الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد الطارف
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة بعنوان :

إجراءات البحث والتحقيق في الجريمة المعلوماتية

مقدمة لإستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص : قانون جنائي وعلوم جنائية

إعداد الطالبين :

- عقاب ليندة
- مصباحي فريد

إشراف الأستاذ :

أحمد حسين

لجنة المناقشة

الاسم واللقب	الرتبة	الجامعة	الصفة
بن نولي زرزور	أستاذ محاضر " أ "	جامعة الشاذلي بن جديد– الطارف	رئيسا
أحمد حسين	أستاذ محاضر " أ "	جامعة الشاذلي بن جديد– الطارف	مشرفا
العايب نصر الدين	أستاذ محاضر " ب"	جامعة الشاذلي بن جديد– الطارف	ممتحنا ومناقشا

السنة الجامعية : 2024/2023

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد

UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة) : عقاب لبنى .....

الحامل لبطاقة التعريف الوطنية رقم: 104589351 .....

الصادرة بتاريخ: 2017/05/15 .....

عن دائرة: عين العسل ولاية الطارف .....

المسجل بقسم : الثانية ماستر علوم جنائية (قانون جنائي) .....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

إجراءات البحث والتحقيق في الجريمة المعلوماتية .....

.....

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2024/06/02

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة) : مصباحي فريد

الحامل لبطاقة التعريف الوطنية رقم: 108224000

الصادرة بتاريخ: 2018/03/12

عن دائرة: بوحوش - الطارف

المسجل بقسم : الشافية ماستر قانون جنائي وعلوم جنائية

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

إجراءات البحث والتحقيق في الجريمة المعلوماتية

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2024/06/02

إمضاء المعني

إهداء

إلى التي لا يمكن للكلمات أن توفي حقها

وإلى التي لا يمكن للأرقام أن تحصي فضائلها.....

الأم التي ربتني وأنارت دربي وأعانتني بالصلوات

والدعوات أطال الله في عمرها وادعو لها بالشفاء العاجل.

إلى روح أبي الغالي الذي عمل بكد في سبيلي

وعلمني الكفاح وأوصلني إلى ما أنا عليه رحمة الله

وأسكنه فسيح جناته.

إلى من لا تكفيني كل معاني الحب

أهديه له "زوجي العزيز"

إلى الأحبة ونبر السعادة أولادي: ملاك

سيف الاسلام، وسيم، عبد الله

إلى كل العائلة والأحباء والأصدقاء، رفقاء الدرب

في الحياة أختي الغالية أمال التي طالما ساندتني في إتمام

مذكرة الماستر دون أن أنسى ابنة أختي "بوكاؤد شيماء"

إلى زملائي وأصدقائي بمحكمة القالة

وخاصة مصلحة تنفيذ العقوبات

لكم مني كل عبارات الشكر والاحترام

الطالبة: عقاب لينـدة

إهداء

الحمد لله والصلاة والسلام على الحبيب

محمد صلى الله عليه وسلم

إلى من كلها الله بالهيبة والوقار إلى من علمني العطاء

دون انتظار إلى من احمل اسمها بكل افتخار

إلى من كان دعاؤها سر نجاحي وحنانهما بلسم جراحي أمي وأبي

يحفظهما الله ويطيل في عمرهما في الخير والصلاح

إلى من بوجودهم أكسب قوة ومحبتهم لا حدود لها إخوتي رعاهم الله

إلى كل من علمني حرف أساتذتي الكرام جزاهم الله كل خير

إلى أصدقائي اللذين كانوا عونا لي على مصاعب

الحياة الدراسية جزاهم الله خيرا

إلى كل هؤلاء شكرا جزيلا

الطالب: مصباحي فريد

شكر وعرفان

أتقدم بالشكر الجزيل في هذا المقام الأول إلى الدكتور القدير والأستاذ المحترم "أحمد حسين" على قبوله مهمة الإشراف على مذكرة الماستر وهو الذي لم يبخل علينا بنصائحه القيمة النابعة من تجربته الطويلة في ميدان البحث العلمي ومتابعته المتواصلة لأطوار انجاز البحث.

أستاذي الفاضل أزكى عبارات الشكر والتقدير كما لا يفوتني أن أتقدم بالشكر إلى أعضاء اللجنة المحترمة وبالإضافة إلى انشغالاتهم المتعلقة لأداء مهام الرسالة العلمية، إلا أنهم أبوا أن يشاركوا في مناقشة هذا العمل يدفعهم إلى ذلك هدف نبيل وهو تطوير مجالات المعرفة العلمية.

لكم منا جزيل الشكر والامتنان وجزاكم الله عنا خير جزاء نضع هذا العمل المتواضع بين يدي كل محب وساع وراءه راجيا من المولى تعالى أن يضيفه لنا في ميزان أعمالنا وأن يتقبله لنا خالصا لوجهه الكريم.

مقدمة

المقدمة :

شهد العالم ثورة مذهلة في مجال التكنولوجيا والاتصالات وتقنية المعلومات حتى أن مقولة أن العالم أصبح قرية صغيرة مقولة شارفت الصواب في معظمها وهذه الثورة في التقنية كان من أهم أوجه انتفاضتها التقدم المذهل في مجال الحواسيب الآلية وملحقاتها والبرامج التي تلحق بها كما بات الإعتماد على هذه التكنولوجيا واضحا جليا في كل الجهات الرسمية والغير الرسمية ، حتى بات العنصر البشري يشكو من إحلال الأجهزة الذكية من حواسيب وبرامج محل الجهد البشري حيث حل الذكاء الإصطناعي محل الذكاء البشري ، على الرغم من أن هذه التكنولوجيا هي صناعة بشرية في الأساس ، وأصبحت الدول تقاس مدى تقدمها بقدرتها على إمتلاك والتعامل مع التكنولوجيا الحديثة في شتى نواحي الحياة ، بالرغم من هذه النعمة الكبيرة التي حلت بالجنس البشري ، إلا أن هذا النعمة صاحبتها نقمة ، تمثلت في الاستخدام الغير قانوني لهذه التكنولوجيا حتى أصبحت هذه لتكنولوجيا تستخدم كمعول هدم لا للبناء ، في أيدي الخارجين عن القانون ذو الصفات الخاصة ، صاحبوا الإجرام ، الذي لا يراق فيه نقطة دماء وبالرغم من خطورة هذه الجرائم ، نجد صعيد آخر أنه خطرا لأن هذه الجريمة عابرة للحدود ، فإن هذا السلوك الإجرامي الذي يستخدم شبكات المعلومات والتكنولوجيا الحديثة يسهل التهرب من العقاب حيث يرتكب الكثير من هذه الجرائم من على بعد دولي.

وقد إنتشرت في الآونة الأخيرة وأصبحت ظاهرة جديرة بالنظر والإعتبار، والإجرام المستحدث ، الذي يتم عن طريق التكنولوجيا ، فهي الجريمة المعلوماتية والتي أصبحت ظاهرة تخترق المجتمع و تهدد دعائمه ، ولعله الجوهر والسبب الرئيسي لتجريم هذه

الجريمة ، وهو ما دعا المشرع الجزائري إلى سن تشريعات تتماشى مع المستجدات على الساحة الإجرامية .

إن الموضوع الدراسة موضوع متسع يجمع بين الجانب التقني لعالم المعلوماتية ، والجانب القانوني المتمثل في الجريمة المعلوماتية ذاتها ، والشق الإجرائي المتعلق

بأعمال البحث والتحقيق الموجهة للكشف عنها ، غير أن دراستنا تهدف وفي ظل تعدد المعطيات إلى تسليط الضوء على الجانب القانوني الإجرائي خصوصا المتعلق بأعمال البحث والتحقيق بشان الجرائم المتعلقة ، مع عدم إقصاء الجانب الموضوعي والتقني للجريمة المعلوماتية ، نظرا لكون الموضوع نقطة تقاطع بين عالم التكنولوجيا المعلومات والقانون.

أهمية الموضوع:

لاشك إن ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق و نحن لا نزال في بداية عصر الانفجار المعلوماتي ، يعني توقع ظهور المزيد و المزيد من هذه الأنماط الجديدة ، التي يتوجب معها تحديث الأنظمة و التعليمات و الجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة و هو ما يستتبع تطوير أسلوب التحقيق و التفتيش فيها .

و لقد قمنا بإختيار هذا الموضوع و جعلناه موضوع دراستنا في هذه المذكرة نظرا لأهميته البالغة لموضوع الإثبات الجنائي في الجرائم المعلوماتية ,و تظهر هذه الأهمية من خلال اعتبار أن موضوع الجرائم المعلوماتية حديث و كثير الانتشار حاليا ، كما أنه من الموضوعات التي تثير جدلا فقهيا لدى فقهاء القانون الجنائي ، إضافة إلى

تعلق هذا الموضوع بالوسائل الحديثة ذلك أنه كلما تطورت الوسائل المعلوماتية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم ، و هذا ما شكل عائق أمام القائمين على البحث و إثبات الجرائم المعلوماتية حيث أن قواعد البحث و التحقيق و أسس الإثبات الجنائي في القوانين التقليدية لا تكفي بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلاءم مع طبيعتها الفنية.

أسباب اختيار الموضوع :

تبرز أسباب اختيار الموضوع من خلال :

– التزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية و تزايد درجة خطورة هذا النشاط و إرتفاع مستوى التهديدات التي يشكلها على الأمن العام يقابله عجز سلطات البحث و التحقيق عن رسم نموذج موحد لهذه الجرائم و الإستقرار على جملة من الإجراءات الخاصة بمتابعتها نظرا لتطورها الدائم و المستمر مما ينتج عنه أحيانا غياب أو جمود النص الإجرامي و عجزه عن تفعيل الإجراءات بسبب عدم ملائمته للجريمة محل البحث و التحقيق .

– الرغبة في التعمق في دراسة و تحليل الآليات القانونية الإجرائية الحديثة الموجهة لمكافحة النشاط الإجرامي الالكتروني .

– إن موضوع البحث يكتسي أهمية بالغة من الناحية العملية فمبرر غياب النصوص الملائمة لمباشرة الإجراءات قد لا يكون السبب الوحيد في ظهور إشكالات متعلقة بإجراءات البحث و التحقيق في مجال الجرائم المعلوماتية ، فقد تتوفر النصوص القانونية المناسبة و تغيب الوسائل المادية الضرورية لتنفيذ الأعمال الخاصة بالبحث

والتحقيق وكلها عوامل تستقطب الإهتمام لأجل معالجتها بالبحث و التحليل، لأجل وصول آلة وضع تصور قانوني و فني في آن واحد يضمن التعريف بموضوع الجريمة المعلوماتية بشقيها المعلوماتي و الإجرائي .

أهداف الدراسة : الهدف من هذه الدراسة هو تسليط الضوء على إجراءات التحقيق والتحري في الجرائم الماسة بأنظمة الاتصال و المعلوماتية و إبراز خصوصيتها بالنسبة للجرائم التقليدية .

إن الغاية الموجودة من هذه الدراسة تتمثل في تحديد طرق و كيفية الوصول وإستخلاص أدلة الإثبات الجنائية في الجرائم المعلوماتية و تهدف هذه الدراسة إلى تقديم رؤية خاصة بشأن التحقيق الجنائي في هذه الجرائم ,كون أن مسرح الجريمة الرقمي هو مسرح إفتراضي غير مرئي ، كما تناولت الدراسة صعوبات التي تواجه التحقيق الجنائي و لفت الإنتباه من خلال هذه الدراسة إلى أن الدليل الرقمي و تحديد ماهيته يعتبر من أهم أدلة الإثبات في الجرائم المعلوماتية .

صعوبات البحث :

إن الوصول إلى وضع خطة متوازنة ومعالجة فعالة ودقيقة لموضوع البحث لم يكن بالسهولة المتوقعة بدءا بالنظر إلى طبيعة الموضوع المزدوجة (القانونية والفنية) والتي شكلت تحديا بالغ الصعوبة نظرا لما يميز الموضوع من دقة المصطلحات والمفاهيم العلمية منها القانونية والتي يصعب التحكم فيها ، وتوظيفها بشكل مناسب ومتلازم ، مع مراعاة عدم تغليب أي من الطابع القانوني على الفني أو العكسي من

ذلك تحت طائلة فقدان البحث لمعالمه المزدوجة إلى مجموعة من الصعوبات الأخرى التي يمكن ذكرها بإيجاز :

– قلة الدراسات في المجال الإجرائي واتجاه أغلبها لمعالجة الظاهرة الإجرامية المعلوماتية من ناحية السلوك الإجرامي والعقوبات المقررة لها دون التركيز على الجانب الإجرائي ، وهو ما جعل الباحث أمام حتمية تجميع المعلومات الخاصة بالموضوع في شكل جزئي ، وإعادة تجميعها بشكل متناسق وفق خطة عمل ذاتية .

– تشعب الموضوع وتداخله مع مصطلحات وجوانب تقنية مما دفعنا الى الإستعانة بعدة تخصصات لفهم بعض المصطلحات والجوانب التقنية ، إضافة الى بذل جهد كبير في دراسة الجوانب الفنية دعما للجوانب القانونية .

إشكالية الدراسة : إن إجراءات البحث و التحقيق في الجنائي العام هي الأساس في البحث و التحقيق في الجرائم الالكترونية تماما كما هو الحال في باقي الجرائم الأخرى فان استخدامها يتوقف على ظروف كل جريمة فالملاحظ إن إجراءات التحقيق في الجرائم المعلوماتية تتصف بالخصوصية من حيث طريقة كشفها و التبليغ عنها و العناية بمسرح الجريمة . و هو ما يدفعنا إلى طرح التساؤل التالي :

إلى أي مدى وفق المشرع الجزائري في وضع آليات قانونية للتحري و التحقيق عن الجريمة الالكترونية ؟.

وتندرج هذه الإشكالية مجموعة من التساؤلات الفرعية المتوافقة ، وتسلسل أفكار البحث والتي يمكننا إيجازها في جملة التساؤلات التالية :

1-هل تكفي القواعد الإجرائية المقررة لإثبات الجرائم التقليدية لكي تسري على الجرائم المعلوماتية ؟

2- ما طبيعة الأدلة المستهدف تحصيلها من خلال أعمال البحث و التحقيق في الجرائم المعلوماتية ؟

3- ما هي المشكلات التي تعيق سريان قواعد القانون الجنائي من حيث المكان في الجرائم المعلوماتية ، ما هي شروط و أسس قبول الدليل الرقمي كدليل إثبات جنائي؟

4-هل يوجد إثبات المؤسساتية المختصة في الكشف عن الجريمة المعلوماتية ؟

المناهج التبعة : لقد إتبعنا في دراستنا هذه مجموعة من المناهج التي تلائم الموضوع أهمها :

المنهج التحليلي :

يعد منهجا رئيسيا ويتضمن دراسة الأساليب التي تستخدم في التحري و مدى مشروعيتها وهذا ما يتم استخلاصه من تحليل النصوص القانونية و دراسة الجوانب الإجرائية الخاصة بها .

المنهج الوصفي :

يعد منهجا ثانويا لأن البحث في مجال الإجراءات الخاصة بالتحري و التحقيق في مجال الجرائم المعلوماتية , يفرض على الباحث إعتماد منهجية علمية خاصة تتماشى و ترتيب الأفكار المطروحة حسب خطة البحث و لذلك فقد اعتمدنا على المنهج الوصفي و كذلك التحليلي من خلال ما ورد في البحث من وصف لمفهوم

النظم المعلوماتية و الجريمة المعلوماتية و مختلف الجهود الفقهية و القانونية المتعلقة بمسألة البحث و التحقيق في الجرائم المعلوماتية إضافة إلى التعرض لمختلف الجهات المختصة بمباشرة هذه الإجراءات ووسائلها و أساليب عملها وصولا إلى نتائج هذه الأعمال و الإجراءات كل ذلك في شكل وصف دقيق .

خطة البحث :

للإجابة على الإشكالية المطروحة و تماشيا مع العنوان المقترح إرتأينا أن نتبع الخطة التالية لدراسة الموضوع حيث قسمناه إلى فصلين :تناولنا في

الفصل الأول : **إجراءات البحث و التحري في الجريمة المعلوماتية** .وذلك في مبحثين المبحث الأول يتعلق بالإختصاص في الجرائم المعلوماتية والمبحث الثاني يتعلق بالإجراءات الخاصة بالبحث في الجرائم المعلوماتية ، أما **الفصل الثاني** : إجراءات التحقيق في الجريمة المعلوماتية وذلك في مبحثين يتعلق المبحث الأول بإجراءات إستخلاص الدليل في الجريمة المعلوماتية والمبحث الثاني يتعلق بخصوصية التحقيق في الجريمة المعلوماتية .

