدية للدعوى، هذه الإجراءات في حد ذاتها ضرورية، فكلما قرب الزمن بين الإجراء والجريمة كانت الأدلة واضحةً أكثر وأسلم ولم يشبها أي تغيير أو تحريف ومن تم كانت أدعى للثقة[2] وفي سبيل مكافحة جرائم الفساد، نص المشرع على مجموعة من أساليب التحري تضاف إلى تلك الأساليب التقليدية، وأطلق على هذه الأساليب عبارة" أساليب التحري الخاصة"، ويتمثل الهدف من هذه الأساليب في الكشف عن هذه الجرائم واستئصال الفساد وردع المفسدين.

الفرع الأول :توسيع الإجراءات الخاصة بالاختصاص في الجرائم المعلوماتية

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه تطويقها والقضاء عليها أو على الأقل الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث وضع قواعد وأحكام خاصة لسلطة التحري والمتابعة الغرض منها هو مواجهتها، وقد وردت هذه الأساليب في قانون

1- محمد ماجد ياقوت، أصول التحقيق الإداري في المخالفات التأديبية، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، بدون سنة نشر، ص 289.

2- محدة محمد، ضمانات المتهم أثناء التحقيق، الجزء الثالث، الطبعة الأولى، دار الهدى، عين مليلة، الجزائر، ص 105.

الإجراءات الجزائية المعدل والمتمم بموجب القانون 22/06 الصادر في 2006/12/20، وقانون الوقاية من الفساد ومكافحته رقم 01/06 المؤرخ في 20 فيفري 2006، وهي: أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وكذلك أسلوب التسرب أو كما سماه قانون الوقاية من الفساد ومكافحته أسلوب الاختراق.

لذلك لابد من شرح هذه الأساليب، وكيف يمكن التوفيق بين هذه الأساليب التي تتم خلسة وما تحمله من معنى الاعتداء على الحريات والحقوق الخاصة للأفراد، خاصة إذا علمنا أن الحرية الخاصة للأفراد وسرية المراسلات مضمونة دستوريا[1] .

أولا : جواز تمديد الاختصاص المحلي والنوعي الدولي للمحاكم الجزائرية :

حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المرسوم التنفيذي رقم 06/348 المؤرخ في 05/10/2006.)

كما أنشئت الأقطاب القضائية الجزائية المتخصصة بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية من بين الجرائم التي تختص بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المواد37 و40 و329 من قانون الإجراءات الجزائية).

كذلك، نظم المشرع الجزائري في القانون رقم 04/09 المؤرخ في 5 أوت 2009، أحكاما جديدة خاصة بالاختصاص في مجال بالجريمة الإلكترونية تتماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصت عليه المادة الثالثة التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية، بالإضافة إلى ذلك، قررت المادة 15 من القانون 04/09 أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة

1- المادة (39) من الدستور الجزائري لعام 1996، معدل ومتمم، التي تنص على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة."

خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

ثانيا :توسيع مجال اختصاص النيابة العامة

بموجب المادة 37 من قانون الإجراءات الجزائية، تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

كذلك سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و144 مكرر1 و144 مكرر2 من قانون العقوبات المعدل والمتمم بالقانون رقم 09/01 المؤرخ في 26 يونيو 2001[1] .

الفرع الثاني :الإجراءات المتعلقة بالتحري والكشف عن الجريمة المعلوماتية

إضافة لما سبق ودائما في إطار المكافحة الإجرائية للجرائم الإلكترونية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرر 5 في إطار تعديل من قانون الإجراءات الجزائية الجزائري بالقانون 22/06 المؤرخ في20/12/2006 التي تنص: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة

1- طرشي نورة، المرجع السابق، ص 134.

الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية، أن يأذن بما يأتي:

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

– وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون، وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.

أولا :الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور

مكن المشرع الجزائي ضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور للكشف عن الجرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة[1] .

وإلتقاط الصور يكون بالتقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص، ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن العامة والخاصة.

أما تسجيل الأصوات، فيتم عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع إلتقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية[2] .

إن ما يهم هو أن مثل هذا الإجراءات يمكن له المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة

1– خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010، ص 72– 73.

2– حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 1990، ص 78.

بتكنولوجيا الإعلام والاتصال ومكافحتها أنه: "مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية[1] .

بالإضافة إلى أن كل متهم بريء حتى تثبت إدانته [2] ذلك هل يجوز إثبات أو نفي الاتهام عن المشتبه فيه، باللجوء إلى وسيلة التسجيل الصوتي أو اعتراض المراسلات أو التقاط الصور في الأماكن العامة والخاصة، وخصوصا أن مثل هذه الإجراءات أو الوسائل قد لا تمس بشخص المتهم فقط، وإنما كذلك بمن يحيطون به من أقاربه أو معارفه؟.

يفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني، يكون الثاني برضا أو بطلب من صاحب الشأن، ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

ويعد هذا الإجراء الحديث من أهم إجراءات التحقيق، مكن المشرع ضابط الشرطة القضائية ممارسته للكشف عن الجرائم التي حددها على سبيل الحصر في المادة 65 مكرر 5 بموجب قانون الإجراءات الجزائية، تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل، بمعنى أنها إجراء للتحري والتحقيق، وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جدية على أنه ضالع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية.

1- المادة 3 من قانون رقم 09- 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

2- تنص المادة (45) من دستور عام 1996 على أنه: "كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته مع كل الضمانات التي يتطلبها القانون.

لكن مع ذلك، نجد المشرع حاول يوفق بين هذه المتعارضات، بأن أجاز هذه الأساليب، ولكن بضوابط وهي مباشرة التحري بإذن من وكيل الجمهورية المختص، وإلتزام أعوان وضباط الشرطة القضائية القائمين بالإجراء السر المهني، وفيما يلي نتولى شرح كلا الضابطين، فالمشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرمة الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة [1] وهو ما سنشير إليه على النحو التالي:

أ – مباشرة التحري بإذن من وكيل الجمهورية

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قررته المادة 04 من القانون 04/09 التي جاء فيها أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة[2] .

ويجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء أكانت سكنية أو غير سكنية، كما يجب أن يتضمن نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدة هذه التدابير لذلك فإن الإذن المسلم من قبل وكيل الجمهورية للتحقيق في جريمة ما لا يصلح للتحقيق في جريمة أخرى، إلا بإذن جديد، كذلك يجب أن يتضمن الإذن كل الأماكن التي توضع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام المتفوه به بصفة خاصة من شخص أو عدة أشخاص[3] .

وعند مباشرة التحريات والتحقيقات، يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص، محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط للصور، وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي

1– المادة (303 مكرر) من الأمر رقم 156/66 معدلة ومتممة بموجب المادة (33) من القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006.

2– المادة(65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

3– المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها [1].بحيث يشتمل المحضر على كل البيانات المذكورة سابقا وتكون محددة تحديدا نافيا للجهالة، ويجب أن يشتمل المحضر على توقيع محرره في نهايته[2] بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة أو المفيدة في إظهار الحقيقة في محضر يودع بملف المتهم، وتنسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض[3] .

ب – إلتزام السر المهني

تكون إجراءات التحري والتحقيق سرية، ومن ثم، فإن بحثها ضمن الضمانات الممنوحة للمتهم [4] والسرية تعني القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس هدفها كما كان عليه من قبل هو تسهيل قمع المتهم، بل صارت وسيلة لضمان الحريات الشخصية[5] .

فقد نص المشرع صراحة على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ملزم قانونا بكتمان السر المهني ويجب أن يتخذ مقدما التدابير اللازمة لضمان احترام ذلك السر[6] وقد نص قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع، وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة[7] في قانون العقوبات وتحت طائلة العقوبات المنصوص

1– المادة (65 مكرر 9) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

2– كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000، ص 271.

3– المادة (65 مكرر 10) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

4– المادة (11) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06

5– سهيلة بوزيرة، مواجهة الصفقات العمومية المشبوهة، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل، 2008، ص 127.

6– المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

7– المادة (45 /3) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

عليها فيه، لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الألية للمعطيات تتم بسرية مطلقة، فيمنع منعا باتا أن يخبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على ضابط الشرطة المأذون له أو المناب أن يفصح عن مضمون محضر التحريات لأي شخص كان، وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضباط الشرطة القضائية ومرؤوسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهددة ببيانات غير مؤكدة[1] .

ثانيا :أسلوب التسرب أو الاختراق

يعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5)، كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة [2] ويشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية المختص، ويجب أن تتم العملية تحت أشرافه ومراقبته، فإن قرر قاضي التحقيق مباشرة هذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن مكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه [3]. وهذا تحت طائلة البطلان المطلق، فيجب أن يكون الإذن مكتوبا يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب.

والتسرب هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم[4] فالتسرب إذن هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم، ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة

1- المادة (11) الأمر رقم 155/66 معدل ومتمم.

2- قدري عبد الفتاح السهاوي، المرجع السابق، ص 191.

3- المادة (65 مكرر 11) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

4- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2009، ص 115.

بعض الجرائم، دون أن يكون مسؤولا جزائيا[1] .وذلك بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية[2] .

ولهذا يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

– اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

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

ويحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب إلا لرؤسائهم السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب المادة (65 مكرر 16) بأن نصت صراحة أنه:" لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات."

كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 50000 دج إلى 2000000 دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس سنوات إلى 10 سنوات والغرامة من 200000 دج إلى 500000 دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من 10 إلى 20 سنة والغرامة من 500000 إلى 1000000 دج[4] .

1– المادة (65 مكرر12) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

2– عيساوي نبيلة، المرجع السابق، ص 02.

3– عبد الرحمن خلفي، المرجع السابق، ص 74– 75.

4– المادة (65 مكرر 14) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

ولضمان نجاح عملية التسرب للكشف عن جرائم الصفقات العمومية، يلتزم المتسرب القيام بهذه العملية بكل الإجراءات المحددة قانونا، وأهمها حصوله على الإذن المكتوب من قبل وكيل الجمهورية المختص بحيث إلتزام هذا الأخير بالإشراف والمراقبة على نجاح العملية، وكما يلتزم المتسرب حفاظا على أمنه وسلامة العملية بعدم الكشف عن هويته، وذلك لخطورة مهمته التي تتطلب جرأة وكفاءة ودقة في العمل.

ورغم أن المشرع أجاز مثل هذه الأفعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون، مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن يحرّضوا المشتبه فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه لارتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء.

الفرع الثالث : إجراءات التحري والحجز والكشف عن الجرائم الإلكترونية بموجب القانون 09/04

بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراءات مراقبة الاتصالات الإلكترونية، وتفتيش وحجز المنظومة المعلوماتية، وعليه سنوجزها كالتالي:

أولا :مراقبة الاتصالات الإلكترونية وتجميعها

القاعدة أنه أضفى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في النظام القانوني الجزائري ، ألا وهو الدستور، وهذا في إطار القواعد العامة التي ت عنى بالحماية القانونية للحياة الخاصة للأفراد ، وهو ما ينطوي عليه بالضرورة حماية بياناتهم الشخصية من المعالجة الآلية، بحيث اعترف المشرع الدستوري الجزائري بها في المادة 77 التي تنص على أنه: "يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما احترام الحق في الشرف، وستر الحياة الخاصة."...

كما أيدت ذلك المادة 46 من دستور سنة 1996 التي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، إلا أنه في تعديل الدستوري لسنة2016 ، حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية، من خلال إضافة فقرتين للمادة أعلاه تنصان على أنه:" لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون انتهاك هذا الحكم[1] .

إن أضافت الفقرتين الثالثة والرابعة في التعديل الأخير، إنما ينم عن اقتناع المشرع الجزائري بضرورة المبادرة إلى وضع الآليات القانونية الكفيلة بحماية البيانات الخاصة بالأشخاص الطبيعيين خلال عملية المعالجة الآلية لها، كما يدل الإقرار الدستوري على أن القانون الخاص بالحماية البيانات هو مسألة وقت فقط، خاصة في ظل النشاط التشريعي الذي الجزائر في العشرية الأخيرة، وأن وزارة البريد وتكنولوجيات الإعلام والاتصال تدرس ابتداء من نوفمبر 2014 مشروع قانون حول حماية البيانات الشخصية على الأنترنيت والذي يفترض أن يصدر قريبا.

علما أن الجزائري هو الوحيد بين الدساتير العربية الذي تطرق لحرمة البيانات الخاصة من المعالجة الإلكترونية، بحيث تكتفي جلها بتكريس الحماية الدستورية للمراسلات بكل أشكالها فقط[2] .

وبهذا يكون المشرع الجزائري رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها، قد خول استثناء السلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية، بالنظر لخطورة بعض الجرائم الإلكترونية المحددة حصرا: تسجيل الاتصالات الإلكترونية في حينها.

1- المادة (3/65 – 4 مكرر) من الأمر رقم 155/66 المعدل والمتمم ومعدل بموجب المادة (14) من القانون رقم 22/06.

2- القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07 مارس 2016.

كما بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية، وذلك على سبيل الحصر، وهذه الحالات هي:

– للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

– لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.

