وزارة التعليم العالي و البحث العلمي

جامعة قاصدي مرباح ورقلة

كلية الحقوق و العلوم السياسية

قسم الحقوق

مذكرة مقدمة لإستكمال متطلبات الحصول على شهادة الماستر في الحقوق

تخصص: قانون جنائي و علوم جنائية

مذكرة بعنوان:

التحقيق الجنائي في الجرائم الإلكترونية

إعداد الطلبة:

باباحمو مسعود

بن النوي رانيا

إشراف الأستاذ:

بوليفة محمد عمران

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
خديجي أحمد	أستاذ محاضر أ	جامعة ورقلة	رئيسا
بوليفة محمد عمران	أستاذ محاضر أ	جامعة ورقلة	مشرفا و مقررا
بكرارشوش محمد	أستاذ محاضر أ	جامعة ورقلة	مناقشا

السنة الجامعية

2022/2021

وزارة التعليم العالي و البحث العلمي

جامعة قاصدي مرباح ورقلة

كلية الحقوق و العلوم السياسية

قسم الحقوق

مذكرة مقدمة لإستكمال متطلبات الحصول على شهادة الماستر في الحقوق

تخصص: قانون جنائي و علوم جنائية

مذكرة بعنوان:

التحقيق الجنائي في الجرائم الإلكترونية

إعداد الطلبة:

باباحمو مسعود

بن النوي رانيا

إشراف الأستاذ:

بوليفة محمد عمران

أعضاء لجنة المناقشة

الاسم واللقب	رتبة العلمية	الجامعة	الصفة
خديجي أحمد	أستاذ محاضر أ	جامعة ورقلة	رئيسا
بوليفة محمد عمران	أستاذ محاضر أ	جامعة ورقلة	مشرفا و مقررا
بكرار شوش محمد	أستاذ محاضر أ	جامعة ورقلة	مناقشا

السنة الجامعية

2022/2021

بسم الله الرحمن الرحيم

صدق الله العظيم

إهداء

قال الله عز و جل: (وَوَصَّيْنَا الْإِنسَانَ بِوَالِدَيْهِ حُسْنًا) الآية 8 من سورة العنكبوت

و عملا بقوله تعالى أهدي ثمرة جهدي إلى هذا إلى التي لا تستوفي الكلمات حقها، إلى التي كانت عمودا لي و سُلمي الذي أرقى به بسمتها غايتي و ما تحت أقدامها جنتي و دعواتها دروعي و مفتاح أبوابي... أمي الرحيمة

و إلى من رباني و كان سندي أبي الغالي أطال الله في عمره و أدام صحته, و لجداتاي أطال الله في عمرهم و رحم روح جدي الزكية الطاهرة. إلى إخواني و إخوتي منبع المحبة مريم، فردوس، عائشة، باية و إبنها و رفيقة دربي إنتصار و كل أفراد العائلة الكريمة، و الأصدقاء.

لكل من كان سببا في نجاحي هذا إلى محمد أبيكر، مصطفى زوزي، إبراهيم باباحمو، مصطفى خواجه. كما أخص بالذكر أستاذي الفاضل محمد قريشي و الذي له الفضل في توجيهي في مساري الجامعي.

مسعود باباحمو

إهداء

الى أمي وأبي "عبد الحميد و وسيلة" من كان اسميهما فخري، دعاؤهما سر نجاحي وحبهما قوتي، اللذان تعبا من أجلي يسهران على نجاحي وتوجيهي ومساندتي الى حد الان. لهما كل الفضل وجعلهما الله في اعلى مراتب الجنة واطال في عمرهما.

الى روح جدي وجدتي رحمهما الله وجعلهم من اهل الجنة.

الى احسن اخت وسندي "آمنة" الى اخي الحبيب "عبد الغني " اللذان أتمنى لهما النجاح و التفوق في جميع ميادين الحياة.

الى كل صديقاتي و حبيباتي الى "منار" و"دنيا" الى كل من كان سندا في حياتي الى الأصدقاء الذين شجعوني على المواصلة و عدم الفشل

الى كل شخص قدم لي ولو ابتسامة جعلتني أصل الى كل ما انا عليه.

رانيا بن النوي

شكر و عرفان

عن أبي هريرة رضي الله عنه أن النبي صلى الله عليه و سلم

قال:"لا يشكر الله من لا يشكر الناس" رواه البخاري

نشكر الله عز و جل على نعمه و توفيقه لإتمام هذا العمل

و نتقدم بشكرنا الجزيل لكل أساتذتنا الكرام طوال مسارنا الدراسي و الشكر موصول لجميع أساتذة قسم الحقوق بكلية الحقوق و العلوم السياسية بورقلة و نتوجه بشكرنا لكل من كان له الفضل علينا و كل من علمنا حرفا و نخص بالذكر أعضاء اللجنة الفاضلة لمناقشة هذه المذكرة و للأستاذ المحترم"بوليفة محمد عمران" على إشرافه لعملنا المتواضع و الذي لم يبخل علينا بنصائح و توجيهاته منذ أول حصة لنا في مسارنا الجامعي أكرمه الله و أحسن إليه

شكرا لكل من ساهم في إنجاز عملنا هذا بمعلومة او نصيحة او كلمة طيبة.

قائمة المختصرات:

- **ج.ر.ج.ج: الجريدة الرسمية للجمهورية الجزائري الديمقراطية الشعبية**
- **ق.إ.ج: قانون الإجراءات الجزائية**
- **ق.ع: قانون العقوبات**
- **د.ذ.د.ن: دون ذكر دار النشر**
- **د.ذ.ب.ن: دون ذكر بلد النشر**
- **ط: الطبعة**
- **ص: الصفحة**

مقدمة

لقد ساعد التطور التكنولوجي الذي نراه اليوم في العديد من المجالات اليومية، حيث تم إبتكار أدوات و أجهزة جعلت الحياة أسهل و أسرع و أفضل، فعلى سبيل المثال ساهم التطور التكنولوجي بإبتكار طرق أسرع لتواصل الأفراد مع بعضهم البعض و مختلف أنحاء العالم. و ساهم أيضا في تحسين العديد من القطاعات المختلفة نتيجة لما تم تقديمه من معدات و تقنيات جديدة تعمل على توفير وقت و جهد الإنسان و من أبرزها قطاعات التعليم, الطب، الصناعة، التجارة و غيرها.

و يعد التطور التكنولوجي سلاح ذو حدين فهو مليء بالإيجابيات،كما هنالك بعض الآثار السلبية له كالتأثير على الأسلحة العسكرية و البيولوجية و الصحة البدنية و النفسية و كذا الحياة الإجتماعية و عالم الإجرام. فالتطور التكنولوجي لتقنية المعلومات والاتصالات قد نجم عنه ظهور نوع خطير من الجرائم هو ما يسمى (بالجريمة الإلكترونية)، والتي أصبحت تهدد أمن الأفراد، والشركات، بل والدول أيضاً على حد سواء.

و لا تختلف على الجرائم التقليدية في أطرافها فتتكون من الجاني و العمل الإجرامي و المجني عليه إلا أنها لا ترتكب في عالمنا الملموس و إنما في عالم إفتراضي أو عن طريق وسائل التكنولوجيا، و لها عدة تسميات منها: الجرائم المعلوماتية، الجرائم السيبرانية Cyber Crime ، الجرائم التقنيات العالية Hitesh Crime ، الجرائم الحاسوب والإنترنت / Computer Crime و غيرها من المسميات. و يعرف جهاز الكمبيوتر بأنه عبارة عن مجموعة من الأجهزة أو الوحدات التي تعمل بصورة متكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلة طبقا لبرنامج محدد تم وضعها مسبقا للحصول على نتائج معينة[1]. ولقد وردت العديد من التعريفات للجريمة الإلكترونية فقد عرفتها تعريف منظمة التعاون الاقتصادي والتنمية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية". كما عرفتها مكتبة المحاسبة العامة في الولايات المتحدة الأمريكية بأنها "تلك الأفعال العمدية التي تسبب خسائر للحكومة ، أو مكاسب للأفراد ، والمرتبطة بتصميم أو استخدام أو تشغيل النظام الذي تقع هذه الأعمال في نطاقه".

[1]– هدى حامد قشقوش, جرائم الحاسب الإلكتروني في التشريع المقارن, دار النهضة العربية, القاهرة, الطبعة الأولى, 1996, ص6.

ومن الناحية القانونية يمكن تعريف الجرمية الإلكترونية بأنها "كل فعل أو امتناع عن فعل يأتيه الإنسان إضراراً بمكونات الحاسب الآلي المادية والمعنوية ، وشبكات الاتصال الخاصة به ، باعتبارها من المصالح والقيم المتطورة التي يحميها قانون العقوبات". كما تجدر الإشارة للتفرقة بين صنفي الجرائم، فيجب علينا الرجوع للقانون، فقد نصت المادة الثانية من القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430

الموافق لـ 5 غشت سنة 2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، على أن الجريمة الإلكترونية هي "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية"[1]. و تحيلنا المادة إلى القانون15/04 المؤرخ في 10 نوفمبر سنة 2004 المعدل و المتمم للأمر 66/156 و المتضمن قانون العقوبات، و ذلك في مواده المذكورة من المادة394مكرر إلى 394مكرر7.

و هو القانون الذي ينص على الجرائم الإلكترونية البحتة كالقرصنة، أما الشق الثاني من المادة الثانية من القانون 04/09 سالف الذكر فيقصد بها تلك الجرائم الكلاسيكية التي يعاقب عليها بالقانون العام و تسهل إرتكابها أو يستعمل فيها تكنولوجيا الإعلام و الإتصال كالقذف و السب و الشتم و التهديد، فهي جرائم تقليدية و لكن عندما تتم عن طريق تكنولوجيات الإعلام و الإتصال عبر وسائل التواصل الإجتماعي مثلا فهنا يمكننا تكييفها كجريمة إلكترونية. فتكنولوجيا الإعلام و الإتصال ساعدت على ظهور طائفة جديدة من المجرمين و التي سعت لإرتكاب نوع حديث من الجرائم يطلق عليهم عدة تسميات منها: المتطرفون، المتجسسون، مخترقو الأنظمة، القراصنة HACKERS ويطلق هذا المسمى على القراصنة الذين يتخذون من الجرائم الإلكترونية والقرصنة هواية ليس أكثر ويكون غرضها تخريبيا ليس هادف،أو الكراكرز CRACKERS وهم القراصنة المحترفون ، ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة ، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية، أو الطائفة الحاقدة تستهدف غالباً هذه الطائفة المنظمات والمنشآت وأرباب العمل ويكون الهدف من ارتكاب الجريمة الإلكترونية بحق هذه الأطراف أو الضحية

[1]– المادة 2 من القانون 04/09 المؤرخ في 5غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها, ج.ر.ج.ج العدد47.

عادة بغية الانتقام والحصول على المنفعة المادية أو السياسية. حيث يهدف هذا النوع من المجرمين لأهداف عديدة و مختلفة كالسعي للحصول على المعلومات السرية بطرق غير مشروعة لسرقتها أو مجرد الاطلاع عليها وأحياناً حذفها أو غزو أجهزة الخوادم التي توفر المعلومات التي تهم الهاكر من خلال شبكة الإنترنت والتلاعب بها وتعطيلها، استقطاب معلومات غير مسموح الاطلاع عليها مخزنة على خوادم جهات تعتمد على التكنولوجيا في تخزين بياناتها السرية كالبنوك والحكومات والمؤسسات، واستخدامها كوسيلة للتهديد للحصول على هدف مادي أو سياسي, السعي للكسب غير المشروع والذي قد يكون ماديا أو معنويا أو سياسية كسرقة أرقام حسابات عملاء البنوك و غيرها من الأهداف. و هناك عدة دوافع تدفع هذه الفئة الإجرامية للقيام بالجرائم الإلكترونية فمنها الدوافع المادية(سعيا في تحقيق الثراء) و منها دوافع شخصية (التعلم: للمبتدئين, الإنتقام: و هو الأكثر خطرا و ضررا, أسباب ذهنية: الغرض منها إثبات القدرات على القرصنة) و هناك دوافع من أجل التسلية فقط كما أن هناك دوافع سياسية كذلك تستهدف الحكومات.

و بما أن إنتشار هذا النوع من الجرائم يزداد أكثر فأكثر كل عام و يأخذ منعطفا متصاعدا في ظل هذا الإنفتاح في الشبكة المعلوماتية حسب آخر الإحصائيات و خاصة في فترات الحجر الصحي التي مررنا بها في ظل جائحة كورونا، فإنه بات من الضروري إيجاد حلول ناجعة و إتخاذ تدابير تجاه المجرمين سواء كانت وقائية عن طريق تحسيس المواطنين و نشر الثقافة القانونية أو ردعية لوقف هذا الزحف الخطير فكان إنشاء مركز الوقاية من جرائم الإعلام الآلي و الجريمة المعلوماتية و مكافحتها و الذي دخل حيز الخدمة سنة 2009، حيث عالج العديد من هذه الجرائم بالاعتماد في التحقيق على مختصين تم تكوينهم لهذا الغرض.

و أهمية موضوع دراستنا هذه هي أن هذا النوع من الجرائم الإلكترونية لا يمكن أن تطبق عليه جميع الإجراءات التقليدية و المألوفة لدينا كرجال قانون و هذا لأنه يتم إرتكابها في عالم إفتراضي غير مادي, و كذا الوسائل المستعملة في القيام بهذا النوع من الجرائم،كما أنه موضوع حديث و لا تزال الدراسات والبحوث متواصلة فيه و يتسم بالنذرة و قلة المراجع و الباحثين فيه. أما عن أهداف بحثنا هذا محاولة تسليط الضوء و إبراز أهمية و دور المشرع في محاولته لمواكبة التشريعات الأخرى المتقدمة لمسايرة الركب و

مدى نجاعة الإجراءات التقليدية في إثبات الوقائع و التنقيب عن الحقيقة، وكذا الوصول لغاية وضع إجراءات كافية للتصدي لهذه الفئة الإجرامية في العالم الإفتراضي و تدارك النقائص.

فكان لنا النصيب أن نبحث في هذا المجال في إطار إنجاز هذه المذكرة. فالجرائم الإلكترونية تعد من أسرع الجرائم تطورا في العالم، حيث تحول واقع الجريمة من واقع مادي ملموس إلى مسرح لامرئي إفتراضي كما أن الضرر الناجم عن هذه الجرائم لا يمكن الإستهانة به و هذا ما يتطلب عملا صارما و إجراءات ناجعة و بحثا دقيقا كون هذه الجرائم عابرة للحدود تتميز بالسرعة في تنفيذها و سرعة و سهولة إتلاف الأدلة ما يصعب عملية التحقيق و الكشف عن هوية المجرم, إن وجود هذا النوع من الجرائم و الذي يمس بحرمة و حقوق الإنسان يدعو إلى خلق إطار قانوني يقوم على تحديدها و تصنيفها و ضبطها و خلق العقوبات و الإجراءات الرادعة لحماية الأفراد و حقوقهم و الحد من إنتشارها. و ترتيبا على ذلك بذلت العديد من الدول و منها الجزائر جهودا كبيرة لتطوير الترسانة القانونية و أساليب البحث و التحقيق القضائي لمكافحة هذا النوع من الجرائم و هذا من بداية القرن 21، و من هنا يثار الإشكال التالي: **هل أن سبب إعتماد المشرع لوسائل مستحدثة في مجال التحقيق في الجرائم الإلكترونية سبيل للإستغناء عن الوسائل التقليدية أم مجرد تدعيم لهذه الأخيرة لعدم تناسبها مع هذا النوع من الجرائم؟**

و للإجابة على هذه الإشكالية فقد إعتمدنا في دراستنا بالمنهج الوصفي التحليلي، وصفي حيث سنركز على وصف الإجراءات و المفاهيم و إستعراض آليات التحقيق و الإستناد إلى أبعادها و عناصرها المختلفة و كذا خصائصها، و تحليلي حيث سنقوم بتحليل تلك المفاهيم و النصوص و الآراء الفقهية حول الإجراءات الموضوعة لهذا النوع من الجرائم. حيث لم نواجه صعوبات كثيرة في مجال بحثنا هذا و رغم نذرة البحوث العلمية في هذا الموضوع و محاولتنا لطلب المساعدة من الجهات الأمنية و المتخصصة إلا أنه تحصلنا على المراجع الكافية لإستيفاء هذا البحث. و نتبع في بحثنا هذا خطة ثنائية حيث نتناول في فصلنا الأول محدودية اجراءات التحقيق التقليدية، أما في الفصل الثاني سنركز ضرورة اعتماد الآليات المستحدثة.

الفصل الأول:

محدودية إجراءات التحقيق التقليدية

لقد ظهرت تكنولوجيا الإعلام من الستينات و السبعينات و إنتشرت في العديد من الدول و كان دخولها للجزائر نهايات القرن 20 و بدايات القرن 21 و حيث كانت بداية إتاحتها للجميع سنة 2004 في إطار دمقرطة الإنترنت، و بعد إنتشار الشبكة العنكبوتية بدأت ظهور هذه الفئة من المجرمين في مجال الجرائم الإلكترونية و كانت آنذاك أولى النصوص المتعلقة بمكافحة هذا النوع من الجرائم، و هو القانون رقم 04-05 المؤرخ في 10نوفمبر 2004 المعدل و المتمم للأمر 66-156 المؤرخ في 8يونيو 1966 و المتضمن قانون العقوبات[1]. لكن لم لدى الدول و التشريعات خيار للتصدي لهذه الجرائم إلا عن طريق الإجراءات التقليدية كالمعاينة، التفتيش، ضبط الأدلة و الخبرة إستبعادا لباقي الإجراءات كالإستجواب و سماع أقول الشهود لعدم وجود أي إشكال أول صعوبات تجاه تطبيقها. كما أن الإجراءات سالفة الذكر تعتبر نجاعتها محدودة لكون الجرائم المتعلقة بالإعلام و الإتصال بحاجة لإجراءات مستحدثة و تطوير الإجراءات الموضوعة للحد من هذه الجرائم لكي تتناسب مع طبيعتها الخاصة.و هذا قبل أن يسارع المشرع لوضع إجراءات خاصة تتعلق بالتحقيق في جرائم الإعلام و الإتصال. و سنركز في فصلنا هذا على الشق الأول و المتمثل في محدودية الإجراءات التقليدية تجاه الجرائم الإلكترونية.

[1] -أنظر ج.ر.ج.ج العدد71,المؤرخة في 10نوفمبر 2004.

المبحث الأول: المعاينة و التفتيش في البيئة المعلوماتية

و سنعرج في هذا المبحث لإجراءات إنتقال للمعاينة(المطلب الأول) ثم نتطرق لإجراءات التفتيش في البيئة المعلوماتية(المطلب الثاني)

المطلب الأول: الإنتقال للمعاينة

تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة ، ومن أهم إجراءات التحقيق على الإطلاق ، نظرا لما يمكن أن توفره من أدلة إثبات، وتزداد أهميتها أكثر إذا تعلق الأمر بالجرائم الالكترونية، باعتبارها من الجرائم المستحدثة وغير مألوفة بالنظر إلى الطبيعة الخاصة للسلوك الإجرامي فيها ، والذي يستوجب ابتكار تقنيات جديدة مناسبة بالمعاينة في هذا المجال[1].

الفرع الأول: مفهوم المعاينة

ينبغي عند التطرق للإطار القانوني للمعاينة الوقوف عند التعريف بها ، وتبيان أهميتها وطبيعتها، والسلطة المختصة بإجرائها وكيفية الانتقال، وشروط معاينة مسرح الجرائم المعلوماتية والذي سنورده كالتالي:

أولا: تعريف المعاينة

يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيه الجريمة الإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة وعن مرتكبها ، وبالتالي يجب على السلطات المختصة بإجراء المعاينة الانتقال إلى أماكن وقوع الجريمة فور ارتكابها ، حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بتغيير أو إزالة كل أو بعض الآثار المادية للجريمة التي تساعد في

[1] –براهيمي جمال, التحقيق الجنائي في الجرائم الإلكترونية, أطروحة لنيل شهادة الدكتوراه, قسم الحقوق, كلية الحقوق و العلوم السياسية, جامعة مولود معمري, تيزي وزو, 2018 , ص56.