الفصل الأول
إجراءات البحث والتحري
في الجريمة المعلوماتية

تمهيد:

تمتاز الإجراءات الجزائية بمجموعة من المراحل بداية من المراحل التي تكون قبل وقوع الجريمة ثم مرحلة التحريات الأولية ما تسمى بمرحلة الاستدلالات أو الحقائق وتنتهي بتحريك الدعوى والمباشرة فيها وتكون مرحلة جمع الاستدلالات من المراحل المهمة التي تمر بها الدعوى الجزائية، حيث تلعب دورا هاما في مساعدة الجهات المختصة في كشف المستور ومعرفة الحقائق وتفصيلها، ومن جهة أخرى تخفف العبء على الجهات القضائية المختصة والتي هي الأخرى خصها المشرع الجزائري من خلال وضعه لقانون الإجراءات الجزائية ، فكل جهة قضائية والاختصاص المسند لها في مجال محاربة الجريمة و الحد منها وكشفها بشتى الطرق والأساليب المنصوص عليها في النصوص القانونية فمن خلال هذا إرتبطت مهمة التحري والبحث بمهام وإختصاص الجهات القضائية كالضبطية القضائية كل وإختصاصاته ومهامه في مجال كشف الجريمة والقضاء عليها .ونتناول في الفصل الأول مبحثين كالآتي:

المبحث الأول: الإختصاص في الجرائم المعلوماتية

التحريات الأولية أو جمع الاستدلالات مصطلح يطلق على نمط سير الإجراءات الجزائية التي ينفذها أعضاء الضبط القضائي عند إرتكاب جريمة ما، وما يقصد من التحري هو البدء بالإجراءات تعد تمهيدية تباشرها الضبطية القضائية قبل البدء في تحريك الدعوى العمومية ،أي بمعنى آخر التثبت من وقوع الجريمة ، والبحث عن القائم بها وجمع الإثباتات والقرائن اللازمة للتحقيق فيها والإستعانة بها للكشف عن الجريمة ، ولا تجيز الجريمة المعلوماتية وبحكم خصوصيتها وطبيعتها . لأي كان من جهات الضبطية

القضائية أو جهات التحقيق أو النيابة العامة أن تأمر البحث والتحقيق بشأنها وتعتبر شروط الإختصاص القضائي من مسائل النظام العام التي يمكن إثارتها في أي مرحلة كانت عليها الدعوى فتتعرض الإجراءات برمتها للبطلان في حالة عدم إستيفائها ، وشروط الإختصاص في مسائل البحث والتحقيق نوعان: إختصاص نوعي وآخر إقليمي ، فلا يمكن لمن يتولى أعمال البحث والتحقيق مباشرة أعماله وهو غير مختص نوعا، كما لا يمكن لمن يتولى الإجراءات نفسها وهو يتمتع بصفة الإختصاص النوعي ممارسة أعماله خارج نطاق إختصاصه الإقليمي .

المطلب الأول : شروط الإختصاص في الجريمة المعلوماتية :

إن المقصود بالإختصاص هو السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها الوطنية داخل أقاليمها، وتعد الجرائم المعلوماتية من أكثر الجرائم التي تطرح مسالة الإختصاص إذ أن الطبيعة التقنية العالية للنظم المعلوماتية المرتبطة بشبكات الإتصال العالمية، يمكن أن تؤدي إلى أن يصبح إقليما أكثر من دولة مسرحا للجريمة الواحدة،الأمر الذي ينجم عنه تنازع في الاختصاص بين هذه الدول فقد يحدث أن ترتكب الجريمة المعلوماتية في إقليم دولة معينة و تتحقق النتيجة في دولة أخرى، وأن التحقيق هو مجموعة القواعد القانونية والفنية التي تباشرها السلطة المختصة لتمحيص الأدلة والكشف عن الحقيقة في الجرائم المعلوماتية بوجودها كأساس موضوع التحقيق المستحدث، وينبغي التطبيق السليم للقانون من خلال التقدير السليم للدليل المستمد من الجريمة ، وإحترام قواعد الإختصاص وعدم تجاوز الحيز المكاني و الزماني خاصة عند عبور الجريمة ، حدود الدولة الواحدة، وإحترام مختلف عناصر التحقيق، مع كفالة حقوق الأفراد لتحقيق توازن عادل بينما تفرض السلطة العامة مع مراعاة مبدأ الشرعية الإجرائية

والحق فيه ،أين يخضع الفرد لقيود تحد من حرية الخصوصية تحديا أمام سلطات التحري والتحقيق في الجرائم المعلوماتية، كما أن قواعد إثبات الجرائم المعلوماتية تعتبر مميزة، ولذلك فقد حرص المشرع الجزائري على إسنادها لجهة قضائية لأجل ضمان كفالة حقيقية لجملة الحقوق والحريات الفردية، وتتمثل عادة هذه الجهة القضائية في هيئة الضبطية القضائية إذا كانت الإجراءات متعلقة بالبحث والتحري، وفي هيئة قضاء التحقيق إذا كانت الإجراءات متعلقة بمرحلة التحقيق القضائي متمثلة في شخص قاضي التحقيق [1] .

كما أن الإختصاص العملي والفني في مجال أعمال البحث والتحري في الجرائم المعلوماتية يعود بالدرجة الأولى إلى دائرة مكافحة الجرائم المعلوماتية التابعة للمديرية العامة للأمن الوطني، وكذلك الفرق التابعة لمركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابعة لسلك الدرك الوطني، وإلى مديرية المراقبة الوقائية واليقظة المعلوماتية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتحت إشرافها،والتي تم الإعلان عن إنشائها رسميا بموجب صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 وتم تعديلها بصدور مرسوم

(1) تعمل كل من الضبطية القضائية على القيام بأعمال البحث والتحري عن الجرائم ما لم يبدأ فيها التحقيق القضائي وذلك من قبل ضباط وأعوان الشرطة القضائية وكذلك بعض الأعوان المنوب بهم هذه المهام وذلك تحت إدارة وكيل الجمهورية وإشراف النائب العام لمجلس القضائي التابع له وإذا ما فتح التحقيق بشان تلك الجرائم تحول دورهم التنفيذ تفويضات جهة التحقيق و تنفيذ طلباتها – راجع نصوص المواد 12 إلى 14 قانون الاجراءات الجزائية .

رئاسي رقم 439/21 الموافق ل7 نوفمبر 2021, مما يجعل منهم العنصر البارز في متابعة هذه الإجراءات بصفة فعلية دون غيرهم.

الفرع الأول : وسائل التحري وجمع الأدلة :

عند القيام بالتحقيق في جريمة ما فإنه يجب على المحقق الإلتزام بقوانين وتشريعات ولوائح مفسرة، وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني، وحيث أن للجرائم المعلوماتية طابعها الخاص المميز لها فإن التحقيق و البحث فيها يحتاج إلى معرفة تامة وإدراك لوسائل وقوع الجريمة و بالتالي حل لغزها و الوصول إلى الجاني، وعليه سنتناول دراسة الوسائل المادية و الوسائل الإجرائية .

1-**الوسائل المادية** : وهي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات و التي يمكن بإستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها [1]: عناوين IP, البريد الإلكتروني وبرامج المحادثة : عنوان الإنترنت هو المسؤول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للمواجهات والشبكات المعنية بنقل الرسالة. وهو يوجد بكل جهاز مرتبط بالإنترنت، ويتكون من أربعة أجزاء، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية والجزء الثاني مزود للخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، و الرابع يحدد جهاز الحاسبة الالكترونية الذي تم الإتصال منه [2].

---

[1] – سليمان بن مهجع العنزي ، وسائل التحقيق في جرائم نظم المعلومات ، رسالة ماجستير في العلوم الشرطية ، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2003، ص 98.

2- arbiat 2000 on line available at www. Arbiat com تم الاطلاع يوم 2024/04/24 20:00 ساعة.

وفي حالة وجود أي مشكلة أو أي أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز، وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال الغير القانونية . ويمكن لمزود خدمة الإنترنت أن يراقب المشترك كما يمكن للشبكة أن تقدم خدمة الإتصال الهاتفي و أن تراقبه أيضا إن توفرت لديها أجهزة وبرامج خاصة لذلك وتوجد أكثر من طريقة يمكن معرفة من خلالها هذا العنوان الخاص بجهاز الحاسبة الالكترونية في حالة الاتصال المباشر منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل Windows وأما في حالة استخدام أحد البرامج التحادثية كأداة الجريمة فإنه يتطلب تحديد هوية المتصل كما حددت رسالة البريد الالكتروني عنوان شخصية مرسلها حتى وإن لم يدون معلوماته في خانة المرسل شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الالكتروني معلومات صحيحة [1].

- **البروكسي (PROXY)** : يعمل كوسيط بين الشبكة و مستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الإتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة .
- **برامج التتبع** : تقوم هذه البرامج بالتعرف على محاولات الإختراق التي تتم مع تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه و يحتوي هذا البيان على إسم الحدث و تاريخ حدوثه وعنوان (IP) التي تمت من خلاله عملية الإختراق وإسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى .

[1] – سليمان بن مهجع العنزي ، وسائل التحقيق في جرائم نظم المعلومات ، رسالة ماجستير في العلوم الشرطية ، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2003 ، ص 99.

- **نظام كشف الإختراق** : ويرمز له إختصارا بالأحرف (IDS) و هذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يحوي حدوثها على أجهزة الحاسبة الإلكترونية أو الشبكة مع تحليلها بحثا على أي إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسبة الإلكترونية أو الشبكة.
- **أدوات الضبط** : هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة المعلوماتية، منها على سبيل المثال أدوات المراجعة وأدوات مراقبة المستخدمين للشبكة وبرامج التسنط على الشبكة، والتقارير التي تنتجها نظم أمن البيانات .
- **أدوات فحص و مراقبة الشبكات** : هذه الأدوات تستخدم في فحص بروتوكول الإنترنت وذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات أداة (ARP) و وظيفتها تحديد مكان الحاسبة الإلكترونية فيزيائيا على الشبكة .
- **برنامج VISUAL ROUTE** : هو عبارة عن برنامج يلتقط أي عملية فحص عملت ضد الشبكة فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها المسح، والمناطق التي مر فيها الهجوم .

2- **الوسائل الإجرائية** : ويقصد بها الإجراءات التي بإستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها و منها :

أ) إقتفاء الأثر.

ب) الإطلاع على عمليات النظام المعلوماتي و أسلوب حمايته.

ج) الإستعانة بالذكاء الإصطناعي .

الفرع الثاني : ضباط الشرطة القضائية:

يتولى ضباط الشرطة القضائية مسائل البحث والتحري في كافة الجرائم بما في ذلك الجرائم المعلوماتية فلا يوجد مانع قانوني يحد من ممارسة هؤلاء لأعمالهم المتعلقة بالبحث والتحري سواء أن يتوفر فيهم شرط الاختصاص النوعي في مجال جرائم المعلوماتية بعد تبليغهم بوقوعها [1] والذي يمكن تحديده في التمتع بصفة ضابط الشرطة القضائية، وذلك تقييدا بما يفرضه نص المادة 5 من الفصل الثالث المتعلقة بالقواعد الإجرائية الخاصة بتفتيش النظم المعلوماتية الواردة في نص القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال وسبل مكافحتها والتي تنص على أنه : يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية ... الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها . وبناءا على ذلك فإن الأشخاص المذكورين في نص المادة 15 قانون 15-02 من قانون الإجراءات الجزائية المعدل والمتمم و التي تحدد قائمة حصرية بصفة الأشخاص المنوط بهم هذه الصفة، هم الأشخاص المخولون قانونا بمباشرة أعمال البحث و التحقيق في جرائم المعلوماتية. [2]

---

[1]– المادة 17 فقرة 1 من قانون الإجراءات الجزائية المعدل بموجب الأمر رقم 15-02 المؤرخ في 23 جويلية 2015 .

[2] –جاء في النص المادة 15 من قانون الإجراءات الجزائية المعدلة بموجب الأمر 02-15 المؤرخ في 23 جويلية 2015 انه يتمتع بصفة ضباط الشرطة القضائية : رؤساء المجالس الشعبية البلدية ضباط الدرك الوطني ,الموظفون التابعون لأسلاك الخاصة للمراقبين و المحافظين وضباط الشرطة للأمن الوطني ذو الرتب في الدرك ورجال الدرك الذين امضوا في سلك الدرك 3 سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك بين وزير العدل و وزير الدفاع الوطني بعد موافقة لجنة خاصة الموظفون التابعون للأسلاك الخاصة للمفتشين و ضباط و أعوان الشرطة الأمن الوطني الذين امضوا في لسلك الدرك 3 سنوات على الأقل و الذين تم تعينهم بموجب قرار مشترك بين وزير العدل و وزير الدفاع الوطني بعد موافقة لجة خاصة .

إن المتمعن في نص المادة لا يكاد أن يتصور أن يقوم رئيس المجلس الشعبي البلدي بتولي أعمال البحث و التحقيق في الجرائم المعلوماتية، فحسب ما بيناه سالفا فإن هذا الإختصاص يعود وبالدرجة الأولى لضباط الشرطة القضائية المنتمين إلى الفرق المتخصصة في مكافحة الجرائم المعلوماتية، والتي تضم محققين من نوع خاص ولذلك وجب تخصيص نص منفرد في قانون الإجراءات الجزائية يحدد الإختصاص النوعي في شخص رجال الشرطة والدرك والأمن العسكري والموظفون التابعون للأسلاك الخاصة للمراقبين، ممن يتمتعون بصفة ضباط الشرطة القضائية حتى يتحقق الإنسجام العام والخاص ممثلا في القانون 09-04 وذلك تجنبا لتداخل الإختصاصات و تضييع فرص إحراز الأدلة والتسبب في إفلات الجاني من المتابعة والعقاب،إذا فالشرط الأساسي من أجل حق ممارسة أعمال البحث والتحري في الجرائم المعلوماتية هو التمتع بصفة ضباط الشرطة القضائية وهذا ما نصت عليه المادة 63 من قانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري بقولها: يقوم ضباط الشرطة القضائية و تحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الإبتدائية بمجرد علمهم بوقوع الجريمة، إما بناءا على تعليمات وكيل الجمهورية أو من تلقاء أنفسهم: ولقد أجاز المشرع حسب مضمون الفقرة الأخيرة من المادة 05 من قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وسبل مكافحتها وفي سبيل تخطي عقبات إنعدام المعرفة الفنية بالنظم المعلوماتية من قبل ضباط الشرطة القضائية، لهؤلاء أن يقوموا بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث بقصد مساعدتهم وتزويدهم بكل المعلومات الضرورية لإنجاز مهامهم دون أن تتعرض الإجراءات المتخذة للبطلان، وهو ما أكدته المادة 65 مكرر 8 قانون 06-22 المعدل و المتمم لقانون الإجراءات الجزائية الجزائري.

المطلب الثاني : الإختصاص النوعي و الإقليمي في الجريمة المعلوماتية :

إن مسائل البحث والتحقيق نوعان من حيث الإختصاص نوعان إختصاص نوعي وإختصاص إقليمي محلي ولا يمكن لمن يتولى أعمال البحث والتحقيق مباشرة أعماله وهو غير مختص نوعيا كما لا يمكن لمن يتولى الإجراءات نفسها وهو يتمتع بصفة الإختصاص النوعي ممارسة أعماله خارج نطاق إختصاصه الإقليمي .

الفرع الأول : الإختصاص النوعي للجهات القضائية :

أولا :جهة النيابة العامة: تعتبر النيابة العامة السلطة المختصة بمباشرة الدعوة العمومية بإسم المجتمع و تتولى مهمة المطالبة بتطبيق القانون [1] ويتولى النائب العام مهمة تمثيل النيابة العامة أمام المجالس القضائية فيما يمثلها لدى المحكمة وكيل الجمهورية أو احد مساعديه [2] .

وتتولى النيابة العامة المتمثلة في شخص وكيل الجمهورية إدارة نشاط الضبطية القضائية كما يتمتع هو نفسه بكافة السلطات والصلاحيات المرتبطة بصفة ضابط الشرطة القضائية فيتولى الأمر بمباشرة جميع الإجراءات اللازمة للبحث والتحري عن الجرائم بما في ذلك الجرائم المعلوماتية [3].

وله في حالة مباشرة الإجراءات الخاصة بالبحث والتحري في الجرائم المعلوماتية حسب أحكام المادة 35 مكرر من قانون الإجراءات الجزائية المستحدثة بموجب الأمر

---

[1]–المادة 29 من قانون الإجراءات الجزائية الجزائري.

[2]– المادتين 34–35 من قانون الإجراءات الجزائية الجزائري.

[3]–المادة 36 من قانون الإجراءات الجزائية الجزائري المعدل بموجب الأمر 15–02 المؤرخ في 23 جويلية 2015 .

15-02 المؤرخ في 23 جويلية 2015 أن يستعين بمساعدين متخصصين في مجال المعلوماتية تحت مسؤوليته ويقدمون أعمالهم في شكل تقارير تلخيصية أو تحليلية تتضمن النتائج المتوصل إليها بناءا على إلتماسات النيابة العامة و هو الإجراء الذي يهدف حسب رأينا إلى تحفيز أعضاء النيابة العامة على التعامل بصفة مباشرة مع جرائم المعلوماتية من أجل إكتشاف الخبرة والمهارات اللازمة في التعامل معها بصفة فورية وسريعة ربحا للوقت وعدم تفويت فرصة إحراز الأدلة في الوقت المناسب قبل إتلافها من قبل الجناة أو ضياعها نظرا لطابعها الإلكتروني، بدل إصدار الأمر بإحالتها على الوحدات الخاصة لمكافحة الجرائم المعلوماتية وما يترتب على ذلك من توفير فرصة للجاني في إتلاف الأدلة ومحوها بسبب طول المدة بين وقوع الجريمة ووقت إكتشافها وإنطلاق الإجراءات بشأنها .