يظهر من خلال استقراء نص هذه المادة، أن المشرع الجزائري يحاول الاستفادة بدوره من التطور التكنولوجي والمميزات التي يخولها، من خلال وضع المشتبهين فيهم تحت المراقبة الإلكترونية، وهي على عكس المراقبة الشخصية أقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها، إلا أنه من جهة أخرى، فإن وضع الشخص تحت المراقبة الإلكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الأنترنيت، من شأنه انتهاك حرمة البيانات ذات الطابع الشخصي له، باعتبار أنه لدواعي فرز المعلومة للتأكد من قيمتها كدليل إثبات أو نفي، يستدعي سماعها أو قراءتها بكل تأني، وهذا ما من شأنه الوصول إما لأنها معلومة ضرورية لاستكمال التحقيقات، أو أنها معلومات شخصية لا دخل لها بالقضية، كما يمكن أن يصار إلى تبرئة الشخص تماما، لكن بعد ماذا؟.

بغرض تأطير هذه العملية الحساسة وتخفيف تأثيراتها السلبية على حماية الحياة الخاصة للأفراد وضع المشرع عدة ضمانات هي:

1 –حصر الحالات التي يمكن اللجوء فيها إلى المراقبة الإلكترونية

هي الحالات التي أوضحتها المادة الرابعة من القانون 04/09 على سبيل الحصر":

أ– للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني

- أو مؤسسات الدولة أو الاقتصاد الوطني.

ج- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون

- اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ المساعدة القضائية الدولية المتبادلة[1] .

بإستقراء الحالات هذه، نجد أن المشرع ق لص من الحالات التي يمكن فيها اللجوء إلى عملية المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، ذلك أنه عندما يتعلق الأمر مثلا بالجرائم الإرهابية والتي تطال المدنيين فإنه لا يمكن الحديث عن حقوق الإنسان، وكذا في حالات تنفيذ المساعدة القضائية، إلا أن إضافة الحالة "ج" والتي تعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية صغيرة كانت أو كبيرة، يؤدي إلى تعميم استخدام الآلية دون حد.

2 -وضع آلية إقرار المراقبة الإلكترونية تحت سلطة القضاء:

تضيف المادة 2/4 من القانون 04/09، بأنه:"لا يجوز إجراء عمليات المراقبة، إلا بإذن مكتوب من السلطات القضائية المختصة."

كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية، إذنا لمدة 6

1- لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي ، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017، ص 6.

أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[1] .

كما تنص المادة 41 من المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر 2015 ، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2] على أن الهيئة تمارس اختصاصاتها الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص.

كما يخضع الموظفون الذين يدعون إلى الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم، وهم يلزمون بذلك بالسر المهني)المادتين 27و28 المرسوم الرئاسي 261/15)

يعتبر وضع هكذا آلية تمس بالحريات الفردية والحياة الخاصة للأفراد تحت يد القضاء المستقل، ضمانة حقيقية باعتبار أن القاضي يهدف إلى الموازنة بين ضرورات التحقيق وإلزامية حماية الأفراد المشتبه فيهم، فمجرد الاشتباه لا يجعل من الفرد مجرما، وهذا ما يسمى ضمانات المحاكمة العادلة.

3 -تحديد تقنيات الرقابة الإلكترونية وحدود استعمال المعطيات المتحصل عليها

تكون الترتيبات التقنية الموضوعة للأغراض المراقبة الإلكترونية موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر أعلاه على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة.

1- لوكال مريم، المرجع السابق، ص 09.

2- نصت المادة 65 مكرر 7 من قانون الإجراءات الجزائية، على أنه: " يتضمن الإذن كل العناصر التي تسمح على التعرف على الاتصالات ويسلم مكتوبا ويكون صالحا لمدة أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية والزمنية، يسلم الإذن لوضع الترتيبات بغير رضا أو علم الأشخاص الذين لهم حق على تلك الأماكن"

أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية فهي تتمثل في: اعتراض المراسلات الإلكترونية[1] تسجيل الأصوات، التقاط الصور[2] تفتيش المنظومات الإلكترونية وحجزها)المادة 5 و7 من القانون 04/09، إلا أن السؤال الأهم هو ما مصير المعلومات المتحصل عليها؟

أجابت المادة 09 من القانون 04/09 المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية يتحدد بحدود ضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.

4 – سن عقوبات لجريمة إفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الإلكترونية

يكون الموظفين القائمين على عمليات المراقبة الإلكترونية قادرين على الاطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني. لهذا جرم المشرع كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة لأغراض شخصية، أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب، أو إفشاء مستندات ناتجة عن التفتيش أو إطلاع عليها شخص لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن مكتوب من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك[3] .

1– مرسوم رئاسي رقم 15–261 مؤرّخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 ص 16.

2– تعرف المادة 2 /والاتصالات الإلكترونية على أنها": أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."

3– المادة 65 مكرر 5 من القانون رقم 15 – 19 المؤرخ في 30 ديسمبر 2015 يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 جوان 1966 ، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 ، الصادرة في 30 ديسمبر 2015

ثانيا :إجراءات تفتيش المنظومة المعلوماتية

قررت المادة 5 من القانون رقم 04/09، أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذلك المعطيات الإلكترونية المخزنة فيها.
- منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة- أ- من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وإذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

وكمثال على المساعدة القضائية الدولية كإجراء جديد لتتبع مجرمي المعلوماتية، قضية توقيف مصالح الأمن الجزائرية لشاب جزائري ببلدية بومرداس بعد تقديم المكتب الفدرالي الأمريكي للتحقيقات شكوى ضده مفادها أن هذا الشاب قد بعث برسالة إلكترونية لهذا المكتب مهددا فيها بوضع قنبلة في أحد أحياء مدينة جوانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبل انطلاق المباراة الكروية بين المنتخب الجزائري والأمريكي في بطولة كأس العالم.

والمشرع الجزائري في المادة الخامسة من القانون رقم 04/09 نص على التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وأن اختلف مضمونه عن التفتيش العادي

بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

غير أن القانون رقم 09/ 04 أجاز إجراء التفتيش على المنظومة الإلكترونية عن بعد، وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها[1] .

ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة الإلكترونية محل البحث أو بالتدابير المتخذة لحماية المعطيات الإلكترونية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها[2] .

كما نص المشرع الجزائري، ودائما في نفس القانون 04/09 على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 5، وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسوبات لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات[3] .

ثالثا :حجز المعطيات المعلوماتية

أكدت المادة 6 من القانون رقم 04/09، أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات

1- المادة 46 من الأمر رقم 15 – 02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40 ، الصادرة في 23 جويلية 2015.

2- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2011-2012، ص 131-132.

3- المادة 05 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة الإلكترونية التي تجري بها العملية، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات، وإذا استحال إجراء الحجز وفقا لما هو منصوص عليه في أحكام المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة الإلكترونية والى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة[1] .

ويمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك[2] .

وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[3] .

وفي إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من القانون رقم 04/09 تحت تصرف السلطات المذكورة، وذلك لتمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

1- طرشي نورة، المرجع السابق، ص 132-133.

2- المادة 07 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

3- المادة 08 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[1].

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب من خلال المادة 12 من القانون رقم 04/09، على مقدمي الخدمات إلتزامات خاصة، هي:

– واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.

– وضع الترتيبات التقنية لحصر إمكانيات الدخول إلي الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجود[2] .

رابعا : دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

لقد نص المشرع الجزائري في مرسوم رئاسي رقم 261/15 المؤرخ في 24 من ذي الحجة عام 1436 هـ/ الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تعد سلطة إدارية مستقلة لدى وزير العدل ستعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وكلفت الهيئة بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

1– المادة 10.09 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

2– مرسوم رئاسي رقم 261/15 المؤرخ في 24 من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،الجريدة الرسمية العدد 53 ص 16.

وتتشكل هذه الهيئة من لجنة مديرة يرأسها الوزير المكلف بالعدل وثلاثة مديريات ومركز للعمليات التقنية وملحقات جهوية، كما يتمثل أعضاؤها في الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيا الإتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا[1] .

وبهذا ضمت الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.

ويتمثل دور هذه الهيئة في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام كالاتصالات ومكافحتها، وهي تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكتًرونية.

كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال وضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة، وذلك تحت سلطة القاضي المختص، وباستثناء أي هيئة وطنية أخرى.

أما فيما بخص مجال تطبيق الوقاية من هذه الجرائم ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات كالإتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيان بإجراءات التفتيش والحجز داخل المنظومة الإلكترونية [2].

1- _طرشي نورة، مرجع سابق ، ص 134.

2- المادة 6 و7 من المرسوم الرئاسي رقم 261-15 المؤرخ في 24 من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها..

وإنشاء هذه الهيئة مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة ومراجعة الترسانة التشريعية بما في ذلك في المجال الجزائي من أجل تحسين حماية حقوق وحريات المواطنين وتشديد العقوبات على أي تقصير في هذا المجال[1] .

ولكن تثبت التقارير الإحصائية للمديرية العام الامن الوطني ،لسنة 2016 الصادرعن الجهاز دور الهئية الوطنية للوقاية من الجرائم المتصلة بتكنواوجيا الاعلام والاتصال ومحكافحتها أن هذا الرقم هو أقل بأضعاف من حجم الاعتداءات الفعلية التي أثبتت تقارير أنها تكون بين 200 إلى 250 اعتداء يوميا بمختلف الأشكال التي وإن وضع المشرع نظام حماية نظام المعالجة الآلية للمعطيات، إلا أنه لم تعالج نصوصه الأفعال المقترفة بشكل مفصل، والتي تتطور بشكل مذهل في الثانية الواحدة وكأنها مسابقة عالمية بين المخترقين والقراصنة حول من يبتكر أكثر جريمة انترنت تطورا وسرعة، وحتى الدول الكبرى لم تتمكن من وضع آليات ووسائل فعالة للحد من الإجرام المعلوماتي أثبتت التقارير الصادرة عن مكتب التحقيقات الفدرالي (FBI) أن جرائم الكمبيوتر تكلف الاقتصاد الأمريكي 67.2 دولار سنويا، وحوالي 64 بالمئة من الشركات الأمريكية؛ تعرضت لخسائر مالية بسبب حوادث اختراق أنظمة الكمبيوتر خلال العام الماضي[2] .

1- برابح يمينة، "تطبيقات الأمن المعلوماتي"، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان، يومي 7 و8 فبراير 2017، ص 9.

2- إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته التي سبق ونص عليها القانون رقم 04/09 المؤرخ في 5 أغسطس 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفصل الثاني
خصوصيّة الجريمة المعلوماتيّة من الناحيّة الإجرائيّة

أن الجريمة الإلكترونية ترتكب بإستخدام التقنية الإلكترونية مما يعني انها ترتكب في فضاء إفتراضي مفرغ، يختلف كليا عن مسرح التقليدي الذي ترتكب فيه الجريمة حيث يتم الإستدلال عليها وضبطها وإثباتها بوسائل تقليدية، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات الجريمة الإلكترونية التي أرتكبت في عالم إفتراضي غير ملموس.

فمن ناحية المنطلق سوف نحاول إبراز خصوصية الجريمة الإلكترونية من الناحية الإجرائية، وهو سنتطرق إليه في المتابعة القضائية في الجريمة الإلكترونية في المبحث الأول و الذي يتضمن مطلبين ، المطلب الأول الاختصاص القضائي في الجريمة الإلكترونية و الفصل الثاني المساعدة القضائية الدولية في مجال الجرائم المعلوماتية،وأيضا أساليب التحري والتحقيق وإثبات في جريمة الإلكترونية في المبحث الثاني والدي يتضمن مطلبين ،المطلب الأول أساليب التحري لتحقيق في الجريمة الإلكترونية و المطلب الثاني أساليب الإثبات في الجريمة الإلكترونية .

المبحث الأول : المتابعة القضائية في جريمة المعلوماتية.

نظرا لطبيعة الخاصة للجريمة الإلكترونية وما نتج عنها من تساؤلات وتناقضات حول إستجابة هذه الجريمة للقواعد الإجرائية التقليدية وبالأخص ما يثار حول قواعد الإختصاص القضائي في الجريمة المعلوماتية، وكذا المساعدة القضائية الدولية في مجال الإلكترونية وهذا ما سنتطرق اليه في مطلبين كالآتي :

المطلب الأول : الإختصاص القضائي في جريمة الإلكترونية

حظي الإختصاص القضائي المتعلق بالجرائم الإلكترونية بالكثير من الإهتمام والجدل لذلك سوف نحاول طرح أهم الإختصاصات في موضوع عبر الفروع الآتية:

الفرع الأول : إختصاص النيابة العامة في تحريك الدعوى العمومية في مجال جرائم الإلكترونية في التشريع الجزائري

يتعين التأكيد هنا بأن الأمر لا يخرج عن نطاق المادة الأولى من قانون الإجراءات الجزائية وفق إستثناءات حددها هذا القانون نفسه، كما سوف نرى ومن الواضح أيضا إن دور النيابة العامة كما رسمته المادة 29 من قانون الإجراءات الجزائية الجزائري وكذا المادة 36 يكون قد توسع في ظل المستحدثات والتطور الحاصل في مجال الجرائم المنظمة والجرائم عابرة الحدود والجرائم الإلكترونية على الأخص.