التنقيب عن الحقيقة ، وحتى لا يقع الشك في الدليل المستنبط منه وهذا ما تضمنته نص المادة 42 من قانون الإجراءات الجزائية الجزائري[1].

وتتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة ، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة ، وإذا كانت الجريمة واقعة على المكونات المادية للأجهزة الالكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص المغنطة ، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعد أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين ، ثم ضبطها وضعها في أحراز مختومة تقدم للنيابة العامة . أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الالكترونية أو بواسطتها ، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الانترنت فيكون الانتقال للمعاينة هنا افتراضيا أو الكترونيا ، ويمكن للمحقق إجراء المعاينة الافتراضية أو الالكترونية بالولوج والانتقال إلى مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه ، أو من خلال مقهى الانترنت أو إحدى مقرات مزود خدمات الانترنت.[2]

ثانيا: طبيعة و أهمية المعاينة

قد تكون المعاينة إجراء تحقيق أو استدلال ، يستهدف إلى إظهار الحقيقة في واقعة يبلغ أمرها إلى السلطات المختصة ، بحيث لا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه إجراؤها من مساس بحقوق الأشخاص ، فإذا تم إجراء المعاينة في مكان عام كانت إجراء استدلال ، أما إذا اقتضت دخول حرمة مسكن خاص كانت إجراء تحقيق.

[1] –غانم نسيمة, معمش زهية, , الإثبات الجنائي في الجرائم المعلوماتية,مذكرة تخرج لنيل شهادة الماستر في الحقوق, كلية الحقوق و العلوم السياسية, جامعة عبد الرحمان ميرة, بجاية, 2013, ص7.

[2] –براهيمي جمال, المرجع السابق,ص58.

وللمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدرا أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة سلطات التحقيق ومرآة صادقة تعكس بأمانة وقائع وملابسات الجريمة ، فهي ناطقة بما أتاه شاهد على ما فعله الجاني دون انحياز أو تعديل أو نقصان[1].

الأصل أن انتقال المحقق الجنائي لإجراء المعاينة أو لمباشرة أي إجراء آخر من إجراءات التحقيق أمر متروك للسلطة التقديرية له ، فلا يقوم به إلا إذا كانت مصلحة من ورائه ، لذلك جرى أن المعاينة هي من إجراءات التحقيق التي يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر التحقيق ، وهذا ما قضت به نص المواد 79-80-42 من قانون الإجراءات الجزائية الجزائري على أن المعاينة تجرى إما من طرف قاضي التحقيق ، وذلك بعد إخطار وكيل الجمهورية الذي له الحق في مرافقته ، وكما يمكن تمديد اختصاص قاضي التحقيق إذا استدعت ضرورة الحالة إلى دوائر اختصاص محاكم مجاورة ، كما يتم أيضا إجراء المعاينة من طرف ضباط الشرطة القضائية الذين عليهم إخطار وكيل الجمهورية فور وصول خبر وقوع الجريمة إلى علمهم وانتقالهم بدون تميل إلى أماكن الواقعة الإجرامية[2].

الفرع الثاني: نطاق إعمال المعاينة

يعتمد المحقق الجنائي لإجراء المعاينة الإلكترونية بحثا عن الأدلة الرقمية على فحص مجموعة مصادر الدليل في البيئة الإلكترونية التي ارتكبت فيها الجريمة المعلوماتية ، والمتمثلة عادة في مكونات أجهزة الحواسيب الخاصة بالجاني والمجني عليه وملحقاتها وكذا أنظمة الاتصال بالانترنت[3].

أولا: معاينة مكونات الحاسب الآلي

تعتبر الحواسيب مصدرا غنيا بالأدلة الإلكترونية خاصة الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوك الأفراد ونشاطاتهم ورغباتهم ، لذلك فان عملية فحص هذه الحواسيب تمثل نقطة البداية في الكشف عن خفايا الجريمة الإلكترونية باعتبار هذه الأجهزة وسيلة تنفيذها أو محل وقوعها . والمعروف أن

[1] -عفيفي كامل عفيفي, جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون, ط2, منشورات الحلبي الحقوقية, بيروت, لبنان, 2007, ص44.

[2] -غانم نسيمة, معمش زهية, المرجع السابق, ص9.

[3] -براهيمي جمال, المرجع السابق, ص59.

الحاسب الآلي يقوم في تركيبته على ثلاثة عناصر أساسية هي ، القطع الصلبة(Hardware) والقطع المرنة او البرمجيات(Software) وكذا المعطيات المعلومات أو البيانات (données informatiques) وهو العنصر الذي يتوزع بين القطع الصلبة و البرمجيات . لذلك فمعاينة هذا الحاسب يستلزم الفحص المادي والمعنوي لكل هذه العناصر نظرا للارتباط الطبيعي بين بعضها البعض . وقد تعتمد عملية الفحص هنا على طريقتين أساسيتين ، الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكوناته وتقديم تقرير كامل إلى طالب الفحص ، ومثل هذه العملية تتطلب من القائم بها معرفة تقنية ومهارة فنية عالية . أما الطريقة الثانية ، فهي الفحص بواسطة حاسب آلي آخر أو أجهزة تقنية عالية للبحث في جزئية او جزئيات عبر الحاسب . وعادة ما تشمل عملية فحص مكونات الحاسب الآلي العناصر التالية :

معاينة القرص الصلب للحاسب الآلي بالفحص الجزئي أو الكلي للبيانات الرقمية ذات الطابع الثنائي المتواجدة بداخله ، والتي تتميز بعدم التشابه فيما بينها رغم وحدة الرقم الثنائي (0- 1) الذي يتكون منه تفصيل هذه البيانات ولتحقيق ذلك ، يقوم المحقق بنزع القرص من الحاسب المراد فحصه بكل عناية وحذر من أي ارتجاج أو اصطدام بأي شيء تفاديا لإتلافه أو تعطيله أو فقد أية بيانات ، ثم يقوم بفحص وتحليل النسخ التي تصدر من القرص بنفسه أو بواسطة الخبير المختص[1].

ثم معاينة البرمجيات يتبع المحقق في هذه العملية طريقتين هما ، الفحص الداخلي للبرمجيات والفحص الخارجي لها . فأما الفحص الداخلي ، فيتم من خلال البحث عن البناء المنطقي للبرمجية بما يكشف عن وجود مجهودا تجديديا في إعداده للعمل حين إنزاله في جهاز الحاسب الآلي ، وذلك بتتبع الخطوات المنطقية التي تعبر عن هذا الجهد . ولعل أكثر ما يسعى المحقق الوصول إليه في إطار الفحص الداخلي هو مصدر الملفات الموجودة داخل البرمجيات التي تفيد في ترتيب حدوث الجريمة الالكترونية ، والتعرف على الكيفية التي تم الإعداد لها . علما أن النسخ عبر الانترنت يختلف عن النسخ باستخدام برمجيات المعالجة (Word Processing) ، فالأول نسخ عبر العالم الافتراضي أما النسخ الثاني فيتم لاستخدام مصنف متداول في العالم المادي. أما الفحص الخارجي ، فيتم بواسطة البحث عن البناء

[1]- خالد ممدوح إبراهيم, فن التحقيق الجنائي في الجرائم الإلكترونية, دار الفكر الجامعي, الإسكندرية, 2009, ص215.

المنطقي للبرمجية للتأكد مما إذا كانت هذه الأخيرة منسوخة أم لا ، ثم مقارنة النسخة الأصلية بالنسخة محل الاشتباه للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة[1].

لا يحتوي النظام المعلوماتي للحاسب على معلومات مكتوبة كما يعتقد معظم الناس ، إنما يتكون من بيانات ثنائية الرقمية يتم إيداعها في الحاسب الآلي في شكل تخزين ، ثم يقوم الحاسب بمعالجتها آليا و إبرازها على هيئة معلومة موحدة كلما تم استدعاؤها من قبل مستخدم الحاسب ، أما إذا لم يتم استدعاء معلومة محددة فان بياناتها تضل مخزنة على حالتها الأصلية داخل الحاسبة لذلك فالمهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر الموجهة من طرف مستخدم الحاسب والاستجابة لها . وعليه ، فالمقصود بمعاينة النظام المعلوماتي للحاسب هو قيام المحقق بفحص و ضبط و كافة المعلومات المخزنة في ذاكرة تخزين الحاسب على شكل ملفات والتي يمكن استردادها عبره بأية حركة استردادية ممكنة، ما دام موضوعها يشكل جريمة[2] .

ثانيا: معاينة أنظمة الإتصال بشبكة الانترنت

أحيانا لا يكفي معاينة مكونات الحاسب وحدها لاستخلاص الدليل الالكتروني ، إنما يتطلب من المحقق فحص أنظمة اتصال الحاسب بشبكة الانترنت كذلك . ويقصد بأنظمة اتصال بشبكة الانترنت بالمفهوم الإجرائي ، تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالانترنت ، لذلك فعملية فحص أو معاينة هذه الأنظمة يشمل بالأساس فحص مسار الانترنت أو ما يعرف ببروتوكول الانترنت ، والنظام الأمني للشبكات ، وكذا فحص الخادم[3].

المطلب الثاني: التفتيش في البيئة المعلوماتية

يعتبر التفتيش من أخطر الحقوق التي منحت للمحقق وذلك لمساسها بالحريات التي تكلفها الدساتير عادة ، ولذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أو تأذن بمباشرته

[1] –عمر محمد أبوبكر بن يوسف, الجرائم الناشئة عن إستخدام الانترنت الأحكام الموضوعية و الجوانب الإجرائية, دار النهضة العربية, القاهرة, 2004,ص1013.

[2]– خالد ممدوح إبراهيم, المرجع السابق, ص222.

[3]– براهيمي جمال, المرجع السابق,ص64.

والأحوال التي تجوز فيها مباشرته وشروط اتخاذ هذا الإجراء بما يمثل ضمانات الحرية الفردية أو حرمة المسكن. إن الأنظمة الجنائية عرفت في مراحل تطورها أنواعا من الاجراءات تنطوى على انتهاك لحقوق الفرد الاولية في سبيل تتبع الجناة ومحاكمتهم ومنها القبض والتفتيش فاذا ما تخلت يد العدالة عن التعرض لحقوق الافراد لاصبحنا إزاء فوضى اجرامية ومن ثم يجب أن يتاح للقائمين على تنفيذ القانون نوع من السلطة في أنكار الحريات الشخصية بالقدر الذي يحول دون تسلط الاجرام على مقدرات الناس وإنما لا ينبغي أن يتجاوز هذا القدر ، ومن هذه الاجراءات التفتيش.[1]

و أمام هذا الوضع فالأمر يتطلب منا التطرق لمفهموم التفتيش و تبيان محل التفتيش و كذا الشروط الخاصة بهذا الإجراء.

الفرع الأول: مفهوم التفتيش

لتحديد مفهوم التفتيش يستوجب علينا تعريف التفتيش و خصائصه و الهدف منه و كذا إبراز أهميته.

أولا: تعريف التفتيش

التفتيش عبارة عن الإطلاع على محل منح له القانون حرمة خاصة بإعتباره مستودع سر صاحبه ، فلا يجوز الإطلاع عليه أو على ما بداخله إلا في الأحوال المنصوص عليها في القانون أو برضاء صاحبه ، وقد يكون محل التفتيش الشخص أو المسكن أو محل أخر الحقه القانون في حكم المسكن.

و يعرف التفتيش بوجه عام بأنه عبارة عن " إجراء من إجراءات التحقيق التي تهدف إلي البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص ، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة"[2].

كما يمكن تعريف التفتيش بأنه إجراء من إجراءات التحقيق يقوم به موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات إرتكابها أو نسبتها إلى المتهم[1].

[1]-خالد ممدوح إبراهيم, المرجع السابق, ص180.

[2]- أحمد فتحي سرور, الوسيط في قانون الإجراءات الجنائية, دار النهضة العربية, الطبعة السابعة, د.ذ.ب.ن, 1993, ص544.

و يعتبر التفتيش في الجريمة المعلوماتية إجراء صعب بالنظر إلى طبيعة الدليل المتحصل منه والذي يسهل إخفاءه وتدميره ، وقد يتصل بدول أخرى مما يزيد صعوبة في الحصول عليه نظرا لتمسك كل دولة بسيادتها . كما أن التفتيش في الأنظمة الإلكترونية يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الشرطة والمحققين والقضاة . كما يجوز أن يصدر إذن التفتيش مقتصرا على تفتيش الكمبيوتر، فإذا كان هذا الأخير متواجدا في أحد المساكن ، يتعين توفر شروط تفتيش المساكن، أما إذا كان الكمبيوتر في حيازة شخص خارج مسكنه أو كان في سيارته خارج المسكن ، فإنه يكفي توفر شروط تفتيش الشخص . عند صدور إذن بتفتيش نظام معين لمعالجة المعلومات آليا للحصول على دليل يفيد في كشف الحقيقة عن جريمة معلوماتية معينة ، يجوز تفتيش كل الملفات المتواجدة في النظام . إذا أسفر التفتيش عن ضبط البيانات المتواجدة في نظام المعالجة الآلية ، فيمكن ضبطها دون ضبط النظام كله ، وذلك بأخذ نسخة من البيانات الموجودة ، ويلتزم المحقق بالتحفظ عليها بشكل يمنع العبث بها.

ونخلص مما سبق أن المقصود بالتفتيش القانوني هو التفتيش عملاً وإجراء من إجراءات التحقيق أي لابد من وقوع جريمة وأن يؤدي الى التوصل لحقيقتها وفاعلها التفتيش عمل قضائي لا يجوز أن يقوم به إلا من خوله القانون صفة الضبطية القضائية وتكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أن هناك مبرراً في القانون لهذا الانتهاك ، لذا فهو يعد من بين أقصي الصلاحيات التي قد تمارسها الدولة ضد المواطن ويعد أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها.[2]

و قد أجاز المشرع الجزائري التفتيش في مجال الجرائم الإلكترونية و هذا بالرجوع لنص المادة 5 من القانون 04/09 و إجراءات القيام به.[3]

[1]- عبد الفتاح بيومي حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت, ط1, دار الفكر الجامعي, الإسكندرية, 2006, ص192.

[2]- عمر محمد أبوبكر بن يونس, الجرائم الناشئة عن إستخدام الانترنت, كلية الحقوق بجامعة المنصورة, 2004, ص852.

[3]- أنظر لنص المادة 5 من القانون 04/09 المؤرخ في 5غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها, ج.ر.ج.ج العدد47.

ثانيا: خصائص و اهداف التفتيش

يتميز التفتيش بمجموعة من الخصائصو اهداف تتمثل في:

الجبر والإكراه يعني أن الإنسان يخضع له عادة مجبراً ، ذلك لأن التفتيش يفترض أنه تعرض قانوني ينطوي على انتهاك لحرمة سر الإنسان أيا كان وعاؤه ، وقد يكون وعاء هذا السر هو الشخص ذاته أو ملابسه أو ما معه من أمتعة ، وقد يكون مسكنه وما إليه من أماكن ، كما قد يكون محل التفتيش رسائل المتهم وأوراقه.

إن التفتيش بما يتضمنه بعد انتهاك قضائي لحرمة الحياة الخاصة التي تعتبر مستودعا للاحتفاظ بالأسرار ، إلا أن هذا الانتهاك محسوب ، بحيث لا يتجاوز القدر الأدبي واللازم لكشف الحقيقة بشأن الحرائم والتوصل إلى الجناة فيها وتوقيع الجزاء المناسب بما يحقق أهداف العقاب.

حيث ان التفتيش يهدف كما قلنا إلى البحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول المعلومات بشأنها ، إذ الهدف من هذا الإجراء يتمثل في الحصول على أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة من أجل إثبات ارتكابها ونسبتها إلى المتهم ، وهذا يعني وبمفهوم المخالفة أنه لا يجوز إجراء التفتيش للتوصل إلى ضبط جريمة مستقبلية أي لم تقع بعد أو يخشى وقوعها[1].

الغاية من التفتيش هي البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الأستدلالات أو حصول التحقيق بشأنها ، وكما تذهب محكمة النقض يكون التفتيش بمناسبة جريمة وقعت وأسند إرتكابها إلى شخص معين وتقوم دلائل كافية على إرتكابه لما بما يبرر إنتهاك حرمة المحل الذي منحه القانون حرمة خاصة.

ذلك أن أول ما يتبادر إلى ذهن الجاني عقب ارتكابه الجريمة هو طمس المعالم والماديات وأزالة كل أثر يدل على وقوع الجريمة أو ما يكشف عن شخصيته ، الأمر الذي يتطلب منه دقة في التخطيط والأعداد والتنفيذ.

والتفتيش يعد من الأجراءات التي لا غنى عنها للمحقق في تقوية أواصر الأدلة أو في إسناد الواقعة قبل المتهم ، فالعثور على أدلة الجريمة من شأنها تقوية الأتهام ضد المتهم وعدم أفلاته من العقاب.

[1]- لدغش رحيمة, ضوابط تفتيش الحاسب الالي, مجلة الحقوق و العلوم الإنسانية, العدد25, المجلد الأول, جامعة الجلفة, ص138.

ثالثا: أهمية التفتيش

إن التفتيش سواء في العالم المادي أو الإفتراضي يعتبر من إجراءات التحقيق له أهمية كبيرة في كشف أسرار و توضيح مسار التحقيق[1], بمعنى أن التفتيش يساعد كثيراً على كشف خبايا وخفايا وأسرار ويجلى غموض أمور كثيرة لها أهميتها في التحقيق ، وإلا لما تعمد المتهم أخفائها أو أيداعها مكمن الأسرار ، وتلك الأهمية قد تتعلق بالواقعة أو أطرافها حيث يكشف التفتيش بالنسبة للواقعة أمور عدة منها ما يتعلق بثبوت وقوعها ومكان أرتكابها والأداة المستعملة في حدوثها ، حيث انه لاشك فيه أن التفتيش بالمكان المحتمل حدوث الواقعة بها كما ورد ببلاغ الشاهد أو المبلغ أو المجنى عليه ويبين أن ما كانت بالواقعة قد حدثت أو لا.

و التفتيش يساعد المحقق في تحديد وقت الحادث كما لو عثر المحقق على آثار بقايا ثقاب كبريت فيدل على أن توقيت أرتكابها ليلا ، كذلك يفيد في تحديد المكان ، ولكن بالطبع بالنسبة للجريمة المعلوماتية فإنها من الجرائم عابرة الحدود مما يصعب تحديد مكانها[2].

اما بالنسبة لأطراف الخصومة فيساعد التفتيش المحقق الجنائي في كشف الباعث الدافع وتحديد شخصية الجاني وحرفته ودرجة خطورته وأسلوبه الأجرامي وعلاقته بالمجنى عليه ، وذلك بتحديد الدافع حيث ان قد يكشف التفتيش عن كراهية الجاني للمجنى عليه عند العثور على أوراق بخط يد الجاني تفيد رغبته فى الأنتقام وتهديده للمجنى عليه.

و يكون تحديد شخصية الجاني بتفتيش المحقق لمسرح الجريمة وعثوره على صورة البطاقة الشخصية أو لمستند رسمى خاص بالجاني الأمر الذي يوصل إليه بسهولة.

تحديد إحترافيته ودرجة خطورته وأسلوبه الأجرامي وذلك بالعثور على أسطوانات بها برامج فك شفرات أو برامج فيروسات ، أو كتب خاصة بأشهر جرائم الكمبيوتر ، أو شهادات علمية تدل علي ان المتهم متخصص ومحترف في مجال الكمبيوتر والشبكات.

كذلك قد يوضح أسلوبه الاجرامي سواء في نوعية المسروقات التي يستولي عليها ، أو في طريق الدخول إلي شبكة المعلومات أو المواقع الإلكترونية المنتشرة علي الإنترنت ، وارتكابه الواقعة ودرجة خطورته

[1]- مانع سلمى, التفتيش كإجراء للتحقيق في الجرائم المعلوماتية, مجلة العلوم الإنسانية, العدد الثاني و العشرون, كلية الحقوق و العلوم السياسية, جامعة بسكرة, 2011, ص230.