ثانيا : إختصاص جهة التحقيق : يختص قاضي التحقيق بإجراءات البحث والتحري إختصاصا أصيلا حسب ما تقتضيه المادة 38 الأمر 69-75 قانون الإجراءات الجزائية وتختص بالتحقيق في الجرائم إما بناءا على طلب من وكيل الجمهورية أو شكوى مصحوبة بالإدعاء المدني ضمن الشروط المنصوص عليها في المادتين 67-73 من نفس القانون ووفق ما تنص عليه المادة 68 من قانون 01-08 من قانون الإجراءات الجزائية فإن القاضي التحقيق يقوم بإتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الإقناع وأدلة النفي وإذا كان من المتعذر عليه القيام بها بنفسه جاز له أن ينيب ويندب ضباط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة ضمن الشروط المنصوص عليها قانونا حسب المواد 138 إلى 192

قانون الإجراءات الجزائية بما في ذلك الجرائم المعلوماتية بما أن النص كان عاما وشاملا ولم يهدف بالتحديد والتخصيص في نوع الجرائم الجائز التحقيق فيها[1] فإن لأشخاص المنوط لهم قانونا مباشرة أعمال التحري والتحقيق في الجرائم المعلوماتية هم ضباط الشرطة القضائية، وكيل الجمهورية، قاضي التحقيق بحكم إختصاصهم النوعي ، وما يلاحظ بهذا الشأن هو غياب دقة النصوص القانونية الإجرائية المحددة للإختصاص النوعي في مجال البحث والتحقيق في الجرائم المعلوماتية، وهو ما يعني تضييق دائرة الإختصاص النوعي في مجال الجرائم المعلوماتية وحصرها في نفس مجال الجرائم العادية بالرغم من تخصيص فرق للبحث والتحقيق في الجرائم المعلوماتية.

الفرع الثاني : الإختصاص الإقليمي في الجرائم المعلوماتية :

تعتبر الجريمة المعلوماتية نوعا خاصا من الجرائم فهي لا تعترف بمبدأ الإقليمية ولا بالحدود الجغرافية فهي بمفهومها وطابعها الدولي قد قبلت مفاهيم الإختصاص الإقليمي للنص الجنائي وكذلك الإجرائي فهي قد تقع في آن واحد وعلى مستوى عدة دول، وذلك بسبب الطابع اللامادي للمعلومات والمعطيات محل للجريمة الذي نتج عنه مبدأ عدم إشتراط وقوع الجريمة المعلوماتية ضمن نطاق الإختصاص الإقليمي للنص الجنائي حتى ينشأ الحق في المتابعة والتحقيق وهي كلها معطيات أثارت إشكاليات ماسة بالمسائل الإجرائية [2]

[1]- حسب ما تنص عليه الفقرة الأخيرة من المادة 5 قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام و الاتصال و سبل مكافحتها فإن قاضي التحقيق و في حالة توليه إجراءات التحقيق بنفس شأن الجريمة المعلوماتية فله أن يستعين بكل شخص له دراية بعمل المنظومة المعلوماتية محل التفتيش بقصد مساعدته على انجاز مهمته .

[2]-myriam quémener – yves charpenel –la cybercriminalité-op-cit p 159

ومن الشروط التي يجب أن تتوفر في المحقق في الجرائم التقليدية صفة الإختصاص المكاني أي أن لا يمارس إجراءات البحث والتحقيق خارج دائرة الإختصاص المكاني ، وقد يمتد التحقيق في جريمة ما إلى ما خارج دائرة الإختصاص وفق ما يستلزم من ظروف التحقيق ومقتضياته ، وتبقى بذلك الإجراءات صحيحة لا بطلان فيها.

إن إعمال الشروط التقليدية لقاعدة الإختصاص المكاني ، أمر لا مفر منه من أجل البحث والتحقيق في مجال الجريمة المعلوماتية ، لكن كل ذلك غير كاف نظرا للطابع المميز لها فهي بذلك تثير إشكالات عدة تجعل من إختصاص المحقق مكانيا غير مجد نظرا لوجود محل البحث والتحقيق خارج نطاق الإختصاص الإقليمي المكلف به، وهو ما يستدعي توضيحه بإيجاز في النقاط التالية :

أولا: قاعدة الإختصاص المكاني في الجرائم المعلوماتية على المستوى الداخلي:

- يمارس عادة وفق أحكام الفقرة 1و2 من المادة 16 ق06-22 من قانون الإجراءات الجزائية الجزائري، ضباط الشرطة القضائية يتولون أعمال البحث والتحري ضمن إختصاصهم المحلي المحدد، أما بالنسبة للجريمة المعلوماتية ووفق ما نصت عليه الفقرة 4 من نفس المادة فإن عمل وإختصاص ضباط الشرطة القضائية يمتد على مستوى الإقليم الوطني من أجل متابعة البحث والمعاينة، وذلك تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا مع إعلام وكيل الجمهورية المختص إقليميا.
- بالنسبة لوكيل الجمهورية فإن الإختصاص الإقليمي محدد وفق نظام إختصاص الأقطاب المتخصصة، وذلك وفق ما تفرضه قواعد المرسوم التنفيذي 06-348

المؤرخ في 5 أكتوبر 2006 والمعدل والمتمم بموجب المرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 .

- بالنسبة لقاضي التحقيق يجوز له حسب نص الفقرة الثالثة والرابعة من مادة 47 ق 06-22 من قانون الإجراءات الجزائية أن يباشر عمليات التفتيش والحجز ليلا أو نهارا وفي أي مكان على إمتداد التراب الوطني إذا تعلق الأمر بالجرائم المعلوماتية وهو ما يعني بالضرورة أن إختصاص كل من وكيل الجمهورية وقاضي التحقيق الإقليمي إذا تعلق الأمر بالجرائم المعلوماتية هو إختصاص وطني.

ثانيا : قاعدة الإختصاص المكاني في الجرائم المعلوماتية على المستوى الخارجي :

بالنظر إلى الطابع الدولي للجريمة فإن أعمال البحث والتحقيق قد تستلزم تعدي نطاق الإختصاص الإقليمي الوطني ليمتد لإقليم دولة أخرى، وإن القواعد الخاصة المتبعة في سبيل ضمان شرعية الإجراءات هي الإتجاه إلى قواعد التعاون الدولي لمكافحة الجرائم المعلوماتية،فإذا تبين أن المعطيات المبحوث عنها والتي يمكن الدخول إليها 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 [1] إذن فما يمكن قوله في شأن أحكام الإختصاص النوعي والمكاني التي تحكم عمل الجهات المختصة بالبحث والتحقيق في الجرائم المعلوماتية على المستوى الوطني ، هو أنه وبالرغم مما تحمله من ضمانات شرعية إجرائية، كضمانات لحقوق

[1]- راجع بشأن ذلك الفقرة 3 من المادة 5 والمواد 16 ،17 ، 18 قانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكتنولوجيات الإعلام والإتصال الوارد في الملحق (02)

وحريات الأفراد إلا أنها تبقى غير متكاملة من حيث مفهومها وأحكامها الواردة في ظل كل من قانون الإجراءات الجزائية، وقانون مكافحة الجرائم المعلوماتية 09-04 .

المبحث الثاني : الإجراءات الخاصة بالبحث في الجرائم المعلوماتية :

إن للجرائم المعلوماتية طبيعة خاصة إذ أن أدلتها غير محسوسة أو تحتاج إلى خبرات فنية وتقنية عالية وعليه سنتناول في هذا البحث دراسة موضوع آلية الكشف والتبليغ عن الجرائم المعلوماتية في المطلب الأول وفي المطلب الثاني الخطوات الأولية لمباشرة أعمال البحث والتحري.

المطلب الأول : آليات الكشف والتبليغ عن الجرائم المعلوماتية :

كما سبق وأن فصلنا بشان خصوصيات الجريمة المعلوماتية فقد أكدنا على طابعها الخفي فهي نادرا ما تكون تحت وصف حالة تلبس إن لم نقل أن ذلك أمر مستحيل فالمجرم المعلوماتي يبذل كل ما في وسعه للإبقاء على جريمته خفية، وما يجعل من أمر كشفها والتبليغ لاحقا عنها أمر صعب، فما هي آليات الكشف عن هذه الجرائم ؟ وكيف يتم التبليغ والتعامل مع التبليغات بشأنها من قبل الجهات المختصة ؟

الفرع الأول : آليات الكشف عن الجرائم المعلوماتية :

إن الإشكال الذي يواجه أجهزة الأمن و المحققين من رجال الضبطية القضائية هو أن الجرائم المعلوماتية لا تصل إلى علم السلطات المعنية بالصور العادية ، وذلك لصعوبة إكتشافها من قبل الأشخاص العاديين وحتى المؤسسات والشركات لا تكتشف هذه الجرائم فور وقوعها على إعتبار أن أغلبها لا يراجع حساباته بشكل يومي، وحتى إن تم ذلك بشكل يومي أو شهري فانه يصعب عليها التأكد من الفوارق في الأرقام التي تبدوا

عادة خسائر أو ديون أو حتى في حالة اكتشافها فإن أغلب تلك الشركات تتردد في التبليغ خوفا على سمعتها [1] وهنا تظهر أهمية دور الأجهزة الأمنية في رصد حركة مرتكبي الجرائم المعلوماتية ، وإكتشاف هذه الجرائم من خلال الرصد الميداني لحركة المعاملات التجارية و مراقبة المشبوهين داخل المؤسسات المالية وحولها، فالقدرة على الملاحظة وقراءة تصرفات الأشخاص العاملين في مجال المعلوماتية والمهتمين بالبرامج وهواة صناعة الأنظمة هي أولى خطوات السيطرة الأمنية على نشاط مرتكبي جرائم الحاسوب ويتعزز كل ذلك من خلال تكثيف المراقبة من قبل الوحدات الخاصة لمكافحة الجريمة المعلوماتية في الأماكن وحول الفئات التالية :

*أسواق أجهزة الحواسيب والبرامج المعلوماتية .

*الرصد الدقيق لحركة المترددين على المواقع المذكورة أعلاه.

*الرصد الدقيق لحركة المشبوهين في مجال الأموال وتجار المخدرات.

*الرصد الدقيق لحركة معتدي جرائم التزوير والإحتيال و معتادي الإجرام المعلوماتي .

إن هذا القدر من التواجد الميداني المنظم يضمن تغطية أمنية على منافذ المعلومات و الحاسوب وله اثر وقائي و رادع في نفس الوقت ، كما يسمح بتوفير المعلومات الأولية

[1] ضياء علي احمد النعمان، مرجع سابق , صفحة 364

عن الجرائم المعلوماتية قبل وقوعها كما يضمن سرعة التبليغ عنها وإتخاذ الإجراءات بحقها [1]

الفرع الثاني : كيفية التبليغ عن الجرائم المعلوماتية :

البلاغ هو إخطار السلطات المختصة بوقوع الجريمة عليه أو على غيره لأن بعض هذه الجرائم جديدة على المجتمع، ويجب حماية البرمجيات والمحافظة عليها و لا يجوز إهمال بلاغ مقدم للسلطة لأن عدم تقصي البلاغ من أجهزة البحث والتحري يؤدي إلى وقوع جرائم كبيرة كالتي تحدث في البورصات العالمية و تؤدي إلى إنخفاض أسهمها وخسارتها[2] فالتبليغ هو المشكلة الحقيقية التي واجهت الجهات القضائية المختصة بمواجهة الجريمة المعلوماتية، فغالبية الهيئات والمؤسسات تخشى الإبلاغ عن الجرائم المعلوماتية خوفا من فقدان عملائها و هو ما ينتج عنه إفلات مرتكبي الجريمة بفعلته، والمبلغ عن الجريمة في جرائم الحاسوب والإنترنت يجب أن يتميز بدرجة مقبولة من الإلمام والمعرفة بالجوانب الفنية للحاسوب. حتى يتمكن من تقديم معلومات تصف الحادثة بشكل جيد، يمكن معه للمحقق الوقوف على طبيعة الجريمة بشكل مقبول يمكنه من مباشرة التحقيق فيها وبالتالي يفترض أن يكون لدى من يتلقى البلاغ المعرفة الكافية

[1] – عبد الفتاح بيومي حجازي، الجوانب الإجرائية لإعمال البحث والتحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية ص 72.

[2] – د عمر ابو بكر يونس ، الجرائم الناشئة عن الانترنت رسالة دكتورا جامعة عين شمس 2000ص 825 .

بالجوانب الفنية للحاسوب والانترنت حتى يستطيع مناقشة المبلغ في الكثير من الجوانب المتعلقة بالجريمة محل البلاغ. [1]

قد يكون التبليغ من خلال ملئ المبلغ للإستمارة الرقمية على الموقع المخصص لتلقي البلاغات والشكاوي كذلك التي يوفرها الموقع الرسمي للإنترنت الأحداث في فرنسا أو تلك المتوفرة على موقع .www.internet.miners.gor.f1 إدارة مكافحة جرائم الحاسبات وشبكات المعلومات المصري على الرابط التالي .www.cc.d.gov.eg :

وتظهر أهمية تلقي البلاغات في أنها تساعد رجال البحث والتحري على تحديد نوع الجريمة المبلغ عنها إن كانت تندرج ضمن الجرائم المعلوماتية، وكذلك وضع تصور مبدئي لخطة العمل المناسبة للبحث والتحري بشأن الجريمة وبالتالي تحديد نوع الخبرة المطلوبة لأجل المعاينة وتحريز الأدلة وما يجب التأكيد عليه أن جهة تلقي البلاغ يجب عليها أن تحرص على أن يقوم المبلغ بالخطوات التالية :

- تجهيز قائمة بأسماء العاملين في المؤسسة أو المشتبه فيهم
- تجهيز نسخة إحتياطية من بيانات الأجهزة المتضررة
- عدم تبليغ أي أحد آخر بالجريمة الواقعة .

المطلب الثاني : الخطوات الأولية لمباشرة أعمال البحث و التحري عن الجرائم المعلوماتية :

[1]– محمد فاروق عبد الحميد ، القواعد الفنية الشرطية للتحقيق و البحث الجنائي ، أكاديمية نايف العربية للعلوم الأمنية الرياض 1999 ص 52.

تعتبر الجريمة المعلوماتية من قبيل الجرائم الخفية أي أنها عبارة عن أنشطة إجرامية تتم في سرية بتخطيط وإعداد مسبق وتنفيذ بطريقة مدروسة من قبل مجرمين متمرسين في عالم الجريمة تجمعهم مصلحة عدم إبلاغ السلطات المختصة عن نشاطهم الإجرامي [1] وفي حالة الإبلاغ أو تقديم شكوى عن نشاط هؤلاء المجرمين لدى السلطات المختصة متمثلة في المصالح الأمنية والقضائية فإن هذه الأخيرة تباشر أعمال الإستدلال والتحري بشأن الجرائم محل البلاغ أو الشكوى فيبادر ضباط الشرطة القضائية و قبل كل شيء بالتأكد من الفرضيات في إطار آداء مهامهم .

الفرع الأول : الإجراءات الأولية للكشف عن الجريمة المعلوماتية :

قبل مباشرة أي إجراء و اتقاء لتضييع الجهد بشان جريمة لم تقع ,أو كانت محل تبليغ كاذب يباشر ضباط الشرطة القضائية إلى التأكد من :

أولا: التأكد من وقوع جريمة فعلية : فلا بد من أجل ضمان صحة الإجراءات الخاصة أن تكون أصلا بصدد جريمة معلوماتية سواء تحت وصف جنحة أو جناية أي استفاء الركن الشرعي [2] في حالة توفر هذه الشروط جاز لأعضاء فريق التحقيق المعلوماتي مباشرة أعمالهم بشان الجريمة المعلوماتية من خلال تحديد ملابساتها وهوية مرتكبيها من خلال إجراءات تسبق عملية الانتقال لأجل المعاينة المادية لمسرح الجريمة لسبب وحيد وهو أن غالبية الجرائم المعلوماتية هي جرائم غير متلبس بها أي أن أعمال البحث والتحقيق بشأنها , عادة ما تنطلق متأخرة بعد وقوعها وفي جرائم خفية تحتاج إلى خبرات فنية هائلة للكشف عنها ويعد الإرشاد الجنائي من أهم المصادر التي يعتمد عليها ضباط

[1]– محمد محمد عنب استخدام التكنولوجيا الحديثة في الإثبات الجنائي . دون ذكر دار النشر – مصر . 2007 . ص 176.

[2]– راجع المواد 394 مكرر الى 394 مكرر 7 من قانون العقوبات الجزائري .