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث أنه بتعديلي 09/01 و14/04 وضع قواعد وأحكام خاصة لسلطة المتابعة والاختصاص، الغرض منها هو مواجهتها، حيث نصت المادة 329من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ومما يتعين الإشارة إليه أن تحريك الدعوى العمومية في جرائم الأنترنت وتقديم الشكاوى بشانها من قبل المتضررين، بات محل إهتمام الهيئات الدولية، فبالإضافة إلى القرارات الصادرة عن الأمم المتحدة بخصوص الجرائم المتصلة بالكمبيوتر في توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد سنة 1994 بالبرازيل بشأن جرائم الكمبيوتر، والذي أبرز الوجود المركز العالمي للشكاوي الخاصة بجرائم الأنترنت، حيث يعتبر هذا المركز من أهم المؤسسات التي ظهرت إلى الوجود في مجال مجابهة جرائم الأنترنت الذي تأسس في الولايات المتحدة الأمريكية سنة 1999.

ومن هنا يتضح أن إختصاص النيابة العامة توسع مجاله ليمتد ويغطي نطاقات أخرى لم تكن مرخصة لها من قبل، إذ أن المادة 37 من ق.إ.ج.ج. بعد تعديله بموجب القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004وبعد أن كان إختصاص المحلي لوكيل الجمهورية محصورا في المجالات التالية:

- بمكان وقوع الجريمة .

- بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة بالمكان الذي تم في دائرته القبض على أحد الأشخاص المشار لهم ولو لسبب آخر.

- فإنه نص على تمديد الإختصاص المحلي لوكيل الجمهورية إلى دائرة إختصاص محاكم أخرى في إطار جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بقوانين الصرف وذلك عن طريق التنظيم [1].

كما جاء في نص المادة 37 ق.إ.ج وبصدور المرسوم التنفيذي رقم 348/06 المؤرخ في 5 أكتوبر 2006 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية

1 – زيبحة زيدان، الجريمة الإلكترونية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، سنة 2011. ،ص 109إلى 111.

وقضاة التحقيق[1] ليكون بذلك قد شمل الإختصاص المحلي للنيابة العامة كل ربوع الوطني في ما يخص الجرائم المعلوماتية، علما أن المحاكم التي تم تمديد إختصاصها أصطلح على تسميتها في التشريع الجزائري بالأقطاب أو محكمة القطب.

والنيابة مجال إختصاص واسع جدا في إطار البحث والتحري عن الجرائم الإلكترونية ومنح الإذن بالتفتيش والقيام بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور كما هو منصوص عليه في المادة 65 مكرر 5 من ق.إ.ج.ج وسوف يأتي شرحه، وهذا بالإضافة إلى إستعمال التقنيات المخزنة وكذا حجز هذه المعطيات هذا فضلا عن إتخاذ التدابير الملائمة والتحفظية في إطار المساعدات الدولية المتبادلة في مجال الجريمة المعلوماتية.

الفرع الثاني : الإختصاص المحلي لقاضي التحقيق في جرائم الإلكترونية

من المعلوم أن المشرع الجزائري سار بوتيرة متسارعة على خطى التشريعات العالمية ، في إطار مواكبة التطور الحاصل في مضمار القانون لمجابهة التطور الحاصل في مجال الإجرام بصوره الحديثة لا سيما ما تعلق بالجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2] ،وفي هدا الاتجاه جاء تعديل قانون الإجراءات الجزائية بموجب القانون رقم 014/04 المؤرخ في 10 /2004/11 ومس التعديل المادة 40 من قانون إ .ج.ج لتصبح كما يلي :

"يتحدد إختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في إقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر" [3] .

يجوز تمديد الإختصاص المحلي لقاضي التحقيق إلى دائرة إختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم

1 – المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق

2 – زيبحة زيدان، مرجع سابق، ص 113 و 114.

3 – المادة 40من ق.إ.ج.ج.المعدل بموجب القانون رقم 014/04 المؤرخ في 2004/11/10.

الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

ومن الملاحظ أن تمديد إختصاص المحلي لقاضي التحقيق مشمولا كما هو الشأن بالنسبة للنيابة العامة بأحكام المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 وقد حددت المادة الأولى من المرسوم المشار له مجال الإختصاص المحلي الممدد في النطاق الأقطاب القضائية المحددة في المواد 2، 3، 4، 5 من نفس المرسوم في الجرائم المذكورة سابقا وما يهمنا في الموضوع هو ما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الفرع الثالث ، الصلاحيات المكانية للضبطية القضائية في الجرائم المعلوماتية

من الواضح أن المشرع الجزائري يكون قد سارع إلى تدارك النقص وسد الفراغ القائم بخصوص مجلات التحقيق الإبتدائي إثر التطور الذي عرفته الجريمة لاسيما بأشكالها الحديثة كما هو الحال في الجرائم الإلكترونية لذلك جاءت تعديلات قانون الإجراءات الجزائية المتعاقبة لاسيما التعديل الذي جاء به القانون 22/06 المؤرخ في 2006/12/20 والذي مدد من صلاحيات الضبطية القضائية ووسع دائرة إختصاصها ودعمه في ذلك القانون رقم 04/09 المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والإتصال ومكافحتها كما سوف نرى[1].

أناط القانون الجزائري بالضبطية القضائية مهمة البحث والتحري عن الجرائم المحددة في قانون العقوبات تماشيا مع المبدأ الدستوري المتعارف عليه:" لا جريمة ولا عقوبة إلا بنص " [2]، وذلك في مرحلة أولية قبل أن يباشر بشأنها التحقيق القضائي، ويتضح من نص المادة 12 قانون إ.ج.ج. أن مناط البحث عن الجرائم بالنسبة للضبطية القضائية ينحصر في جمع الأدلة والبحث عن مرتكبي تلك الجرائم فإذا ما إبتدأ التحقيق القضائي تقلص دورها، لينحصر في تنفيذ طلبات جهات التحقيق القضائي وإنجاز ما توجه إليهم من طلبات ويدير وكيل الجمهورية إدارة الضبط القضائي.

1 – زيبحة زيدان، مرجع سابق، ص 155.

2 – المادة 46 من الدستور 1996.

كما نصت عليه المدة ة18 مكرر من قانون إ.ج.ج في إطار الصلاحيات المحددة بنص المادة 36 من قانون إ.ج.ج.وكل ذلك تحت إشراف النائب العام وتحت رقابة غرفة الإتهام بدائرة إختصاص المجلس التابعين له، وفقا لأحكام المادة 206 من قانون الإجراءات الجزائية.

والمعلوم أن ضباط الشرطة القضائية نوعان : ويتمثل النوع الأول في هم الذين يتمتعون بإختصاص عام ويختصون بإجراءات الإستدلال بشأن للجرائم المنصوص عليها في قانون العقوبات، أما النوع الثاني فهم ذو الإختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر.

أما ما يهمنا في الموضوع هو دور الضبطية ومجال إختصاصها فيما يتعلق بالجرائم المعلوماتية، وعليه فإن الإختصاص الإقليمي لضباط الشرطة القضائية في مجال الجرائم المعلوماتية[1]، حسب ما نصت عليه المادة 16 ق.إ.ج.ج. بالقول :" يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة" [2].

إلا أنه يجوز لهم - في حالة الإستعجال -أن يباشروا مهمتهم في كافة دائرة إختصاص المجلس القضائي الملحقين به، وكذلك في كافة الإقليم الوطني إذا طلب منهم ذلك من القاضي المختصين قانونا.

غير أنه يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد إختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني .

ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات[3] مع العلم أنه يدخل من ضمن

1 – زيبحة زيدان، مرجع سابق، ص 116 و 177.

2 – المادة 16 من القانون الإجراءات الجزائية الجزائري .

3 – زيبحة زيدان ، مرجع سابق، ص 118.

إختصاصات ومهام ضباط الشرطة القضائية الإنابة القضائية المرخص بها من طرف السلطة القضائية المختصة في سبيل ملاحقة الجرائم الإلكترونية .

المطلب الثاني :المساعدة القضائية الدولية في مجال الجرائم المعلوماتية

نظرا للطبيعة الخاصة التي تتميز بها الجريمة الإلكترونية بإعتبارها جريمة عابرة للحدود ، فإن ذلك دفع بعض الدول إلى ضرورة اللجوء إلى المساعدة القضائية المتبادلة من أجل ضبط هذه الجريمة وملاحقة مرتكبيها وتسلط العقاب عليهم، ولكن هذه المساعدة القضائية الدولية لا تخلو من المعيقات والقيود التي تقف أمام تطبيقها وهذا ما سنتناوله في الفروع الآتية.

الفرع الأول : التعاون القضائي الدولي وتبادل المعلومات لملاحقة الجرائم المعلوماتية.

لما كانت جرائم الإلكترونية ذات طابع عالمي وبالتالي يمكن أن تتعدى أثارها عدة دول ، فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم، يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث أرتكبت الجريمة أو جزء منها، مثل معاينة مواقع الأنترنت في الخارج، أو ضبط الأقراص الصلبة التي توجد عليها معلومات غير مشروعة أو صور إباحية، أو تفتيش الوحدات الطرفية في حالة الإتصال عن بعد أو القبض على المتهمين، أو سماع الشهود، أو اللجوء إلى الإنابة القضائية، أو تقديم المعلومات التي يمكن أن تساهم في التحقيق في هذه الجرائم، وكل ذلك لا يتحقق بدون مساعدة الدول الأخرى، ولذلك تتضمن معظم الإتفاقيات الخاصة بالجرائم التقليدية نصوصا تقضي بضرورة اللجوء إلى المساعدة المتبادلة بهدف تحقيق السرعة والفعالية في إجراءات ملاحقة وعقاب مرتكبي هذه الجرائم.[1]

ويمكن تعريف المساعدة القضائية الدولية بأنها :" كل إجراء قضائي تقوم به دولة من شأن تسهيل مهمة المحاكمة في دولة أخرى، بصدد جريمة من الجرائم"[2] وتتخذ المساعدة القضائية في المجال الجنائي صور عديدة منها: تبادل المعلومات : وهو يشمل تقديم

1 – جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، سنة 2001 ص 79.

2 – سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية ، دراسة مقارنة، رسالة دكتوراه ، كلية الحقوق ، جامعة عين الشمس، سنة 1997، ص 425.

المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة ما، عن الإتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي إتخذت ضدهم وبالإضافة الى نقل الإجراءات ويقصد بها قيام دولة بناءا على إتفاقية، إتخاذ إجراءات جنائية بصدد جريمة إرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، وذلك إذا توافرت شروط معينة .

1- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها.

2- أن يكون الإجراء المطلوب إتخاذه مقرر في قانون الدولة المطلوب إليها عن ذات الجريمة .

3- أن يكون إجراء المطلوب إتخاذه يؤدي إلى الوصول إلى الحقيقة .

وقد أقر المجلس الأوروبي إتفاقية نقل الإجراءات الجنائية التي تعطي للأطراف المنظمة إمكانية محاكمة الجاني طبقا لقوانينها، بناءا على طلب دولة أخرى طرف من هذه الإتفاقية بشرط أن يكون الفعل معاقبا عليه في الدولتين. [1]

أما بالنسبة للجزائر وبمناسبة صدور القانون رقم 04/09 المؤرخ في 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والإتصال ومكافحتها فقد أكدت في المادة 16 منه على أنه في إطار التحقيقات والتحريات القضائية التي تمت مباشرتها، وتتبع الجرائم المنصوص عليها في هذا القانون 04/09 والكشف عن مرتكبيها فإن السلطات الجزائية المختصة بإمكانها تبادل المساعدات القضائية في المستوى الدولي.

وفي النقطة المتعلقة بجمع الأدلة الخاصة بالجريمة الإلكترونية وجمع الأدلة يعد من إجراءات التحقيق القضائي، ويمكن أن يكون بواسطة الدخول إلى المنظومة الإلكترونية المشكوك في تخزينها للمعلومات المبحوث عنها كما أشير لها في المادة05 من القانون المذكور أعلاه، وأنه ونظرا للطابع الخاص لهذا النوع من الجرائم وما يتطلبه تعقبها من سرعة، فإن

1 – طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر ، الإسكندرية، سنة 2009.، ص 598و 599.

المشرع أجاز في حالة الإستعجال قبول طلبات المساعدة القضائية الدولية حتى وإن ورد عن طريق وسائل الإتصال السريعة مثل : الفاكس أو البريد الإليكتروني ، شريطة التأكد من صحتها.[1]

وبهذا الصدد أوجبت المادة 36 من القانون رقم 06/05 لصادر في 08/23/ 2005 والمتعلق بمكافحة التهريب المعدل بالأمر رقم 09/06 في 2006/07/15 :" على أنه وفي حالة توجيه الطلب إلكترونيا من طرف السلطات الأجنبية يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا "[2].