[2]- خالد ممدوح إبراهيم, المرجع السابق, ص184.

الاجرامية ، وكلها أشياء هامة للمحقق الجنائي بلا شك في تحديد الأسلوب الذي يسلكه في التعامل مع المتهم سواء عند الضبط أو عند توجيه الإتهام.

ان تفتيش مسرح الجريمة المعلوماتي من شأنه أن يلقي الضوء على تعدد الجناه أو أن الجاني شخص واحد، ويظهر ذلك جليا عند إجراء تفتيش للنظام المعلوماتي وما قد يسفر عنه من العثور على أدوات وأجهزة إلكترونية أستخدمت في إرتكاب الواقعة.[1]

الفرع الثاني: محل التفتيش

يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره في الجريمة التقليدية فإن التفتيش ينصب على شخص المتهم أو غير المتهم ، وكذلك على مسكن المتهم وما في حكمه وملحقاته ، أو على مسكن غير المتهم وما في حكمه وملحقاته .

لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية ، ولما كان المستودع في الجرائم الالكترونية هو الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية (Hard Ware) كوحدات المعالجة المركزية (processeur) ، وحدات الإدخال والإخراج ووحدات التخزين أو ما يسمى بوحدة التحكم (Unité De Controle) ومكونات أخرى منطقية (Soft Ware) كبرامج النظام الأساسية ، البرامج التطبيقية ، والبيانات المعالجة آليا ، كما أن له شبكات اتصالات بعدية سلكية ولاسلكية متواجدة على مستوى المحلي و الدولي[2]، فان الأمر يتطلب منا البحث في مدى قابلية جميع هذه المكونات للتفتيش ولكي يتم التفتيش على هذه الحال ، كما ينبغي الإشارة إلى 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 أو الهاتف النقال الذكي .

أولا: تفتيش الأشخاص و الأماكن

إن التفتيش المعلوماتي قد ينصب على أشياء مادية لذلك يمكن أن يكون شخصا محلا له ، ونقصد هنا الأشخاص مستخدمي الحاسوب ومزودي الخدمات وخبراء البرامج والأنظمة الالكترونية ومهندسي

[1]- المرجع السابق, ص186.

[2] -براهيمي جمال, المرجع السابق, ص15.

الصيانة ، وكل شخص يحوز أجهزة أو معدات معلوماتية أي كانت طبيعتها يمكن استخدامها في ارتكاب جريمة من جرائم التجارة الالكترونية وتحمل معلومات عن التجارة الالكترونية وعن التلاعب بها كالحاسوب المحمول باليد ، الحاسوب المفكرة ، قرص صلب أو مرن . إذن فالشخص يمكن أن يكون محلا للتفتيش بكل ما في حوزته من ملابس وأمتعه تعتبر من توابعه حتى ولو كانت موضوعة أمامه طالما ثبت من ظروف الحال أنها خاصة به ، وهناك اختلاف فقهي بشأن اعتبار السيارة التي تستخدم في نقل الأجهزة المعلوماتية من توابع الشخص يجوز تفتيشها وفقا لقواعد تفتيش الأشخاص أم لا[1] ، فظهرت ثلاث اتجاهات، حيث يرى أصحاب الاتجاه الأول أن السيارة تخضع لقواعد تفتيش المنازل وليس الأشخاص وتتمتع بحرمة المسكن سواء كانت داخلية أو خارجية. أما الثاني فيرى أصحابه أن السيارة إذا كانت في مكان عام تدخل في مفهوم أمتعة الشخص أما إذا كانت في مكان خاص له فهي تخضع لحرمة المسكن وقواعد تفتيشه .

لا يضفي أصحاب هذا الاتجاه على السيارة حرمة المسكن ويخضعها لذات القواعد المتعلقة بتفتيش الأشخاص .

وقد رجح الرأي الأخير على أساس أنه أقرب للمنطق والواقع فالسيارة وغيرها من وسائل النقل لا تأخذ حكم المسكن فإذا كنا بصدد تفتيش شخص ثبتت حيازته لأجهزة معلوماتية تحتوي معلومات وأدلة عن ارتكاب جريمة من جرائم التجارة الالكترونية كقرص مرن أو جهاز محمول يحتوي مواقع تمت زيارتها أو بيانات تمت معالجتها بطرق غير مشروعة فيستوي في ذلك أن يحملها في يده أو يضعها في سيارته فالأمر سواء فالمهم أنها في حيازته وثبت نسبتها له . والأماكن أيضا يمكن أن تكون محلا للتفتيش الذي نحن بصدده كتفتيش محال الإقامة لأشخاص مشتبه فيهم لحيازتهم أشياء وأجهزة معلوماتية تستخدم في ارتكاب جرائم التجارة الالكترونية .[2] فالأماكن و الأشخاص بصفة عامة يمكن أن تكون محلا للتفتيش المعلوماتي لأن المقصود بهذا المصطلح ليس طريقة التفتيش التي يجب أن تتم بأساليب وطرق اليكترونية بل الهدف هو الحصول وضبط الأجهزة والمعلومات الالكترونية التي تستخدم في ارتكاب جرائم التجارة الالكترونية ، لذلك فإن أي مكان مهما كانت طبيعته يحتوي مكونات مادية أو معنوية لجهاز الحاسوب

[1]- مانع سلمى, المرجع السابق, ص232-233.

[2] -أحمد فتحي مسرور, الوسيط في قانون الإجراءات الجنائية, المرجع السابق, ص449.

وشبكة الاتصال يصلح أن يكون محلا للتفتيش ويخضع في ذالك للقواعد العامة الواردة في التشريعات الإجرائية.

ثانيا: تفتيش المكونات المادية للحاسب الآلي

نقصد هنا أن ينصب التفتيش على المكونات المادية لجهاز الحاسوب وملحقاته كالشاشات، الذاكرات، الطابعات من خلال الولوج بداخلها بحثا عن أدلة متصلة بجريمة من جرائم التجارة الالكترونية وهنا لا يوجد أي خلاف في أنها تخضع للقواعد التقليدية العامة للتفتيش الذي ينصب على مكونات مادية ملموسة مع مراعاة الجانب الفني للتفتيش فقط من أجل ضمان عدم تلف الأجهزة والمعدات .

إذا فحكم تفتيش المكونات المادية لابد فيه من مراعاة المكان الذي توجد فيه هذه المكونات هل هو عام أو خاص من أجل المحافظة على شرعية الإجراءات ومراعاة شروط تفتيش الأماكن الخاصة المقررة في القوانين الإجرائية المقارنة[1] ، كالمواد 44-45- 47 من قانون الإجراءات الجزائية الجزائري التي تقتضي ضرورة الحصول على رضا صاحب المسكن المكتوب والموقع من طرفه فضلا عن حضوره هو أو ممثله لإجراء التفتيش ومراعاة المواعيد الخاصة للقيام به.أما إذا كانت هذه المكونات المادية متواجدة في مكان عام كمقاهي الانترنت والمكاتب ووسائل النقل فإنها تخضع للقواعد الإجرائية الخاصة بتفتيش الأشخاص . ومن الإشكالات التي تواجه التفتيش للمكونات المادية كونها منعزلة أو مرتبطة بأجهزة أخرى في أماكن أخرى داخل نفس الدولة أو حتى دول أخرى ، لحل هذا الإشكال ظهرت فرضيتان، الاولى هي اتصال أجهزة الحاسوب محل الجريمة الالكترونية بحاسوب آخر أو نهاية طرفية داخل نفس الدولة، و تتحقق هذه الفرضية حينما يقوم المتهم بتحويل عب الأنترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أو منظومة معلوماتية مملوكة للغير متواجدة في مكان آخر و تخزينها فيها[2]. فهناك بعض التشريعات الإجرائية التي تعرضت صرامة لدراسة هذه النقطة كالتشريعين الألماني والهولندي الذين أجازا إمكانية امتداد التفتيش إلى الأجهزة المتصلة بالجهاز محل الجريمة شريطة ثبوت جدية المعلومات والبيانات الموجودة فيه لإظهار الحقيقة.

[1]- نبيلة هبة هروال,الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة, دار الفكر الجامعي, الإسكندرية,ص237.

[2]- جميل عبد الباقي الصغير, أدلة الإثبات الجنائي و التكنولوجيا الحديثة, دار النهضة,2001, ص113.

اما الفرضية الثانية فهي اتصال جهاز الحاسوب محل الجريمة بحاسوب آخر أو نهاية طرفية خارج الدولة، وهذه المشكلة تعتبر من أهم المشاكل الإجرائية التي يحتاج لها عند جمع الأدلة حيث يلجأ لها مرتكبوا جرائم التجارة الالكترونية من خلال تخزين بيانات والمعلومات المجرمة في أنظمة تقنية أخرى خارج الدولة عبر شبكة الاتصال لعرقلة التحقيق وأول من أثار هذه الإشكالية هو الأستاذ Vlirch Sieber في تقرير له قدمه في مؤتمر A.I.D.P و قد حاولت بعض التشريعات الإجرائية المقارنة حل هذه الإشكالية و تقرير صحة التفتيش عن بعد المعبر عنه بTeleperqisition حتى لو امتد لإقليم دولة أخرى دون أن يمثل ذلك أي مساس بمبدأ سيادة الدولة ، و قد نص على هذا المبدأ نص المادة 125 من مشروع قانون جريمة الحاسوب الهولندي. بينما بقت معظم التشريعات الأخرى كالألماني والفرنسي وغيرها غير مؤيدة لهذه الفكرة على أساس أنها تشكل انتهاكا واضحا لمبدأ سيادة الدولة وهذا هو الرأي الراجح فقها وقانونا حيث لا يمكن مباشرة التفتيش إذا كان جهاز الحاسوب ا متصل بأجهزة أخرى خارج الدولة إلا في إطار المساعدات المتبادلة بين الدول و بين الأجهزة المختصة بالتحري والتفتيش على المستويات الدولية في جرائم التجارة الإلكترونية[1] .

ونحن بدورنا نؤيد هذا الرأي للمحافظة على المبادئ الأساسية التي لا يمكن انتهاكها بحجة طبيعة البيئة الالكترونية وما تقتضيه من معاملات لذلك لابد من تنظيم هذه المسألة بموجب الاتفاقيات الدولية التي يجب أن تنص صراحة على أن التفتيش في هذه الحالة لا يشكل اختراقا لمبدأ سيادة الدولة وفيما عدا ذلك فلا يمكن تطبيقه دون طلب إذن من الجهات المختصة داخل دولة أخرى . هذا وقد سمحت اتفاقية بودابست السابق بيانه في المادة 32 حيث أجازت امتداد التفتيش للأجهزة المتصلة داخل دوال أخرى بالجهاز محل الجريمة إذا كانت الأجهزة متاحة للجمهور ورضي بها صاحب التفتيش . و هذا ما انطبق على التصنت والمراقبة الإلكترونية لشبكات الحاسوب أيضا رغم ما ثارته من إشكالات إلا أن الراجح فقها وقانونا هو جواز المراقبة الإلكترونية للاتصالات المعلوماتية

[1] –مانع سلمى, المرجع السابق, ص234.

عبر شبكات تبادل المعلومات و أجهزة تليكس والفاكس ونقل البيانات متى كان الهدف منها البحث عن الدليل وهذا ما تبنته أغلب التشريعات الإجرائية كالفرنسي والهولندي[1] .

ثالثا: تفتيش المكونات المنطقية للحاسب الآلي

إن تطبيق قواعد التفتيش التقليدية على التفتيش المعلوماتي لا يثير أي إشكال في حالة ما إذا انصب على المكونات المادية كجهاز الحاسوب و ملحقاته نظرا لتوفر الطبيعة المادية الملموسة للأدلة التي تتمثل أساسا في أجهزة الكترونية وأدواته لكن الإشكال يثار عندما ينصب التفتيش على البيانات والمعلومات ومعالجتها الكترونية في بيئة الكترونية غير مادية . و تعرف الكيانات المنطقية للحاسب بأنها " مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات".

و هنا أثار تفتيش المكونات المنطقية للحاسب الآلي خلافا كبيرا في الفقه بشأن جواز تفتيشها من عدمه فصلاحية المكونات المعنوية للتفتيش هي محل جدل ، كما يلي:

الرأي الأول : فذهب رأي أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة ، فإن هذا المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة ، ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي) وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب ، ويرى بعض الفقهاء في فرنسا أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا بالمعنى المألوف للمصطلح ولذا لا يمكن ضبطه وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم 34 من القواعد الفيدرالية الخاصة بالإجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس[2].

[1]- نفس المرجع, ص236.

[2]- رابحي عزيزة, التفتيش في نظم المعالجة الالية للمعطيات, قسم الحقوق, كلية الحقوق و العلوم السياسية, جامعة طاهري محمد, بشار, ص397.

الرأي الثاني : وهناك على النقيض رأي آخر يرى على أنه يسمح بضبط بيانات الحاسب غير المحسوسة أي يجوز ضبط البيانات الالكترونية بمختلف اشكالها ، ويستند هذا الرأي في ذلك على القوانين الاجرائية عندما تنص على اصدار الاذن بضبط أي شيء فلذلك يجب تفسيره بحيث يشمل بيانات الحاسب الآلي المحسوسة وغير المحسوسة ، لأن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها[1] . و في هذا المعنى نجد المادة 251 من قانون الإجراءات الجنائي اليوناني تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل ويفسر الفقه اليوناني عبارة أي شيء بأنها تشتمل بالضبط البيانات المخزنة أو المعالجة إلكترونيا.

ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان إذ بمقدور المحقق ان يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية ، و وتمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة إرتكبت أو يشتبه في ارتكابها أو ان هناك نية في أن يستخدم في إرتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة.

كذلك الشأن بالنسبة للمشرع الفرنسي حيث قام بتعديل نصوص التفتيش بالقانون رقم 2004/545 المؤرخ في جوان 2004 حيث قام بإضافة عبارة " المعطيات المعلوماتية " في المادة 94 من قانون الإجراءات الجزائية لتصبح المادة على النحو التالي : "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة ". أما عن المشرع الجزائري فانه استجاب للرأي القائل بأن طبيعة المعلومات المعالجة تتطلب قواعد خاصة وعلى هذا الأساس أجاز تفتيش المعطيات ولكن بموجب نص جديد و هو المادة 5 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال و مكافحتها ، حيث سمح لضباط الشرطة القضائية في إطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 من هذا القانون و من بين هذه الحالات توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني ، وللوقاية من الجرائم الماسة بأمن

[1] –علي عدنان الفيل, إجراءات التحري و جمع الأدلة و التحقيق الإبتدائيدراسة مقارنة, المكتب الجامعي الحديث,2012,ص42.

الدولة ، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وكذا منظومة تخزين معلوماتية[1] .

رابعا: تفتيش شبكات المعلومات المتصلة بالحاسب الالي

يقصد بالشبكة المعلوماتية ، اتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيا أو لاسلكيا أو بواسطة الأقمار الصناعية ، وقد تكون هذه الأجهزة مرتبطة ببعضها البعض في موقع واحد فيطلق عليها الشبكة المحلية ، أو موزعة على عدة أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف أو المجال المغناطيسي فتسمى الشبكة الممتدة أو شبكة الانترنت.

لذلك يثير إخضاع شبكات المعلومات المتصلة بالحاسب الآلي لعملية التفتيش صعوبات كبيرة ، تتعلق بالدرجة الأولى بالطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش ، فقد يكون الموقع الفعلي لهذه المعلومات داخل اختصاص قضائي آخر في إقليم دولة واحدة أو في إقليم دولة أو عدة دول أخرى ، وهو ما يزيد الأمر تعقيدا باعتبار الشبكة المعلوماتية ممتدة عبر أرجاء العالم[2]. ومن هنا يثار التساؤل حول مدى جواز إمداد التفتيش إلى الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا كانت متواجدة في دوائر اختصاص مختلفة ويمكن أن نتصور هنا إحتمالين مختلفتين يتمثل الاول في إتصال حاسب المتهم بحاسب آلي آخر أو منظومة معلوماتية متواجدة في موقع آخر داخل إقليم الدولة نفسها، حيث تتحقق هذه الفرضية حينما يقوم المتهم بتحويل عبر الانترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أو منظومة معلوماتية مملوكة للغير متواجدة في مكان آخر وتخزينها فيها .ففي هذه الحالة تواجه سلطات التحقيق مشكلة تجاوز الاختصاص المكاني من ناحية ، والاعتداء على حرمة خصوصية الغير من ناحية أخرى ، لاسيما في الدول العربية التي لم تفصل قوانينها الإجرائية في هذه المسألة بعد فبالنسبة لقانون الجرائم المعلوماتية الأسترالي لعام2001 الذي سمح بعمليات التفتيش على وجه السرعة للبيانات خارج المواقع التي تم اختراقها عن بعد بواسطة الحواسيب الجاري تفتيشها, و ذلك

[1]- رشيدة بوكر, جرائم الإعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن, منشورات الحلبي الحقوقية بيروت, لبنان, ط1, 2012, ص398.

[2]- بن نعوم خالد أمين, إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري,مذكرة لنيل شهادة الماستر, قسم الحقوق, كلية الحقوق و العلوم السياسية, جامعة عبد الحميد بن باديس, مستغانم, 2019, ص55.

دون إشتراط الحصول على موافقة مسبقة من السلطات المختصة عن ذلك[1]. ولم يتأخر المشرع الجزائري عن التشريعات الأخرى ، إذ نص في المادة 2/5 من القانون رقم 09/04 لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه " ... في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك " . والملاحظ هنا أن تمديد التفتيش إلى منظومة معلوماتية أخرى مشكوك فيها يكتسي طابعا خاصا ، فهو يتم عن بعد وبشكل سريع تماشيا مع طابع السرعة الفائقة الذي يجري عليه نقل المعلومات ، و واضح أيضا أن الولوج إلى منظومة المعلومات يتم هنا بمجرد الشك أو الاعتقاد بتواجد المعلومات محل البحث داخل هذه المنظومة أو تلك ، لذلك أوجب المشرع أن يكتسي هذا الإجراء طابعه الرسمي ويقع تحت طائلة القانون ، أن يكون الدخول إلى النظام المعلوماتي المقصود قانونيا ومتماشيا مع مقتضيات حماية الحياة الخاصة للأفراد ، وهما الأمرين التي علق المشرع تحقيقهما على شرط إبلاغ الجهات القضائية المختصة مسبقا بذلك ، ولا شك أن الجهات المختصة المقصودة في هذه المادة هي وكيل الجهورية وقاضي التحقيق باعتبارهما الجهة المؤهلة بمنح الإذن بالتفتيش . ومما يتعين الإشارة إليه أيضا ، أن المشرع الجزائري استطاع أن يتجاوز مسألة تفتيش المنظومة المعلوماتية عن بعد بصفة نهائية ، حينما وسع في التعديل لقانون الإجراءات الجزائية اختصاصات ضباط الشرطة القضائية في مجال التحقيق عن الجرائم المعلوماتية ، وأجاز إمكانية قيام هذه السلطات بالتفتيش في أي وقت من الليل و النهار و في أي مكان على امتداد كافة التراب الوطني.

اما الإحتمال الثاني فيظر من خلال إتصال حاسب المتهم بحاسب آخر أو منظومة معلوماتية متواجدة في إقليم دولة أجنبية ويتحقق هذا الاحتمال حينما يقوم المجرم الالكتروني بتخزين بيانات أو معلومات تفيد إثبات الجريمة في حاسب أو منظومة معلوماتية متواجدة خارج إقليم الدولة التي يقيم فيها ، عن طريق شبكة الانترنت بهدف عرقلة سلطات البحث و التحري من الوصول إلى الدليل . وفي مثل هذه

[1] –طرشي نورة, مكافحة الجريمة المعلوماتية , مذكرة لنيل شهادة الماجستير في القانون, كلية الحقوق و العلوم السياسية, جامعة الجزائر1, 2001, ص110.