الشرطة القضائية في عمليات البحث والتحري لجمع المعلومات ونصوص في مجال الجرائم المعلوماتية فنجد أن هيئات الضبطية أصبحت تجند عناصرها للدخول إلى العالم الافتراضي وبالخصوص مواقع التواصل الاجتماعي وقاعات الدردشة خصوصا تلك المعروف عنها تطرفها وميول العدوانية، وذلك تحت أسماء مستعارة يقصد البحث عن الجرائم ومرتكبيها، فضباط الشرطة القضائية ما عليهم سوى الإتصال بالشبكة وإعتماد أسلوب النقاش والدردشة الالكترونية مع الغير ومختلف الهيئات وبمجرد بروز مؤشرات عن هوية المجرم المعلوماتي أو الجرائم المعلوماتية كالإحتيال أو الإستغلال الجنسي للأطفال يبادر هؤلاء السؤال مثلا عن طرق الحصول على بطاقات الإئتمان المزورة أو عن مواعيد إستدراج الأطفال وهي المعلومات التي يستعين بها مزود الخدمة بالانترنت الذي يمكن أن يوفر بواسطة برمجيات خاصة مكان وجود المجرم ، وقد أتاح التشريع الجزائري اللجوء إلى هذا الأسلوب حسب مانصت عليه المادة 65 مكرر 5 ق 06-22 إلى غاية المادة 65 مكرر 18 قانون الإجراءات الجزائية، وذلك في حالة الجرائم المعلوماتية بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق وتحت الرقابة الأولى لمدة 4 أشهر قابلة للتجديد.

الفرع الثاني : إجراءات الوضع تحت المراقبة الالكترونية :

أقرت اتفاقية "بودابست" نظام المراقبة الالكترونية في المادة 21 منها تحت عنوان اعتراض معطيات المحتوى حيث ألزمت كل دولة طرف فيها ضرورة تبني جملة من الإجراءات من أجل تخويل هيئاتها وأجهزتها القضائية المختصة سلطة اتخاذ أسلوب مراقبة المعطيات المتعلقة بمحتوى الاتصالات والمنقولة عن طريق الأنظمة المعلوماتية وتجميدها وتسجيلها عن طريق الوسائل الفنية المتوفرة [1] ، كما تبنى المشرع الجزائري مصطلح المراقبة الإلكترونية كغيرها من التشريعات المقارنة الذي إستمده من نص الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي سنتها منظمة الأمم المتحدة في إطار الجريمة المنظمة حيث نصت المادة 20 من هذه الإتفاقية على أنه تقوم كل دولة طرف ضمن حدود إمكانياتها وفق الشروط المنصوص عليها في قانونها الداخلي إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك، بإتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب و كذلك ما تراه مناسبا من استخدام أساليب تحري خاصة أخرى مثل المراقبة الالكترونية أو غيرها من أشكال

1- تنص المادة 21 من اتفاقية بودابست على ما يلي « يجب على كل طرف أن يتبنى الاجراءات التشريعية أية إجراءات أخرى يرى أنها ضرورية من اجل تخويل سلطته المختصة سلطة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي ، الإمكانات التالية :

. أ : جمع او تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة عل أرضه .

. ب : إلزام مقدم الخدمات في نطاق قدراته الفنية المتوافرة على ان يجمع او يسجل عن طريق تطبيق الوسائل الفنية الموجودة عل أرضها ويمنح السلطات المختصة عونه ومساعديه من اجل تجميع او تسجيل في الوقت الفعلي المعطيات المتعلقة بمحتوى اتصالات معنية على ارض منقولة عن طرق نظام معلوماتي ...» بوكر رشيدة ، جرائم الاعتداء على النظم المعالجة الآلية في التشريع الجزائري و المقارن ، منشورات الحلبي الحقوقية ط 1 ، لبنان 212 ص 367 .

المقارنة[1] وهذا ما أكد عليه المشرع الجزائري بموجب المادة 3 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام و الاتصال .

ولا يفوتنا أن ننوه أن إجراء مراقبة الإتصالات الإلكترونية إنما يقصد به إعتراض الإتصالات الإلكترونية أثناء بثها أي في الزمن الفعلي لنقلها بين أطراف الاتصال وليس الحصول على إتصالات إلكترونية مخزنة، ذلك أن لكل من النوعين إجراءات خاصة به وهذا ما يستنتج من نصوص المواثيق الدولية والقانونية المذكورة أعلاه إذ نجد اتفاقية "بودابست" قد عبرت عن زمن الإعتراض بعبارة " في الوقت الفعلي " والإتفاقية العربية لمكافحة جرائم تقنية المعلومات" عبرت عنه بعبارة "بشكل فوري" أما المشرع الجزائري فقد وردت تحت عبارة " في حينها"

كما تجدر الإشارة إلى أن المشرع الجزائري لم يتبنى إجراء المراقبة المعلوماتية للإتصالات في القانون رقم 09-04 كإجراء تقتضيه التحريات أو التحقيقات أو من ضمن طرق الحصول على الأدلة الرقمية فقط بل أدرجه ضمن الإجراءات الوقائية من بعض الجرائم التي تشكل خطرا على امن الدولة وهي كما حددتها المادة 04 من هذا القانون الجرائم الإرهابية والتخريبية وكذا الجرائم الماسة بأمن الدولة منها الجرائم التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني كما يلاحظ أن المشرع الجزائري سمح بإجراء مراقبة الاتصالات الالكترونية بمجرد وجود احتمال التورط مستقبلا في ارتكاب إحدى هذه الجرائم وقبل وقوعها حتى غير أن احتمال وقوع جريمة الكترونية

[1]- بن بدة عبد الحليم ،المراقبة الالكترونية كإجراء استخلاص دليل الكتروني بين الحق في الخصوصية ومشروعية الدليل الالكتروني ، المجلة الاكادمية للبحث القانوني المجلد 1 ، العدد 3 ، 2019 ص 230.

ضعيف جدا إن لم نقل منعدم لأنها جرائم مميزة وغير مرئية وليس لها أي مقدمات مادية بل قد تكشف على سبيل المصادفة ولعل هذا يعود لتخوف المشرع الجزائري من وقوع هذه الجرائم ونحن نرى أنها خطورة ايجابية وجريئة تحسب له على إعتبار أن هذا الإجراء من بين اخطر الإجراءات مساسا بخصوصية الأفراد.

خلاصة الفصل الأول :

تم التطرق في هذا الفصل إلى الأجهزة المختصة في مكافحة الجريمة المعلوماتية متمثلة في الأجهزة الأمنية المتمثلة في الأمن الوطني، الدرك الوطني، سواء على المستوى الوطني أو المحلي والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، بعد ذلك تم التطرق إلى الإجراءات القانونية للتحري من اجل الكشف ومكافحة الجريمة المعلوماتية التي تمكن المحقق من التعرف على الجاني وتوقيفه و تقديمه أمام النيابة العامة لمتابعته جزائيا.

الفصل الثاني
إجراءات التحقيق
في الجريمة المعلوماتية

تمهيد :

يخضع الإثبات في المسائل الجنائية لقواعد المخالفة عن تلك المحتكم لها في المسائل المدنية ويعود ذلك لإعتبارات موضوعية ومنها ما يرجع لأهمية الدعوى الجنائية، فالقواعد التي تحكم المسائل الجنائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة الجريمة أول هاته القواعد حرية القاضي في تكوين قاعدته وقناعته فله أن يوجه تحقيقه في الجلسة بالشكل الذي يراه مناسبا وملائما للوصول إلى الحقيقة، كما أن له مطلق الحرية في تقدير أدلة الدعوى، وثاني القواعد التي تحكم الإثبات في المسائل الجنائية، فالإثبات نشاط إجرامي موجه للوصول إلى اليقين القضائي قطعا وفقا لمعيار الحقيقة الواقعية والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة الالكترونية وبين الواقعة المعروضة ولتحقق ذلك يستعمل وسائل معينة، ووسيلة الجريمة الإلكترونية هي الدليل الإلكتروني، ودراستنا للفصل الثاني في إجراءات التحقيق في الجريمة المعلوماتية في مجال الدعوى العمومية قسمناها إلى مبحثين الأول: إجراءات إستخلاص الدليل في الجريمة المعلوماتية و المبحث الثاني: خصوصية التحقيق في الجريمة المعلوماتية.

المبحث الأول : إجراءات إستخلاص الدليل في الجريمة المعلوماتية :

إن التطور الحالي الذي لحق ثورة المعلوماتية قد إنعكس أثره على الجرائم التي تولدت عنه فإنعكس أثره على قانون العقوبات ،كما أن عكس أثره على قانون الإجراءات الجزائية خاصة في مجال الإثبات الذي أثر بدوره على التطور الهائل الذي لحق الأدلة الجزائية ، بسبب تطور طرق إرتكاب الجريمة و بالنظر إلى الطبيعة الخاصة لتلك الجرائم المتمثلة في صعوبة إثباتها أو صعوبة التوصل إلى مرتكبيها بأدوات البحث الجنائي التقليدية الأمر الذي إستوجب على سلطات الضبط القضائي مسايرة هذه الأنماط من الجرائم عن طريق الاستعانة بالتقنيات العلمية الحديثة فالجريمة المعلوماتية تعتبر كأي جريمة من الجرائم المنصوص عليها في قانون العقوبات و القوانين الأخرى ، لذلك تتميز الجريمة المعلوماتية عن غيرها في الدعوى العمومية و هذه الدعوى تتم بمراحل لجمع الدليل الالكتروني و إستنادا لما سبق تقسم هذا المبحث إلى مطلبين : المطلب الأول : مفهوم الدليل الإلكتروني و أنواعه و المطلب الثاني :إجراءات و مشروعية الدليل الالكتروني .

المطلب الأول : مفهوم الدليل الإلكتروني و أنواعه :

تستند عملية الإثبات الجنائي في جرائم الحاسوب و الإنترنت على الدليل الالكتروني باعتباره الوسيلة الوحيدة و الرئيسية لإثبات هذه الجرائم الحديثة العهد ، و لهذا سوف نقوم في هذا المطلب بتعريفه و تقسيمه .

الفرع الأول : تعريف الدليل الإلكتروني : عرف الدليل الإلكتروني بأنه الدليل الذي يجد أساسا له في العالم الافتراضي و يقود إلى الجريمة ، فهو كل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني بحيث تمكن الحاسوب من إنجاز مهمة ما [1] و عرف كذلك بأنه معلومات يقبلها العقل و المنطق و يعتمدها العلم ، يتم الحصول عليها بإجراءات علمية و قانونية بترجمة المعلومات و البيانات المخزنة في الحاسوب و ملحقاته و شبكات الإتصال و يمكن استخدامها في أي مرحلة من مراحل التحقيق و المحاكمة لإثبات حقيقة الفعل أو الشئ أو شخص له علاقة بالجريمة ، و كذلك عرف الدليل الجنائي الإلكتروني بأنه الدليل المأخوذ في أجهزة الحاسوب و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ، من الممكن تجميعها و تحليلها بإستخدام برامج و تطبيقات خاصة ، و يتم تقديمها في شكل دليل يمكن إعتماده أمام القضاء[2].

و لم يتفق الفقه الجنائي حتى الآن حول تعريف موحد للدليل الإلكتروني ، و ذلك راجع الى التطور المستمر الذي يطرأ على البيئة التقنية التي ينشأ فيها ، و تجعله من الأدلة المتطورة بطبيعتها ، لاسيما أن العالم الافتراضي لا يزال في بداية عهده و لم يبلغ ذروته ، وأن العالم الإلكتروني أو الرقمي من غير الممكن إحتوائه ، فقد عرفه البعض بأنه " الدليل المأخوذ من أجهزة الحاسب الآلي ، و يكون في شكل ذبذبات رقمية و نبضات مغناطيسية يمكن جمعها أو تحليلها باستخدام برامج و تطبيقات تكنولوجية خاصة و يتم تقديمها في شكل دليل علمي يمكن إعتماده أمام القضاء الجنائي .

---

[1]– - د. عمر يونس ،جرائم الكمبيوتر و الانترنت ص 969 .

[2]– ممدوح عبد الحميد عبد المطلب ،البحث و التحقيق الجنائي الرقمي في جرائم الحاسب الآلي و الانترنت ، دار الكتب القانونية ،مصر 2006 ص 88.

و يعتقد البعض أن الأدلة الجنائية ما هي إلا مرحلة متقدمة في الأدلة التقليدية المادية التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان إلى الإستعانة بجميع ما يبتكره العلم من الوسائل التقنية العالية بما فيها جهاز الحاسب، و لكن الحقيقة تثبت عكس ذلك تماما، لأن الأدلة الالكترونية هي نوع آخر من الأدلة الجنائية الجديدة التي لها من الخصائص العلمية والمواصفات القانونية ما يميزها عن غيرها من وسائل الإثبات التقليدية، وهذه المواصفات والخصائص مرتبطة أساسا بطبيعة البيئة التي يتواجد فيها وهي البيئة الإفتراضية التي إنعكست على طبيعة هذه الأدلة وجعلته يتصف بهذه المميزات.

أولا : الدليل الإلكتروني دليل علمي : يتصف الدليل الإلكتروني بأنه علمي لأنه مشكل من معطيات إلكترونية غير ملموسة يتم إستخلاصها من طبيعة تقنية المعلومات ذات المبنى العلمي ، و أن ما يسري على الدليل العلمي يسري على الدليل الإلكتروني .

ثانيا : الدليل الإلكتروني دليل تقني : بمعنى أنه مستوحى في البيئة التقنية التي يتواجد فيها، والمتمثلة في مختلف الأجهزة التكنولوجية للإعلام و الإتصال من أجهزة الحاسوب و الهواتف و الشبكات، ولا يمكن أن نتصور وجود الدليل الالكتروني خارج هذا الإطار[1]

ثالثا : صعوبة التخلص من الدليل الإلكتروني : تعد هذه الخاصية أهم ميزة يتمتع بها الدليل الإلكتروني عن غيره من الأدلة المادية ، و إذا كان من اليسير جدا التخلص من الأدلة المادية نهائيا دون إمكانية استعادتها كالوثائق و الأشرطة بتمزيقها و حرقها ، أو

[1]- على محمود حمودة ، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي ، ورقة عمل المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية ، دبي 2003 ص 22.

بصمات الأصابع بمسحها من موضعها ، أو حتى الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة ، فان الحال غير ذلك بالنسبة للأدلة الإلكترونية ، إذ يمكن إسترجاعها بعد محوها و إظهارها بعد إخفائها و إصلاحها بعد إتلافها ، و ذلك بإستخدام أدوات و برمجيات ذات الطبيعة الرقمية صممت لهذا الغرض مثل : البرمجيات .

رابعا : الرقمية الثنائية للدليل الإلكتروني : مفادها أن الدليل الإلكتروني يتكون من تعداد غير محدود لأرقام ثنائية في هيئة واحد صفر (1-0) و التي تتميز بعدم التشابه فيما بينها رغم وحدة الرقم الثنائي الذي تتشكل منه ، مثلا المعلومات و البيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص أو حروف أو أرقام أو صور أو تسجيلات صوتية ليس لها الوجود المادي الذي نعرفه في شكل ورقي ، إنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد و هو الرقم الثنائي المذكور أعلاه [1].

الفرع الثاني : أنواع الدليل الإلكتروني :

إن أدلة الإثبات في جرائم الحاسوب و الإنترنت تختلف عن أدلة الإثبات في الجرائم العادية ، لأن الجرائم المعلوماتية تتم في بيئة غير مادية عبر نظام الحاسوب و شبكة الإنترنت حيث يمكن للجاني ان يعبث ببيانات الحاسوب أو برامجه و ذلك في وقت قياسي قد يكون جزءا من الثانية ، كما يمكن محوها في زمن قياسي ، مما يصعب الحصول على دليل مادي في مثل هذه الجرائم ، حيث تغلب الطبيعة الإلكترونية على الدليل المتوافر .

---

[1]- عبد الحميد عبد المطلب ، استخدام بروتوكول () TP; TCP في بحث و تحقيق الجرائم على الكمبيوتر، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية ، المنعقد بدبي في الفترة الممتدة من 26-28-08-2003 منشور على موقع الكتروني التالي : www.arablaw.info.com:08.

حيث أن الدليل الإلكتروني له عدة صور و أنواع ، وقد قسمها البعض إلى الأقسام الرئيسية التالية :

- أدلة إلكترونية خاصة بأجهزة الحاسوب و شبكاته .
- أدلة إلكترونية خاصة بالشبكة الدولية للمعلومات و الإنترنت .
- أدلة الكترونية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة الدولية للمعلومات [1] .

و كذلك قسم الدليل الإلكتروني الجناية لقسمين : الأول إعتبر ليكون وسيلة إثبات و الثاني لم يعد كوسيلة إثبات على النحو التالي :

اولا : أدلة أعدت لتكون وسيلة إثبات :

أ : السجلات التي تم إنشاؤها بواسطة الحاسوب تلقائيا و تعتبر هذه السجلات من مخرجات الحاسوب التي لم يساهم الأفراد في إنشائها مثل سجلات الهاتف و فواتير البطاقات البنكية .