كما نصت المادة 17 من قانون 04/09 على أنه :" تتم الإستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو إتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية ذات الصلة و الإتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل ".[3]

الفرع الثاني : القيود الواردة على طلبات المساعدة القضائية الدولية

نادت بعض الدول بضرورة إنشاء وحدات خاصة بمكافحة الجريمة الإلكترونية بواسطة الحاسب الآلي والأنترنت أُسْوَةً بجهات البحث الجنائي، الوطنية والدولية والتي هي الأنتربول لإثبات الجريمة عند وقوعها وتحديدا أدلتها وفاعلها، وهو كذلك ما يعني إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الإعتداء على المعلومات الخاصة في الأنترنت، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها[4]

- ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية، إلا أن هناك عوائق تحول دون ذلك، تجعل هذا التعاون صعبا لما يلي :

1 – زيبحة زيدان ، مرجع سابق، ص 145.

2 – المادة 36 من القانون رقم 06/05 الصادر في 2005/08/23 المتعلق بمكافحة التهريب المعدل بالأمر رقم 09/06 في 2006/07/15.

3 – المادة 17 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

4 – إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، جامعة الإمارات، في سنة 2000، ص 228.

أولا : عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي ذلك أن الانظمة القانونية في بلدان العالم قاطبة لم تتفق على صورة محددة يندرج في إطارها ما يسمى " بإساءة إستخدام نظم المعلومات الواجب إتباعها"، كذلك ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه، وذلك نتاج طبيعي لقصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي، ومن ثم الجريمة الإلكترونية [1] والخلاف المتمثل في أن يره البعض مباحا نظرا للطبيعة الخاصة للمعلوماتية عبر الأنترنت يراه الآخر غير مباح، ومن ثم يجرم الإعتداء عليه بالنقل أو النسخ، مرد ذلك إلى طبيعة النظام القانوني السائد في كل بلد من البلدان، صحيح ان بعض الدول مثل فرنسا والولايات المتحدة الأمريكية وكندا أصدرت تشريعات تتعلق بالجريمة الإلكترونية إلا أن هذه التشريعات لازالت في مهدها ولعل عدم الإتفاق بين الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة الإلكترونية يغري قراصنة الحاسب الآلي على إرتكاب الجرائم الإلكترونية .

ثانيا : عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة الإلكترونية بين الدول المختلفة، خاصة ما تعلق منها بأعمال الإستدلال أو التحقيق، لاسيما وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط أو التفتيش في النظام معلوماتي معين هو أمر غاية في صعوبة، فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته.

ثالثا : عدم وجود معاهدات ثنائية أو جماعية بين الدول على النحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الأنترنت، ومن ثم تطور الجريمة الإلكترونية بذات السرعة على النحو يؤدي إلى إرباك المشرع وسلطات الأمن في الدول ومن

1 – مؤتمر القانون والكمبيوتر و الأنترنت، جامعة الإمارت، كلية الشريعة والقانون عام 2000، عن الدكتور عبد الفتاح بيومي حجازي ، الإثبات الجنائي في الجرائم الكمبيوتر والأنترنت، طبعةخاصة 2009، بهجات للطباعة والتجليد، جمهورية مصر العربية ، سنة 2009،ص 188.

ثم يظهر الأثر السلبي في التعاون الدولي، وهو ما حاولت الأمم المتحدة الإهتماما به، وكذلك بلدان أوروبا.[1]

رابعا: مشكلة الإختصاص في الجرائم الحاسب الآلي: وهي من المشكلات التي تعرقل الحصول على الدليل في الجريمة الإلكترونية ذلك أن هذه الجرائم من أكثر الجرائم التي تثير مسألة الإختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع الجريمة الحاسب الآلي في مكان معين، وينتج أثارها في مقاطعة أخرى داخل الدولة أو خارجها، ومن هنا تنشا مشكلة البحث عن الأدلة الجنائية على شبكة الأنترنت وسبق لها أن أخترقت مواقع عديدة في دول مثل الصين والكويت وجورجيا والفتنام، بل هاجمت وكالة الفضاء الأمريكية - ناسا نقلا عن الإتحاد الإماراتية - العدد 9345 يوم 2001/02/04 خارج دائرة الإختصاص التي قدم فيها البلاغ، أو تم تحريك الدعوى الجنائية فيها، وكذلك تظهر مشكلات تتعلق بفحص لبيانات في مراكز معلومات دولا أخرى، وهو ما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدولة.[2]

ونرى في هذا الخصوص أن مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس المعيار الذي سبق لمحكمة النقض وان أرسته، وإعتمده المشرع وهو مكان القبض على المتهم او محل إقامة المتهم أو مكان وقوع الجريمة، فأي مكان من الأماكن المذكورة ينعقد الإختصاص القضائي لسلطات التحقيق والمحاكمة فيه بالجريمة المعلوماتية، لكن على المستوى الدولي فإن الأمر في حاجة إلى الإتفاقيات الدولية ثنائية أو الجماعية .[3]

أما بخصوص المشرع الجزائري فإن اللجوء إلى الأنابة القضائية أو المساعدات القضائية فإنها مقيدة بشروط منها:

---

1 – عبد الفتاح البيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر و الأنترنت طبعة خاصة ، بهجات للطباعة والتجليد، جمهورية مصر العربية، 2009.، ص 189 و 190.

2 – محمد الأمين البشري، بحث بعنوان التحقيق في جرائم الحاسب الآلي، مقدم إلى المؤتمر القانون والكمبيوتر والأنترنت، المنفعة في الفترة من 1–3 مايو 2000بكلية الشريعة والقانون بدولة الإمارات، ص 58.

3 – عبد الفتاح بيومي الحجازي، مرجع سابق، ص 192.

1- إنها تتم وفقا للإتفاقيات الدولية التي أبرمت في مجال تبادل المعلومات وإتخاذ الإجراءات التحفظية أو تسليم المجرمين في ما هو مرتبط بالجريمة الإليكترونية.

2- تخضع لمبدأ المعاملة بالمثل وهو المبدأ الذي أكدته أيضا المادة 29 من القانون رقم 01/05 صادر في 2005/02/06 والمتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحته .

اما لقيود الواردة عليها فقد حصرتهاالمادة 18 من القانون 04/09 فيما يلي :

- أنها لا تنفذ ولا يمكن الإستجابة لها في الحالات التالية :

1- إذا كان فيها مساس بالسيادة الوطنية.

2- إذا كانت ماسة بالنظام العام.

- ويمكن الإستجابة لها بشروط منها :

1- شرط المحافظة على السرية المعلومة المبلغة لتلك الدولة .

1- شرط عدم إستعمالها في غير الحالة المحددة والموضحة حصريا في طلب المساعدة القضائية وقد ألزمت الإتفاقية الدولية الموضوعة للتوقيع بمقر الأمم المتحدة في نيويورك في 2005/09/14 والخاصة بقمع الأعمال الإرهاب النووي[1] ألزمت الدول الأطراف بإتخاذ التدابير لحماية سرية المعلومات التي يحصل عليها سرا بموجب هذه الإتفاقية من دولة أخرى .

مما لاشك فيه أن السلطات الجزائرية باشرت العديد من الأعمال الإجرائية في إطار المساعدة القضائية الدولية وإتخذت حيال ذلك تدابير منها إحالة بعض المتهمين على العدالة[2] فعلى سبيل المثال تم فتح تحقيق قضائي في 800 قضية متعلقة بالجريمة الإلكترونية منذ دخول القانون رقم 04/09 الصادر في 2009/08/05 حيز التنفيذ وهي القضايا التي تورطت فيها جزائريون وأجانب إستهدفت شبكات وقواعد البيانات لمؤسسات الجزائرية وأجنبية وأمثلتها

1 – صادقت عليها الجزائر بتحفظ بموجب مرسوم رئاسي رقم 270/10 مؤرخ في 03 نوفمبر 2010 عن الأستاذ زيبحة زيدان، مرجع سابق، ص 146.

2 – زيبحة زيدان، مرجع سابق، 145 وما بعدها.

كثيرة ففي إطار تنفيذ المساعدة القضائية الدولية والإنابة القضائية تمت متابعة شاب جزائري وإحالته على العدالة بمحكمة الجنح بباتنة وهو شاب عمره 21 سنة تقني سامي في الإعلام ، قام بإختراق موقع شركة أمريكية متخصص في حماية المعلومات والبرامج الإليكترونية لعديد من الشركات الأمريكية ثم عمل على إستغلال تلك المعلومات لصالح شركات منافسة مقابل مبالغ مالية .

وإثر إيداع شكوى من قبل الشركة المتضررة لدى الشرطة الأمريكية قدمت هذه الأخيرة المعلومات الكافية بشأن المتهم المشار له إلى مصالح امن الجزائري .

وهناك حالة أخرى أيضا تتعلق بمتابعة ومحاكمة شاب جزائري وهو طالب جامعي بقسم الإعلام الآلي بعنابة من طرف سلطات الأمن الجزائري وهذا الشاب تمكن من قرصنة عدد كبير من البطاقات البنكية عقب إختراقه لمواقع إليكترونية لمؤسسات أجنبية في أوروبا والولايات المتحدة الأمريكية وفي كندا وتمكن من سحب أموال معتبرة وإثر المعلومات المتبادلة مع الأمن الجزائري في إطار المساعدة القضائية الدولية تمت متابعة البريد الإليكتروني الذي كان يستعمله " الهاركز" المتهم المشار له والذي أدين حكم من طرف محكمة الجنح بعنابة ثم إستفاد بتدابير المنفعة العامة وفقا لما ورد في الفصل الأول مكرر بالمادة 05 مكرر1 إلى المادة 05 مكرر06 من القانون العقوبات الجزائري، وهناك العديد من الأمثلة حتى بالمقابل بالنسبة لما تعرضت له مؤسسات جزائرية من أعمال قرصنة وإختراق ومن أمثلة ذلك إختراق موقع الشروق أونلاين ومحاولة تخريبه من طرف هاكرز مصرين[1]وبالرغم من نجاح السلطات في إثبات الجرائم الإلكترونية والقبض على المجرمين المعلوماتيين في إطار المساعدة القضائية الدولية نسبيا إلا أن القيود الواردة عليها تحول بينها وبين النجاح في مواضيع عدة أخرى.

لذلك يلاحظ أن التشريعات الجنائية المطبقة حاليا في معظم دول العالم ترتكز على الصفة الإقليمية فيما يتعلق بتطبيق قواعد الإجراءات الجنائية عن طريق السلطات غير الوطنية، وهو ذات ما سبق التنويه إليه من أن التشريعات الجنائية لا تتقدم بذات السرعة التي تتقدم بها وتنمو حركة الإتصالات والإلكترونية التي عمت العالم كله، لذلك لا مناص من الإتفاقيات

1 – زيبحة زيدان، مرجع سابق،ص 147 وما بعدها.

الثنائية أو الجماعية بين الدول لتسهيل التحقيق في الجرائم الإلكترونية وبالرغم من إبرام بعض هذه الإتفاقيات فأن دلك لم يفي بالمطلوب في حل مشكلات الإختصاص وتبادل الأدلة الجنائية وتسليم المجرمين، لذلك فالحاجة ماسة إلى التشريعات جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسب الآلي في كل المجالات .[1]

المبحث الثاني : أساليب التحري والتحقيق والإثبات في الجريمة الإلكترونية

الجريمة الإلكترونية تمتاز بخصائص وعناصر تميزها عن الجرائم التقليدية المنصوص عليها في القوانين، فأن قواعد هذه القوانين تبدو قاصرة إزاء ملاحقة مرتكب الجريمة الإلكترونية وهذا ما يبرز كأمر واقع مسألة صعوبة جمع الإستدلالات و الأدلة في جريمة المعلوماتية، وأيضا تطبيق الإجراءات الجنائية التقليدية، وعلى هذا الأساس فقد قسمنا هذا المبحث إلى مطلبين، يتضمن الأول : أساليب التحري والتحقيق في الجريمة الإلكترونية والثاني أساليب الإثبات في الجريمة الإلكترونية .

المطلب الأول : أساليب التحري والتحقيق في الجريمة الإلكترونية

لم يعرف المشرع الجزائري عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية لكنه أرسى قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تلد مع التطور الحاصل في حقل الجريمة الإلكترونية لظاهرة حديثة وبهذا الصدد جاء القانون رقم 04/09 المؤرخ في

1 – Johannes F.NIJIbaer , challenges for the low of Evidence, leiden ,INREP,1999,p16.

2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها ومنها ما نصت عليه المادة 03 منه مما تتطلبه مستلزمات التحريات والتحقيقات القضائية كما سيأتي ذكره.

الفرع الأول : مراقبة الإتصالات الإليكترونية

نص القانون رقم 04/09 المؤرخ في 2009/08/05 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولجيات الإعلام و الإتصال ومكافحتها في المادة 03 منه على ما يلي :" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفها للقواعد المنصوص عليها في قانون الإجراءات الجزائية في هذا القانون وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجرءات التفتيش والحجز داخل منظومة الإلكترونية ".

ومن الواضح أو المراقبة الإتصالات حددها القانون على سبيل الإستثناء وفي حالات محددة حصرها في المادة 04 من القانون المشار له وهي :

1- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو االجرائم الماسة بأمن الدولة.

2- في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني او المؤسسات الدولة أو الإقتصاد الوطني.

3- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث جارية ويكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإليكترونية .

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

1 – المادة 04 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال ومكافحتها .

والملاحظ أن المشرع ونظرا لما يترتب عن تطبيق هذه التدابير ميدانيا من مساس بحرية الحياة الخاصة وخصوصيتها وهي مقدسة ومحمية دستوريا، كما أشير لها سابقا فإنه ربط القيام بها بشرط الحصول على إذن مكتوب من السلطة القضائية المختصة .