الحالة تواجه سلطات التحقيق مشكلة كبيرة تتمثل في مدى جواز تمديدها إجراءات البحث والتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهت ها المختصة الإذن بالتفتيش والدخول في المجال الجغرافي لدولة أخرى ، وهو ما يسمي بالتفتيش العابر للحدود[1] . في هذا الإطار خول المشرع الجزائري لسلطات التحقيق والبحث الحق بتفتيش عن بعد الأنظمة المعلوماتية المتصلة أو جزء منها حتى ولو كانت متواجدة خارج الإقليم الوطني ، وذلك بنصه في المادة 3/5 من القانون رقم 09/04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على انه " ... إذا تبين مسبقا أن هذه المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فان الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل " . الملاحظ في هذه المادة ، أن المشرع الجزائري لم يسمح للسلطات القضائية المختصة وضباط الشرطة القضائية بتوسيع نطاق التفتيش الالكتروني ليشمل المعطيات المخزنة في منظومة معلوماتية تقع خارج القطر الوطني ، إلا في إطار المساعدة القضائية المتبادلة وفي نطاق الاتفاقيات الدولية المبرمة في مجال ملاحقة الإجرام المعلوماتي. كما انه وخلافا للتشريعات سالفة الذكر لم يضع أية حالة استثنائية تسمح بالخروج عن هذا الإطار. ولكن بالمقابل ونظراً للطابع الخاص لهذا النوع من الجرائم وما يتطلبه تعقبها من سرعة ، أجاز المشرع لسلطات الاستدلال في حالة الاستعجال تقديم وقبول طلبات المساعدة القضائية الدولية عن طريق وسائل الاتصالات السريعة مثل الفاكس أو البريد الالكتروني شريطة التأكد من صحتها.

الفرع الثالث: ضوابط التفتيش

إن التفتيش إجراء من إجراءات التحقيق و التنقيب عن الحقيقة في الجرائم المعلوماتية إلا أن ذلك لا يعني أنه يكون مطلقا نظرا لما فيه من مساس بحقوق و حريات الأفراد و لذلك فقد أحيط بجملة من الشروط منها الشكلية و منها الموضوعية و سوف نتطرق لها كالتالي:

أولا: الشروط الموضوعية

يقصد بهذه الضوابط بصفة عامة ، الشروط اللازمة لإجراء تفتيش صحيح ، وهي في الغالب تكون سابقة له ، ويمكن حصرها في ثلاثة ضوابط أساسية : السبب ، المحل والسلطة المختصة للقيام به.

[1]– حسين بن سعيد بن سيف الغافري, السياسة الجنائية في مواجهة جرائم الانترنت, رسالة لنيل شهادة الدكتوراه في القانون, كلية الحقوق, جامعة عين الشمس, القاهرة, 2005, ص376.

وجود سبب للتفتيش في البيئة الإلكترونية، فسبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث ، ويتمثل في وقوع جريمة ما جناية أو جنحة ، اتهام شخص أو أشخاص معنيين بارتكابها أو المشاركة فيها ، وتوافر قرائن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المشتبه فيه أو المتهم أو في مسكنه أو بشخص غيره أو مسكنه، وهو ما ينطبق على الجريمة الإلكترونية[1].

اما محل التفتيش و هو شرط من الشروط الموضوعية لصحة التفتيش وكما بينا في السابق فهو يشمل ثلاث عناصر أساسية وهي الأشخاص السابق بيانهم والأماكن التي توجد فيها أجهزة أو أدوات الكترونية أو رقمية، المكونات المادية والمعنوية لجهاز الحاسوب وما يرتبط به من ملحقات وشبكات الاتصال.[2]

وبالنسبة لسلطة المختصة بالتفتيش فإن هذا إجراء هو من إجراءات التحقيق التي تمس بالحرية الشخصية للأفراد ، حرصت التشريعات الجنائية على إسنادها لجهة قضائية تكمل تلك الحريات والحقوق وتضمنها .و يجب أن يقوم بتفتيش نظم الحاسوب الآلي سلطة مختصة بالتحقيق ، وقد جعل المشرع المصري الاختصاص بالتفتيش كإجراء التحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة وذلك على خلاف التشريع الفرنسي والجزائري الذين أناطا الاختصاص الأصيل بقاضي التحقيق ، أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس ، أما انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة القضائية ما عدا بعض الجرائم التي تناط بالمدعي العام.[3]

ثانيا: الشروط الشكلية

إن الغرض من إحاطة التفتيش بضمانات شكلية إلى جانب الضمانات الموضوعية هو ليس تحقيق مصلحة القضاء في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة ، وضمان مشروعية هذه الأخيرة فقط ، إنما تعتبر كذلك بمثابة سياج أمني لحماية الحقوق والحريات العامة الفردية ومع هذا فتطبيق تلك الضمانات في مجال التفتيش الالكتروني من شأنها أن تتحول إلى عقبات تحول دون تحقيق الهدف من

[1] –ليندا بن طالب, التفتيش في الجريمة المعلوماتية, مجلة العلوم القانونية و السياسية, العدد16, جامعة مولود معمري بتيزي وزو, الجزائر, 2007, ص492.

[2] –مانع سلمى, المرجع السابق, ص238.

[3]– عبدالله الهلالي, تفتيش نظام الحاسب الآلي و ضمانات متهم المعلومات دراسة مقارنة, د.ذ.د.ن, ط1, القاهرة, ص76.

إجراء التفتيش بدلا من كونها ضمانات في مجال التفتيش التقليدي[1]، حيث ان المشرع الجزائري حدد أوقات التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا و قد نص على ذلك في قانون الإجراءات الجزائية "لا يجوز البدء في التفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا و لا بعد الساعة الثامنة مساء " .... إلا أنه و في حالات استثنائية يجوز الخروج عن تلك القاعدة فعند ما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم الأموال و الإرهاب وكذلك الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة ساعات النها ر أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص ويتبين من النص أعلاه أن المشرع الجزائري أجاز إجراء التفتيش في أي وقت من أوقات النهار و الليل في جرائم معينة حددها المشرع ومن بينها الجرائم المتعلقة بالمعالجة الآلية للمعطيات.[2]

و للتفتيش لعل من أهم الضمانات الشكلية التي يتطلبها القانون في التفتيش هو حضور شخص أو أشخاص أثناء تفتيش المتهم . والهدف من وراء هذا الإجراء هو ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط[3] . والأصل أن الشخص الذي يستوجب القانون حضوره هو المتهم ، وهذا الشرط يكون قائما حتما في تفتيش الأشخاص طالما أن التفتيش يقع عليهم ، غير أنه من المتصور تفتيش المسكن في غيبة صاحبه ، ولذلك قضت التشريعات بأن يكون التفتيش في حضور المتهم أو من ينوبه ، ومنها التشريع الإجرائي الجزائري والذي اشترط أن يتم تفتيش المنازل في حضور المتهم ، وفي حالة إذا تعذر عليه الحضور وقت ذلك الإجراء ، كان على ضابط الشرطة القضائية أن يكلفه بتعيين ممثل له ، وإذا امتنع عن ذلك أو كان هاربا كان من الواجب أن ينيب عنه شاهدين من غير الموظفين الخاضعين للسلطة الإدارية لضابط الشرطة القضائية[4].

كما ان محضر التفتيش في الجرائم الماسة بالمعطيات الرقمية تسمى محاضر الشرطة القضائية محاضر البحث الإبتدائي و تكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة و نسبتها إلى فاعلها

[1]- براهيمي جمال, المرجع السابق, ص40.

[2] -عزالدين عثماني, إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الإتصال و المعلوماتية, مجلة دائرة البحوث و الدراسات القانونية و السياسية, العدد الرابع, جامعة تبسة,2018, ص57.

[3]- لدغش رحيمة, المرجع السابق, ص143.

[4]- نبيلة هبة هروال, المرجع السابق, ص256.

من جهة ، ومن خطورة الصلاحيات الواسعة الممنوحة بموجبها لضابط الشرطة القضائية لذلك عرف المشرع الجزائري محاضر الشرطة القضائية بأنها الوثائق المكتوبة التي يحررها ضابط الشرطة القضائية أثناء ممارسته لمهامه و يضمنها ما عاينه أو تلقاه من صلاحيات أو قام به من عمليات تدخل في اختصاصه. و القاعدة المسلم بها أن أعمال التحقيق جميعا ينبغي كتابتها ، والكتابة تشمل جميع إجراءات التحقيق سواء كانت معاينة ، سماع شهود أو إجراءات التفتيش وتنص المادة 68 فقرة 2 من ق إ ج " وتحرر نسخة عن هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أوضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل . " وبقصد حماية الحريات الفردية والمنع من التعسف ، ألزم المشرع الجزائري ضباط الشرطة القضائية المنتدبين للتحقيق تحرير المحاضر المثبتة لما قاموا به من إجراءات مبينين فيها الإجراءات ، والمحضر بشكل عام له مجموعة من البيانات الواجب توافرها إضافة إلى الأشخاص المؤهلين لتحريره[1].

المبحث الثاني: ضبط الأدلة و ندب الخبير

و بعدما تناولنا إجراءات المعاينة و التفتيش في البيئة الإلكترونية تليها و بعد وجود الأدلة يليها ضبط تلك الأدلة و الإستعانة بالخبرة لتحليلها. و من خلال هذا المبحث سنوضح إجراءات ضبط الأدلة(المطلب الأول) و كذا ندب الخبير(المطلب الثاني).

المطلب الاول: ضبط الأدلة

فبما أن النتيجة المترتبة عن إجراء التفتيش هي الضبط, ففي هذه الحالة يجب إتباع إجراءات ضبط الأشياء و الأدلة الرقمية, و لهذا يتوجب علينا تحديد مفهوم الضبط و ذلك من خلال تعريفه و تبيان طبيعته و محله و كذا مدى صلاحية ضبط الأدلة في الجرائم المعلوماتية.

الفرع الأول: مفهوم الضبط

و لتحديد مفهوم الضبط سنقوم بتعريفه و تحديد طبيعته و محله كالتالي:

أولا: تعريف الضبط

يعتبر الضبط من إجراءات جمع الأدلة ، وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه ، ويقصد به وضع اليد على الأشياء المتعلقة بجريمة وقعت والتي تفيد في كشف الحقيقة

[1] –رابحي عزيزة, المرجع السابق, ص408.

عنها و عن مرتكبيها ، و وضعها في أحراز مختومة ولتقدم إلى الجهة القضائية المختصة كدليل إثبات[1].
وتحصيل الأدلة في الجرائم الالكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الآلي وملحقاته ، الأقراص الصلبة ، الأقراص والأشرطة الممغنطة ، الطباعة ، البرامج اللينة والمراشد ، البطاقات الممغنطة وبطاقات الائتمان والمعدات المستعملة في شبكة الانترنت مثل المودم. وقد يرتبط الدليل الالكتروني بالمكونات المعنوية للحاسب ، كمختلف البرامج والبيانات المعالجة آليا والمراسلات والاتصالات الالكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الالكتروني[2]. وقد تبنى المشرع الجزائري في القانون 09/04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها اجراءات خاصة بضبط البيانات المعلوماتية تحت عنوان حجز المعطيات المعلوماتية، وخص لها المواد(06-07-08).[3]

ثانيا: الطبيعة القانونية ومحل الضبط

أما من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق ، فإذا كان الشيء في حيازة شخص واقتضى الأمر تجريده من حيازته وقت ضبطه كان الضبط بمثابة إجراء تحقيق ، أما إذا كان نزع الشيء قد تم دون الاعتداء على حيازة قائمة ، فيكون الضبط بمثابة إجراء استدلال.[4]

ومن حيث محل الضبط فإنه يرد على المكونات المادية للحاسب الآلي كما أنه قد يرد على البيانات المعنوية و هذا الأخير قد أثار جدلا فقهيا واسعا بخصوص القيام بضبه حيث أنه غير ملموس و غير قابل للحجز، والشرط اللازم لصحة الضبط أن يكون الشيء مفيد في كشف الحقيقة فكل ما يحقق هذا الهدف يصح ضبطه كما أن الضبط لا يرد إلا على الأشياء ، أما الأشخاص فلا يصلحوا محلا للضبط ، وإنما المصطلح الأصح هو القبض والقبض يختلف تماما عن ضبط الأشياء[5].

وقد نظم المشرع الجزائري القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون رقم 04/09 تحت تسمية " حجز المعطيات المعلوماتية " ، حيث قضت المادة 06 من نفس القانون على نسخ المعطيات

[1]- خالد عياد الحلبي, إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت, دار الثقافة للنشر و التوزيع, عمان,الأردن, 2011, ص170.

[2]- براهيمي جمال, المرجع السابق, ص47.

[3] -آيت عبدالمالك نادية, فلاح عبد القادر, التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري, مجلة الأستاذ الباحث للدراسات القانونية و السياسية, المجلد04, العدد الثاني, 2019, ص1698.

[4]- خالد عياد الحلبي, المرجع السابق, ص168.

[5] -عبدالله حسين علي محمود, سرقة المعلومات المخزنة في الحاسب الالي, ط2 دار النهضة العربية, القاهرة, 2001, ص264.

محل البحث ، وكذلك المعطيات اللازمة لفهمها على دعامة تخزين الكترونية التي تكتشفها السلطات المختصة عند القيام بالتفتيش في المنظومة المعلوماتية ، وتكون هذه المعطيات تفيد إظهار الحقيقة وقابلة للحجز ، وتوضع في الأحراز مع وجوب قيام السلطة المختصة بحماية سلامة المعطيات المخزنة في المنظومة المعلوماتية ، كما يجوز استخدام الوسائل التقنية وفقا لما يستهدفه التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتوى المعطيات[1].

الفرع الثاني: مدى صلاحية ضبط الأدلة في الجرائم الإلكترونية

ثمة صعوبة باعتبار مكونات الحاسب الآلي من الأشياء التي يمكن ضبطها وبالخصوص ضبط الشبكة الإلكترونية والمكونات المعنوية للحاسب الآلي التي تشمل محتوى أنظمة المعالجة الآلية للمعطيات ، وفيما يلي تلقي الضوء على مدى قابلية كل من المكونات المادية والمعنوية والرسائل ومراقبة الاتصالات الإلكترونية لأن تكون محلا للضبط[2].

أولا: ضبط المكونات المادية والمعنوية للحاسب الآلي

إن ضبط المكونات المادية للحاسب الآلي وملحقاته الذي يشمل على جهاز الحاسوب ومكوناته الأساسية والثانوية لا تثير أية صعوبة ، لأن الضبط يرد على أشياء مادية كالدعامة المادية للبرامج والأسطوانات والأشرطة[3].

ومن المكونات المادية التي تكون محلا للضبط ما يلي : وحدة المعالجة المركزية ، لوحة المفاتيح والشاشة والفارة ، والأقراص والأشرطة المغناطيسية التي يقوم البعض بتخزينها في البنوك أوفي مراكز التوثيق الحكومية الأمنية ، ولوحة الدوائر الإلكترونية ، وأجهزة الاتصال عبر شبكة الانترنت كأجهزة المودم[4].

تكمن المشكلة في الأشياء المعنوية للحاسب الآلي التي تتضمن البرامج والبيانات ، ويثور التساؤل إلى مدى صلاحيتها كمحل للضبط ، حيث أن البعض من الفقهاء يتجه إلى اعتبارها لا تصلح كمحل للضبط ، وهذا ما ذهب إليه الفقه الألماني واللوكسمبرجي ، أما البعض الآخر من الفقهاء يرون إمكانية تطوير النصوص التقليدية للضبط على البرامج والبيانات المخزنة ، لكون الغاية من التفتيش تتحقق

[1]– غانم نسيمة, معمش زهية, المرجع السابق, ص30.

[2] – نفس المرجع, ص27.

[3] –عفيفي كامل عفيفي, المرجع السابق, ص373.

[4] –عبدالله حسين علي محمود, المرجع السابق, ص399.

بضبط الأدلة المادية التي تفيد في كشف الحقيقة ، ومن هذا الاتجاه الفقه الكندي الذي يرى أن غرض الضبط لم يقتصر بضبط الأشياء المادية المحسوسة ، بل تطور إلى أغراض أخرى منها الحصول على المعلومات والبيانات وضبطها للوصول إلى الأدلة[1] ، غير أن المسألة الصعبة تكمن في الخلاف حول مدى خضوع المكونات غير المادية للحاسوب للضبط وفقا للنصوص التقليدية وكذا في إجراءات ضبطها سواء تعلق الأمر ببرامج الحاسوب أو بياناته. و قد أوضحنا موقف المشرع الجزائري تجاه هذه المسألة سابقا. كما أن أما المادة 07 من القانون 09/04نصت على أنه في حالة استحالة إجراء الحجز وفقا لما نصت عليه المادة 06 وذلك لأسباب فنية ، فعلى السلطة المختصة بالتفتيش القيام بالتقنيات الواجبة للمنع من الوصول إلى محتوى المعطيات أو نسخها مع الاحتفاظ بها من طرف الأشخاص المصرح لهم بذلك كذلك نص المادة 08 تعلقت بالمعطيات التي يشكل محتواها جريمة ، فعلى السلطة المباشرة بالتفتيش أن تصدر أمر بتكليف أي شخص مؤهل فنيا وتقنيا لاستخدام الوسائل التقنية المناسبة من أجل منع الإطلاع على محتوى هذه المعطيات ؛ أما المادة 09 من نفس القانون ، فيتضح من خلالها أن المعلومات المتحصل عليها عن طريق المراقبة وفقا لهذا القانون ، لا يجوز استخدامها إلا في الحدود الضرورية التي يقتضيها التحري أو التحقيق القضائي ، وذلك تحت طائلة العقوبات التي نص عليها التشريع المعمول به. ومن خلال مضمون هذه النصوص ، نجد أن المشرع الجزائري تنبه للقصور الموجود في مصطلح ضبط الكيانات المنطقية للحاسوب ، حيث استخدم مصطلح حجز وليس ضبط باعتبار أن مصطلح حجز يتلاءم مع الأشياء غير المادية.[2]

ثانيا: ضبط الرسائل و مراقبة الاتصالات الالكترونية

سهلت ثورة المعلومات الاتصال بين الأفراد التي انعكس أثرها على مختلف ميادين الحياة ، ومن ناحية أخرى فقد سببت الكثير من أضرار شخصية عن طريق جرائم عدة مستحدثة خصوصا انتهاك أسرار الأشخاص بواسطة الوسائل الإلكترونية ، ونظرا لصلة المراسلات بالحياة الخاصة للأفراد عمدت الدول على حماية هذه الأسرار الشخصية عن طريق إرساء نصوص دستورية تضمن عدم الاعتداء على خصوصية المراسلات. و من بينها الدستور الجزائري لسنة 2020 في نص المادة 47 منه على أن "لكل

[1] –عفيفي كامل عفيفي, المرجع السابق,ص374.

[2] –غانم نسيمة, معمش زهية, المرجع السابق, ص30.

شخص الحق في حماية حياته الخاصة, لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة في أي شكل كانت...".

غير أن القوانين الإجرائية تجيز ضبط الرسائل ومراقبة المحادثات الهاتفية وفقا لقواعد وشروط معينة ، من أجل المحافظة على حقوق المجتمع ونظام الأمن والآداب العامة. وهذا ما يتضح من خلال نصوص المواد من 65مكرر5 إلى 65مكرر10 من قانون الإجراءات الجزائية ، حيث قضت هذه المادة على أنه في حالة الضرورة لإجراء أساليب تحريات خاصة في بعض من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية ، أو وضع ترتيبات تقنية دون موافقة المعنيين ، من أجل التقاط وتثبيت وبث وتسجيل الكلام من طرف شخص أو عدة أشخاص في أماكن خاصة أو عامة أو التقاط صور شخص أو عدة أشخاص يتواجدون في مكان خاص ، وتتم هذه العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص ، أما في حالة فتح تحقيق قضائي تتم العمليات بناء على إذن من قاضي التحقيق وتحت رقابته المباشرة. وكما نصت المادة 3 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على ما يلي : " مع مراعاة القوانين التي تراعي سرية المراسلات والاتصالات ، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية ، وفقا للقواعد المنصوص عليها في الإجراءات الجزائية في هذا القانون ، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

المطلب الثاني: ندب الخبير

تقدم الخبرة عونا كبيرا للقضاء ولجميع جهات المختصة بالدعوى الجنائية من خلال أداء مهمتها التي بدونها يستحيل الوصول إلى رأي بشأن المسائل الفنية ، والتي من خلالها يمكن التوصل إلى ظهور الحقيقة المبنية على حقائق علمية فنية والذي يعتبر العنصر المميز لها عن غيرها من إجراءات الإثبات.