ب : السجلات التي حفظ جزء منها بالإدخال و جزء تم إنشاؤها بواسطة الحاسوب مثل : رسائل غرف المحادثة المتبادلة على الإنترنت و رسائل البريد الإلكتروني [2]

ثانيا : أدلة لم تعد لتكون وسيلة إثبات :

و هذا النوع من الدليل الالكتروني نشأ دون إرادة الفرد وله أثر يتركه الجاني دون ان يكون راغبا في وجوده و يسمى بالبصمة الإلكترونية و تتجسد في الآثار التي يتركها

---

[1]– د.ممدوح عبد المطلب ، البحث و التحقيق الجنائي ، ص 88

[2]- خالد ممدوح ابراهيم ، الدليل الالكتروني في جرائم المعلوماتية ، بحث منشور على موقع كلية الحقوق لجامعة المنصورة على شبكة الانترنت ص2 www.f-low.com

مستخدم شبكة الإنترنت بسبب تسجيل الرسائل منه أو التي يستقبلها و كافة الاتصالات التي تمت من خلال الحاسوب او شبكة الإنترنت[1] .

حيث أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل من صدر عنه ، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة و لو بعد فترة زمنية من نشوئها ، فالإتصالات التي تجري عبر الإنترنت و المراسلات الصادرة عن الشخص أو التي يتلقاها ،كلها يمكن ضبطها بواسطة تقنية خاصة بذلك [2].

المطلب الثاني : إجراءات و مشروعية الدليل الإلكتروني :

إن مجرد وجود دليل يثبت وقوع الجريمة و نسبها لشخص معين لا يكفي الحكم بالإدانة ، إذ يلزم أن يكون لهذا الدليل قيمته القانونية و هذه القيمة للدليل الجنائي تتوقف على مسألتين رئيسيتين : الأولى المشروعية و الثانية اليقينية في دلالته على الوقائع المراد إثباتها .

الفرع الأول : مشروعية الدليل الإلكتروني : تعرف المشروعية بأنها التوافق و التقيد بأحكام القانون في إطاره و مضمونه العام حيث تهدف المشروعية لتقرير الضمانات الأساسية للأفراد، و حماية حقوقهم و حرياتهم الشخصية ضد تعسف السلطة القضائية ، و يجب أن يكون الدليل الإلكتروني متحصلا بطريقة مشروعة ، و يقصد بالشرعية في المقام الأول عدم مخالفة الأحكام التي تهدف الى صيانة كرامة الإنسان و حماية حقوقه، و ذلك ما تتضمنه الدساتير الحديثة ، بحيث يتقيد بها المشرع عند وضع قانون الإجراءات

---

[1]- عبد القتاح بيومي حجازي ، الدليل الرقمي في جرائم الكمبيوتر و الانترنت ، بهجة للطباعة و النشر ، القاهرة 2009 ص 64.

[2]- ممدوح عبد المطلب، مرجع سابق، البحث والتحقيق الجنائي، ص108.

الجزائية، فكل دليل مستمد بصفته مخالفة لهذه الأحكام يعتبر باطلا بطلانا مطلقا و يعني مبدأ المشروعية الدليل الجنائي الالكتروني بما يتضمنه من مفاهيم الإلكترونية ، ضرورة اتفاق الإجراء مع القواعد القانونية و الأنظمة المتبعة في وحدات المجتمع المتحضر ، أي إن قاعدة مشروعية الدليل الجنائي لا يقتصر فقط على مجرد المطابقة مع القاعدة القانونية بل يجب ان تراعي المبادئ السامية لحقوق الإنسان و قواعد النظام و حسن الآداب في المجتمع، وتفادي الطرق الغير المشروعة في تحصيل الدليل الإلكتروني كالإكراه المادي أو المعنوي، التدليس إتجاه المتهم من أهم ضمانات مشروعية الدليل الإلكتروني .

فإذا كانت المعلومات التي تشكل جريمة مخزنة في ذاكرة الحاسوب أو على الأقراص الصلبة أو المرنة فان التساؤل الذي يدور حول مدى إمكانية الحصول عليها من المتهم نفسه أو من غيره إذا كان يعلم سبيل الوصول إليها بإرادته أو من خلال إجباره على ذلك ؟ إن الإجابة عن هذا التساؤل دفعت بالفقه إلى اتخاذ موقفين :

الإتجاه الأول : يرى أنه لا يجوز إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظامه المعلوماتي، و إلزامه بالكشف عن الثغرات أو كلمات السر الخاصة بالدخول عملا بمبدأ لا يجوز إلزام الشخص نفسه بإتهام نفسه .

أما بالنسبة للشهود فان أنصار هذا الاتجاه يرون بأن الشاهد غير مجبر على تقديم المساعدة للحصول على الدليل الالكتروني ، أين يتمتع الشاهد بحرية الرفض عن الإجابة أمام المحكمة عن كل ما يعرفه و بالتالي يصعب إجباره على تقديم بيانات معلوماتية كونه

مؤهل للوصول إليها لمعرفته كلمة السر ، و إن تعاون من تلقاء نفسه فهو يقترب للخبرة منه للشهادة .

الإتجاه الثاني : يتفق مع الرأي القائل بعدم جواز إجبار المتهم على إدانة نفسه غير أن له موقف آخر تجاه إلتزامات الشاهد فيرى أن من إلتزامات الشاهد طبع ملفات البيانات و الإفصاح عن كلمة السر ، ماعدا الحالات المتعلقة بالمحافظة على سر المهنة فإنه يكون حرا في الإلتزام بآداء الشهادة إستجابة لسلطات التحقيق عند إصدارها أمر القائم بتشغيل النظام من أجل تقديم المعلومات اللازمة الخاصة إما بإفصاح عن كلمات المرور السرية الشفرات الخاصة بتشغيل البرامج[1].

أولا: شروط صحة الدليل المعلوماتي:

إن الأدلة الالكترونية إما أن تكون مخرجات ورقية ليتم انتاجها بواسطة الطابعة أو غير ورقية أي إلكترونية كالبيانات المخزنة على الأقراص الصلبة أو الأقراص المضغوطة أو غيرها من الأشكال الإلكترونية وقد تكمن في شكل عرض على الشاشة الخاصة بالحاسوب سواء كانت مخزنة على ذاكرة الحاسوب أو على شبكة الأنترنت ويكون الدليل الإلكتروني غير قابل للتعامل إذا ما شابه البطلان فلا يصح الإسناد عليه[2].

ا. **أن يكون الدليل الإلكتروني ذا علاقة بموضوع الجريمة المعلوماتية:** نصت على ضرورة توافر هذا الشرط المادة 407 من ق الإثبات الفدرالي الأمريكي ، و أسمته بمبدأ

[1] علي حسن أحمد الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، بحث منشور على الموقع الإلكتروني لمركز الإعلام الأمني، أكاديمية الشرطة البحرينية، مملكة البحرين، أفريل 2011، ص02، تاريخ التصفح: 2014/05/29.

[2] علي حسن أحمد الطوالية، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، مرجع سابق، ص05.

العلاقة الكاشفة حيث يتطلب ضرورة أن تكون هناك علاقة ما بين الدليل و ما بين الواقعة محل الدعوى ، و هو مبدأ لا يتحقق إلا بتحقق شرط آخر و هو مطابقة الدليل الإلكتروني المستخرج للأصل المخزن من الحاسوب بداخله .

II. **أن يكون الدليل الإلكتروني يقيني غير قابل للشك** : يشترط في الأدلة الإلكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة ، ذلك أنه لا مجال لدحض قرينة البراءة و افتراض عكسها إلا عندما يصل القاضي إلى درجة من القناعة تتسم بالجزم و اليقين[1]، و اليقين في النظم هو عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة و يتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى و ما يتطلع في ذهنه من تصورات و إحتمالات ذات درجة عالية من التأكيد و يمكن الوصول إلى اليقين عن طريق نوعين من المعرفة إحداهما حسية تدرك بالحواس و الأخرى معرفية تدرك بالعقل عن طريق التحليل و الاستنتاج .

III. **قابلية الدليل الإلكتروني للمناقشة** : يقصد بهذا الشرط وجوب مناقشة الدليل الجنائي بصفة عامة أي أن القاضي لا يمكن أن يؤسس قناعته إلا على العناصر الإثباتية التي طرحت للمناقشة في جلسات المحاكمة، و خضعت لحرية مناقشة أطراف الدعوى و هو ما يعني أن الأدلة الإلكترونية سواء المتحصل عليها من الحاسوب أو من شبكة الأنترنت سواء أكانت مطبوعة أو بيانات معروضة على الشاشة، وما تجدر إليه هو أن المشرع الجزائري بموجب المادة 212 من ق ا ج الجزائية في فـ2 بنصه : " و لا

[1] سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي، بحث مقدم في أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، كلية الحقوق جامعة بسكرة الجزائر.

يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه" فالقاضي ولكي تكون له السيادة و الهيمنة على الدعوى الجنائية فيجب أن يكون متدربا على كيفية التعامل مع تقنية المعلوماتية و تعقيداتها بشكل واف حتى يضمن له هذا التأهيل العلمي نجاح مهمته، إذا فالدليل الإلكتروني و بحسب ما إستعرضناه هو دليل على قدم المساواة مع باقي أنواع الأدلة الجنائية، بالرغم من مميزاته و خصائصه غير المألوفة في مجال الإثبات الجنائي،وذلك ما يمكن تفسيره بأنه متناسب و الجريمة الناشئ عنها التي تتميز هي الأخرى بمميزات و خصائص تخرج عن ما ألفناه بشان الجرائم التقليدية المادية .

الفرع الثاني : إجراءات حديثة لاستخلاص الدليل الإلكتروني :

كما سبق يلاحظ ان هناك قصورا بخصوص أساليب التحري التقليدية في إستخلاص الدليل الإلكتروني فالمشرع أجاز إستخلاص الدليل عموما وفق ضوابط إجرائية معينة، كما أن هذه الإجراءات تخص إستخلاص الدليل من الجرائم سواء كانت تقليدية أو مستحدثة و الأكيد أن هذه الإجراءات غير كافية لإستيعاب كافة أشكال الجريمة الإلكترونية فهي تحتاج من المشرع تدعيمها أو إستحداثات أخرى جديدة لمواكبة التطورات التقنية في مجال مكافحة الجريمة الإلكترونية، و ما قام به المشرع الجزائري في التعديلات المتتالية لأحكام قانون الإجراءات الجزائية بإدراج قواعد إجرائية جزائية جديدة و في الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة الخاصة للأفراد .

فنص المشرع الجزائري على إجراءات خاصة تهدف الى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و بعض الجرائم الأخرى و تتمثل هذه الإجراءات

في التسرب و إعتراض المراسلات و كذلك من خلال القانون 01-02 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و إستحداث إجرائين آخرين هما : المراقبة الإلكترونية و حفظ المعطيات[1].

أولا: الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب المادة 65 مكرر 5 الى 65 مكرر18 :

I. التسرب (الإختراق) وإعتراض المراسلات : تعتبر الجريمة المعلوماتية من بين الجرائم التي يمكن اللجوء فيها إلى إجراء التسرب و إعتراض المراسلات إذا اقتضت ذلك مقتضيات وضرورات التحري و التحقيق بشأنها.

1) التسرب (الإختراق) :إستحدث المشرع الجزائري إجراءات التسرب بموجب المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري التي تنص على " عندما تقتضي ضروريات التحري أو التحقيق يجوز لوكيل الجمهورية أو لقاضي التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه، بعد إخطار وكيل الجمهورية، أن يأذن تحت الرقابة حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه و بخلاف إجراءات التحري السابقة الذكر التي لم يعرفها المشرع الجزائري ، أورد تعريف التسرب بموجب نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري، يقصد بالتسرب قيام ضباط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم، يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال

(1) معتوق عبد اللطيف الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري ، و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر ، باتنة ، كلية الحقوق و العلوم السياسية قسم الحقوق 2011-2012 ص 106.

المذكورة في المادة 65 مكرر 14 أدناه و لا يجوز تحت طائلة البطلان ان تشكل هذه الأفعال تحريضا على إرتكاب الجرائم .

كما حدد المشرع نطاق تطبيق التسرب بموجب المادة 65 مكرر 5 سالفة الذكر و التي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ويلاحظ أن التسرب عملية تتسم بالتعقيد، فهو من تقنيات التحري و التحقيق الخاصة تسمح لضباط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، و ذلك تحت مسؤولية ضابط الشرطة القضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم و كشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية و تقديم المتسرب لنفسه على أنه فاعل أو شريك.

و التسرب كغيره من الإجراءات الحديثة له ضوابط و شروط شكلية و أخرى موضوعية حتى يعتد به :

- الضوابط الشكلية : و المتمثلة في:

أ. تحرير التقرير : و يلزم ضابط الشرطة القضائية المكلف بعملية التنسيق بتحرير تقرير كتابي يتضمن بيان مفصل عن جميع العناصر المتعلقة بالعملية و يجب ان يذكر في التقرير ووفق الترتيب الزمني جميع المعلومات ذات الصلة كالأفعال التي إستدعت حدوث عملية التسرب و كذا تحديد هوية العناصر المشتبه تورطهم في الجريمة .

ب: الحصول على إذن بالتسرب : و هذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية وعليه فالجهة القضائية المختصة بإصدار الإذن هو وكيل الجمهورية أو قاضي التحقيق و منه لا يجوز لضابط أو أعوان الشرطة القضائية القيام به حماية للحقوق المكرسة دستوريا .

ج: مدة التسرب : نصت المادة 65 مكرر 15 فـ3 حيث تنص : .....و يحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة 4 أشهر و لكن مراعاة لمقتضيات التحقيق الابتدائي يمكن تجديد هذه المدة ضمن نفس الشروط الشكلية و الزمنية السابقة .

- الضوابط الموضوعية : تتمثل الضوابط الموضوعية لعملية التسرب في شرطين رئيسيين :

أ : **التسبيب و نوع الجريمة** : فالتسبيب يعد أساس العمل القضائي، وعليه يجب على وكيل الجمهورية أو قاضي التحقيق عند إصدار الإذن بالتسرب توضيح الأدلة القانونية و الموضوعية بعد تقدير جميع العناصر المعروضة علية من طرف ضابط الشرطة القضائية [1] .

ب : **نوع الجريمة** : و قد حصرها المشرع في المادة 65 مكرر 5 من قانون الإجراءات الجزائية في سبعة أنواع الجرائم التالية : جرائم المخدرات ، الجريمة المنظمة العابرة للحدود الوطنية ، جرائم الماسة بأنظمة المعالجة الآلية للمعطيات جرائم تبييض الأموال ، الجرائم الموصوفة بأفعال إرهابية أو تخريبية ، جرائم متعلقة بالتشريع الخاص بالصرف و جرائم الفساد [2] .

---

[1] سيدهم سيدهم محمد ، محاضرة حول التسرب حسب تعديل قانون الإجراءات الجزائية ،محكمة فرندة ، مجلس قضاء تيارت.

[2] المادة 65 مكرر 12 من ق ا ج ز ، احمد بوسقيعة، التحقيق القضائي ،دار هومة . ط 6 ، الجزائر ،2009 ص 114.

ثانيا: الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب القانون 09-04 :

نظرا للطبيعة الخاصة للجرائم الالكترونية ، لم يكتفي المشرع بإستخدام هذه الأساليب حينما تقع و لكن أيضا قبل وقوعها ، و عليه صدر القانون رقم 09-04 المؤرخ في 15 اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و مكافحتها و الذي جاء لتكريس إطار قانوني أكثر ملائمة و إنسجاما مع خصوصية و خطورة الجريمة الإلكترونية نص هذا القانون على جملة من الإجراءات الهامة و عليه سنتناول مراقبة الإتصالات الإلكترونية و حالات اللجوء اليها .

I. **مراقبة الإتصالات الإلكترونية و حالات اللجوء إليها** : سنحاول التطرق من خلال هذه الفقرة الى المقصود بمراقبة الإتصالات الإلكترونية و حالات اللجوء إليها و شروطها .

1) : **المقصود بمراقبة الإتصالات الإلكترونية** : لم يتطرق المشرع الجزائري شأنه شأن أغلب التشريعات المقارنة إلى تعريف مراقبة الإتصالات الإلكترونية لكنه بالمقابل أوضح لنا مفهوم الإتصالات الإلكترونية بموجب المادة 2 من قانون رقم 09-04 سالف الذكر، الإتصالات الإلكترونية أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية .

(2) : **حالات اللجوء للمراقبة الإلكترونية** : مما لا شك فيه أن مراقبة الأحاديث و الإتصالات الخاصة كالتي تتم بالوسائل الإلكترونية تمس بحق الإنسان في الخصوصية المكفولة دستوريا في مختلف التشريعات الحديثة و عليه لم يترك المشرع الجزائري الأمر على إطلاقه استجابة للمواثيق الدولية و حماية لحقوق الإنسان في هذا

المجال حيث نصت المادة 4 من قانون 09-04 سالف الذكر حالات التي يجوز فيها مراقبة الإتصالات الالكترونية حيث تنص على :

يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 من القانون 09-04 في الحالات الآتية:

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

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

– مقتضيات التحريات كالتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية .

– في إطار تنفيذ طلبات المساعدة القضائية الدولية، لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة المختصة .

المبحث الثاني : خصوصية التحقيق في الجريمة المعلوماتية :

تعتبر إجراءات البحث و التحري المستحدثة مكسبا هاما لسلطات التحقيق في الكشف عن بعض الجرائم من بينها الجرائم المعلوماتية، و كما سبق و ذكرنا لضبط الأدلة الرقمية و جمعها من الموضوعات المستحدثة و المتطورة و ذلك بتعميق المعرفة في مجال التحقيق و إجراءات القانونية الصحيحة الواجب إتباعها من قبل السلطات القضائية المختصة في الكشف عن هذه الجرائم و عليه سنتناول في المبحث الثاني مطلبين:

المطلب الأول: التفتيش في الجريمة المعلوماتية وفي المطلب الثاني: الضبط و الخبرة القضائية في الجريمة المعلوماتية .

المطلب الأول : التفتيش في الجريمة المعلوماتية :

تعتبر أسرار الإنسان جزء مهم من حياته اليومية، ومن المنطلق يحق للفرد التمسك بعدم انتهاكها سواء كان في مسكنه ،و مراسلاته أو معلومة مخزنة في حاسوبه الخاص به أو نظامه المعلوماتي، و هذا الحق يعتبر من الحقوق الدستورية للمواطن ، لكن قد يتطلب في بعض الأحيان انتهاك هذا الحق من اجل الوصول الى الحقيقة التي يتطلبها القانون وهذا الخرق يكون بموجب إجراء نص عليه القانون و هو التفتيش[1] و سنقسم هذا المطلب إلى فرعين :

الفرع الأول : الإطار العام للتفتيش في الجريمة المعلوماتية :

نظرا للاختلاف بين التفتيش في المكان المادي للواقعة الإجرامية كإجراء تقليدي، وبين إجراءه في البيئة الإلكترونية التي تتميز بكونها مكان إفتراضي معنوي ، فإن الفقه أثيرت لديه إشكالية المصطلح الذي يناسبه مقارنة بالتفتيش الذي يتلاءم فقط مع الأدلة المادية في المسرح المادي للجريمة، و سوف نعرج على رأي الفقه و هذا بعد تناول تعريف التفتيش التقليدي، و نتطرق كذلك للمصطلح الذي استعمله المشرع الفرنسي و الجزائري .

---

[1] عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، جامعة عجمان للعلوم والتكنولوجيا، الإمارات، مجلد 22، العدد 213/86، ص259.

أولا: تعريف التفتيش التقليدي : بعيدا عن التفتيش في البيئة الإلكترونية ، يعرف الفقه[1] التفتيش التقليدي بأنه إجراء من إجراءات التحقيق الإبتدائي، فثمرته هي ضبط الأشياء المتعلقة بالجريمة ، و التي تفيد في كشف الحقيقة و التي قد تستمد منها أهم أدلة الجريمة اذ قد تكون أداة ارتكابها أو موضوعها أو متحصلاتها، فهدفه هو جمع الأدلة المادية على وقوع الجريمة و نسبتها إلى المتهم ، و على خلاف إجراءات التحقيق الأخرى التي هدفها جمع الأدلة المادية . كالخبرة و المعاينة فإن التفتيش يمس بحرمة الحياة الخاصة ، و حرمة المسكن لذلك نجد التشريعات تقرر إبطاله في حالة عدم مراعاة الضمانات و القيود المقررة لإجرائه .

ثانيا: رأي الفقه حول مصطلح التفتيش في البيئة الإلكترونية : يرى الفقه أن التفتيش في البيئة المعلوماتية الأجدر إخضاعه لأحكام خاصة تتلاءم و الطبيعة الخاصة للجريمة الإلكترونية والأدلة المتوصل إليها، إن التفتيش التقليدي يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، وغايته دوما الحصول على الدليل المادي وهذا يتنافى مع الطبيعة الغير مادية لبرامج و بيانات الحاسب الآلي و كذا شبكة الإنترنت فهي مجرد برامج و بيانات إلكترونية، ليس لها أي مظهر مادي محسوس في العالم الخارجي ، و رغم ذلك فإن الفقه والتشريعات التي صدرت في هذا المجال أجازت بأن يرد التفتيش على هذه البيانات غير المحسوسة المتواجدة على مستوى أنظمة الحوسبة وشبكات الإتصال و في الوسائط الإلكترونية كالأسطوانات والأقراص الممغنطة ومخرجات

---

[1] انظر ذلك : محمود نجيب حسني ، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات ، الجزء الأول دار النهضة العربية ، القاهرة،2013 ص 592 و احمد شوقي الشلقاني ، مبادئ الإجراءات الجزائية في التشريع الجزائري ، الجزء الاول ، ديوان المطبوعات الجزائرية ، الجزائر 1998 ص 240 ،2241،و مصطفى محمد موسى ، التحقيق في الجرائم الإلكترونية الطبعة الأولى دار التجهيزات الفنية ، القاهرة ،2009 ص 189 و على عدنان الفيل، إجراءات التحري و جمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية المكتب الجامعي الحديث الإسكندرية، 2012 ص 38.

الحاسب الآلي و عليه فهو يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط و أحكام .

كما أن المشرع الجزائري إستخدم في المادة الخامسة من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها مصطلح الدخول إلى منظومة معلوماتية بغرض التفتيش بمعنى أن الدخول هو التفتيش طبقا لأحكام قانون الإجراءات الجزائية و لكنه يكون على نظام المعالجة الآلية للمعطيات أو مستخرجاتها المحمولة على وسائط إلكترونية .

لم يعرف المشرع الجزائري إجراء التفتيش إلا انه أحاطه بجملة من الضوابط لما يترتب عنها مساس بحرية الأشخاص و حياتهم الخاصة و إنما عرف المنظومة المعلوماتية في المادة 02 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال [1] .

و بمعنى آخر هو الإطلاع على محل منحه القانون حماية خاصة بإعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسب الآلي أو أنظمة أو شبكة الإنترنت .

ثالثا: خصائص التفتيش الالكتروني : من خلال التعريف الذي وضعه الفقه للتفتيش على نظم المعلوماتية يتبين أنه يتميز عن غيره من الإجراءات التي تهدف إلى إثبات الجريمة كالشهود و الخبرة و المعاينة بعدة خصائص أهمها:

[1] المادة 02 من القانون رقم : 09-04 ، المرجع السابق .

- إن التفتيش في المنظومة المعلوماتية شأنه في ذلك شأن التفتيش يشكل عام فيه تعرض قانوني لحرية المتهم الشخصية أو لحرمة مسكنه بغير إرادته، و فيه إعتداء على أسراره و حياته
- يعتبر التفتيش وسيلة من وسائل التحري عن مختلف الأدلة المعنوية و المادية للجريمة ، يهدف إلى جمع الأدلة التي تؤدي إلى كشف الحقيقة و ضبطها و الوصول الى دليل حاسم .
- يعتبر التفتيش قيدا على حرمة و حصانة الشخص ، فهو إعتداء على أسراره[1] سواء الموجودة على مستوى نظامه المعلوماتي أو جهاز حاسوبه أو حتى بريده الإلكتروني و فيه مساس بقاعدة حرمة الشخص في حد ذاته أو في رسائله، ويترتب على كون التفتيش يتضمن مساسا بحق السر أنه يخرج عن نطاقه كل إجراء يمس شيئا مكشوفا ظاهرا للعيان فلا يعد تفتيشا .
- يسمح التفتيش أو البحث في الشبكات الإلكترونية عن الجرائم المعلوماتية بإستخدام قواعد و أساليب تخص بتقنيات خاصة فريدة و غير مسبوقة ، فهو يعكس التفتيش في معناه التقليدي لا يتطلب في كثير من الأحيان الانتقال الى مساكن الأشخاص الذين يشتبه أنهم ساهموا في ارتكاب الجريمة و إنما قد يتم عن بعد أو ما يعرف بالتفتيش على الخط perquisition en ligne كما تتطلب تحقيقها أن يكون متخصصا في التحقيق الجنائي و معالجة البيانات و المراجعات و الحسابات .

[1] رضا هميسي تفتيش المنظومات المعلوماتية في القانون الجزائري ، مجلة العلوم القانونية و السياسية ، جامعة ورقلة ، العدد5 ، سنة 2012ص 161.

- يتميز تفتيش المنظومات المعلوماتية أن المحتوى المعلوماتي يتميز بطابعه اللامادي و تجاوزه الحدود الوطنية و سهولة إتلافه أو مسحه و تغييره في أوقات قياسية فهو تفتيش للفضاء الإفتراضي و أوعية التخزين و للبيانات التي يحفظها جهاز الحاسوب .
- كما يتميز التفتيش في الفضاء الرقمي بأنه عملية معقدة و متشابكة تقتضي من القائمين عليها أن يكون على دراية واسعة و كفاءة عالية في البحث عن المعلومة وفي معالجة المعطيات و تحليلها .
- أن تفتيش الأنظمة المعلوماتية فيه مساس خطير بالحياة الخاصة ، كونه يتضمن وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية و فيه تسجيل و تجميع فوري لهذه الإتصالات و كذا القيام بعمليات التفتيش و الحجز داخل المنظومات المعلوماتية و لعل المثال الواضح الآثار التي يتركها متصفح الإنترنت ، و التي من خلالها يمكن تجميع كم هائل عن حياته الخاصة ، من خلال صفحات الويب التي أطلع عليها و وقت دخوله الى الشبكة و مدة بقائه فيها و الأشخاص الذين تواصل معهم .

رابعا: ضوابط التفتيش و السلطة المختصة به:

نجد ضوابط معينة يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات التي تمس حريتهم كالتفتيش و هدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم و بين حقوق الأفراد و حرياتهم و تنقسم الضوابط العامة للتفتيش إلى نوعين ، ضوابط موضوعية و شكلية :

ا. **الضوابط الموضوعية لتفتيش نظم الحاسوب** : يقصد بهذه الضوابط بصفة عامة الشروط اللازمة لإجراء تفتيش صحيح و هي في الغالب تكون سابقة له و يمكن حصرها في ثلاثة ضوابط أساسية : السبب ، المحل و السلطة المختصة للقيام به[1].

1) **وجود سبب للتفتيش في البيئة الإلكترونية** : سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل من أجل الوصول إلى حقيقة الحدث و يتمثل في وقوع جريمة ما جناية أو جنحة، إتهام شخص أو أشخاص معنيين بإرتكابها أو المشاركة فيها و توافر قرائن قوية على وجود أشياء تفيد في كشف الحقيقة لدى المشتبه فيه أو المتهم في مسكنه أو بشخص غيره و هو ما ينطبق على الجريمة الإلكترونية .

2) **محل التفتيش** : يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره ففي الجريمة التقليدية التفتيش ينصب على شخص المتهم أو غير المتهم و كذلك على مسكن المتهم و ما في حكمه و ملحقاته أو على مسكن غيره و ما في حكمه و ملحقاته لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية و كذلك شبكات الإتصال الخاصة به.

ولكي يتم التفتيش على هذه الحال ينبغي الإشارة الى أن هذه الأخيرة لا تكون قائمة بذاتها بل تكون إما موضوعة في مكان ما كالمسكن أو المكتب أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول او الهاتف النقال .

3) **الإذن بالتفتيش** : ينص المشرع الجزائري في المادة 44 من قانون الإجراءات الجزائية أنه إلا يمكن القيام بإجراء التفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو

[1] لندة بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، السنة 2017، ص491-490.

قاضي التحقيق، و قد إشترط المشرع وجوب إستظهاره قبل الدخول الى المسكن و الشروع في تفتيشه، كما أوجب أن يتضمن الإذن بيان وصف الجرم محل البحث عن الدليل و عنوان الأماكن المراد تفتيشها و الحجز عليها، أي أن يكون مسببا و الهدف من هذا الأخير هي توضيح الهدف من التفتيش و التحقق من مدى مشروعيته، ذلك أن الإذن حسب المادة 44 السالفة الذكر إذا لم يتضمن التسبيب يقع تحت طائلة البطلان إذ أن إشتراط المشرع للتسبيب يتيح للقضاء تقدير صحة الأمر بالتفتيش و تقرير بطلانه إذا ثبت ان الهدف منه غاية أخرى غير المحددة بالقانون و لا يشترط في التسبيب أن يكون مفصلا بل يكفي بيان الجرم بالإستناد الى الدلائل المستخلصة من طرف الضبطية القضائية في تحرياتها[1] .

أما المشرع الجزائري في القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة في قانون رقم 09-04 لا نجده يتحدث عن هذا الشرط كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق والسلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.

رابعا : السلطة المختصة بالتفتيش : بالرجوع الى نص المادة 4 [2]فقرة أ من القانون رقم 09-04 التي تبين كيفيات المراقبة للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في نفس المادة الفقرة الأخيرة إذ يختص النائب العام لدى مجلس قضاء الجزائر

---

[1] الهام بن خليفة التفتيش كإجراء تقليدي لجمع أدلة الجرائم المتصلة بالتكنولوجيا الإعلام و الاتصال ، جامعة الشهيد حمة لخضر ، الوادي دون سنة ص 36 .

[2] المادة 4 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.

بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، و مكافحتها المنصوص عليها بموجب المادة 13 من نفس القانون أذنا لمدة ستة أشهر قابلة للتجديد و ذلك على أساس طبيعة و نوعية الترتيبات التقنية المراد أخذها . فيما عدا هذه الحالة الخاصة و بموجب نص المادة 05 من القانون 09-04 التي تنص على انه : " يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عنها في المادة 04 أعلاه الدخول بغرض التفتيش ...." إذ يتعين الرجوع إلى التدابير التي نص عليها قانون الإجراءات الجزائية في مجال التحري و التفتيش بالنسبة للجرائم الالكترونية ،و بالضرورة في مجال الإختصاص بالنسبة لوكيل الجمهورية و قاضي التحقيق الذي يحدده المرسوم التنفيذي رقم : 06-348 المؤرخ في :2006/10/05 و المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق و باعتبارهما أيضا الجهة المؤهلة بمنح الإذن بالتفتيش وفقا للشروط المنصوص عنها بموجب نص المادة 44 من قانون الإجراءات جزائية بتمديد الإختصاص لكل من وكيل الجمهورية و قاضي التحقيق في جرائم معينة من بينها الجرائم الماسة بالمعالجة الآلية للمعطيات .

و عليه يمكن القول أن المشرع الجزائري حدد بوضوح الجهة القضائية المختصة سواء في مجال الإذن بوضع ترتيبات للمراقبة الإلكترونية للحيلولة دون الإعتداء على منظومة معلوماتية أو في مجال الدخول بغرض التفتيش و لو عن بعد لمنظومة معلوماتية او جزء منها او منظومة تخزين معلوماتية سواء تقع داخل الإقليم الوطني او خارجه فكيف يتم ذلك ؟

خامسا: تمديد التفتيش الى منظومة معلوماتية أو جزء منها : نظرا لخطورة هذه الجريمة المستحدثة و بقصد ملاحقة المجرم المعلوماتي نص المشرع على تمديد إجراء التفتيش سواء داخل الإقليم الوطني أو خارجه سنوضح هذا فيما يأتي :

I. تمديد التفتيش داخل الإقليم الوطني :

أدى سوء إستخدام الفضاء السيبراني[1] إلى بروز جرائم مستحدثة تسمى بالجرائم المعلوماتية إذ يمكن للمجرم الدخول و الإنتقال من منظومة معلوماتية لأخرى بما يسمح له بتغيير أو تدمير المعطيات ناهيك عن صعوبة تتبعه و إيجاد دليل ضده لذا نص المشرع الجزائري في المادة 5 من القانون 09-04 على انه " يجوز للسلطات القضائية المختصة ....الدخول بغرض التفتيش و لو عن بعد الى :

1- منظومة معلوماتية أو جزء منها و كذا المعطيات المخزنة فيها .

2- منظومة تخزين معلوماتية .

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة اذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها عن طريق المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطات القضائية المختصة مسبقا "فتمديد التفتيش إلى منظومة معلوماتية أخرى ، مشكوك فيها يتطلب إجراءات خاصة فهو يتم عن بعد و بشكل سريع تماشيا مع السرعة الهائلة في نقل المعلومات و أيضا متى توفر الشك

[1] يقصد بالفضاء السيبيراني : العوالم الافتراضية التي تنقلها الشبكات المعلوماتية ، انظر حسين بن سعيد الغافري المرجع السابق السياسة الجنائية في مواجهة جرائم الانترنت ، دار النهضة العربية ، القاهرة 2009، ص 14.

في وجود معطيات مبحوث عنها مخزنة في منظومة معلوماتية أخرى، و لكن يتم الوصول اليها عن طريق الدخول من منظومة معلوماتية أولى.

في هذا الصدد تنص المادة 5 الفقرة الأخيرة من القانون 09-04 السالفة الذكر على أنه يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

II. **تمديد التفتيش خارج الإقليم الوطني** : في هذا الصدد نصت المادة 15 من القانون 09-04 على أنه زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال المرتكبة خارج الإقليم الوطني عندا يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني .

و بذلك أقر المشرع إجراءات صارمة لملاحقة هذا النوع من الجرائم خارج الإقليم الوطني و ذلك حينما وسع من نطاق التفتيش بموجب نص المادة 05 الفقرة 04 من القانون 09-04 :...." إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل "،غير أن المشرع الجزائري لم يترك الأمر

على إطلاقه و نظرا لمقتضيات تتعلق بالسيادة الوطنية وضع شروطا و قيودا للمساعدة القضائية في مجال مكافحة هذا النوع من الجرائم المستحدثة .

الفرع الثاني : شروط تفتيش الجرائم المعلوماتية : يمكن تقسيم شروط تفتيش نظم الحاسبة الالكترونية الى نوعين موضوعية و شكلية .

وأن هذه الضوابط أو الشروط الشكلية لا تهدف الى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب بل تقيم سياجا يحمي الحقوق و الحريات الفردية و تتمثل هذه الضوابط الشكلية في[1] :

أولا : إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون :

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية وذلك لضمان الإطمئنان على سلامة الإجراء بإعتبار أن التفتيش فيه إطلاع على أسرار الغير، فبالنسبة لتفتيش الأشخاص لم تشترط التشريعات الإجرائية لصحته حضور الشهود أما فيما يتعلق بتفتيش المساكن، ينص القانون الجزائري على وجوب حصول إجراء التفتيش المتعلق بحضور المشتبه فيه أو المتهم عندما يتم تفتيش مسكنه سواء من طرف قاضي التحقيق أو ضابط الشرطة القضائية و إذا تعذر ذلك بامتناعه عن حضور التفتيش او كان هاربا يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة القائم بالتفتيش[2] .

---

[1] لندة بن طالب، المرجع السابق، ص493.

[2] المادة 45 من الأمر 66-155 المؤرخ في 8 يونيو 1966 يتضمن قانون الاجراءات الجزائية المتمم بالأمر رقم 11-02 المؤرخ في 23 فبراير 2011، الجريدة الرسمية، العدد 2012-2011.

و يلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم 06-22 من المادة 45 منه حيث إستغنى على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و الحكمة من ذلك ترجع الى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني خاصة و أن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله و التلاعب فيه حتى عن بعد . كما أن هذه الضمانة بدأت تتضاءل أهميتها على الدول التي تؤخذ بنظام التفتيش عن بعد أو ما يطلق عليه الفقه الفرنسي " التفتيش على المباشر perquisition en ligne"

ثانيا : الميعاد الزمني لإجراء التفتيش في الجرائم المعلوماتية :

يقصد بشرط الميعاد الزمني في التفتيش، أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع، وذلك حرصا على تضييق الإعتداء على الحرية الفردية و حرمة المسكن. إن القانون الجزائري يحظر تفتيش المنازل و ما في حكمها في وقت معين و هو محدد في القانون الإجراءات الجزائية من خلال المادة 47 من الساعة الخامسة صباحا الى الساعة الثامنة مساءا .

و هناك حالات استثنائية يجوز فيها الخروج عن هذه المواعيد و يصبح إجراء التفتيش في أي ساعة من ساعات الليل و النهار و تتمثل في :

- رضا صريح من صاحب المنزل
- حالة النداءات من داخل المنزل

- التحقيق في جميع الجرائم المعاقب عليها في المواد 342 إلى 348 من قانون العقوبات .

وأن المشرع الجزائري قد أورد في قانون الإجراءات الجزائية المادة 3/64 " أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 3/47 من هذا القانون تطبق الأحكام الواردة في تلك المادة و كذا أحكام المادة 47 مكرر حيث أجاز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناءا على إذن مسبق من وكيل الجمهورية المختص "، وجاء في نص المادة 3/47 من قانون الإجراءات الجزائية حيث إستثنى تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في هذه المادة من بينها الجرائم الماسة بأنظمة المعالجة الآلية المعطيات. والملاحظ المشرع غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن بإعتباره مستودع أسرارهم،إلا أن ما يبرره و يقل من خطورته الطبيعة الخاصة لهذه الجرائم خاصة الجريمة الالكترونية و طبيعة الدليل لإثباتها فهو قابل للمحو و التعديل في أقل من ثانية لأن مرتكبها ذو دراية بالأمور التقنية ، و ما يزيد من الصعوبة إذا كان هذا الدليل الإلكتروني هو الوحيد في الدعوى الجنائية ، أما بالنسبة للأماكن العامة، فإذا وجد الشخص و هو يحمل معه مكونات الحاسوب في هذه الأماكن السالفة الذكر أو كان مسيطرا عليها أو حائزا لها فان تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص و بنفس الضمانات و القيود المنصوص عليها في هذا المجال .

ثالثا : محضر التفتيش في الجرائم المعلوماتية :

لأن التفتيش يعتبر من أعمال التحقيق ، فيستدعي ذلك إفراغه في محضر يثبت فيه ما أنجز التفتيش عنه من أدلة، والقانون لم يتطلب شكلا محددا ، و بالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجبه القواعد العامة في المحاضر عموما،بأن يكون مكتوبا بالغة الرسمية و أن يكون مؤرخا و موقعا عليه، كما يجب ان يتضمن كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب و الإنترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية .

رابعا: الشروط الموضوعية للتفتيش : و تلخص هذه القواعد كالتالي : [1]

- وقوع جريمة إلكترونية .
- ارتكاب شخص او أشخاص معنيين لإحدى الجرائم الالكترونية او الاشتراك فيها .
- توافر أدلة قوية و قرائن على وجود أشياء او أجهزة أو معدات معلوماتية أو الكترونية تفيد في الكشف عن الحقيقة .

ـ أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية و المعنوية و شبكات الاتصال الخاص به.

الفرع الثالث: الطبيعة القانونية للتفتيش :

للجرائم الالكترونية إجراءات تفتيش خاصة و ذلك لخصوصية هذه الجرائم التي تمتاز بسرعة ارتكابها و تدمير أدلتها، حيث أنها تمتاز عن غيرها من الجرائم الأخرى و تحتاج لعدة مراحل لتنفيذها .

---

[1] عبد الفتاح البيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت ، الطبعة الأولى، دار الفكر الجامعي 2006 ص 386، 385.

إن وسائل تكنولوجيا المعلومات ، تتكون من وسائل كهرومغناطيسية بصرية كهر وكيميائية ، مادية و غير مادية ، و كلمة كهرومغناطيسي تشمل كل نظام لتلقي الإشارات بواسطة الأسلاك الكهربائية و الموجات اللاسلكية و كل مصدر آخر للطاقة و هذه الإجراءات بالغة الصعوبة ، كون أن وسائل التكنولوجيا المعلومات تتكون من مجموعة وسائل مترابطة و غير مترابطة ، تستعمل لتخزين المعلومات و ترتيبها و تنظيمها و إسترجاعها و معالجتها و تبادلها ، و تشمل جميع المداخل و المخارج المرتبطة بها سلكيا أو لاسلكيا، وهذه مميزات خاصة بالتقنية الحديثة، يحتاج تفتيشها إضافة إلى أشخاص متخصصين بالتعامل مع مكوناتها إلى وسائل تقنية حديثة .

أولا: آلية التفتيش في الجرائم الإلكترونية :

إن السلطة القائمة بالتفتيش في الجرائم الالكترونية تضع إلية للتفتيش بعد حصولها على المعلومات الضرورية و اللازمة والتي من خلالها حددت وسائل تكنولوجيا المعلومات التي ارتكبت بواسطتها الجريمة الإلكترونية ، سواء كانت تلك الوسائل بحوزة أشخاص ، او داخل الأماكن .

إن التفتيش في الجرائم الإلكترونية تحتاج إلى فريق متكامل يكون له دور في نجاح التفتيش و الحصول على الأدلة[1] ، ويكون بعدد كافي من الأشخاص المتخصصين في وسائل تكنولوجيا المعلومات ، ويكون تشكيله ملائم مع طبيعة الجرائم الإلكترونية، و تحديدا لمكافحة سرعة تدمير الأدلة الالكترونية و التخلص منها .

[1] ابراهيم راسخ، التحقيق الجنائي العلمي، أكاديمية شرطة دبي، الإمارات العربية المتحدة، الطبعة الأولى، 191، ص292،393.

إن إجراءات التفتيش في الجرائم الإلكترونية لا يمكن لشخص واحد القيام بها ، بل بحاجة الى تعاون عدة أشخاص لضمان نجاحه ، كون إجراءات التفتيش بحاجة الى أشخاص فنيين متخصصين في تفتيش وسائل تكنولوجيا المعلومات يسانده فريق امني متخصص بفرض السيطرة الأمنية على المكان المراد تفتيشه لضبط مداخله و مخارجه .

ثانيا: الإجراءات الفنية للتفتيش في الجرائم الإلكترونية: التفتيش التقليدي هو يهدف إلى البحث عن البحث الأشياء المادية المتعلقة بالجريمة وتفيد في كشف الحقيقة ، و لكن التفتيش في الجرائم الالكترونية يهدف للبحث عن أشياء مادية و معنوية لوسائل تكنولوجيا المعلومات ، كون أن الأدلة الالكترونية تحفظ و تخزن داخل تلك الوسائل ، لذلك سنتناول تفتيش مكونات وسائل تكنولوجيا المعلومات .

ا. **تفتيش مكونات وسائل تكنولوجيا المعلومات** : تفتيش مكونات وسائل تكنولوجيا المعلومات يحتاج إلى أشخاص ذوي خبرة كونها تتكون من مكونات مادية و أخرى غير مادية ، إجراء تفتيش على مكونات وسائل تكنولوجيا المعلومات، يخضع لصفة مكان وجودها، سواء بحوزة الأشخاص أو داخل الأماكن سواء كانت منعزلة، أو متصلة بأجهزة أخرى عن طريق شبكات الخاصة أو العامة، داخل الدولة او خارجها ، لذلك سنبحث بتفتيش المكونات المادية بوسائل تكنولوجيا المعلومات أولا ، و تفتيش المكونات المعنوية ثانيا .

1- تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات : يهدف تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات التي هي عبارة عن المواد التي توجد بمكان

الحادث أو الصلة به إلى البحث عن شيء يتصل بجريمة إلكترونية وقعت ويفيد بكشف الحقيقة عنها وعن مرتكبيها .

إن تفتيش المكونات المادية لوسائل تكنولوجيا المعلومات لا يثير أي مشكلة قانونية طالما تمت وفق الإجراءات القانونية وتطبق عليها القواعد التقليدية للتفتيش[1] و لكن مكان وجودها له أهمية، حيث يتوقف تفتيشها على طبيعة المكان الموجودة فيه ، فإذا كانت بحيازة الشخص فإنها تخضع لقواعد لتفتيش الأشخاص ، وإذا كانت موجودة في مكان فان تفتيشها يخضع لقواعد تفتيش الأماكن بنفس الضمانات و الشروط .

2) تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات : إن تفتيش المكونات الغير مادية لوسائل تكنولوجيا المعلومات ، يثير صعوبات و مشاكل قانونية نظرا لطبيعتها الغير ملموسة ، ونظرا لخصوصيتها وطرق تخزينها وأماكن وجودها.فالمشرع الفرنسي أضاف كلمة المعطيات المعلوماتية الى أشياء الواردة بالنص لتشمل المكونات الغير مادية لوسائل تكنولوجيا المعلومات .

المطلب الثاني : الضبط و الخبرة القضائية في الجرائم المعلوماتية :

إن الحديث عن مسالة الضبط و الخبرة القضائية في الجرائم المعلوماتية يقودنا الى ابرازها وفق التسلسل المنطقي التالي :

[1] هلالي عبد الله احمد ، تفتيش نظم الحاسب الالي و ضمانات المتهم المعلوماتي ، دراسة مقارنة ، الطبعة الثانية ، دون ناشر ، 2008 ص 73 .

الفرع الأول : الضبط في الجرائم المعلوماتية :

الضبط يعني وضع اليد على شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة و عن مرتكبيها ، والهدف الذي تسعى إليه السلطة التحقيق من القيام بالتفتيش، و هو ضبط الأدلة و الوثائق و الأشياء التي تفيد في كشف الجريمة و إماطة اللثام عن غموضها و تحقيق العدالة و لذلك ينبغي التقييد بالقواعد الإجرائية التي تحدد الأماكن التي يجوز تفتيشها أو الأشخاص الذين يجري تفتيشهم و ينصب الضبط عن الأشياء المادية و الأشياء الغير المادية كما هو الحال في مراقبة المحادثات الهاتفية و تسجيل المحادثات الخاصة و على ما هو مخزن في أجهزة الحاسوب أو مخزن على أقراص أو على الدعامات الأخرى، و نظرا لكون الضبط محله في مجال الجرائم المعلوماتية ، البيانات المعالجة إلكترونيا فقد ثار التساؤل هل يصلح هذا النوع من البيانات لأن يكون محل للضبط الذي يعني كما رأينا وضع اليد على الشيء المادي الملموس ؟

إنقسم الفقه إلى إتجاهين عن الإجابة على هذا التساؤل . يرى البعض أن بيانات الحاسوب لا تصلح لان تكون محل للضبط لانتفاء الكيان المادي عنها ، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس و يستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة .

و يرى الإتجاه الثاني ان البيانات المعالجة الكترونيا ما هي إلا ذبذبات الكترونية أو موجات كهرومغنطسية تقبل التسجيل و الحفظ و التخزين على وسائل مادية و بإمكان نقلها و بثها و إعادة إنتاجها فوجودها المادي لا يمكن إنكاره .

و عملية ضبط البيانات المعالجة إلكترونيا تواجهها عدة صعوبات:

- وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهات الشرطة و التحقيق في عملية التفتيش و الضبط و التحفظ .

- يمثل التفتيش و الضبط أحيانا إعتداء على حقوق الغير ، أو على حرمة حياته الخاصة فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق و الحريات و لقد سبق القول أن أجهزة الحاسوب و مخرجاتها و المعدات التي تستعملها شبكة الانترنت ، و الأقراص المدمجة و الدعامات الأخرى المخزنة عليها البيانات و المعلومات تصلح لتفتيشها و ضبطها لأنها أشياء مادية تحتوي على برامج و بيانات و معلومات مخزنة عليها و الأشياء التي يمكن ضبطها بالحاسوب أو الأشياء المرتبطة به تتحصر فيما يلي :

أولا: جهاز الحاسوب ، المكون من الشاشة و لوحة المفاتيح ، و الفارة و غيرها من المعدات .

ثانيا : قرص التخزين الثابت و أقراص الليزر و الأقراص المرنة .

ثالثا : الأشرطة الممغنطة .

رابعا :الاوراق التي تم طباعتها و المحفوظة في الملفات .

الفرع الثاني : الخبرة القضائية في الجرائم المعلوماتية :

أصبحت الاستعانة بالخبرة القضائية في فحص الأدلة و تحليلها أمرا ملحا لإثبات الجرائم المعلوماتية اذ لا يعقل ان يفصل القاضي في قضايا تقنية المعلومات دون إستناده إلى أراء الخبراء الفنيين في هذا المجال و على هذا الأساس نحاول معرفة المقصود بالخبرة القضائية و بيان أهميتها في إثبات الجرائم المعلوماتية .

أولا: تعريف الخبرة القضائية : تعتبر الخبرة القضائية عموما وسيلة قررها المشرع لمساعدة القاضي في تقدير المسائل التي يحتاج إثباتها إلى معرفة فنية خاصة و لهذا فان الخبرة تفترض وجود واقعة مادية أو شيئا يصدر الخبير حكمه فيه وذلك عن طريق التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية فهي حقيقتها ليست دليلا مستقلا عن الدليل القولي او المادي ، و إنما هي تقييم في هذه الادلة [1] و تعرف الخبرة على انها تنقيب و بحث يرتبط بمادة تتطلب معارف علمية او فنية خاصة لا تتوافر سوى لدى المحقق او القاضي . كما عرفها جانب من الفقه المقارن على أنها "الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال اثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها الى معرفة فنية أو دراية علمية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله و ثقافته ".

و من المتفق عليه أن للخبرة أهمية بالغة في إثبات الجرائم بأنواعها لأنها تدير الدرب لسلطات التحقيق و القضاء للوصول الى الحقيقة و تحقيق العدالة الجنائية ، لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في مواد من 143 الى 156 من قانون الاجراءات الجزائية و التي أجازت لجهات التحقيق و الحكم تعيين خبراء في المسائل التي تستدعي ذلك إذ تنص المادة 143 من قانون الاجراءات الجزائية "لجهات التحقيق أو الحكم عندما تعرض لها مسالة ذات طابع فني أن تأمر بندب خبير إما بناءا على طلب النيابة العامة أو من تلقاء نفسها أو الخصوم "[2] .

---

[1] خالد ممدوح ابراهيم ، في التحقيق الجنائي في الجرائم المعلوماتية المرجع السابق صفحة 283.

[2] ينظر المادة 143 من قانون الإجراءات الجزائية .