ومن المعلوم أن الرسالة الإلكترونية ذات طابع خاص لكنها لا تختلف عن الرسالة الورقية من حيث حفظها أو الإستغناء عنها وإهمالها ، ولكن ما يتميز الرسالة الإلكترونية انه يمكن الوصول إليها عن طريق صناديق البريد الخاصة أو الملفات المحفوظة أو الرجوع إلى سلة المهملات، ومن أجل التحقيق الذي يجري بغرض ضبط المرسلات الإلكترونية فإنه يستلزم الولوج إلى البريد الإلكتروني (E- mail) [1]، وبعد تحديد صندوق البريد للمتهم المشكو منه يتمحور العمل حول ثلاث (3) عناصر وهي : الوارد (IN)، الصادر (OUT)، الحفظ وسلة المهملات(TRASH).

فبذلك يمكن مراجعة قائمة الرسائل التي وصلت إلى المشكو منه في الوارد والعكس بالنسبة للمراسلة منه على القائمة الصادرة وكذا الشأن بالنسبة للرسائل المحفوظة أو المهملة غير أن ما يجب تأكيده هنا هو أن المشرع ونظرا لحساسية الموضوع والذي يعد مرتبطا بقدر كبير بذاتية الأشخاص فقد جعل تدابير وإجراءات التحقيق تحت طائلة المسؤولية الجزائية عندما نص في المادة 04 من القانون 04/09 فقرة (د)والأخيرة على أن الترتيبات التقنية الموضوعية للأعراض المنصوص عليها في الفقرة(أ) من نفس المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والإعتداءات على أمن الدولة ومكافحتها وذلك تحت طائلة العقوبات المنصوص عليها في القانون العقوبات بالنسبة للمساس بالحرية الخاصة للغير[2] وهذا ما نص عليه الدستور الجزائري في المادة 39 من بالقول:" بسرية المراسلات و الإتصالات الخاصة بكل إشكالها مضمونة ".[3]

1 – البريد الإليكتروني: وهو إرسال وإستقبال للرسائل الإليكترونية عن طريق شبكة الأنترنت، عن الأستاذ زيبحة زيدان ، مرجع سابق، ص 128.

2 – زيبحة زيدان ، مرجع سابق ، ص 128 و 129.

3 – المادة 39 من الدستور الجزائري لسنة 1996.

وكذلك قد تم ضمان هذا المبدأ في الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة الأمم المتحدة في 1948/12/10 في المادة 12 منه على :" أنه لا يجوز أن يتعرض أحد لتدخل تعسفي في حياته الخاصة أو مراسلاته ولكل شخص الحق في الحماية القانونية ضد هذا التدخل.[1]

الفرع الثاني : إجرءات التفتيش للمنظومة الإلكترونية

أولا : تعريف التفتيش

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش وبقدر ما إعتبره إجراء من إجراءات التحقيق وإحاطة بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم ومما يؤكد ذلك إهتمام الدستور الجزائري بهذه النقطة إذ نص في المادة 40 منه بالقول :" فلا تفتيش إلا بمقتضى القانون وفي إطار إحترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"[2].

وكما هو الشأن في مختلف التشريعات العربية فإن التعريفات تجمع على أن التفتيش هو إجراء من إجراءات التحقيق " يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة ونسبتها إلى المتهم ، تحقق وقوعها في محل يتمتع بحرمة وذلك وفقا للضمانات والقيود القانونية المقررة "[3]، ويعرف كذلك التفتيش بأنه إجراء من إجراءات التحقيق " غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة في شأنها"[4].

1 – المادة 12 من الإعلان العالمي لحقوق الإنسان صادر عن الجمعية العامة للأمم المتحدة بتاريخ 1948/12/10.

2 – زيبحة زيدان ، مرجع سابق، ص 130.

3 – رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، وفي التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت ، لبنان، سنة، 2012، ص 394.

4 – هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانا المتهم المعلوماتي ، ط1 دار النهضة العربية القاهرة، سنة 1997، ص 45.

وإذا كان التفتيش المتعارف عليه في القواعد الإجرائية العامة نوعان: تفتيش المساكن وتفتيش الأشخاص، كما نص على ذلك قانون إ.ج.ج. في المواد 44 و 64 منه فإن التفتيش المنصب على المنظومة الإلكترونية يختلف عنه كلية من حيث الشروط الشكلية والموضوعية.

ويثور السؤال عن إمكانية التفتيش وفقا لضوابط المتعارف عليها في الجرائم التقليدية والغاية منه في مجال الجرائم المعلوماتية؟

والغرض من هذا السؤال يتضح من أن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة بينما البيانات الإليكترونية ليس لها حسب جوهرها مظهر ملموس في العالم الخارجي ، ومع ذلك فيمكن أن يرد، التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة، ومخرجات الحاسبة الإلكترونية[1].

ولهذا أجاز لفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل لتفتيش البيانات المعالجة إلكترونيا، والمخزنة بالحاسبة الإلكترونية ثم ضبطها والتحفظ عليها ، او ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات ، والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام.[2]

ثانيا : تفتيش المنظومة المعلوماتية

نص القانون 04/09 في المادة 05 منه على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى :

1- منظومة معلوماتية أو جزء منها وكذا المعطيات الإلكترونية المخزنة فيها.

2- منظومة الإلكترونية .

---

1 – M. Moherenschloger ,computer crimes and others crimes against information technology in the Germany,Rev ,int,dr, pen ,1993p319,spec349.

2 – علي عدنان الفيل إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي للنشر، كلية الحقوق، جامعة الموصل،سنة 2011، ص 39.

يلاحظ إذن بأن التفتيش في الوضعيات المشار لها يأخذ منحنين فهو إما أن يكون عملا من أعمال التحقيق تقوم به السلطات القضائية المختصة وإما يكون من أعمال الإستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطة المختصة في كلتا الحالتين فإن المستهدف هنا هو جهاز الكمبيوتر (الحاسوب) بمكوناته المادية والمعنوية فالحاسوب كما هو معروف يتكون من مكونات مادية، وهي مجموعة وحدات لكل منها وظيفة معينة وهي متصلة ببعضها في شكل نظام متكامل منها وحدات الإدخال ومهمتها إستقبال البيانات الإلكترونية والغير المعالجة ولها مهام أيضا داخل جهاز الحاسوب فهي تمر إلى الوحدات الذاكرة للمعالجة أو التخزين ووحدة الذاكرة هي التي تقوم بتخزين البرامج والمعلومات وبما تحتويه من ذاكرة رئيسته وعشوائية وذاكرة القراءة ثم وحدة الحاسب والمنطق، أما وحدة الإخراج فتحتوي على أجهزة الشاشة والطابعة ومشغلات الأقراص، أما المكونات المعنوية للجهاز الكمبيوتر والتي تسمى أيضا بالكيانات المنطقية وهي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات.

ومما سبق يمكن القول بأن التفتيش وعند ما يستهدف الكيانات المادية للحاسوب لا يشكل أي عائق إذ أنه من السهولة بمكان ضبط الأجهزة وحجزها أو إتلافها وإنما الإشكال يثور عند ما ينصب التفتيش على المكونات الكمبيوتر المعنوية أو المنطقية كالبرامج وقواعد البيانات ذلك أن التفتيش عن هذه البيانات يتطلب الكشف عن لرقم السري (CODE) لمرور إلى الملفات وكذا الكلمات السر أو الشفرات أو ترميز البيانات.[1]

ثالثا : شروط تفتيش المنظومة الإلكترونية

يمكن تقسيم شروط التفتيش للمنظومة الإلكترونية إلى نوعين موضوعية والأخرى شكلية.

1- الشروط الموضوعية لتفتيش المنظومة المعلوماتية

وتنحصر هذه الشروط في

1 – زيبحة زيدان ، مرجع سابق، ص 131.

أ - وقوع جريمة الإلكترونية :

والجريمة الإلكترونية هي كل فعل غير مشروع بإستخدام الحاسبة الإليكترونية لتحقيق أغراض غير مشروعة [1]، وحتى يكون التفتيش صحيحا متفقا وصحيح قانونيا فإننا لابد وأن يكون بصدد جريمة معلوماتية مما يعتبر القانون جناية أو جنحة. [2]

ب - تورط شخص أو أشخاص معينين في إرتكاب الجريمة الإلكترونية أو الإشتراك فيها:

ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الإعتقاد بأنه قد ساهم في إرتكاب الجريمة الإلكترونية سوء وصفه فاعلا لها أو شريكا فيها وفي مجال الحاسبة الإلكترونية .

ج - توافر إمارات قوية أو أدلة تفيد في الكشف عن الجريمة الإلكترونية :

لا يوجد التفتيش إلا إذا توافرت لدى المحق أسباب كافية على أنه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات إستخدمت في جريمة الإلكترونية أو أشياء متحصلة منها.

د - محل التفتيش الخاص بنظام الحاسبة الإلكترونية:

وهي كل مكونات الحاسبة سواء كانت مادية أو معنوية أو شبكات الإتصال الخاصة بها بالإضافة إلى الأشخاص الذين يستخدمون الحاسبة الإلكترونية محل التفتيش.[3]

2- الشروط الشكلية لتفتيش المنظومة الإلكترونية :

يستخلص من نص المادة 05 من القانون 04/09 المشار سابقا بأن التفتيش في مجال الجرائم الإلكترونية والذي يختلف كلية عن التفتيش العادي يتوقف أساسا على طبيعة المكان

1 – هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، سنة 1992،ص 30.

2 – خالد ممدوح إبراهيم، فن التحقيقي الجنائي في جرائم الإليكترونية، الطبعة الأولى دار الفكر الجامعي للنشر ، الإسكندرية ، 2009 .، ص 210.

3 – على عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي للنشر، كلية الحقوق، جامعة الموصل،سنة 2011. ، ص 50.

الذي يحتوي أجهزة الكمبيوتر ومكوناته وفيما إذا كان خاصا أم عاما هذا فضلا عن تحديد الإقليم فيما إذا كان وطنيا أن أجنبيا .[1]

ويمكن تحديد أهم عناصر التفتيش فما يلي من خلال القواعد العامة للقانون الإجراءات الجزائية كالتالي: وفقا للأحكام المادة 44 من ق.إ.ج لاسيما بعد التعديل بموجب القانون 22/06 في 2006/09/20 وهي :

أ - وجود إذن مكتوب صادر من وكيل الجمهورية او قاضي التحقيق .

ب - الإستظهار بالإذن قبل الدخول المنزل المراد تفتيشه.

ج - أن يتضمن الإذن وصف الجريمة البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.

د - حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.

هـ - في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين لسلطته.[2]

أما التفتيش في الأماكن العامة وهي التي يرتدوها العامة في كل وقت ولا يتمتع بحرمة المنزل فيمكن دخولها خلاف الأماكان الخاصة وتفتيشها إذا ما تم غلقها إنتهاء فترة العمل وإنصراف العامة.

رابعا : تفتيش المنظومة الإلكترونية عن بعد

أجاز القانون الجزائري 4/09 المشار له سابقا القيام بتفتيش المنظومة الإلكترونية عن بعد ويقتضي ذلك الدخول إليها دون إذن صاحبها والولوج إلى الكيان المنطقي للحاسوب فالتفتيش هما يستهدف أشياء معنوية وفنية وليست مادية كالبرامج وقواعد البيانات ، ولأن هذه قد تكون وسيلة لإرتكاب الجريمة .

1 – زيبحة زيدان، مرجع يابق،ص 133.

2 – المادة 44 من القانون الإجراءات الجزائية المعدل بموجب القانون رقم 22/06 في 2006/09/20.

فقد أجاز المشرع الجزائري من افراغ او نسخ تلك المعلومات المشكوك فيها والتي من شأنها الإفادة في الكشف عن الجريمة او مرتكبيها أو حجز المعطيات وضبطها كدليل إثبات ضد المتهم يقدم أمام المحكمة .

إلا أنه برنامج الحاسوب وقاعدة البيانات تتمتع بالحماية القانونية في القانون الداخلي وفي إتفاقيات الدولية كما هو الشأن في التشريع الجزائري إذ إعتبر برنامج الحاسوب وقاعدة البيانات مصنفات محمية بموجب القانون رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة.

لكن رغم ذلك فقد أجيز التفتيش عن بعد وفق ما تقتضيه الحاجة القانونية [1]

خامسا : تمديد التفتيش إلى منظومة معلوماتية أخرى او جزء منها

نصت المادة 05 من القانون رقم 04/09 على ما يلي:

في الحالة المنصوص عليها في الفقرة ـ أـ من هذه المادة:" إذا كانت هناك أساب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، بجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها، بعد إعلام السلطة القضائية المختصة مسبقا بذلك" [2] ، والملاحظ هنا أن التفتيش في هذه الحالة يكتسي طابع خاص فهو يجري عن بعد وثانيا يتم بشكل سريع وتماشيا مع سرعة الفائقة الذي يجري عليه نقل المعلومات وذلك طبقا تحت طائلة القانون في إطار حماية الحياة الخاصة للأفراد.

سادسا : الجهة القضائية المختصة بالإشراف على المعطيات التفتيش

1 – زبيحة زيدان، مرجع سابق، ص 135.