الفرع الأول: مفهوم الخبرة

لتحديد مفهوم الخبرة القضائية في الجرائم الإلكترونية يتوجب علينا الوقوف عند تعريف الخبرة و أهميتها و كذلك أنواعها و القواعد الفنية التي تحكمها.

أولا: تعريف الخبرة القضائية

تعد الخبرة إجراء من إجراءات جمع الأدلة بعد إحاطة الموضوع بمعلومات فنية تسمح باستنتاج والوصول إلى الدليل ، فالخبرة تعتبر وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الأدلة أو تحديد مدلولها من خلال الاستعانة بالمعلومات العلمية ، حيث يستند القاضي إلى الخبرة لاتخاذ القرار المناسب. أما الخبير فهو كل شخص تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة.

و أدركت العديد من دول العالم أهمية الخبرة و لم تكتفي بالنصوص القانونية التقليدية فقط بل سارعت لتدعيمها بنصوص قانونية جديدة خاصة بها, و منها التشريع الجزائري إذ نص في المادة 5 الفقرة الأخيرة من القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيا الإعلام والاتصال ومكافحتها بأنه " يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها "

ثانيا: تعيين الخبير

إن أهم صعوبة تواجه الخبرة هي تكوين الخبير المناسب للاستعانة به ، باعتبار أن الخبرة في مجال المعلوماتية لا تعتمد على الشروط التقليدية الخاصة بتعيين الخبير ، بل يتطلب الأمر شروط تتلاءم مع التطورات الطارئة في مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصة في المسائل الفنية والعلمية ، فيحتاج الشخص لكي يكون خبيرا قضائيا في مجال الجريمة المعلوماتية بشكل خاص أن يتمتع بشروط خاصة ، حيث يجب أن يكون مؤهلا ومهنيا ومتحصلا على شهادة ودراسات عليا في فرع التخصص ، وأن يخضع للتدريب العملي والقانوني مع استمراريته للتدريب والدراسة خلال مسيرته الوظيفة من أجل مواكبة كل جديد يطرأ على تخصصه لأداء مهمته ، فيتطلب من الخبير أن يكون ملما بالجوانب الفنية والتقنية[1].

و الأصل أن يختار الخبراء حسب التخصص من الجداول التي تعدها المجالس القضائية بعد استطلاع رأي النيابة العامة ، ولكن استثناء في حالة عدم توفر الخبرة المطلوبة في جداول الخبراء يجوز لجهات التحقيق

[1] –غانم نسيمة, معمش زهية, المرجع السابق,ص36.

أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول[1] . كما ان عملية اختبار الخبير أمرا متروكا لجهات التحقيق ، فبمفهوم نص المادة 147من قانون الإجراءات الجزائية الجزائري مثلا للقاضي أن يندب خبيرا واحدا أو خبراء متعددين حسب الحاجة ، ولا تهم طبيعة الخبير سواء كان شخصا طبيعيا أو شخصا معنويا كمؤسسة متخصصة تعمل في مجال الخبرة التقنية[2]. واعتقد أن مثل هذا التوجه يتجاوب مع الحالة التي عليها الخبرة التقنية اليوم ، سيما أمام ما يثيره مجال تقنية المعلومات من جدل واسع حول مقدمات التعامل معه ، و كذا النتائج الممكن تحقيقها فيه .

مع هذا فرغم أن القانون لا يمنع جهات التحقيق من ندب خبير أو عدة خبراء حتى من غير المقيدين بالجدول ، يبقي هذا التوجه قاصرا ويحتاج إلى تطوير في مجال الجرائم الالكترونية حتى يسمح بالاستعانة بخبراء الرقمنة والإعلام الآلي من الدول الأجنبية ولو عن بعد ، وهو أمر تسمح به مقومات العالم الافتراضي باعتباره بيئة اتصالية رقمية عالمية ومعمول به لدى بعض الدول المتقدمة[3].

هذا و نشير إلى أن كل التشريعات إتفقت على ضرورة أداء الخبير اليمين القانونية قبل مباشرة مهامه و ذلك شأن المشرع الجزائري الذي أوجب ذلك في نص المادة 145 من قانون الإجراءات الجزائية.

ثالثا: أهمية الخبرة و مجالاتها في الجريمة المعلوماتية

تظهر أهمية الخبرة في مجال الجريمة المعلوماتية لتعلقها الوثيق بالحاسبات وشبكات الاتصال المرتبطة بالتخصصات العلمية والفنية الدقيقة ، ومع التطور السريع لها يصعب على المختصين مواكبتها واستيعابها، بالإضافة إلى أنه لا يوجد خبير يستطيع التعامل مع جميع الجرائم المعلوماتية نظرا لتعدد أنماط هذا النوع من الجرائم[4].

أفرز التطور الهائل في مجال تكنولوجيا المعلومات على العديد من الأنشطة المستحدثة, منها العمليات المصرفية الإلكترونية ، الإدارة الإلكترونية والتجارة الإلكترونية ، مما يقتضي تنوع الجرائم التي تقع على هذه

[1] –أنظر لنص المادة144 من قانون الإجراءات الجزائية الجزائري.

[2] –بوكر رشيدة, المرجع السابق, ص426.

[3]– براهيمي جمال, المرجع السابق, ص74.

[4] –عبدالله حسين علي محمود, المرجع السابق,ص392.

العمليات وفقا لنوع الوسائل الإلكترونية المستخدمة في ارتكابها ، من بين هذه الجرائم لدينا الغش أثناء نقل البيانات أو بثها و التلاعب في البيانات أو في البرامج سواء الأساسية منها أو برامج التطبيقات.

الفرع الثاني: الجوانب الفنية للخبرة الإلكترونية

نظرا للطبيعة الفنية و العلمية البحتة التي تتميز بها الجرائم الالكترونية ، فان عملية تحري الحقيقة وتجميع الأدلة الرقمية فيها تعد من أصعب التحديات التي تواجه الخبير التقني ، لذلك كان لزاما عليه اعتماد تقنيات ومهارات علمية مهمة والاستعانة بوسائل تكنولوجيا متطورة لرفع هذا التحدي.

أولا: تقنيات الخبرة الإلكترونية

و تتمثل في تقنيات متعلقة بالتشغيل و الفحص و مدى ترابط الدليل المادي بالرقمي و كذا تدوين تلك النتائج و إعداد التقرير.

حيث ان تقنيات ماقبل التشغيل و الفحص تكمن في التأكد من صلاحية وحدات نظام الأجهزة الالكترونية المتعلقة بالجريمة للتشغيل و التحقق من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها، ثم تسجيل وتوثيق معطيات وحدات المكونات المضبوطة ،كالنوع والطراز والرقم التسلسلي.[1]

اما تقنيات التشغيل و الفحص فيقوم الخبير في هذه المرحلة باستكمال تسجيل البيانات التي لم يتم ضبطها من خلال قراءة جهاز الحاسب الآلي ، ويحدد أنواع البرمجيات كبرامج النظام ، برامج التطبيقات وأي من البرامج له علاقة بموضوع الجريمة التي تحقق المعالجة فيها الصور في جرائم التزييف أو التعديل أو التلاعب ... الخ مع إبراز إذا كانت مستندات أو معلومات لها دلالة بموضوع الجريمة كبصمات الأصابع في جرائم التزوير ووجود رسائل تهديد في جرائم القتل وغيرها ، وكذلك ينبغي عليه اكتشاف المستندات أو النصوص المخبأة داخل الصور ، وأن يقوم بتحويل الدليل الرقمي إلى مكونات مادية بواسطة طباعة الملفات أو تصوير محتواها أو وضعها وعاء حسب نوع البيانات المكونة ، ويجب أن يقوم باسترجاع الملفات التي تم محوها على الأصل عن طريق استخدام أحد برامج استعادة البيانات بالنسبة للملفات والسجلات المعطلة أو التالفة وذلك باستخدام برنامج Eassy Recover 4 all

[1]- غازي عبد الرحمان هيان الرشيد, الحماية القانونية من الجرائم المعلوماتية, رسالة لنيل درجة الدكتوراه في القانون, كلية الحقوق, الجامعة الإسلامية لبنان, 2004, ص530.

Professionalوالعمل على تخزين السجلات أو البيانات والقيام بنسخ طبق الأصل من الأقراص أو الأسطوانات لفحصها[1].

بنسبة لتحديد مدى ترابط الدليل المادي و الدليل الرقمي فيتم في هذه الخطوة فحص الدليل المادي المضبوط مع الدليل المستخرج من جهاز الحاسب الآلي والربط بينها ليصبح الدليل موثوق ويقيني حتى يتسنى قبوله أمام المحكمة.

وفي الاخير تدوين النتائج و إعداد التقرير حيث يقوم الخبير بتقديم تقرير موقعا منه لما توصل إليه من نتائج من بداية إجرائه للخبرة ، وغاليا ما يرفق معه الملاحق الإيضاحية سواء كانت مصورة أو مسجلة وغيرها ، ويقدم الملف إلى جهة التحقيق أو جهة الحكم. ومن المتخصص أجل الوصول إلى فعلى الخبير الفني أن يستخدم الأساليب الحقيقة ، وهناك أسلوبين لعمل الخبير التقني :

الأسلوب الأول يكون بتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها مثل التهديد أو النصب أو جرائم النسخ أو دعارة الأطفال ، ثم القيام بتحليل رقمي لها من أجل معرفة كيفية برمجتها وتحديد عناصر حركتها وطريقة الوصول إلى معرفتها ، ومن ثم الوصول إلى معرفة برتوكول الانترنت (IP) الذي نسب أو ارتبط بجهاز الكمبيوتر الذي صدر عنه هذه المواقع .

اما الأسلوب الثاني فيكون بتجميع وتحصيل مجموعة المواقع التي لا يمثل موضوعها جريمة بحد ذاتها ، وإنما يؤدي متابعة موضوعها إلى ارتكاب الجرائم مثل المواقع التي تقوم بالمساعدة للتعرف على جرعات المخدرات أو المؤثرات العقلية أو كيفية إعداد القنابل وتخزينها.[2]

ثانيا: الوسائل العلمية لإنجاز الخبرة الإلكترونية

يعتمد الخبير في شرح ملابسات الجريمة الالكترونية واستخلاص الدليل الرقمي الذي يساعده على الكشف عن المجرم الالكتروني على جملة من الوسائل العلمية ، والتي تمثل في الغالب أدوات فنية تستخدم في بنية نظام المعلومات . ونذكر منها مايلي :

[1] –غانم نسيمة, معمش زهية, المرجع السابق, ص41.

[2]– عمر محمد أبوبكر بن يونس, المرجع السابق, ص1043–1044.

برتوكول الانترنت (IP) : أو ما يسمى بعنوان الانترنت هو نظام يشبه عنوان البريد العادي يعمل على تراسل حزم البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها ، فهو موجود بكل جهاز الكتروني مرتبط بشبكة الانترنت ويتكون من أربعة أجزاء كل جزء يتكون من أربعة خانات ، ويشير الجزء الأول من اليسار إلى المنطقة الجغرافية ، والجزء الثاني لمزود الخدمة ، والثالث لمجموعة الأجهزة الالكترونية المرتبطة، والجزء الرابع يحدد الجهاز الذي تم الاتصال منه[1]. وفي حالة وقوع جريمة الكترونية فيمكن للخبير إتباع المسار التراسلي للبرتوكول (IP) للبحث عن رقم الجهاز المستعمل في ارتكاب الجريمة ، ومن ثم تحديد موقعه ومنه معرفة الجاني .

نظام البروكسي (PROXY) : يشتغل هذا النظام كوسيط بين شبكة الانترنت ومستخدميها يضمن توفير خدمات الذاكرة الجاهزة ، ويقوم هذا النظام على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة ، فيتحقق نظام البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل ، ويقوم بإرسالها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة العالمية مرة أخرى ، أما إذا لم يتم تنزيلها من قبل ، فيقوم بتحويل الطلب إلى الشبكة العالمية مستعينا في ذلك بأحد عناوين (IP)[2] .

ومن أهم مزايا هذا النظام أن الذاكرة المتوفرة لديه تحتفظ وتخزن كل عمليات التنزيل التي تمت عليه والتي يمكن أن تساعد الخبير على اقتناء أدلة إثبات مهمة ، مما يجعل دور البروكسي قويا و فعالا في عملية إثبات الجريمة الالكترونية .

برنامج (Trace route) : يتم عادة ادراج هذا البرنامج ضمن نظم تشغيل الحاسب الرئيسية ، ويعتبر ذا أهمية بالغة في الكشف الجنائي ، إذ يحدد بدقة الأجهزة الالكترونية التي اشتركت في نقل البيانات على الانترنت بتحديد مساراتها وصولا إلى المرسل إليه ، كما يمكنه أن يستدعى ويحيط بالملفات التي تم الولوج إليها وكافة عمليات الاختراق والعبور أو التجاوز خلال الإعداد للجريمة ، وكافة المعلومات

[1] –سليمان بن مهجع العنزي, وسائل التحقيق في جرائم نظم المعلومات, رسالة لنيل درجة ماجستير في العلوم الشرطية, كلية الدراسات العليا, جامعة نايف العربية, الرياض,2003, ص98.

[2] –نفس المرجع, ص99.

المتعلقة بدخول أشخاص مواقع معينة وتحديد مسارات تنقلاتهم فيها الى غاية خروجهم من هذه المواقع ، وعليه فكل هذه المسارات تتضمن عادة آثار أو أدلة رقمية يمكن الاستدلال بها على الجريمة[1].

أنظمة كشف الاختراق (IDS) : يكمن دور هذه الفئة من البرامج في مراقبة العماليات التي تحدث على الأجهزة الالكترونية المرتبطة بشبكة الانترنت وتسجيلها فور وقوعها في سجلات خاصة داخل هذه الأجهزة ، ومن بين هذه الأنظمة برنامج (hack 1.2 Tracer V) الذي يتكون من شاشة رئيسية تقدم للمستخدم بيانا شاملا بعملية الاختراق التي تعرض لها جهازه ، يذكر فيه اسم وتاريخ الواقعة والعنوان (IP) الذي تمت من خلاله عملية الاختراق واسم مزود خدمة الانترنت المستضيف للمخترق ورقم المنفذ والبوابة الخاصة وبيانات الشبكة التي يتبعها مزود الخدمة للمخترق بما فيها أرقام هواتفها .

برامج مراجعة العماليات الحاسوبية واسترجاعها (Auditing Tools) : هي برامج تستعمل لمراقبة مختلف العماليات التي تجري على ملفات وأنظمة تشغيل حاسب معين وتسجيلها في ملفات تسمى (Logs) ، واسترجاع هذه الملفات في حالة محوها و حذفها. ومن أمثلتها برنامج (Event Viewer) لبيئة النوافذ وبرنامج (Syslogd) لبيئة يونيكس ، وبرنامج (Recover) . وتأتي هذه البرامج إما مضمنة في أنظمة التشغيل أو كبرامج مستقلة يتم تركيبها على أنظمة التشغيل ، وفي كلتا الحالتين لا بد من تفعيلها وإعدادها للعمل مسبقا قبل وقوع الجريمة الالكترونية حتى تتمكن من تسجيل كل المعلومات المتعلقة بهذه الجريمة والتي من شانها أن تساعد الخبير في استنباط الأدلة والقرائن المفيدة لإثبات الجريمة وانتسابها إلى مرتكبها[2].

برنامج الدمج وفك الدمج (pkzip) : يستعين الخبير الالكتروني بهذا البرنامج عادة لفك البرامج التي قام المجرم الالكتروني بدمجها قصد التعرف على طبيعة البيانات التي يحتويها وتحليلها ، ودمج البرامج هي تقنية عالية يستعملها المجرم الالكتروني لإخفاء معلومات معينة لا يمكن الاطلاع عليها إلا بعد فك الدمج .

[1]-براهيمي جمال, المرجع السابق, ص79.

[2]- حسين بن سعيد بن سيف الغافري, المرجع السابق, ص16.

الذكاء الاصطناعي : نقصد بالذكاء الاصطناعي تقنيات وبرامج الحاسب الآلي التي يستعين بها الخبير الالكتروني لحصر الأسباب والفرضيات المتعلقة بالجريمة ، وجمع الأدلة الجنائية وتحليلها واستخلاص الحقائق منها ، عن طريق عمليات حسابية يتم حلها بواسطة برامج الحاسب الآلي صممت خصيصا لهذا الغرض كبرنامج (Xtree Progold) الذي يستخدم للعثور على الملفات المبحوث عنها في أي مكان على الشبكة أو الأقراص الصلبة أو الأقراص المرنة المضغوطة ، وقراءة محتوياتها في صورتها الأصلية من اجل التحليل والتقويم[1].

[1] –براهيمي جمال, المرجع السابق,ص81.

خلاصة الفصل الاول

و كخلاصة لهذا الفصل نرى أن إجراءات المعاينة و التفتيش في البيئة الإفتراضية(الإلكترونية) مختلفة عن الواقع الملموس من جوانب عدة, و هذا بسبب طبيعة الجرائم الإلكترونية حيث يتم تطبيقها مع مراعات الضوابط الخاصة بها, حيث تتمثل أولى إجراءات التحقيق في الجريمة المعلوماتية في الإنتقال للمعاينة, و يختلف ذلك حسب طبيعة الجريمة كما بيّنا طبيعة هذا الإجراء و أهميته و كذا السلطة المختصة بالقيام به و المكونات الخاضعة للمعاينة, و الأمر لا يختلف عن إجراء التفتيش كذلك, فبعدما قمنا بتحديد مفهومه و الإطار القانوني له تطرقنا للضوابط و الأطر الفنية التي تحكم إجراء التفيش الإلكتروني, و النتيجة المترتبة عن معاينة مسرح الجريمة و تفتيشه هي الحصول على الأدلة و ضبطها ثم الإستعانة بالخبراء لمساعدة رجال التحقيق في إجراءاتهم و ذلك بأنهم أهل الإختصاص في المجال المعلوماتي و إستعمال الوسائل العلمية الأكثر تناسبا لطبيعة الجريمة.

الفصل الثاني:

ضرورة إعتماد الآليات المستحدثة

إن تغلغل التكنولوجيا الحديثة في مختلف أوجه الحياة اليومية سواء على المجال الشخصي أو النشاط العملي أدى الى ضرورة وضع أُسس و قوانين تضبطها، وذلك من أجل حماية المجتمع عامة و مستعمليها خاصة.

حيث أن توسع النشاط السيبراني و إستعماله قد أدى إلى ظهور نوع خاص من الجرائم التي عادة ما نجدها في ميادين ملموسة مثل جرائم الإحتيال والنصب والتي نسقطها على الجانب الافتراضي، فأصبح الأشخاص الطبيعية والمعنوية مستعملين مختلف منصات الشراء والبيع عرضة لهذا نوع من الجرائم كما قد نجد جريمة التهديد والإبتزاز كما هو منتشر حاليا حيث يتم إستعمال ضعف طرف المهدد للضغط عليه أو على عائلته فإنتقل أركان الجريمة من الواقع الى العالم الإفتراضي.

وعلى ذلك سنحاول في هذا الفصل تسليط الضوء على الآليات التي وضعها المشرع من أجل البحث والتحري والتحقيق في هذه الجرائم من خلال مبحثين، سنتطرق في المبحث الأول إلى عملية التسرب و حفظ المعطيات، ثم ننتقل في المبحث الثاني الى إعتراض المراسلات وتسجيل الأصوات والتقاط الصور ثم أخيرا المراقبة الإلكترونية.