كما قام بتعزيز قدرات النيابة العامة في معالجة قضايا ذات طابع تقني و ذلك باستحداث وظيفة المساعدين المتخصصين الدائمين بموجب المادة 35 مكرر من الأمر 15-02 المعدل و المتمم من قانون الإجراءات الجزائية حيث يكون هؤلاء المساعدين تحت تصرف النيابة العامة بشكل دائم للإستعانة لآرائهم و خبرتهم في مختلف المسائل الفنية أثناء التحريات الأولية .

و لم يتخلف المشرع عن هذه التشريعات، إذ لم يكتفي بهذه النصوص التقليدية و نظم أعمال الخبرة في بعض النصوص الخاصة مثلما جاء في المادة 5 من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها [1] إذ سمح للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث و التحري لمساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهامها ولعل إستخدام المشرع هنا لعبارة اي شخص له دراية أمر مقصود حتى يوسع من دائرة المساعدة القضائية في مجال مكافحة الجرائم الالكترونية لتشمل الى جانب الخبير ، جميع المتخصصين و العاملين في مجال التكنولوجيا الإعلام و الإتصال مثل مهندس الإعلام الآلي و مزودي خدمات الإنترنت و غيرها .

ثانيا: الضوابط القانونية و الفنية التي تحكم الخبرة القضائية : بإعتبار الخبرة القضائية إجراء من إجراءات التحقيق و الإثبات الجنائي تم إخضاعها لمجموعة من الضوابط القانونية التي تعتبر كضمانات هامة تساعد في إنجاز أعمال الخبرة و تضمن مشروعية

[1] ينظر المادة 5 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها المشار إليها سابقا.

الحصول على الدليل الإلكتروني و حجيته في إثبات الجرائم الإلكترونية تتمثل هذه الضوابط فيما يلي :

- إختيار الخبير من جدول الخبراء الأصل أن يختار الخبراء حسب التخصص من الجداول التي تعدها المجالس القضائية بعد إستطلاع رأي النيابة العامة و لكن كإستثناء في حالة ما لم يتضمن جدول الخبراء المتخصصين في مجال الخبرة فإنه يجوز لجهات التحقيق إختيار الخبراء ليسوا مقيدون في هذا الجدول و هذا ما نص عليه المشرع الفرنسي بموجب الفقرة الثانية من المادة 157 قانون الإجراءات الجزائية التي أجازت استثناء و بقرار مسببا للمحكمة ان تختار خبراء ليسوا من هذه الجداول ، و هو ما أكده المشرع الجزائري في المادة 144 من قانون الإجراءات الجزائية [1] وتبقى كيفية اختيار الخبير في المسالة مطروحة أمرا متروكا لجهات التحقيق ، و لعل المشرع الجزائري أجاز للقضاة الاستعانة بجهات مماثلة عن طريق الهيئة الوطنية للوقاية من الجرائم الالكترونية كما اشرنا سابقا . إذ تتولى الخبرات القضائية لمساعدة السلطات القضائية و تبادلها مع العديد من الدول في اطار التعاون و المساعدة القضائية .

[1] تنص المادة 144 من قانون الإجراءات الجزائية على " يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع النيابة العامة اما بالنسبة للمشرع المصري فلم يعد يعمل بنظام الجداول و ذلك بعد ان قفل المرسوم رقم 96 لسنة 1952 الخاص بتنظيم الخبرة لدى جهات القضاء هذه الجداول ، ليقوم بأعمال الخبرة امام جهات القضاء حسب المادة الثانية من هذا المرسوم خبراء وزارة العدل و مصلحة الطب الشرعي و المصالح الأخرى التي يعهد اليها بأعمال الخبرة ، وكل ما ترى جهات القضاء ضرورة الاستعانة برأيهم الفني من غير ما ذكروا لمزيد من التفاصيل ينظر الدكتورة بوكر رشيدة، الحماية الجزائية للتعاملات الالكترونية ، المرجع السابق ، ص 384 و ما بعدها .

خلاصة الفصل الثاني :

على ضوء دراستنا في هذا الفصل يعد التفتيش في الجريمة المعلوماتية التي أقرها المشرع الجزائري من أصعب إجراءات البحث و التحري الأمر الذي يتطلب خبرة واسعة و كفاءة عالية وقد أخضعها لمجموعة من الضوابط الموضوعية و الشكلية المقررة في قانون الإجراءات الجزائية إلا أنه نظرا لطبيعتها و خصوصية الجريمة المعلوماتية فإنه أورد بشأنها بعض الإستثناءات التي تشكل خروجا عن القواعد المألوفة في التفتيش التقليدي تترتب عدم مراعاة هذه الضوابط بطلان إجراء التفتيش عملا بمبدأ الشرعية الجزائية، و التفتيش في الجرائم المعلوماتية من أدق و أخطر إجراءات التحقيق كونه يمس خصوصية الناس بالإطلاع على أسرارهم المخزنة في وسائل تكنولوجيا المعلومات و بحاجة إلى أشخاص مؤهلين و مدربين تدريبا قانونيا و فنيا للتعامل مع وسائل تكنولوجيا المعلومات و التغلب على التحديات الفنية التي يمتاز بها .

خاتمة

خاتمة :

بعدما فرغنا بحمد الله وتوفيقه من دراسة موضوعنا المتمثل في إجراءات البحث والتحقيق في الجريمة المعلوماتية والذي حصرناه في مرحلة البحث والتحقيق عن الجريمة الإلكترونية تعرضنا لمجموعة من الإشكالات العديدة التي طرحتها المواجهة الإجرائية لهذا النوع من الجرائم وخلصنا في الأخير لمجموعة من النتائج التي تعتبر إجابة عن هذه التساؤلات المطروحة سابقا ، تتمثل أهم هذه النتائج في :

1) – إن التقنية المعلوماتية أصبحت من أساسيات حياة الدول والشعوب ولا يمكن تصور فكرة التخلي عنها ، نظرا لتزايد مجالات إستعمالاتها في كافة المجالات وذلك بالرغم من كافة التهديدات التي تشكلها الجريمة المعلوماتية على أمن وسلامة نظمها ومستعمليها

2) – يستحيل القضاء على الظاهرة الإجرامية المعلوماتية بشكل نهائي وذلك لإتصالها المباشر بتقنية المعلوماتية ، ففكرة التخلي عن هذه التقنية هي الحل الوحيد لمشروع القضاء على الجريمة المعلوماتية وذلك بالرغم من درجة التطور التي اليها المنظومة القانونية العقابية منها والإجرائية في مجال مكافحة الجريمة المعلوماتية .

3) – إن إجراءات البحث التحري والتحقيق المعلوماتي هي إجراءات من نوع خاص يشترط لمباشرتها التقيد بمجموعة من الشروط أهمها شرط التقيد بالنص الإجرائي الملائم ، لما قد تنطوي عليه هذه الاجراءات من مساس بالحريات الفردية وإطلاع على مستودع أسرار الأفراد كالتصنت الإلكتروني وإعتراض البريد الإلكتروني

وحجز المعطيات و البيانات الشخصية وكل ذلك حفاظا على سلامة الإجراءات من طائلة البطلان وكذلك حفاظا على حريات الأفراد وكرامتهم

4) – يقترن نجاح إجراءات البحث والتحقيق في الجرائم المعلوماتية بمدى براعة وفعالية وجاهزية الجهات المختصة بمباشرة الاجراءات لتتبع الأدلة الإلكترونية ، وتحصيلها وحفظها بغرض عرضها على الجهات المختصة بتقديرها ذلك لأن الدليل الإلكتروني هو دليل من نوع خاص لا يشترك مع باقي الأدلة الجنائية في أي صفة مميزة فهو ذو طبيعة رقمية غير مادية .

بناءا على النتائج المسجلة نقدم المقترحات التالية :

1) – ضرورة العمل على تحسين ضحايا الجرائم المعلوماتية بضرورة التبليغ عن أي جريمة معلوماتية ، قد يقعون ضحايا لها وذلك من أجل السماح للجهات المكلفة بالبحث والتحقيق بالإطلاع على مدى جسامة وحقيقة الجريمة المعلوماتية ، إضافة إلى لإطلاع على كافة الأساليب الإجرامية المستعملة في مجال الجريمة المعلوماتية والتي يمكن أن تبقى محل خفاء في حال عدم تبليغ الضحايا عن الجرائم المعلوماتية التي تستهدفهم

2) – تعزيز عمل الجهات الأمنية والقضائية في مجال مكافحة الجرائم المعلوماتية ، وذلك من خلال حسن تدريب الكفاءات العاملة على طبيعة الإجراءات المتخذة في مجال الجرائم المعلوماتية ومدى خصوصية هذا النوع من الجرائم والمجرمين في أن واحد ، اضافة الى تعزيزهم بأحدث الوسائل التكنولوجية في مجال

المعلوماتية من حواسيب وبرامج معلوماتية ، تسمح لها بتأدية مهامهم على أكمل وجه

3) – وضع سجل أمني إلكتروني يتضمن قائمة بمجرمي المعلوماتية يسمح بوضعهم تحت المراقبة الأمنية أي رصد نشاطاتهم المشبوهة عبر الشبكة والتي تنذر بوقوع جريمة معلوماتية .

4) – تعديل قانون الإجراءات الجزائية على وجه الإستعجال من خلال إدراج قسم بأعمال البحث والتحقيق في الجرائم المعلوماتية ، وذلك من خلال إفراد نص نصوص قانونية خاصة بالإجراءات الجزائية المتبعة خلال مرحلة البحث والتحري وكذلك التحقيق بشكل مفصل وواضح بسن قواعد الإختصاص النوعي والمحلي بدقة ووضوح ، إضافة إلى طبيعة الاجراءات المتخذة في هذا الشأن وذلك للقضاء على كل لبس قد ينشأ جراء المزج بين النصوص العامة والخاصة .

5) – إذن كانت جملة من المقترحات التي يرى الباحث بضرورة تبنيها وتجسيدها على أرض الواقع من اجل الوصول الى ضمان فعالية قصوى في عمل الجهات المختصة بالبحث والتحقيق في الجرائم المعلوماتية وبالتالي تجسيد السياسة الهادفة على تأمين فضاء المعلوماتية ومكافحة الجرائم المعلوماتية .

الملخص :

تطرح الجريمة العديد من المشاكل من ناحية القانون الاجرائي ، إذ يصعب على المحققين إجراء تحقيق وجمع الأدلة الرقمية بإتباع الإجراءات التقليدية ، كالمعاينة التفتيش ، الضبط ..... الخ في هذا السياق ورغبة منعا في مكافحة فعالة للجريمة المعلوماتية ، تبنت الجزائر أساليب جديدة للتحري ، من خلال تعديل قانون العقوبات بموجب القانون رقم 06-22 بتاريخ 2006/12/20. عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، وفي 2009 أصدر المشرع الجزائري القانون رقم 09-04 المؤرخ في 2009/08/05 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها ، في هذا القانون خلق المشرع أليات جديدة خاصة للتحري من أجل مكافحة الجريمة المعلوماتية ، إلا أن هذه الأساليب الحديثة أثارت مشكلة مدى مشروعيتها ، خاصة وأنها تمس بالحقوق والحريات الأساسية للفرد والمعترف بها في الإتفاقيات الدولية ولحل هذا الإشكال فقد وضعت شروط وضمانات يقتضي على السلطات القضائية مراعاتها عند الإذن بهذه الأساليب .

<u>الكلمات المفتاحية:</u>

01- جريمة إلكترونية.

02- تفتيش إلكتروني.

03- مراقبة إلكترونية.

04- إتصالات إلكترونية.

Summary

The crime poses many problems in terms of procedural law, as it is difficult for investigators to conduct an investigation and collect digital evidence following traditional procedures, such as inspection, inspection, seizure ..... In this context and in order to prevent an effective fight against cybercrime, Algeria has adopted new methods of Investigation, through the amendment of the Penal Code by Law No. 22-06 of 20/12/2006. In 2009, the Algerian legislature issued Law No. 04-09 dated 05/08/2009, by adding new procedures applied to crimes of infringement of Automated Data Processing Systems. The law contains special rules for the prevention and Combating of crimes related to information and Communication Technology. in this law, the legislator has created special good investigative mechanisms to Combat Information crime. however, these modern methods have raised the problem of their legality, especially since they affect the fundamental rights and freedoms of the individual recognized in international conventions .to solve this problem, conditions and guarantees have been established that judicial authorities are required to take into account when authorizing these methods.

Key words :

01) Electronic Crime .

02) electronic inspection

03) electronic monitoring.

04) Electronic Communications.

الكتب والمراجع:

1. إبراهيم راسخ، التحقيق الجنائي العلمي، أكاديمية شرطة دبي، الإمارات العربية المتحدة، الطبعة الأولى، ص393، 392.
2. أحسن بوسقيعة، التحقيق القضائي، ط2، الديوان الوطني للأشغال التربوية، الجزائر 2002.
3. إلهام بن خليفة، التفتيش كإجراء تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، جامعة الشهيد حصة لخضر، الوادي دون سنة.
4. بن بدة عن الحليم، المراقبة الإلكترونية كالإجراء لأشخاص الدليل الإلكتروني بين الخصوصية ومشروعية الدليل الإلكتروني المجلة الأكاديمية، البحث القانوني المجلد 1 العدد 2019/3.
5. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة 2009، ص14.
6. خالد ممدوح ابراهيم، الدليل الإلكتروني في جرائم المعلوماتية، بحث منشور على موقع كلية الحقوق لجامعة المنصورة على شبكة الإنترنت.
7. رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياحة، جامعة ورقلة العدد 5 سنة 2012 ص161 .
8. سامية بلجراف، سلطة القاضي في قبول وتقدير الدليل الرقمي، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-17 نوفمبر 2015، كلية الحقوق جامعة بسكرة الجزائر.
9. ضياء علي أحمد النعمات، مرجع سابق، ص364

10. عادل عبد الله خميس المهري ، التفتيش في الجرائم المعلوماتية جامعة عجمان للعلوم والتكنولوجيا الإمارات المجلد 22- العدد 86/ 2013ص 259.

11. عبد الحميد عبد المطلب، بحث وتحقيق الجرائم على الكمبيوتر، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية العمليات الإلكترونية.

12. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال البحث والتحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة ضوء القواعد العامة للإجراءات الجنائية.

13. علي حسن أحمد الطوالية، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي، بحث منشور على الموقع الالكتروني لمركز الإعلام الأمني، أكاديمية الشرطة البحرينية –البحرين- أفريل 2011- ص2.

14. علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ورقة عمل المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 2003.

15. عمر يونس، جرائم الكمبيوتر والأنترنت.

16. ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، سنة 2017، ص 490-491.

17. محمد فاروق عبد الحميد، القواعد الفنية للشرطة للتحقيق والبحث الجنائي، أكاديمية نايف العربية للعلوم الأمنية الرياض 1999.

18. محمد محمد – عنب استخدام التكنولوجيا الحديثة – في الاثبات الجنائي –دون ذكر الله دار النشر – مصر 2007.

19. محمود نجيب حسني، شرح قانون الإجراءات الجزائية وفقا لأحداث التعديلات، الجزء الأول، دار النهضة العربية القاهرة، 2013، ص592.
20. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنات، دار الكتب القانونية، مصر-2006، ص88.
21. هلالي عبد الله أحمد، تقنين نظم الحاسب الآلي وضمنات المتهم المعلوماتي، دراسة مقارنة الطبعة الثانية دون ناشر 2008.

الرسائل العلمية:

1. سليمان بن مهجع الفنرزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض 2003.
2. سيدهم سيدي محمد، محاضرة حول التسرب حسب تعديل قانون إ ج الجزائية محكمة فرندة مجلس قضاء تيارت.
3. عمر أبو بكر يونس، الجرائم الناشئة عن الانترنت، رسالة دكتوراه جامعة عين شمس 2000، ص825.
4. معتوق عبد اللطيف، الإطار لمكافحة جرائم المعلوماتية في التشريع والتشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية قسم الحقوق 2011-2012.

القوانين:

- القانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها المنشور في الجريدة الرسمية الجزائرية الديمقراطية الشعبية رقم 47 الصادرة بتاريخ 2009/08/16.
- اتفاقية بودابست لمكافحة الجرائم المعلوماتية المنبثقة عن إجتماع المجلس الأوربي ببوداست المجرمة رقم 85 /1 يناير 2001/11/21.

ب – الأوامر :

1. الأمر رقم 66-155 المؤرخ في 18 صفر 1386 الموافق ل 8 جوان 1966 المتضمن قانون الإجراءات الجزائية الجزائري المنشور في الجريدة الرسمية للجمهورية الجزائرية العدد رقم 4 الصادرة 1966/06/10.

2. الأمر رقم 15-02 المؤرخ 2015/07/23 المتضمن تعديل أحكام قانون الاجراءات الجزائية المنشور في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية رقم 40 الصادرة بتاريخ 2015/07/23.

مراجع باللغة الأجنبية :

A- Arabiat 2000 on line available at www araiad .com.

B- Myria quéméner , yves charpenel – la cbercimnalite op –cit.

فهرس المحتويات