2 – المادة 05 من القانون رقم 05/09 المتعلق بالجرائم الماسة بتكنولوجيات الإعلام والإتصال ومكافحتها.

حسب القانون 04/09 في المادة 04 منه وهي المتعلقة :" بمباشرة المراقبة بغية الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة"، ففي هذه الحالة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 من نفس القانون وهي الهيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات.

إذن الإختصاص يؤول في هذه الحالة الى منح الإذن للنائب العام على ان تكون مدة الإذن ستة(06) أشهر قابلة للتجديد.

أما فيما عدا حالة المنحصرة في الفقرة - أ-من المادة04 من القانون 04/09 فإنه يتعين الرجوع إلى التدابير التي رسمها قانون إ.ج.ج في مجال التحري والتفتيش بالنسبة للجرائم الإليكترونية وبالضرورة يعود الإختصاص لوكيل الجمهورية وكذا قاضي التحقيق بإعتبارهما الجهة المؤهلة بمنح الإذن بالتفتيش ويحدد ذلك المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 والمتضمن تمدد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق. [1]

الفرع الثالث: إجراء الحجز داخل المنظومة المعلوماتية

تجدر الإشارة إلى القول بأن حجز الأشياء المادية كالمعدات والأوراق والمستندات يعد شيئا سهلا وغير مثير لأية إشكاليات في نظر القانون، غير أنه ليس من السهل أبدا توقيع الحجز داخل منظومة معلوماتية ذلك أن المعلمات هي في الأصل شيء معنوي.

وقد إختلفت التشريعات العالمية حول إمكانية حجز الكيانات الغير المادية المخزنة في برامج وذاكرة الحاسوب .

و عليه فقد إعتبر البعض أنه لا يسوغ ضبطها إلا بعد تحويلها إلى كيان مادي كطباعتها أو تصورها ، في حين إعتبرها البعض الأخر بأن برامج الحاسوب كيانا ماديا ملموس إذ هو

1 – زيبحة زيدان، مرجع سابق،ص 140.

عبارة عن نبضات إليكترونية ممغنطة، ورأى إتجاه أخر أن المعلومات في حالتها لا تقبل التملك ولا يمكن أم يكون محلا للإعتداء ولا محلا للملكية الفكرية .[1]

غير أن المشرع الجزائري وقبل صدور القانون 04/09 كان قد أضفى حماية قانونية لقواعد البيانات بموجب الأمر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة له، وإعتبر قواعد البيانات من المصنفات المحمية .

وفي إطار الحماية البيئة الجنائية لحقوق المؤلف وطبقا الأحكام المواد 146/145 من الامر 05/03 ، يتولى ضباط الشرطة القضائية أو الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة له ، معاينة المساس بحقوق المؤلف كما يتولون بصفة تحفظية حجز دعائم المصنفات ووضعها تحت حراسة الديوان، وتفصل الجهة القضائية في طلب الحجز التحفظي خلال 03 أيام من تاريخ إخطارها.

وعلى الوجه العموم فأن المشرع الجزائري إنحاز إلى الإتجاه القائل بإمكانية حجز المعلومة طبقا للأحكام المادة 06 من القانون 04/09 حيث يمكن حجز المنظومة الإلكترونية برمتها إذا كان ضروريا ولمصلحة التحقيق وذلك بعد نسخها على دعامة مادية كطبعها على الورق أو ضبطها على الشاشة.

وضبط الإدلة عن طريق الحجز المعطيات أو البيانات يجري وفقا لمقتضيات قانون الإجراءات الجزائية ، بالإضافة إلى التدابيرأخرى منها المصادر للأجهزة والبرامج والوسائل المستخدمة مع إغلاق الموقع الجريمة قد نص عليها القانون العقوبات في مادته 394مكرر6.

وقد نصت المادة 84 من إ.ج.ج على ضوابط المتعلقة بالأدلة منها ما يلي :

- الإطلاع على المستندات المبحوث عنها وذلك مخول لقاضي التحقيق أو ضابط الشرطة القضائية الذي أنابه عنه فقط.

1 – هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص 596،وأيضا : هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 256.

- الإحترام التام لمقتضيات وضرورات التحقيق وعلى الأخص ضمان سر المهنة وحقوق الدفاع.

- وعلى الفور يتم فرز الأشياء المضبوطة ووضعها في أحراز مختومة حيث لا يتم فتحها إلا بحضور المتهم مصحوبا بمحاميه حسب المادة 84 ف.إ.ج.ج.[1]

الفرع الرابع : إلتزامات مقدمي الخدمات في مساعدة السلطات

بموجب المادة 10 من القانون 04/09 ألزمت مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش، كما ألزمتهم أيضا بكتمان السر بخصوص العمليات التي ينجزونها بطلب المحققين وما تحصل عن ذلك من المعلومات، وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إفشاء أسرار التحيق، ويطلق على مقدمي الخدمات في مجال الانترنت تسمية الوسائط في خدمة الأنترنت ويمكن دورهم في تمكين مستخدم الأنترنت من الدخول إلى الشبكة والإطلاع عليها عما يبحث عنه، وقد عرفت المادة الأولى الفقرة الثالثة من الإتفاقية الأوروبية لمكافحة جرائم الإلكترونية التي تم إقرارها في بودابست لسنة 2001 :" عرفت مزودي الخدمات بأنهم كل شخص طبيعي أو معنوي يقوم بتزويد المستخدمين بالخدمات التي تمكن وتسهل الإتصالات بين أجهزة الكمبيوتر وكذلك كل من يتولى معالجة المعطيات المخزنة نيابة عن المزود الخدمة ".[2]

لعل هذه هي أهم إجراءات البحث والتحري في الجريمة الإلكترونية التي تطرقنا إليها بشكل مختصر لأنه لا يسعنا التفصيل فيها كلها التي تطرقنا إليها بشكل مختصر لأنه لا يسعنا التفصيل فيها كلها وذلك لتعددها ، علما أن ما قدمناه في هذا المطلب كانت عبارة عن الإجراءات جاءت في القانون 04/09 سابق الذكر.

يضاف إلى ذلك ما نصت عليه المادة 65 مكرر 5 من قانون الإجراءات الجزائية المتمثلة في مايلي:

1 – زيبحة زيدان، مرجع سابق، ص 148.

2 – زيبحة زيدان، مرجع سابق،ص 153.

1 -إعتراض المراسلات التي يتم عن طريق وسائل الإتصال السلكية واللاسلكية:

والتي يتم عن طريق وسائل الإتصال السلكية واللاسلكية وذلك بواسطة ترتيبات تقنية يتم وضعها دون موافقة المعينين، ومن أجل التصنت وإلتقاط ويتبث بث وتسجيل الكلام المتفوه به بصفة سرية من أجل تحصيل الدليل.

2- إعتراض البريد الإلكتروني:

بإعتباره نظام للتراسل بإستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا، حيث يتم إعتراضه إلا بإذن من وكيل الجمهورية في إطار التحري و التحقيق الإبتدائي.

3- إلتقاط الصور :

ويندرج ذلك تحت طائفة الترتيبات التقنية التي تهدف إلى إلتقاط الصور لشخص او لعدة أشخاص يتواجدون في مكان خاص ودون الأماكن العامة حسب المادة 65 من ق.إ.ج.ج.

4- إجراءات التسرب:

يعتبر هذا الإجراء مستحدثا في مجال التحريات والتحقيقات وقد نص عليه المشرع في المادة 65 مكرر5 من ق.إ.ج.ج.، وكذلك في المادة 65 مكرر 11 بموجب التعديل بالقانون رقم 22/06 المؤرخ في 2006/12/20، ويقصد به قيام ضباط أو عون الشرطة القضائية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإهامهم أنه فاعل معهم أو شريك لهم.[1]

المطلب الثاني : أساليب الإثبات في الجريمة المعلوماتية

يعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حددها المشرع وإعترف لها بالقيمة القانونية، وتتمثل وسائل الإثبات الرئيسية في الجريمة الإلكترونية في

1 – زيبحة زيدان ، مرجع سابق ، من ص 157 إلي 169.

المعاينة والخبرة وهذا ما أخذت به معظم التشريعات الدول، أما التفتيش فقد أدرجه المشرع الجزائري بموجب القانون 04/09 كأسلوب التحري والتحقيق اكثر منه كأسلوب الإثبات، أما الأساليب الأخرى المتمثلة في إجراءات الإستجواب والمواجهة وسماع الشهود فلم نتطرق إليها على أساسها أنها إجراءات خاصة بالأفراد وتتم في مواجهة البشر وليست فنية كما هو الحال بالنسبة للأسلوب المعاينة والخبرة، بالإضافة إلى تطرقنا إلى دليل آخر مستحدث يتناسب مع الطبيعة الخاصة للجريمة الإلكترونية وهو إعتماد الدليل التقني أو الإلكتروني في إثبات، وهذا ما سوف نتطرق في الفروع الأتية :

الفرع الأول : إعتماد المعاينة في الإثبات

أولا : تعريف المعاينة:

للمعانية أهمية قصوى في إثبات الواقعة، وهي إثبات مادي ومباشرة لحالة الأشخاص والأشياء والأمكنة ذات الصلة بالحادث وتتم بواسطة عضو النيابة العامة أو من يندبه من ضباط الشرطة القضائية، وتتمتع المعاينة في الكشف عن الغموض وإظهار الحقيقة في الجريمة الإلكترونية بنفس درجة من الأهمية في الجرائم التقليدية[1].

ثانيا : أهمية المعاينة في الجرائم المعلوماتية

للمعاينة أهمية بالغة في أدلة المعاينة وفي إقتناع المحكمة في كثير من القضايا، إلا أنه يمكن القول أن السلطات المختصة التي تقوم بإجراءات المعاينة أو التي تتكفل بها تواجهها صعوبات في بعض الأحيان، كون أن الجرائم الإلكترونية لا تختلف أثارها مادية وقد تطول

1 – خالد ممدوح إبراهيم، مرجع سابق، ص 147 وما بعدها.

الفترة الزمنية بين وقوع الجريمة وإكتشافها مما يعرض الأثار الناجمة عنها إلى المحور أو التلف أو العبث بها [1].

وحتى يكون للمعاينة في الجرائم المتعلقة بشبكة الأنترنت فائدة في كشف الحقيقة عنها وعن مرتكبيها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما لي :

1- تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة .

2- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام .

3- التحفظ على المحتويات سلة المهملات.

4- التحفظ على المستندات الإدخال والمخرجات الورقية لكمبيوتر ذات صلة بالجريمة لرفع البصمات والتي قد توجد بها. [2]

5 - قصر مباشرة المعاينة على فئة معنية من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الكمبيوتر والشبكات والنظم المعلوماتية. [3]

وما هو جدير بالذكر أن المعاينة قد تكون الحل في بعض أنواع الجرائم الإلكترونية ولتحقق المعاينة لابد من وجود مسرح جريمة وهذا ما يصعب تحديده وصعوبة الحفاظ على الأثار المادية إن وجدت، وتكون عقبة الأساسية أمام المعاينة في الجريمة الإلكترونية عندما ترتكب داخل الفضاء المعلوماتي، فالمحقق يتعامل مع نبضات إلكترومغناطسية وبيانات مخزنة في نظام المعلوماتي .

1 – هشام رستم ، الجواني الإجرائية للجرائم الإلكترونية ، مرجع سابق، ص 59

2 – هشام رستم، قانون العقوبات والمخاطر تقنية معلومات، مرجع سابق، ص 126-127.

3 – Taylor ,R, computer crime, criminal investigation edited, « by Charles Swanson ,N, chamelin and L. Teritto hill,inc.5 edition,1992,p450.

ولذلك تقتضي المعاينة جهات قضائية مختصة بها مؤهلة وتتمع بالخبرة في مجال هذه التقنية، حيث يقوم المحققين بالإطلاع على مختلف الوثائق المحفوظة والمراسلات الإلكترونية المرتكبة في الجريمة وفك الشفرات وإقتفاء آثر الإتصلات الإليكترونية من جهاز الحاسب الخاص بالجاني وكذا الخاص بالضحية، حيث تستخدم كل من الإجراءات كدليل وكإثبات للجريمة المعلوماتية، ومن أمثلة فائدة المعاينة التي أتت بنتيجة ، وهو ما قامت به الشرطة الفرنسية في مداهمة منزل شخص كان يستغل الأطفال عن طريق الأنترنت ونشر صور إباحية فتمت المعاينة وثم القبض على الجاني وحجز مختلف الأجهزة المتصلة بالإنترنت الخاصة بجهازه، ما يمكن قوله ان المعاينة تحتاج إلى الضبطية قضائية مؤهلة لهذه التقنية مع التوصية في إعادة النظر في التشريع الذي ينظمها وهذا الأمر أضحى ضرورة لابد منها من أجل فتح المجال العمل الإستدلالي.[1]

الفرع الثاني : إعتماد الخبرة في الإثبات الجريمة المعلماتية

أولا : تعريف الخبرة

يقصد بالخبرة - بصفة عامة- المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة أو نتيجة دراسات خاصة تلقاها أو نتيجة الإثنين معا أي العمل والدراسة ، ومن هنا يطلق على ذوي هذه المهارات "بالخبراء".[2]

والخبرة هي الوسيلة من الوسائل الإثبات التي تهدف إلى الكشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالإستعانة بالمعلومات العلمية والتي لا تتوفر سواء لدى المحقق أو القاضي، فهي بحث مسائل مادية أو فنية يصعب على المحقق أن يثبت طريقة فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، وتكمن أهمية الخبرة في أنها تنير الطريق لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية لتحقيق العدالة في المجال

1 – محمد أمين الرومي، جرائم الكمبيوتر و أنترنت/ دار المطبوعات الجامعية ، الإسكندرية، سنة 2003،ص 139.