المبحث الاول: التسرب و إفشاء المعطيات

لقد أثر التطور التكنولوجي و المعلوماتي على نوعية الجرائم حيث أنه أدى إلى ظهور أنماط جديدة و مستحدثة من الجرائم عرفت بالجرائم الإلكترونية أو الجرائم المعلوماتية، و بالمقابل أثرت على وسائل التحقيق في هذه الجرائم، إذ أصبحت الطرق التقليدية التي جاءت بها النصوص قانون الإجراءات الجزائية غير كافية لإستخلاص الدليل في هذا النوع من الجرائم الذي يحتاج إلى تقنيات جديدة تتناسب مع طبيعتها.

وإعتبارا للطبيعة الخاصة للجرائم الإلكترونية في عناصرها و وسائل و تقنيات إرتكابها، إضطر المشرع الجزائري إلى إعادة النظر في كثير من المسائل الإجرائية خاصة فيما يخص إو يتعلق بمسالة التحقيق إو التحري و الإثبات، بإعتبارها أهم موضوعات هذا القانون، لأن الدليل الازم للإثبات في هذا نوع من الجرائم هو ذو طبيعة فنية وتقنية، و هو الأمر الذي لا يمكن إستخلاصه بالطرق أو الوسائل التقليدية وهذا ما يؤدي في بعض الحالات إلى إفلات المجرمين.

وهذا ما سنحاول تطرق إليه في هذا المبحث حيث سيندرج فيه عملية او إجراء التسرب (المطلب الاول) ثم عملية حفظ و إفشاء المعطيات (مطلب الثاني).

المطلب الاول: إجراء التسرب

امام التطور المذهل الذي يشهده العالم و مجتمعنا في ميدان الاجرام و تطور طرقه واساليبه، كان على المشرع اللجوء الى طرق فعالة وجديدة، لمواجهة هذا الخطر. ومن بين هذه طرق والاساليب نجد تحيين و استحداث اجراء التسرب، وعليه سنحاول الاحاطة بهذا الموضوع من خلال مفهوم التسرب وصورة(فرع الاول) ثم شروط التسرب (فرع الثاني).

الفرع الاول: مفهوم التسرب

سنتطرق في فرعنا هذا الى تعريف التسرب اولا ثم ننتقل الى صوره ثانيا.

اولا: تعريف التسرب:

يعتبر التسرب أسلوب او تقنية حديثة للبحث والتحري، استحدثها المشرع الجزائري بمقتضى تعديل قانون الاجراءات الجزائية، حيث عرفه المشرع بموجب المادة 65 مكرر12 من قانون الاجراءات الجزائية على انه "قيام ضابط او عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة المكلف بتنسيق العملية، بمراقبة الاشخاص المشتبه فيه ارتكابهم جناية او جنحة بإيهامهم انه فاعل معهم او شريك لهم او خاف."[1]

اضافة الى ذلك هناك عدة تعريفات فقهية من بينها:

عرف التسرب على انه "تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط شرطة القضائية بالتوغل داخل جماعة اجرامية، وذلك تحت مسؤولية ضابط شرطة القضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة اشخاص مشتبه فيهم وكشف انشطتهم الاجرامية. وذلك بإخفاء الهوية الحقيقية و تقديم المتسرب نفسه على انه فاعل او شريك."[2]

التسرب هو اجراء يقوم به ضابط الشرطة القضائية او احد اعوانه ، تحت مسؤولية الضابط يوهم الاشخاص المشتبه في ارتكابهم جريمة من الجرائم التي تعتبر جناية او جنحة بانه واحد منهم ليتمكن من مراقبتهم قصد الكشف عن ملابسات هذه الجريمة والاحاطة بمرتكبيها"[3]

ومنه نستنتج من تعريف القانوني والفقهي للتسرب انه عبارة على عملية ميدانية تكون تحت رقابة و مسؤولية ضابط شرطة، حيث يقوم ضابط او عون شرطة القضائية بالتوغل داخل جماعة اجرامية، من اجل التحقيق والتحري و يكون بإيهامهم قصد الكشف عن ملابسات الجريمة.

---

[1] -المادة 65مكرر12 فقرة 01، قانون اجراءات جزائية .

[2] -وداعي عزالدين، التسرب كأسلوب من اساليب البحث والتحري الخاصة على ضوء قانون الاجراءات الجزائية والمقارن، المجلة الاكاديمية للبحث القانوني، مختبر البحث حول فعالية القانونية، المجلد 16، العدد الثاني، كلية الحقوق و العلوم السياسية، جامعة بجاية، الجزائر 2017، ص204

[3] -روابح سعيد، كمال بوبعاية، الاساليب المستحدثة ضمن استراتيجية الكشف عن الجرائم المستحدثة في التشريع الجزائري "التسرب نموذجا"، دفاتر البحوث العلمية، المجلد 9، العدد1، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، مسيلة2021، ص247.

ثانيا: صور التسرب:

نصت المادة 65 مكرر 12 ارس عملية التسرب ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية ، في صورة فاعل أو شريك لهم أو كخاف ، على النحو الآتي:

المتسرب كفاعل فطبقا لنص المادة 65 مكرر 12 يقوم ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتباكهم جناية أو جنحة بإيهامهم أنه فاعل معهم للحصول على دليل.

والفاعل حسب المادة 41 من قانون العقوبات الجزائري[1] ، هو كل من يساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة او الولاية أو التحايل أو التدليس الإجرامي.

اما المتسرب كشريك فهي الصورة الثانية التي يتم فيها المتسرب عمليته من اجل كشف مرتكبي الجرائم المنصوص عليها قانونا في المادة 65 مكرر 12 من قانون الإجراءات الجنائية, حيث يقوم المتسرب بإيهامهم بأنه شريك معهم.

ويعتبر شريكا في الجريمة حسب المادة 42 من قانون العقوبات كل من" لم يشترك اشتراكا مباشرا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك".

و يدخل في حكم الشريك بحسب نص المادة 43 من قانون العقوبات "كل من اعتاد أن يقدم مسكنا أو ملجأ أو مكانا للاجتماع لواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو العنف ضد أمن الدولة أو الأمن العام أو الأشخاص أو الأموال مع علمه بسلوكهم الاجرامي."[2]

[1] – المادة 41 من قانون من الأمر 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم.

[2] - أنظر للمادة43 من قانون العقوبات.

وبنسبة للمتسرب كخاف هي الصورة الثالثة التي يقوم فيها المتسرب بإيهام مرتكبي الجرائم السالفة الذكر بأنه واحد منهم وذلك من خلال إخفائه للأشياء التي تتم عملية اختلاسها أو تبديدها أو تم تحصيلها من خلال ارتكاب هذه الجرائم كليا او جزئيا.[1]

الفرع الثاني: شروط عملية التسرب

نظرا لخطورة واهمية عملية التسرب وضمانا لمشروعية الدليل مستمد من هذه العملية فقد نظم المشرع الجزائري مجموعة من شروط شكلية و موضوعية لهذه العملية في قانون الاجراءات الجزائية بموجب قانون 06-22 ، وهذا ما سنحاول شرحه في هذا الفرع.

اولا: الشروط الشكلية

يستوجب قانون الاجراءات الجزائية شروط شكلية يجب مراعاتها عند لجوء الى التسرب حفاظا للحريات الفردية من التعسف او الانحراف في استخدام السلطة[2]. وتتمثل هذه شروط في:

أ- تقرير عملية التسرب:

يقوم ضباط الشرطة القضائية قبل مباشرة عملية التسرب كتابة تقرير الى وكيل الجمهورية ، وذلك طبقا لمبدا عام المطبق على اعمال الشرطة القضائية والمنصوص عليها في المادة 18 من قانون الاجراءات الجزائية[3]. وبالنسبة لإجراء التسرب نجد ان المشرع نص في المادة 65مكرر13 على:" يحرر ضابط الشرطة القضائية المكلف بالتنسيق عملية التسرب تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي تعرض للخطر امن الضباط او العون التسرب وكذا الاشخاص المسخرين طبقا للمادة65 مكرر14 ادناه[4]."

---

[1] - رفيدة صاحبي، التسرب كألية لمكافحة الظاهرة الاجرامية، مذكرة مكملة لنيل شهادة الماستر في الحقوق تحصص قانون جنائي و علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي2018-2019، ص42-43

[2] - صالح شنين، التسرب في قانون الاجراءات الجنائية الجزائرية حماية للنظام العام والحريات أم حماية للنظام العام، المجلة الجزائرية للقانون المقارن، المجلد01، العدد02، جامعة عبد الرحمان ميرة، بجاية 2015، ص123.

[3] -المادة 18، قانون الاجراءات الجزائية الجزائري ، مرجع سابق.

[4] - أنظر المادة65مكرر13، قانون اجراءات الجزائية.

والتي يفهم منها صراحة انه يجب على ضابط الشرطة القضائية المكلف بالتنسيق العملية و قبل مباشرتها ان يقوم بتحرير بتقرير مفصل يجمع اكبر عدد ممكن من المعلومات حول الجريمة محل البحث والتحري وكذا الجدوى من طلب اتخاذ هذه العملية حتى يتسنى للجيهات القضائية المختصة ان تاذن مباشرتها[1].

و يقدم بعدها هذا التقرير الى وكيل الجمهورية او قاضي التحقيق مرفقا بطلب الاذن اجراء التسرب.

ب– الإذن بالتسرب:

حسب المادة65مكرر11 من قانون الاجراءات الاجرائية، فقد جعل المشرع الجزائري اختصاص اصدار الاذن بإجراء التسرب لوكيل الجمهورية، وفي حالة تحقيق يتم التسرب بناء على اذن من قاضي تحقيق وتحت رقابته المباشرة بعد اخطار وكيل الجمهورية[2].

يعرف الاذن بانه عبارة عن تفويض يصدر من السلطة المختصة الى احد الضباط الشرطة القضائية مخولا اياه اجراء عملية التسرب[3].

او هو محرر رسمي صادر من جهة مختصة هي وكيل الجمهورية او قاضي تحقيق مسلم الى ضابط الشرطة القضائية[4].

1– شروط الاذن:

لقد نصت المادة 65مكرر15 على شروط الاذن و تتمثل فيما يلي:[5]

ان يكون مكتوبا، طبقا للقاعدة العامة التي تقضي بان إجراءات التحري والتحقيق يجب إثباتها بالكتابة، فإنه تبعا لذلك نص المشرع على ضرورة خضوع الاذن المرخص بإجراء عملية التسرب لشكلية معينة، إذ يجب إفراغ أو إيراد محتواه في شكل محرر بمعنى أن يتم تدوينه وصياغته في ورقة تحمل كل الرسميات الخاصة والمتعلقة بالجهة القضائية[6].

[1] - شيخ ناجية، اجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة، المعارف، المجلد13، العدد02، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو،2018،ص5.
[2] - المادة65مكرر11، ق.ا.ج.
[3] - صالح شنين. مرجع سابق.ص124.
[4] - نفس المرجع,ص124.
[5] - المادة65مكرر15، ق.ا.ج.
[6] -رفيدة صاحبي، المرجع السابق، ص24.

و ان يكون مسببا، لان التسبيب يعتبر ضمانة أساسية لعدم تعسف الجهة اذنة بالتسرب، وبهذا فإنه يتعين على وكيل الجمهورية أو قاضي التحقيق أن يضمن إذنه بالأسباب الداعية للقيام بالتسرب أي المبررات الموضوعية التي استوجبت اللجوء إلى التسرب ومثالها فشل الأساليب التقليدية للتحري في ضبط وكشف الجناة[1]، مع ذكر هوية الضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته

و يسلم الاذن لمدة اقصاها اربعة(4) اشهر قابلة للتجديد حسب مقتضيات التحري او التحقيق ضمن نفس الشروط الشكلية والزمنية. و يجب ان تودع الرخصة في الملف الاجراءات بعد الانتهاء من عملية التسرب. حيث يجوز للقاضي الذي رخص بإجراء التسرب ان يأمر بوقفه قبل انقضاء المدة المحددة. يراقب وكيل الجمهورية المختص او قاضي التحقيق العمليات المأذون بها من الناحية المشروعية، و من ناحية الموضوعية من خلال تقدير مدى قيمة و كفاءة ادلة الاثبات الموجودة في محاضر الضبطية القضائية.[2]

ثانيا: الشروط الموضوعية للتسرب:

اشترط المشرع اضافة الى شروط الشكلية ضرورة توافر شروط الموضوعية عند ممارسة هذا الاجراء، قصد التأكد من صحة هذه التحريات و جدية المعلومان التي تتضمنها.

أ- دوافع اللجوء الى عملية التسرب:

اجاز المشرع الجزائري اللجوء الى اسلوب التسرب، اذا كان هذا الاجراء هو الوحيد والانسب الذي يمكن بواسطته اظهار الحقيقة بعد ان اثبتت الوسائل التقليدية للبحث والتحري عدم نجاعتها.[3]

بمعنى ان اللجوء الى هذا الاجراء يكون عند الضرورة الملحة التي يقتضها التحري والتحقيق، وذلك بغرض جمع البيانات والاستدلالات.

[1] - نفس المرجع،ص25.
[2] - صالح شنين، مرجع السابق، ص125.
[3] -جبارة حياة، حموم ليدية، التسرب كآلية خاصة للبحث والتحري في الجرائم الخطيرة، مذكرة لنيل شهادة الماستر في القانون تخصص: القانون الجنائي والعلوم الإجرامية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو 2017-2018، ص31.

وهذا ما اكده المشرع الجزائري في المادة65مكرر11 عندما استخدم عبارة "عندما تقتضي ضرورات التحري او التحقيق"[1]، ليترك لكل من وكيل الجمهورية وقاضي تحقيق السلطة التقديرية الكاملة في تقييم و تقدير مدى ضرورة اللجوء الى اجراء التسرب.[2]

ب- الجرائم المقصودة بعملية التسرب:

ان الجرائم المستهدفة باجراء التسرب هي تلك الجرائم التي تتسم بالتخطيط والتنظيم و بالسرعة و الفعالية.

وقد نص عليها المشرع الجزائري و جرمها بموجب المادة 65مكرر05 من القانون 06-22، والتي هي مذكورة على سبيل الحصر وهي[3]جرائم المخدرات او الجريمة المنظمة العابرة للحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الالية للمعطيات او جرائم تبييض الاموال او الارهاب او الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد.

ج- سرية عملية التسرب

يتوقف نجاح عملية التسرب على شرط موضوعي اساسي وهو السرية، حيث بواسطتها يتحقق السير الحسن للعملية، وقد اجاز المشرع الجزائري لضباط الشرطة القضائية استعمال الهوية المستعارة، و هدف منها الحفاظ على سلامة و امن العون او ضابط المتوغل في المجموعة الاجرامية.

و تتاكد الرغبة الحقيقية و الشديدة للمشرع في احاطة العملية بالسرية التامة من خلال نص المادة65مكرر16 من قانون الاجراءات الجزائية، التي نصت على جزاءات صارمة في حالة الكشف عن هوية ضابط او عون الشرطة القضائية.

[1] -المادة 65مكرر11، ق.ا.ج. مرجع سابق.

[2] - صالح شنين ، مرجع السابق،ص

[3] - المادة65 مكرر05 قانون الاجراءات الجزائية، مرجع سابق.

لم يتوقف المشرع عند هذا الحد، بل اضافة بموجب المادة65مكرر18 انه"يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه، بوصفه شاهدا عن العملية". فبالتالي لن يتم سماع اقوال العون او ضابط المتسرب، و لن يتم استدعاؤه لادلاء بالشهادة امام القضاء[1].

المطلب الثاني: حفظ و افشاء المعطيات

يعد الحفظ والإفشاء العاجلان للمعطيات المعلوماتية بالنسبة لغالبية الدول اجراءين جديدين للبحث والتحري في مجال مكافحة الجرائم الإلكترونية، وقد تمت الإشارة إليهما لأول مرة في لائحة الجمعية العامة لمنظمة الأمم المتحدة رقم(65-63) لمؤرخة في 22-01 2001 -المتعلقة بمكافحة إساءة استعمال تكنولوجيا المعلومات لاغراض اجرامية، إذ نصت في المادة (01 الفقرة "و") على ضرورة سماح الدول الأعضاء لجهاتها المختصة بالاستدلال أمر مزودي خدمات الاتصالات القيام بالحفظ السريع للمعطيات الالكترونية المتعلقة بالتحقيقات الجنائية وبعدها تضمنت اتفاقية بودابست لمكافحة الج ارئم الالكترونية لعام 2001 إج ارءي الحفظ والإفشاء على البيانات المخزنة في نظم المعلوماتية، وألزمت الدول الموقعة على الاتفاقية من خلال المادتين(16 و 17) باتخاذ الاجراءات التي ترى أنها ضرورية من أجل السماح للسلطات المختصة بأن تأمر بالحفظ والإفشاء العاجلين على المعطيات المعلوماتية المخزنة، بما فيها المتعلقة بالمرور، والمخزنة بواسطة نظام معلوماتي، وعلى وجه الخصوص عندما تكون هناك أسباب تدعو للاعتقاد بتعرض تلك المعطيات للفقدان أو التلف[2].

حيث ان المشرع الجزائري نص على هذا في القانون رقم 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما.

جاءت المادة 10 من نفس القانون بعدد من الالتزامات تفرض على مزودي الخدمات الانترنيت بتقديم المساعدة بخصوص العمليات التي ينجزونها للسلطات المكلفة بالبحث و الاستدلال من بينها (حفظ المعطيات المعلوماتية المتعلقة بالسير ووضعها تحت تصرف القائمين بالتحقيق)[3]

[1] – المادة18 قانون الاجراءات الجزائية.

[2] – برا هيمي جمال، مرجع سابق، ص99- 100.

[3] – المادة 10 من قانون 04/09, مرجع سابق.

الفرع الاول: حفظ المعطيات السير

سوف نتطرق في فصلنا هذا الى مفهوم عملية الحفظ ثم الى ضمانات الاشخاص للمعلوماتهم

اولا: مفهوم حفظ المعطيات السير

الحفظ على المعطيات الالكترونية هو قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل قصد تمكين جهات الاستدلال من الاستفادة منها واستعمالها لاغراض التحقيق[1].

وينبغي التنويه في هذا الإطار إلى أن عملية الحفظ هنا لا تخص كل المعطيات الالكترونية بمختلف نماذجها إنما تخص معطيات المرور فقط أو كما يسميها البعض حركة السير، التي عرفتها المادة الأولى فقرة "د" من اتفاقية بودابست بأنها " صنف من بيانات الحاسب التي تشكل محلا لنظام قانوني محدد، إذ يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة "[2].

وعرفها كذلك المشرع الجزائري في المادة (02) الفقرة (ه) من القانون رقم 04/09 بأنها " أية معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات، توضح مصدر لاتصال، الوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة[3] ."

ومن ضمن معطيات المرور التي يتعين على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لاغراض التحقيق، تلك التي حددها المشرع الجزائري في المادة11 من قانون 04/09 على النحو التالي:

[1] – برا هيمي جمال، مرجع سابق، ص101.

[2] - نفس المرجع سابق، ص102

[3] – المادة 02 فقرة "ه" قانون 04/09، مرجع سابق.

المعطيات التي تسمح بالتعرف على مستعملي الخدمة و المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال و الخصائص التقنية وكذا تاريخ و وقت و مدة الاتصال و المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها و المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.[1]

ثانيا: ضمانات المشتبه فيه أثناء عملية حفظ معطيات السير

نظرا لتعارض عملية التحفظ على المعطيات الالكترونية مع الحق في الخصوصية فقد قيدها القانون بجملة من الشروط والالتزامات التي وضعها على عاتق مقدمي الخدمات أو أي كيان آخر يقع عليه عبئ الحفظ و هي احترام المدة المحددة لعملية الحفظ حيث تعتبر عملية الحفظ تدبيرا مؤقتا يتم اللجوء إليه بموجب أمر توجهه السلطات المختصة إلى مقدم خدمات الاتصال تلزمه بالحفظ على البيانات الالكترونية فترة معينة من الزمن و وضعها تحت تصرفها لغرض التحقيق، وتحديد مدة الحفظ يسمح بتعجيل الاجراءات المتابعة الجزائية إن كان لها محل[2].

و حدد المشرع الجزائري مدة الحفظ بسنة واحدة وهو ما يستنتج من المادة (11) من القانون رقم 04/09 التي تنص على أن "... تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل..."[3]

اضافة الى ضرورة احترام المدة المقررة لعملية الحفظ العاجل لمعطيات السير، يلتزم كذلك مقدمو الخدمات بالحفاظ على سرية كل الاجراءات والتدابير التي تفرضها هذه العملية طيلة المدة المقررة لها. ولعل الغرض من فرض هذا الالتزام هو ضمان حماية الحق في الخصوصية من جهة، و تجنب إحداث تغيرات في البيانات أو محوها من طرف أشخاص آخرين من جهة اخرى.

حرص المشرع الجزائري بدوره على ضرورة تحلي مزودي الخدمات بكتمان سرية عملية الحفظ وكذا سرية المعطيات المخزنة طيلة فترة الاحتفاظ بها، وعدم الإفشاء بها إلا لسلطات التحقيق المختصة، وذلك تحت طائلة العقوبات المقررة لإفشاء اسرار التحري و التحقيق[1].

[1] – المادة 11 من قانون 04/09, مرجع سابق.

[2] – برا هيمي جمال، مرجع سابق، ص104.

[3] – المادة 11 من قانون 04/09، مرجع سابق.

الفرع الثاني: الإفشاء العاجل لمعطيات السير

لقد تبنى المشرع الجزائري اجراء الإفشاء العاجل لمعطيات السير لغرض التحقيق وجعله التزاما على عاتق كل مقدمي الخدمات، وذلك من خلال نصه في المادة10 من القانون 04/09 على انه ": في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ... و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة11 أدناه، تحت تصرف السلطات المذكورة . "...بناء على ما سبق فكما تلزم سلطة التحقيق مقدمي الخدمات بالحفظ العاجل على معطيات المرور فإنها تلزمهم بالإفشاء السريع لها، أو لمن تعينه من قبلها عن تلك المعطيات المهمة المتعلقة بالمرور ووضعها تحت تصرفهم لفحصها قبل أن يتم التلاعب بها، قصد الوصول إلى تحديد هوية كل مقدمي الخدمة الآخرين، والطريق الذي بمقتضاه تم الاتصال. وبهذه الطريقة يكون بمقدور السلطة المكلفة بالبحث والتحري أن تكشف منبع الاتصال ومصبه، وهي المعلومات التي قد تقوده إلى معرفة هوية الأشخاص المتورطين في ارتكاب الجريمة الالكترونية. وتجدر الإشارة هنا إلى انه عند اللجوء لتلك الاجراءات يجب مراعاة الحدود والضمانات القانونية المتعلقة بالخصوصية، وحقوق وحريات الإنسان بشكل عام، بما يحقق التوازن بين إقامة العدالة و المحافظة على تلك الحقوق[2].

المبحث الثاني: اعتراض المراسلات و المراقبة الالكترونية

إن االاستخدام الهائل للأفرد والمؤسسات لوسائل الاتصال الحديثة والاستعمال المفرط لشبكات المعلوماتية في الآونة الأخيرة ، جعل المشرع في العديد من الدول يدرك الصعوبات البحث و التحري في الجرائم التي تحدث على مستوى هذه شبكات، حيث ان المشرع الجزائري لم يمنع من ذلك مما ادي الى تعديل قانون الاجراءات الجزائري و استحداث وسائل و اجراءات من اجل التحقيق و من بينها او اهمها هو اعتراض المراسلات و التقاط الصور(المطلب الاول) و المراقبة الالكترونية(المطلب الثاني)

[1] – المادة 10 قانون 04/09، مرجع سابق.

[2] – براهيمي جمال، مرجع سابق، ص107-108.

المطلب الاول: اعتراض المراسلات

لقد استحدث المشرع الجزائري فصلا كاملا تحت عنوان "اعتراض المراسلات وتسجيل الاصوات والتقاط الصور" في قانون الإجراءات الجزائية[1]. حيث اتاحة لضابط الشرطة القضائية القيام ببعض الاعمال الخاصة بالبحث والتحري عن الجرائم الالكترونية كما أجاز لوكيل الجمهورية أن يأمر ضابط الشرطة القضائية باعتراض المراسلات التي تجري عن طريق الوسائل السلكية واللاسلكية ووضع الترتيبات التقنية الالتقاط الصور وتسجيل المكالمات السرية دون موافقة المعني[2].

حيث إن اعتراض المراسلات وتسجيل الأصوات والتقاط الصور إجراءات تمس بحرمة الحياة الخاصة للفرد التي أقرتها التشريعات الدولية والداخلية، مما استوجب على المشرع إجازتها ضمن مجموعة من الضوابط القانونية ورتب جزاءات على عدم احترامها.

الفرع الاول: تعريف اعتراض المراسلات و التسجيل الصوتي والتقاط الصور:

سنتطرق في فرعنا هذا الى تعريف كل من اعتراض المراسلات و تسجيل الصوتي والتقاط صور اولا ثم ننتقل الى شروط اجوء الى هذا نوع من الاليات ثانيا.

اولا: تعريف اعتراض المراسلات

عرفته لجنة الخبراء للبرلمان الاوروبي في اجتماع لها عقد "بستراسبورغ" في 16 اكتوبر 2006 حول موضوع اساليب التحري التقنية و علاقتها بالأفعال الارهابية بانة" عملية مراقبة سرية للمراسلات السلكية و اللاسلكية، وذلك في اطار البحث والتحري عن الجرائم وجمع الادلة والمعلومات حول الاشخاص المشتبه فيهم بارتكابهم الجرائم او مشاركتهم فيها"[3]

---

[1] – الفصل الرابع، الباب الثاني، الكتاب الاول من قانون الاجراءات الجزائية.

[2] – فلاح عبد القادر.ايت عبد المالك نادية, المرجع السابق, ص1699.

[3] – لبيض عادل، نزلي بشرى، اثبات الجريمة الالكترونية، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر، التخصص: قانون جنائي، جامعة قاصدي مرباح ورقلة، سنة 2017-2018، ص48

ثانيا: تعريف التسجيل الصوتي و التقاط الصور:

ان المشرع الجزائري لم يعطي تعريفا صريحا لتسجيل الاصوات، بل عرفه ضمنيا في قانون الاجراءات الجزائية على انه "وضع واستعمال الوسائل والترتيبات التقنية دون موافقة المعنيين، من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية، من طرف شخص او عدة اشخاص يتواجدون في اماكن خاصة او عمومية[1].

حيث يتم تسجيل الاتصالات الالكترونية التي تكون تحت المراقبة ويتم تقديم هذه التسجيلات الى السلطات المختصة دون سواها، وهذا ما نص عليه المشرع في المادة 25 من المرسوم الرئاسي 15-261 على ان تسجيل الاتصالات الالكترونية التي تكون موضوع مراقبة، وتحرر وفقا للشروط والاشكال المنصوص عليها في قانون الاجراءات الجزائية[2]

فرع الثاني: شروط عملية اعتراض المراسلات

لعملية اتراض المراسلات لها شروط وذلك من اجل الحفاظ على خصوصية الافراد وهذا ما سنحاول توضيحه.

اولا: شروط الشكلية

قيد المشرع إجراءات التحري الخاصة بمجموعة من الضوابط شكلية ، تتمثل في:

أ– الاذن القضائي:

جعل المشرع الجزائري بموجب المادة65مكرر05 من ق.ا.ج الاختصاص بالاذن باجراء هذه العملية لوكيل الجمهورية، وفي حالة فتح تحقيق قضائي تتم العمليات بناء على اذن من قاضي التحقيق و تحت مراقبته المباشرة.

[1] – المادة 65مكرر05، قانون الاجراءات الجزائية.

[2] - لبيض عادل، نزلي بشرى، مرجع سابق،ص49.

حيث يجب أن يكون الإذن حسب المادة 65مكرر07 من ق.ا.ج مكتوبا بعبارات واضحة، يتضمن كل العناصر التي تسمح لضابط الشرطة القضائية بالتعرف على الاتصالات المطلوب التقاطها و الأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذا الإجراء .كما يجب أن يكون الإذن محدد المدة يسلم لمدة أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية، وذلك للحد من التعسف في التعدي على حرمة الحياة الخاصة بالقدر الضروري لكشف عن الحقيقة.[1]

ب- تنفيذ عمليات المراقبة

يلتزم أعضاء الضبط القضائي أثناء تنفيذ عمليات الاعتراض والتسجيل والتصوير بما يأتي :

1- كتمان السر المهني:

يسمح الإذن لضابط الشرطة القضائية المأذون له أو المناب باعتراض المراسلات السلكية و اللاسلكية وتسجيل الأصوات والتقاط الصور دون المساس بالسر المهني ، و جسد المشرع هذه الحماية من خلال: تعيين الأشخاص المؤهلين للاطلاع على الأسرار، وفرض عقوبات على من يفشي أسرار الناس مخالفة لقواعد الإجراءات الجزائية ووضع قواعد وضبط الإجراءات الواجب على أعضاء الشرطة القضائية إتباعها[2].

2- كيفية وضع الترتيبات التقنية

يسمح الإذن بوضع الترتيبات التقنية دون موافقة المعنيين ودون علمهم، إذ يجوز لضابط الشرطة القضائية ولاي عون مؤهل مسخر من طرفه دخول المساكن لوضع أجهزة الاعتراض والتصنت والتصوير والتسجيل، دون التقيد بالزمن المحدد في المادة 41 ق.إ.ج و دون علم ورضا صاحب المسكن وذلك

[1]- صالح شنين، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، المجلة الاكاديمية للبحوث، المجلد01، العدد 02، جامعة عبد الرحمان ميرة، بجاية، 2010، ص68.

[2] - محلق جميلة، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، التواصل في الاقتصاد والإدارة والقانون عدد 42 ، كلية الحقوق والعلوم السياسية، جامعة باجي مختار عنابة، جوان 2015، ص181.

يعد خروجا صريحا من المشرع عن شروط التفتيش. و هناك من يرى أن إجراء مراقبة المكالمات الهاتفية إجراء من نوع خاص إجراء يماثل التفتيش لكنه ليس في الحقيقة تفتيشا[1].

ج- محضر العمليات:

استوجب المشرع الجزائري في المادة 65مكرر09 ق.ا.ج على ضابط الشرطة القضائية المأذون له او مناب من طرف القاضي المختص ان يحرر محضرا عن كل عملية اعتراض و تسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي او السمعي البصري، ويذكر في المحظر تاريخ و ساعة بداية هذه العمليات و الانتهاء منها.

كما ذكرة المادة65مكرر10 من ق.ا.ج انه ينسح ضابط الشرطة القضائية او العون المأذون له الصور والمراسلات او المحادثات و تودع في الملف.

تنسخ و تترجم المكالمات التي باللغة الاجنبية، عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض.

ولا يكون لهذه المحاضر قوة في الاثبات الا اذا كانت صحيحة في الشكل طبقا للمادة214 من ق.ا.ج والادلة الواردة بها لها حجية نسبية، أي صحيحة ما لم يقدم ما يخالفها، على خلاف الادلة [2].

ثانيا: الشروط الموضوعية.

أجاز المشرع إجراءات التحري الخاصة عند توفر مجموعة من الشروط تتعلق بطبيعة الجريمة والسلطة المختصة وبضرورة التحر ي والتحقيق، كما يأتي:

أ- طبيعة الجريمة.

لقد حصر المشرع الجزائري الجرائم التي يجوز لجوء فيها الى وسائل التحقيق الخاصة والتي تتمثل في اعتراض المراسلات وتسجيل الاصوات والتقاط الصور بمناسبة حالة تلبس أو التحقيق الابتدائي[3] في جرائم على سبيل الحصر هي: **جرائم المخدرات و الجريمة المنظمة العابرة للحدود الوطنية و الجرائم الماسة بأنظمة**

[1] - محلق جميلة. مرجع سابق، ص181.
[2] - المادة 214 من قانون الاجراءات الجزائية، مرجع سابق.
[3] - المادة65مكرر05، قانون الاجراءات الجزائية.

المعالجة الآلية للمعطيات و جرائم تبييض الأموال و جرائم الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد. إذا اكتشف أثناء إجراءات التحري الخاصة جرائم أخرى غير مذكورة في الإذن فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة.[1]

ب- ضرورة التحري أو التحقيق.

لقد فرض المشرع الجزائري لجوء الى هذا النوع من التحقيق الا في الجرائم المتلبس بها او في تحقيق الابتدائي، و في حالة فشل وسائل التحقيق الكلاسيكية او التقليدية، ،كما تبرر بمدى تحقيق التوازن بين المصلحة العامة والمصلحة الخاصة، مصلحة الدولة في فاعلية العدالة الجنائية بملاحقة المجرم وعقابه أما مصلحة الفرد فتتحقق في الحفاظ على حياته الخاصة.

ج- الجهة المختصة:

لقد حدد المشرع الجزائري في قانون الاجراءات الجزائية من له السلطة في لجوء الى هذا النوع من وسائل التحقيق والتحري، حيث انه اجاز لوكيل الجمهورية او ضابط الشرطة القضائية الذي اذن له باستعمال الوسائل الخاصة في البحث والتحري، ولقاضي التحقيق او ضابط الشرطة الذي ينوبه، ان يسخر ويكلف كل عون مؤهل وصاحب خبرة في مجال المواصلات يعمل لدى مصالح او هيئة عمومية او خاصة مكلفة بالمواصلات السلكية واللاسلكية، لاستخدامه بالتكفل بالجوانب التقنية لعمليات اعتراض المراسلات وتسجيل صوتي.[2]

المطلب الثاني: المراقبة الالكترونية

قد تبنى المشرع الجزائري مصطلح المراقبة الالكترونية كغيره من التشريعات المقارنة الذي استمدته من نص الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي سنتها منظمة الأمم المتحدة في إطار مكافحة الجريمة المنظمة، حيث نصّت المادة 20 من تلك الاتفاقية على" :تقوم كل دولة طرف ضمن حدود إمكانيتها ووفقاً للشروط المنصوص عليها في قانونها الداخلي، إذا كانت المبادئ الأساسية لنظامها القانوني الداخلي تسمح بذلك، باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم

[1] - محلق جميلة. مرجع سابق، ص179.
[2] المادة 65 مكرر13، قانون الاجراءات الجزائية.

المراقب، وكذلك ما تراه مناسباً من استخدام أساليب تحري خاصة أخرى، مثل المراقبة الالكترونية أو غيرها من أشكال المراقبة[1]."

الفرع الأول: تعريف المراقبة الالكترونية

لمشرع الجزائري لم يتصدّ لضبط تعريف المراقبة الالكترونية لا في مواد قانون الإجراءات الجزائيّة ولا في مواد القانون رقم 04/09 المتعلق بالقواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وإنما ترك ذلك للفقه الذي اختلف هو الأخر في ضبط تعريف دقيق وموحّد لإجراء المراقبة الالكترونية، حيث عرّفها بعض الفقه بأنّها إجراء يتعمّد فيه الإنصات والتسجيل ومحلها المحادثات الخاصّة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت ممّا يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكيّة واللاسلكية.

أمّا البعض الأخر فقد عرّفها بأنّها: "إجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانوناً بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض".[2]

قامت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بستراسبورغ في 06 أكتوبر 2006، لدراسة أساليب التحرّي التقنية وعلاقتها بالأفعال الإرهابية، بتعريف إجراء المراقبة الالكترونية بأنها: "عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات "حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة

من خلال التعريفات السابقة يتضح لنا أنّ مفهوم المراقبة الإلكترونية يعني التنصّت ومن ناحية أخرى التسجيل، بالإضافة إلى إشارة تلك التعريفات إلى محل المراقبة الإلكترونية وهي الأحاديث الشخصية والمحادثات السلكية واللاسلكية فضلاً عن تبيان التعريفات السابقة ضرورة حصول التنصّت أو التسجيل

[1] – بن بادة عبد الحليم، "المراقبة الإلكترونية كإجراء الاستخلاص الدليل الإلكتروني" بين الحق في الخصوصية ومشروعية الدليل الإلكتروني""، المجلة الأكاديمية للبحث القانوني، المجلد 10 ،العدد03 ،2019 ،ص390.

[2] – بن بادة عبد الحليم،ص391.

خلسة دون علم صاحب الحديث وبواسطة إحدى الوسائل أو الأدوات العلمية الحديثة. كما أكّدت أغلب التعريفات على ضرورة أن تتم عمليّة المراقبة الإلكترونية من طرف جهات مختصّة وبإذن من الجهات القضائيّة ذات الصلة.[1]

الفرع الثاني: ضوابط اللجوء إلى إجراء المراقبة الالكترونية ومشروعيتها

يعتبر إجراء المراقبة الالكترونية إجراء خطيرا جداً باعتباره ينتهك أهم الحقوق المكفولة دستورياً وهي سريّة المراسلات والاتصالات، حيث أحاطها المشرّع الجزائري بجملة من الاعتبارات والضوابط التي تسمح القيام به والحدود التي يمكن أن نقف عندها حتى لا نصطدم بمسألة حقوق الإنسان وحرّياته.

اولا: حالات اللجوء إلى إجراء المراقبة الإلكترونية.

نصّت المادة 04 من القانون رقم 04/09[2] إلى الحالات التي إذا توّفرت يمكن فيها اللجوء إلى إجراء المراقبة الإلكترونية وهي كالتالي:

أ– الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسّة بأمن الدّولة، فهنا طبّق المشرع الجزائري مستوى من مستويات السياسة الجنائيّة وهو المستوى الوقائي على غرار المستويين التجريمي والعقابي.

ب – في حالة توفّر معلومات عن احتمال اعتداء على منظومة معلوماتيّة على نحو يهدّد النظام العام أو الدفاع الوطني أو مؤسسات الدّولة أو الاقتصاد الوطني.

ج– لمقتضيات التحرّي والتحقيقات القضائيّة عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

د– في إطار تنفيذ طلبات المساعدة القضائيّة الدوليّة المتبادلة.

[1] – براهيمي جمال، مرجع سابق، ص92-93.

[2] – المادة 04 من قانون04/09.

باستقراء الحالات المذكورة في المادّة رقم 04 من القانون رقم 04/09، يتبيّن لنا أنّ المشرع حصر الحالات التي يمكن اللجوء فيها إلى عمليّة المراقبة الالكترونيّة مثل اقتصارها على الجرائم التي تمس بالأمن الوطني وذلك لأنّه عندما يتعلق الأمر بالجرائم الإرهابيّة التي تطال المدنيين لا يمكن الحديث عن حقوق الإنسان وعن حق الشخص في الخصوصية لأنّ المصلحة العامّة في خطر بالإضافة كذلك إلى حالات المساعدة القضائيّة، إلاّ أنّ إضافة الحالة الواردة في الفقرة "ج" من المادّة الرابعة سالفة الذكر والمتعلقة بإمكانية اللجوء في كل قضيّة مستعصية إلى المراقبة الإلكترونيّة صغيرة كانت أو كبيرة يؤدّي إلى تعميم استخدام الآلية دون حد.