2 – خالد الممدوح إبراهيم، مرجع سابق، ص 283.

الجزائي، لذا فقد إهتم المشرع الجزائري بالإستعانة بالخبراء لجهات التحقيق، وأجاز للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم[1].

ثانيا: تعريف الخبير

الخبير هو شخص مختص فنيا في مجالات مختلفة ومتنوعة سواء كانت فنية أو علمية أو غيرها من المجالات الأخرى.

ويستطيع بما له من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلى الخبرة فنية. [2]

وتجدر الإشارة في هذا الإطار، أن بعض الفقه يرى أنه لا يشترط في الخبير المنتدب أن يكون متخرجا من معاهد أو الجامعات المتخصصة في دراسات الحاسوب والأنترنت بل يكفي إكتسابه مهارة موهبة إستعمال الحاسوب والأنترنت و التعامل مع تقنية المعلومات. [3]

ثالثا : أهمية الخبرة في مجال الجريمة الإلكترونية .

تكتسب الخبرة الفنية في جريمة الإلكترونية أهمية بالغة نظرا لأن الحاسبات وشبكات الإتصال بينها على أنواع ونماذج متعددة كذلك فأن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يعصب معها على المتخصص تتبعها وإستعابها [4] والإستعانة بخبير فني في المسائل الفنية البحثة خاصة في مجال الجرائم الإلكترونية فهو أمر وجوبي، لأن الأمر يتعلق بمسائل معقدة ومحل الجريمة فيها غير مادي ولا يكشف عن غموضها إلا متخصص وعلى درجة كبيرة من التميز .

---

1 – رشيدة بوكر،، مرجع سابق، ص 424.

– عائشة بن قارة مصطفى، حجية الدليل الإليكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير، كلية الحقوق ، جامعة الإسكندرية، سنة 2009.، ص 88 و 89.

2 – خالد ممدوح إبراهيم، مرجع سابق، ص 285 و 286.

3 – رشيدة بوكر ، مرجع سابق، ص 426 و 427.

4 – علي عدنان الفيل، المرجع السابق ، ص 26 و 27.

و كما أن عملية تجميع الدليل الرقمي تعد من أصعب الأمور التي تواجه الخبير التقني في مجال الجريمة الإلكترونية ، لذلك كان لزاما عليه إتباع خطوات وأساليب علمية تتناسب مع البيئة التي يتواجد بها هذا النوع من الدليل[1].

وبدا من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة المعلوماتية، وأن نجاح الإستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء، وهذا ما يدعو إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق في الجرائم الإلكترونية لنجاح تحقيق في مثل هذه الجرائم، ونظرا لأن الجريمة الإلكترونية لها خصوصيتها فإن الخبير المعلوماتي قد يكون من أولئك الجناة الذين سبق لهم إرتكاب مثل هذه الجرائم وتم تكوينهم وإعادة تأهيلهم كأفراد موطنين صالحين في المجتمع [2] .

رابعا ، مدى حجية تقرير الخبير التقني

يحرر الخبير لدى إنتهاء أعمال الخبرة تقريرا يجب أن يشتمل على وصف ما قام به من أعمال ونتائجها، وطبقا للمادة 215 من قانون إ.ج.ج تكون هذه التقارير مجرد إستدلالات لإنارة القاضي، ولذلك يكون رأي الخبير يعطي دائما بصفة إستشارية ولا يقيده فهو ليس بحكم وليس له قيمة قضائية أكثر من شهادة شهود، فيجوز للقاضي أن يأخذ بالخبرة أو يطرحها و أن يفاضل بين تقارير الخبراء ويأخذ بما يرتاح إليه، حيث أن كل ما يتعلق بالدعوى يجب أن ينتهي عند قاضي الموضوع لكي يتولى الفصل فيه والكلمة الأخيرة ترجع لمحكمة الموضوع وهذا الأمريسري على الناتج من الخبرة في إطار تكنولوجيا المعلومات، حيث يظل القاضي هو الخبير الأعلى.[3]

1 . – هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم الإلكترونية ، مكتبة الآلات الحديثة، الطبعة الأولى 1994 ص 42-143،

2 –.خيرت محرز، التحقيق في الجرائم الحاسب الآلي، دار الكتاب الحديث للطباعة و التوزيع ، القاهرة، سنة 2012.، ص 96 و 97.

3 – رشيدة بوكر ، مرجع سابق، ص 429.

الفرع الثالث : إعتماد الدليل التقني في الإثبات

أولا : تعريف الدليل التقني

تعددت التعريف التي قبلت بشأن الدليل التقني وتباينت لذا سنعرض أهم هذه التعريفات فيما يلي :

هناك من يعرفه بأنه:" معلومات يقبلها المنطق والعقل ويعتمد العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم الإلكترونية وملحقاتها وشبكات الإتصال ويمكن إستخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة او جاني او مجني عليه"، أو أنه يشمل "جميع البيانات الرقمية التي يمكن أن تثبت إن هناك جريمة قد أرتكبت ".

والدليل الرقمي أو الإليكتروني أو الرقمي هو عبارة عن :" كل البيانات التي يمكن أن إعدادها أو تخزينها في شكل رقمي في الحاسوب"، ويمكن تعريف البيانات الرقمية بأنها مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت والصورة، أو, أنه الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل نبضات كهرومغناطسية، ممكن تجميعها وتحليلها بإستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال من أجل تقديمه أمام أجهزة تطبيق القانون .[1]

وما هو جدير بالذكر أن هناك فرق بين الدليل التقني وبرامج الحاسب الآلي يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في القيام بمختلف العمليات التي يحتويها النظام المعلوماتي عند إعطاء الأوامر بالقيام بذلك، أما الدليل التقني فله أهمية كبرى ودور أساسي في معرفة كيفية حدوث جرائم الإلكترونية بهدف إثباتها ونسبتها إلى مرتكبيها.[2]

ثانيا : تقدير القاضي الجزائي للدليل التقني

1 – رشيدة بوكر ، مرجع سابق، ص 382 و383.

2 – عائشة بن قارة مصطفى، مرجع سابق، ص 31.

إذا توافرت في الدليل التقني الشروط العامة لما يمكن أن يتمثل أساسا لإنبعاث الثقة فيه، فإنه قد يبدو من غير المعقول أن يعيد القاضي تقييم هذا الدليل ودلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، وبالتالي فلا حرية للقاضي في مناقشة الحقائق العلمية الثابتة.

رغم أن هنالك إمكانية التشكيك في سلامة الدليل التقني بسبب قابلية للعبث إلا أن تلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم خاصة إذا توافرت في الدليل التقني الشروط الخاصة بسلامته من العبث والخطأ، ورغم ذلك تبقى مسألة الأدلة العلمية والفنية في الإثبات راجعة الى السلطة التقديرية للقاضي لأنه يبقى المسيطر حقيقة وبإستطاعتة تفسير الشك لصالح المتهم.[1]

ثالث : حجية الدليل الإليكتروني في الإثبات

إن الخصوصية الجريمة الإلكترونية والتي تتميز بالطابع الفني، دفع المشرع الجزائري بأن يبادر في مواكبة التطور القانوني على المستوى الدولي وتماشيا مع التطور التكنولوجي، بتمهيد للطريق أمام إستخلاص الدليل الإليكتروني في القانون رقم 04/09 في المادة 06 منه[2]، مراعيا بذلك الإعمال بالقواعد العامة التي من الضروري توافرها في الدليل الإليكتروني وهي مبدأ المشروعية، بمعنى أنه لا يكون مستخلصا بطريقة مخالفة لأحكام القانون ولا مبادئ دستورية خاصة ما تعلق منها بحماية الحريات الأساسية .

ومما هو مستقر عليه فإن القاضي الجزائري ملزم بفحص الدليل الإليكتروني لكي يتواصل إلى تشكيل قناعة إنطلاقا من عرض هذا الدليل على مناقشة الأطراف، وهو ما نصت عليه المواد 212و 234 من قانون إ .ج.ج.[3]

1 – رشيدة بوكر ، مرجع سابق، 507.

2 – المادة 06 من القانون رقم 04/09 والتي تنص :" على حجز المعطيات الإلكترونية وذلك بإفراغها أو نسخها على دعامة تخزين إليكترونية قابلة للحجز الوضع في أحراز".

3 – زيبجة ، زيدان، مرجع سابق، ص 173.

وبذلك يتضح لنا الدليل التقني له حجية في الإثبات وذلك بما يتميز به من موضوعية وكفاءة، ومحكم وفق قواعد علمية عملية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته، ويساعد القاضي من التقليل من الأخطاء القضائية و الإقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة .[1]

والإستدلال على ذلك نلاحظ إن الفقه الفرنسي يتناول حجية الدليل التقني في المواد الجزائية ضمن مسألة قبول الأدلة الناشة عن الآدلة الناشئة عن الآلة أو الأدلة العلمية مثل: الردارات، الأجهزة السنمائية، أجهزة التصوير ، أشرطة التسجيل، أجهزة التنصت.[2]

وبظهور الدليل التقني فقد زاد من دور الإثبات العلمي وإستتبعه تعاظم دور الخبراء في القيام بدور فعال في إبداء خبرتهم الفنية، كذلك فقد توفر التقنية العلمية طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في وضع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة عملية قد يصعب إثبات عكسها، مما يدفع هذا الأمر بالإعتقاد بأنه بمقدار إتساع مساحة الأدلة العلمية بمقدار ما يكون انكماش وتضاؤل دور القاضي الجزائي في التقدير خاصة أمام غياب الثقافة الإلكترونية للقاضي.[3]، ولكن هذا لا ينفي حقيقة الضرورة الماسة للدليل لتقني لأنه يتماشى مع طبيعة الجريمة الإلكترونية ومع التطور التكنولوجي الحاصل مما يستدعي الامر عدم التوقف عند مضمون الدليل الإليكتروني فقط بل يجب التركيز والإهتمام بتطوير الإجراءات التي يترتب عليها الحصول على هذا الدليل مع إشتراط ضرورة مشروعيتها وخلوها من العبث والخطأ .بإعتبار أن الدليل الإليكتروني أو التقني له حجية في الإثبات خاصة في التشريعات التي تأخذ بمبدأ حرية الإثبات وسلطة القاضي التقديرية كما في التشريع الجزائري.

1 – بوكر رشيدة ، مرجع سابق، ص 497.

2 – هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجزائية ، الطبيعة الثانية ، دار النهضة العربية، القاهرة، سنة 2008.، ص 42 و 43.

3 – أ – رشيدة بوكر ، مرجع سابق، ص498.

خاتمة

الخاتمة

في الأخير نخلص، إلى أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام، ومن ثم كان لابد أن يبادر إلى تبني سياسة موسعة ومحكمة، تستهدف إيقاف كل التحديات التي يطرحها هذا الإجرام، وإيمانا بأهمية الوقوف أمام التحديات التي تفرضها هذه الجريمة، ارتأينا ختم هذا البحث ببعض الاقتراحات والتوصيات التي قد تساهم في التقليل من الآثار السلبية لكثير من التحديات المصاحبة لوسائل الاتصال الجديدة، وتندرج هذه التوصيات تحت النقاط الآتية:

1 – إعطاء جرائم التقنية حقها من الأهمية في مؤسسات التشريع الوطنية والدولية على السواء، مع التركيز على أهمية إدراج نصوص هذه الأخيرة ضمن التشريعات الوطنية المختلفة، باعتبار أن جرائم الإنترنت ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية، والاهتمام بالتعاون الدولي في مجال المكافحة لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية والكمبيوتر وشبكة الانترنت ككل.

2 – تعديل بعض التشريعات الحالية بما يتلائم مع طبيعة جرائم الإنترنت والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح، وخاصة وأن في مجال الملكية الفكرية فالتشريع الوحيد الذي تقع برامج المعالجة الآلية للمعطيات تحت حمايته هو قانون حقوق المؤلف وحتى في هذا إطار هذا القانون لا تتعدى الحماية شكل البرنامج فقط، لهذا السبب تبرز أهمية البحث عن إطار أكبر وأوسع لبرامج الكمبيوتر يتعدى النصوص التقليدية لجريمة التقليد المنصوص عليها في قانون حقوق المؤلف والحقوق المجاورة.

3 – نظرا لطبيعة الجريمة الإلكترونية الخاصة وكيان بيئتها غير المحسوس تظهر صعوبة مهام السلطات شبه القضائية والسلطات القضائية في أداء دورها للكشف عن الجريمة والبحث عن أدلتها فحتى؛ وإن نجحت الدّول نسبيا في تطبيق الأساليب الإجرائية التقليدية كالمعاينة والتفتيش والضبط وإضفاء بعض الخصوصيات والشروط عليها، لتتلائم وطبيعة الجريمة

المعلوماتية، تبقى بعض الصعوبات دائما للكشف عن هذه الجريمة والمتمثلة في قلة الآثار المادية التي تتركها وكثرة الأشخاص الذين يترددون على مسرحها بين فترة ارتكابها وفترة اكتشافها، مما يصعب عملية الكشف عنها.