ثانيا: أطراف المراقبة الإلكترونية

لعبت الثورة التكنولوجية الحديثة في عصرنا الحالي، دورا بارزا في مراقبة المراسلات الالكترونيّة بوسائل تكنولوجيا الإعلام والاتصال المتطوّرة التي تتميّز بدقّة متناهية ومقدرة فائقة على مسافات بعيدة وبالتالي فهي تتطلب أطراف فيها كما يلي:

1- المُراقِب الالكتروني:[1]

هو ضابط الشرطة القضائيّة المكلف بمهمّة الذي يتتبّع المشتبه فيه بواسطة التقنية الإلكترونيّة على شبكة الانترنت، وتسند هذه المهمّة عادة إلى كل شخص يحسن الاستخدام الأمثل للحاسوب الآلي الرقمي ونظمه وبرامجه ووسائل الاتصال الإلكترونيّة الرقمية، وأن يكون الشخص المكلف بالمهمّة ملماً بالمهارات الالكترونية والتقنية لشبكة الانترنت، لكن هذه المهمّة في حد ذاتها تتطلب من الضابط المكلف بالعمليّة أن تتوافر فيه قدرات عالية ومواصفات معيّنة مثل طاقة الاستيعاب نظًار للكم الهائل من المعلومات والمعرفة المتزايدة على الشبكة العنكبوتيّة في كل لحظة وثانية حيث ينبغي عليه أن يتمتع بقراءة سريعة وفي أقل وقت ممكن مثل قراءة حوالي 1000 كلمة في الدقيقة الواحدة واستيعاب للمقروء بمعدّل يصل إلى 60% تقريبا والاحتفاظ بالمعلومات لمدّة أسبوع على شبكة الانترنت.

[1] - بن بادة عبد الحليم،ص395.

2- المُراقَب الالكتروني:

هو المشتبه فيه على الشبكة المتمثل في بعض المواقع من الانترنت والبريد الالكتروني وصفحات الفيسبوك وغيرها المخالفة للقانون بالإضافة لبعض الأشخاص المشتبه فيهم، أو أيّة جهة توضع تحت المراقبة ولا يمكن القيام بهذا الإجراء إلاّ بعد الحصول على إذن مكتوب ومسبّب ومحدّد المدّة بصرف النظر عن جنسيّة الهدف طالما أنّ عمل المشتبه فيه يضر بأمن البلاد ومصالحها[1]

[1] - مرجع سابق، ص396

خلاصة الفصل الثاني

من خلال ما تم التطرق اليه في هذا الفصل نجد انه المشرع الجزائري في محاولته مواكبة او عصرنة القوانين من اجل ان تحيط بجميع انواع الجرائم المنتشرة حيث انه وضع الية التسرب والتي وضحناها في المبحث الاول، من خلال مخاطرة عنصر من ممثلي امن الدولة(ضابط شرطة القضائية) داخل جماعة اجرامية ما تحت مراقبة و تسير محاولة منه لتفكيك تلك العصابة والحصول على الادلة الازمة، كما وضع المشرع اجراءات لهذا نوع من الالية وذلك لخطورتها على الشخص المكلف بالمهمة كما هو منصوص عليه في مواد 65مكرر15 الي 65مكرر18.

اما في المبحث الثاني فظهر وجوب ذكر الية او اجراء اعتراض المراسلات والمراقبة الالكترونية ومن خلال التسمية يتوضح لنا خطورة هذا الاجراء ليس من ناحية الجسدية او الامنية مثل التسرب وانما من الجانب المعنوي حيث ان اعتراض المراسلات يقصد الدخول في الحيز الشخصي لشخص او اشخاص معينة بهدف الحصول على ذلائل المثبتة للجريمة المقترفة وتكون دائما باذن من وكيل الجمهورية كما هو مشار اليه في المادة65مكرر05 و بمراقبة او باذن من قاضي التحقيق في حالة فتح التحقيق الجنائي، اما بالنسبة للمراقبة الالكترونية فتخضع لضوابط التي نصت عليها المادة 04 من قانون 09-04.

خاتمة

خاتمة

من خلال ما تم تطرق إليه في هذه الدراسة التي حاولنا تقديمها على فصلين لتوضيح سبب إعتماد المشرع لوسائل مستحدثة في مجال التحقيق في الجرائم الإلكترونية، حيث توصلنا إلى أن الوسائل التقليدية في البحث والتحري كانت غير كافية وغير متناسبة مع الجرائم المستحدثة أو الجرائم الإلكترونية وهذا ما أدى بالمشرع الجزائري إلى تعديل قانون الإجراءات الجزائية و إضافة القانون رقم 09-04 المتعلق أو متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، حيث تعتبر هذه الاجراءات جريئة من قبل المشرع الجزائري وذلك نظرا لخصوصيتها و مجال اعمالها خاصة فيما يخص اعتراض المراسلات و المراقبة الالكترونية وذلك باعتبارها مساس بمبدا الخصوصية.

وبناء على ما تقدم بالوسع تقديم جملة من الاقتراحات او توصيات المتمثلة فيما يلي:

نقترح ان يتم انشاء وحدة مستقلة خاصة بمكافحة الجرائم المعلوماتية مثل بعض الدول حيث يتكون افرادها من مختصين في المجال ويتم تكوينهم و تدريبهم على اعلى المستويات وهذا لاحترافية المجرمين واتلافهم للادلة وهذا الاخير يتطلب محققين محترفين.

نتمنى ان يتم عقد اتفاقية عالمية او اقليمية مشتركة بين العديد من الدول لتسهيل الاجراءات لكون الجرائم لما فيها من تطورات سريعة وطرق مختلفة.

ايضا ضرورة قيام المشرع الجزائري بتحديد و كشف الغموض فيما يتعلق بالمدة الزمنية اللازمة من اجل القيام بالمراقبة الالكترونية.

وفي النهاية نرى ان مجال بحثنا هذا نادر و قلّت فيه البحوث القانونية والعلمية نتمى ان نرى دراسات اعمق و بحوث واسعة في هذا المجال مستقبلا.

قائمة المراجع

Les Références

1- النصوص القانونية

- مرسوم رئاسي رقم 20-442 مؤرخ في 15 جمادى الاولى عام 1442 الموافق لـ 30ديسمبر سنة2020، يتعلق باصدار التعديل الدستوري، المصادق عليه في استفتاء اول نوفمبر 2020.

- قانون رقم 09-04 المؤرخ في 14شعبان عام1430 الموافق لـ 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

- قانون رقم06-22 مؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر سنة 2006، يعدل و يتمم الامر66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ8 يوليو سنة1966 والمتضمن قانون الاجراءات الجزائية.

- القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 ، يعدل ويتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

- القانون رقم 04-14 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 ، يعدل ويتمم للأمر رقم 66-155 المؤرخ في 18صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الاجراءات الجزائية.

2 – الاطروحات والمذكرات:

1- بشرى نزلي ، عادل لبيض ، اثبات الجريمة الالكترونية، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر، التخصص: قانون جنائي، جامعة قاصدي مرباح ورقلة، سنة 2017-2018،

2- حسين بن سعيد بن سيف الغافري, السياسة الجنائية في مواجهة جرائم الانترنت, رسالة لنيل شهادة الدكتوراه في القانون, كلية الحقوق, جامعة عين الشمس, القاهرة, 2005

3- حياة جبارة، ليدية حموم ، التسرب كآلية خاصة للبحث والتحري في الجرائم الخطيرة، مذكرة لنيل شهادة الماستر في القانون تخصص: القانون الجنائي والعلوم الإجرامية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو 2017-2018

4- جمال براهيمي, التحقيق الجنائي في الجرائم الإلكترونية, أطروحة لنيل شهادة الدكتوراه, قسم الحقوق, كلية الحقوق و العلوم السياسية, جامعة مولود معمري, تيزي وزو, 2018

5- خالد أمين بن نعوم, إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري,مذكرة لنيل شهادة الماستر, قسم الحقوق, كلية الحقوق و العلوم السياسية, جامعة عبد الحميد بن باديس, مستغانم, 2019

6- رفيـدة صاحبي، التسرب كألية لمكافحة الظاهرة الاجرامية، مذكرة مكملة لنيل شهادة الماستر في الحقوق تحصص قانون جنائي و علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي2018-2019،

7- سليمان بن مهجع العنزي, وسائل التحقيق في جرائم نظم المعلومات, رسالة لنيل درجة ماجستير في العلوم الشرطية, كلية الدراسات العليا, جامعة نايف العربية, الرياض,2003

8- عبد الرحمان هيان الرشيد غازي, الحماية القانونية من الجرائم المعلوماتية, رسالة لنيل درجة الدكتوراه في القانون, كلية الحقوق, الجامعة الإسلامية لبنان, 2004

9- نسيمة غانم, معمش زهية, , الإثبات الجنائي في الجرائم المعلوماتية,مذكرة تخرج لنيل شهادة الماستر في الحقوق, كلية الحقوق و العلوم السياسية, جامعة عبد الرحمان ميرة, بجاية, 2013

10- نورة طرشي, مكافحة الجريمة المعلوماتية , مذكرة لنيل شهادة الماجستير في القانون, كلية الحقوق و العلوم السياسية, جامعة الجزائر1, 2001

3-الكتب:

1- أحمد فتحي سرور, الوسيط في قانون الإجراءات الجنائية, دار النهضة العربية, الطبعة السابعة, , 1993,

2- جميل عبد الباقي الصغير, أدلة الإثبات الجنائي و التكنولوجيا الحديثة, دار النهضة,2001

3- خالد عياد الحلبي, إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت, دار الثقافة للنشر و التوزيع, عمان,الأردن, 2011

4- خالد ممدوح إبراهيم, فن التحقيق الجنائي في الجرائم الإلكترونية, دار الفكر الجامعي, الإسكندرية, 2009

5- رشيدة بوكر, جرائم الإعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن, منشورات الحلبي الحقوقية بيروت, لبنان, ط1, 2012,

6- عبد الفتاح بيومي حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الإنترنت, ط1, دار الفكر الجامعي, الإسكندرية, 2006,

7- عبدالله الهلالي, تفتيش نظام الحاسب الآلي و ضمانات متهم المعلومات دراسة مقارنة, د.ذ.د.ن, ط1, القاهرة

8- عبدالله حسين علي محمود, سرقة المعلومات المخزنة في الحاسب الالي, ط2 دار النهضة العربية, القاهرة, 2001

9- عفيفي كامل عفيفي, جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون, ط2, منشورات الحلبي الحقوقية, بيروت, لبنان, 2007

10- عمر محمد أبوبكر بن يوسف, الجرائم الناشئة عن إستخدام الانترنت الأحكام الموضوعية و الجوانب الإجرائية, دار النهضة العربية, القاهرة, 2004

11- نبيلة هبة هروال, الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة, دار الفكر الجامعي, الإسكندرية.

12- هدى حامد قشقوش, جرائم الحاسب الإلكتروني في التشريع المقارن, دار النهضة العربية, القاهرة, الطبعة الأولى, 1996.

4- المقالات:

1- جميلة محلق ، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، التواصل في الاقتصاد والإدارة والقانون عدد 42 ، كلية الحقوق والعلوم السياسية، جامعة باجي مختار عنابة، جوان 2015،

2- رحيمة لدغش, ضوابط تفتيش الحاسب الالي, مجلة الحقوق و العلوم الإنسانية, العدد25, المجلد الأول, جامعة الجلفة,

3- سعيد روابح ،كمال بوبعاية، الاساليب المستحدثة ضمن استراتيجية الكشف عن الجرائم المستحدثة في التشريع الجزائري "التسرب نموذجا"، دفاتر البحوث العلمية، المجلد 9، العدد1، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، مسيلة2021

4- سلمى مانع، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية, مجلة العلوم الإنسانية, العدد الثاني و العشرون, كلية الحقوق و العلوم السياسية, جامعة بسكرة, 2011

5- صالح شنين، التسرب في قانون الاجراءات الجنائية الجزائرية حماية للنظام العام والحريات أم حماية للنظام العام، المجلة الجزائرية للقانون المقارن، المجلد01، العدد02، جامعة عبد الرحمان ميرة، بجاية 2015

6- صالح شنين، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، المجلة الاكاديمية للبحوث، المجلد01، العدد 02، جامعة عبد الرحمان ميرة، بجاية، 2010

7- عبد الحليم بن بادة ، "المراقبة الإلكترونية كإجراء الاستخلاص الدليل الإلكتروني" بين الحق في الخصوصية ومشروعية الدليل الإلكتروني""، المجلة الأكاديمية للبحث القانوني، المجلد 10 ،العدد03 2019،

8- عزالدين عثماني, إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الإتصال و المعلوماتية, مجلة دائرة البحوث و الدراسات القانونية و السياسية, العدد الرابع, جامعة تبسة,2018

9- عزالدين وداعي ، التسرب كأسلوب من اساليب البحث والتحري الخاصة على ضوء قانون الاجراءات الجزائية والمقارن، المجلة الاكاديمية للبحث القانوني، مختبر البحث حول فعالية القانونية، المجلد 16، العدد الثاني، كلية الحقوق و العلوم السياسية، جامعة بجاية، الجزائر 2017،

10- علي عدنان الفيل, إجراءات التحري و جمع الأدلة و التحقيق الإبتدائيدراسة مقارنة, المكتب الجامعي الحديث,2012

11- عمر محمد أبوبكر بن يونس, الجرائم الناشئة عن إستخدام الانترنت, كلية الحقوق بجامعة المنصورة, 2004

12- عزيزة رابحي, التفتيش في نظم المعالجة الالية للمعطيات, قسم الحقوق, كلية الحقوق و العلوم السياسية, جامعة طاهري محمد, بشار

13- ليندا بن طالب, التفتيش في الجريمة المعلوماتية, مجلة العلوم القانونية و السياسية, العدد16, جامعة مولود معمري بتيزي وزو, الجزائر, 2007

14- ناجية شيخ ، اجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة، المعارف، المجلد13، العدد02، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو،2018

15- نادية آيت عبدالمالك, فلاح عبد القادر, التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري, مجلة الأستاذ الباحث للدراسات القانونية و السياسية, المجلد04, العدد الثاني, 2019

فهرس

الفهرس

المقدمة.....1-4

الفصل الاول: محدودية اجراءات التحقيق التقليدية

المبحث الاول: المعاينة والتفتيش في البيئة المعلوماتية..... 6

المطلب الاول: الانتقال الى المعاينة 7

الفرع الاول: مفهوم المعاينة.....7

اولا: تعريف المعاينة.....7

ثانيا: طبيعة واهمية المعاينة.....8

الفرع الثاني: نطاق اعمال المعاينة 9

اولا: معابنة مكونات الخاسب الالي.....9

ثانيا: معاينة انظمة الاتصال بشبكة الانترنيت.....11

المطلب الثاني: تفتيش في البيئة المعلوماتية.....11

الفرع الاول: مفهوم التفتيش.....12

اولا: تعريف التفتيش..... 12

ثانيا: خصائص واهداف التفتيش..... 14

ثالثا: اهمية التفتيش.....15

الفرع الثاني: محل التفتيش.....16

اولا: تفتيس الاشخاص والاماكن.....16

ثانيا:تفتيش المكونات المادية للحاسب الالي.....18

ثالثا: تفتيش المكونات المنطقية للحاسب الالي 20

رابعا: تفتيش شبكات المعلومات المتصلة بالحاسب الالي 22

الفرع الثالث: ضوابط التفتيش 24

اولا: الشروط الموضوعية 24

ثانيا: الشروط الشكلية 25

المبحث الثاني: ضبط الادلة و ندب الخبير.....27

المطلب الاول: ضبط الادلة 27

الفرع لاول: مفهوم ضبط الادلة 27

اولا :تعريف الضبط.....27

ثانيا: الطبيعة القانونية و محل الضبط.....28

الفرع الثاني: مدى صلاحية ضبط الادلة في الجرائم الالكترونية.....29
اولا: ضبط المكونات المادية والمعنوية للحاسب الالي.....29
ثانيا: ضبط الرسائل ومراقبة الاتصالات الالكترونية.....30
المطلب الثاني: ندب الخبير.....31
الفرع الول: مفهوم الخبرة.....31
اولا: تعريف الخبرة القضائية.....31
ثانيا: تعيين خبير.....32
ثالثا: اهمية الخبرة و مجالاتها في الجريمة المعلوماتية.....33
الفرع الثاني: الجوانب الفنية للخبرة الالكترونية.....34
اولا: تقنيات الخبرة الالكترونية.....34
ثانيا: الوسائل العلمية لانجاز الخبرة الالكترونية.....35
خلاصة الفصل الاول.....39

الفصل الثاني: ضرورة اعتماد الاليات المستحدثة

المبحث الاول: التسرب و حفظ افشاء المعطيات 42
المطلب الاول: التسرب 42
الفرع الاول: مفهوم التسرب.....43
اولا: تعريف التسرب.....43
ثانيا: صور التسرب. 44
الفرع الثاني: شروط عملية التسرب.....45
اولا: الشروط الشكلية 45
ثانيا: الشروط الموضوعية.....47
المطلب الثاني: حفظ و افشاء المعطيات.....49
الفرع الاول:حفظ معطيات السير.....50
اولا:مفهوم حفظ معطيات السير.....50
ثانيا: ضمانات المشتبه فيهم اثناء عملية حفظ معطيات السير.....51
الفرع الثاني: افشاء العاجل لمعطيات السير.....52
المبحث الثاني: اعتراض المراسلات و المراقبة الالكترونية.....52
المطلب الاول: اعتراض المراسلات والتسجيل الصوتي و التقاط الصور.....53

فرع الاول: تعريف اعتراض المراسلات والتسجيل الصوتي والتقاط الصور.....53
اولا: تعريف اعتراض المراسلات 53
ثانيا: تعريف التسجيل الصوتي و التقاط الصور.....54
الفرع الثاني: شروط عملية اعتراض المراسلات.....54
اولا: الشروط الشكلية.....54
ثانيا: الشروط الموضوعية.....56
المطلب الثاني: المراقبة الالكترونية.....57
الفرع الاول: تعريف المراقبة الالكترونية 58
الفرع الثاني ضوابط اللجوء الى اجراء المراقبة الالكترونية.....59
اولا: حالات اللجوء الى المراقبة الالكترونية.....59
ثانيا: اطراف المراقبة الالكترونية.....60
خلاصة الفصل الثاني.....**62**
خاتمة.....**63**
قائمة المراجع.....**65-69**

الملخص

لا شك أن التطور التكنولوجي و الإنتشار الواسع لمواقع التواصل الإجتماعي المنفتحة قد أدى لظهور نمط إجرامي آخر غير مألوف، حيث برزت خطورة هذا الإجرام في تطوره السريع والخصائص التي يتميز بها عن الجرائم التقليدية، ومع ظهور هذه الجرائم الإلكترونية أدى بالمشرع الجزائري الى إستحداث مجموعة من الإجراءات التحقيق والتحري إضافة إلى الإجراءات التقليدية، و سلطة مختصة من أجل مكافحة هذه الأخيرة و ردع المجرمين وذلك لأنها تختلف عن الجرائم التقليدية لكونها ترتكب في العالم الافتراضي.

الكلمات المفتاحية: جريمة الالكترونية، التحقيق الجنائي، التفتيش، الآليات المستحدثة للتحقيق،التطور التكنولوجي، مواقع التواصل الاجتماعي، التحقيق والتحري.

Sommaire

Il ne fait aucun doute que le développement technologique et la large diffusion des sites de réseaux sociaux ouverts ont conduit à l'émergence d'un autre modèle criminel inconnu, car la gravité de ce crime est apparue dans son développement rapide et les caractéristiques qui le distinguent des crimes traditionnels, et avec l'émergence de ces crimes électroniques a conduit le législateur algérien à développer un ensemble de procédures d'investigation en plus des procédures classiques, et une autorité compétente afin de combattre ces dernières et dissuader les criminels, car elles se distinguent des crimes classiques parce qu'elles sont comites dans le monde virtuel.

Mots-clés : criminalité électronique, enquête criminelle, inspection, nouveaux mécanismes d'investigation, le développement technologique, des sites de réseaux sociaux, procédures d'investigation .

Summary

There is no doubt that the technological development and the wide spread of open social networking sites have led to the emergence of another unfamiliar criminal pattern, as the seriousness of this crime has emerged in its rapid development and the characteristics that distinguish it from traditional crimes, and with the emergence of these electronic crimes led the Algerian legislator to develop a set of procedures Investigation and investigation in addition to the traditional procedures, and a competent authority in order to combat the latter and deter criminals, because they differ from traditional crimes because they are committed in the virtual world.

Keywords: electronic crime, criminal investigation, inspection, new investigation mechanisms, the technological development, social networking sites, of procedures Investigation.