4 – عقد دورات مكثفة للعاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوبات، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الإنترنت.

5 – مساعدة شركات التقنية والإنترنت العربية في اتخاذ إجراءات أمنية مناسبة، سواء من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة، والبرامج.

6 – التنسيق لإنشاء مركز معلومات عربي مشترك يهتم برصد وتحليل جرائم الحاسوب، يضم معلومات مكتملة عن أي واقعة ومعلومات عن المدانين والمشتبه بهم، حيث أن جريمة الإنترنت لا تحدها حدود وطنية، أو قومية.

7 – سرعة تماشي عملية التشريع مع المعطيات الواقعية، والإسراع في إصدار القوانين التنظيمية، من خلال محاولة وضع مدونة قواعد السلوك في مجال المعلوماتية، تتناسب والتطورات التي يعرفها الإجرام المعلوماتي.

8 – كما تظهر ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات وتسليم المجرمين وقبول أي دولة للأدلة المجموعة في دول أخرى.

–ضرورة وضع تشريعات فيكل الدول تتتسق مع الأحكام القانونية الدولية في مجال مواجهة هذه الجرائم، وتنظيم الأحكام الإجرائية الخاصة بمواجتها..

– إعداد بر امج أمن المعلومات من خلال إعداد خطط التدريب المختلفة مع تعيين المتخصصين في كل جهة لتتولى مسؤولية الأمن المعلوماتي.

– .وضع ضوابط لمقاهي الانترنت وحصر المترددين عليها وعمل قاعدة بيانات لهم حتى يسهل متابعتهم منح سلطات التحقيق الصلاحية القانونية والتدريب العملي اللازم لاختراق نظام الحاسوب وضبط ما يحتويه من بيانات مخزنة.

– ضرورة التعاون الدولي لمواجهة مشاكل صور السلوك المنحرف المتمثل في جرائم الكمبيوتر والانترنت، وذلك بعقد المزيد من الإتفاقيات الثنائية والجماعية.

وأخيرا في رأينا، أن أحسن حماية هي الحماية الوقائية ن بحيث من الأفضل نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية)عدم الاحتفاظ ببيانات شخصية أو مالية على الأجهزة، عدم نشر معلومات شخصية، عدم إعطاء كلمة السر..الخ.)

قائمة المراجع

قائمة المراجع

أ- الكتب

1. رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الآلية، وفي التشريع الجزائري المقارن، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت ، لبنان، سنة، 2012،
2. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001
3. أسامة سمير حسين، الإحتيال الإليكتروني (الوجه القبيح للتكنولوجيا) ، الحنادرية للنشر والتوزيع ، الأردن الطبعة الأولى ، سنة 2011،
4. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية
5. – عبد الفتاح البيومي الحجازي ، مبادئ الإجراءات الجنائية في الجرائم الكمبيوتر و الأنترنت، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى سنة 2006
6. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999.
7. سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية ، دراسة مقارنة)، رسالة دكتوراه ، كلية الحقوق ، جامعة عين الشمس، سنة 1997
8. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر ، الإسكندرية، سنة 2009
9. محمد دباس الحميد، ماركو إبراهيم نينو، حماية الأنظمة المعلومات، دار حامد للنشر والتوزيع، عمان ، الطبعة الأولى ، سنة 2007
10. جعفر حسين جاسم الطائي، جرائم تكنولوجيا المعلومات(رؤية جديدة للجريمة المعلوماتية)، دار البداية ،عمان سنة 2007،
11. نسرين عبد الحميد نبيه، الجريمة الإلكترونية والمجرم المعلوماتي، منشأة المعارف للنشر والتوزيع ، الأردن، دون سنة

12. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، دار الجامعة الجديدة، 2008.
13. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، الطبعة الثانية،
14. محمد ماجد ياقوت، أصول التحقيق الإداري في المخالفات التأديبية، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، بدون سنة نشر
15. طارق الدسوقي عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، الطبعة الأولى، دار الجامعة الجديدة، 2009،
16. محمد زكي أبو عامر، الإجراءات الجنائية، ط 8، دار الجامعة الجديدة، مصر، 2008.
17. هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة،2000.
18. زيبحة زيدان، الجريمة الإلكترونية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، سنة 2011
19. خيرت محرز، التحقيق في الجرائم الحاسب الآلي، دار الكتاب الحديث للطباعة و التوزيع ، القاهرة، سنة 2012.
20. نهلا عبد القادر المومني الجرائم المعلوماتية، الطبعة 2 ، دار الثقافة للنشر والتوزيع، سنة 2001
21. محمد عبيد الكعبي، الجرائم الناشئة عن الإستعمال الغير المشروع للشبكة الانترنت، دار النهضة العربية، القاهرة سنة2001،
22. نائلة عادل فريد قورة،، جرائم الحاسب الإقتصادية، دراسة نظرية تطبيقية، منشورات الحلبي القانونية القاهرة،؟ سنة 2005، ص 48.
23. طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعية الجديدة للنشر ، الإسكندرية، سنة 2009
24. ايمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار النشر، دون بلد النشر، سنة 2004، ص 17.

25. سامي صادق الملا، اعتراف المتهم، دار الفكر العربي، الطبعة الأولى، 1998

26. محمد ماجد ياقوت، أصول التحقيق الإداري في المخالفات التأديبية، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، بدون سنة نشر، ص 289.

27. محدة محمد، ضمانات المتهم أثناء التحقيق، الجزء الثالث، الطبعة الأولى، دار الهدى، عين مليلة، الجزائر

28. خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010

29. حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 1990، ص 78.

30. كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000،

31. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009،

32. علي عدنان الفيل إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي للنشر، كلية الحقوق، جامعة الموصل،سنة 2011

33. خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010

34. حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 1990، ص 78.

35. كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000،

36. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009،

37. محمد أمين الرومي، جرائم الكمبيوتر و أنترنت/ دار المطبوعات الجامعية ، الإسكندرية، سنة 2003،

38. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، سنة 1992

39. خالد ممدوح إبراهيم، فن التحقيقي الجنائي في جرائم الإليكترونية، الطبعة الأولى دار الفكر الجامعي للنشر ، الإسكندرية ، 2009

40. على عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي للنشر، كلية الحقوق، جامعة الموصل،سنة 2011

41. إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، جامعة الإمارات، في سنة 2000 مؤتمر القانون والكمبيوتر و الأنترنت، جامعة الإمارت، كلية الشريعة والقانون عام 2000،

42. عبد الفتاح بيومي حجازي ، الإثبات الجنائي في الجرائم الكمبيوتر والأنترنت، طبعةخاصة 2009، بهجات للطباعة والتجليد، جمهورية مصر العربية ، سنة 2009

43. هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانا المتهم المعلوماتي ، ط1 دار النهضة العربية القاهرة، سنة 1997

44. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009

45. هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم الإلكترونية ، مكتبة الآلات الحديثة، الطبعة الأولى 1994

ب- المذكرات والرسائل

1. محمد الأمين البشري، بحث بعنوان التحقيق في جرائم الحاسب الآلي، مقدم إلى المؤتمر القانون والكمبيوتر والأنترنت، المنفعة في الفترة من 1-3 مايو 2000بكلية الشريعة والقانون بدولة الإمارات، ص 58.
2. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012
3. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر1، 2011-2012.
4. عائشة بن قارة مصطفى، حجية الدليل الإليكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير كلية الحقوق ، جامعة الإسكندرية، سنة 2009،
5. سهيلة بوزبرة، مواجهة الصفقات العمومية المشبوهة، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل، 2008
6. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007
7. هشام رستم، جرائم الحاسب كصورة من صور الجرائم الإقتصادية المستحدثة بحث مقدم إلى لجنة العلمية بمصر لمنع الجريمة الإلكترونية ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيط ، العدد 17 ، سنة 1995 ص 107 و 108.
8. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2011-2012

ج- الندوات والمؤتمرات

1. برابح يمينة، تطبيقات الأمن المعلوماتي، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017.

2. لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي، بالملتقى الوطني الموسوم بـ: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7 و8 فبراير 2017.

د- الاتفاقيات والقوانين

1. الإعلان العالمي لحقوق الإنسان صادر عن الجمعية العامة للأمم المتحدة بتاريخ 1948./12/10

1- القوانين

1. القانون رقم 06/05 الصادر في 2005/08/23 المتعلق بمكافحة التهريب المعدل بالأمر رقم 09/06 في 2006/07/15.
2. القانون رقم 15 – 19 المؤرخ في 30 ديسمبر 2015 يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 جوان 1966 ، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71 ، الصادرة في 30 ديسمبر 2015
3. القانون رقم 04/09 المؤرخ في 5 أغسطس 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
4. القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.
5. القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14 ، الصادرة في 07 مارس 2016.
6. القانون رقم 14/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية، الجريدة الرسمية العدد (71) لسنة 2004.
7. القانون رقم 06-22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 والمتضمن قانون الإجراءات الجزائية، المنشور في الجريدة الرسمية رقم 84 الصادرة سنة 2006.

8. القانون رقم 04/09 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، 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.
9. القانون رقم 15/04 المؤرخ في 27 رمضان 1425 هـ الموافق/ لـ10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات رقم 156/66 المؤرخ في 18 صفر 1386 هـ/ الموافق ل 8 يوليو 1966، الجديدة الرسمية العدد (71) لسنة 2004.

2- المراسيم

1. مرسوم رئاسي رقم 261-15 المؤرخ في 24 من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 ، الصادرة في 08 أكتوبر 2015.
2. المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق
3. المرسوم الرئاسي رقم 261-15 المؤرخ في 24 من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها..

3- الاوامر

1. الأمر رقم 156/66 معدلة ومتممة بموجب المادة (33) من القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006.
2. الأمر رقم 15 – 02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40 ، الصادرة في 23 جويلية 2015

3. الأمر رقم 07/03 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع، المعدل للأمر رقم 17/93 المؤرخ في 1993/12/07 المتعلق بحماية الاختراعات المعدل للأمر 54/66 في 1963/03/03 المتعلق بشهادات المخترعين وإجازات الاختراع.
4. الأمر رقم 05/03 الصادر بتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة.

المراجع باللغة الاجنبية

[1] - MARWE VANDER ,computer crimes and other grimes against information Technology in south Africa ,"R.I.D.P",1993;p554.
[1] -Klaus Tiede man, Fraude et autres délits d'affaires commis a l'aide d'ordinateurs électroniques, Rev, drpén , crim, 1984, p 612.
[1] - Jack Bologna, Corporate Fraud, hte Basic of prevention and Detction , Butter worth, 1984,p11.

1. WASIK Martin , computer crimes and other crimes against information tesnnology in the unit kingdom "R.I.D.P" , 1991,p19.
2. MASCALA Corinne , criminalité et contrat électronique, Travaux de l'association, CAPITANT Henir , journées National paris, 2000,p118.
3. D.B.PARKER, comibattre la criminalité informatique , edoros,1987,p142.
4. Johannes F.NIJIbaer , challenges for the low of Evidence, leiden ,INREP,1999,p16.
5. M. Moherenschloger ,computer crimes and others crimes against information technology in the Germany,Rev ,int,dr, pen ,1993p319,spec349.
6. Taylor ,R, computer crime, criminal investigation edited, « by Charles Swanson ,N, chamelin and L. Teritto hill,inc.5 edition,1992,p450.
7. Taylor Robert ,op.cit ,p01.

الفهرس

مـلخص مذكرة الماستر

إستخلاصنا أهام النتائج في هذه الموضوع في إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية

إذ وجدنا من خلال الموصضوع إن عالم تقنية المعلومات الحديثة عالم واسع لا يحده حد، وان الوسائل المستعملة في ارتكاب الجريمة الالكترونية متشعبة ومتنوعة وخاصة في اتباع الجرائم المعاوماتية التي تقوم بها الجها المتخصصة في الكشف عن الجرائم ولابد من تطوير الكشف عن الجرائم والمتابعة من قبل الجهات المتخصصة

وهذا الامر يتطلب وقفة من قبل المشرع والقضاء لاتخاذ مجموعة من الخطوات الاصلاحية لمواجهة هذا النوع من الجرائم.

الكلمات المفتاحية:

1/البحث والتحري 2/الجرائمة الإلكترونية 3/ اجراءات التفتيش4/إختصاص القضائي 5/الاثبات في الجرائم

Abstract of The master thesis

We extracted the most important findings on this topic in the investigation procedures and gathering evidence in information crimes

As we found through the subject that the world of modern information technology is a wide world with no limitations, and that the means used in the commission of electronic crime are manifold and varied, especially in following the peculiar crimes carried out by the body specialized in the detection of crimes, and the detection of crimes and follow-up must be developed by the specialized authorities

This matter requires a pause by the legislator and the judiciary to take a set of reform steps to confront this type of crime.

key words:

/ 1Research and investigation 2 / Informational crime 3 / Inspection procedures 4 / Judicial jurisdiction 5 / Evidence of crimes