وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي– تبسة–
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة لنيل شهادة المـاستر في
القانون الجنائي والعلوم الجنائية
الموسومة بـــ

التفتيش الالكتروني

إعداد الطالب:
عمار جباري

إشراف الأستاذ:
سايح بوساحية

لجنة المناقشة

الاسم و اللقب	الدرجة العلمية	الجامعةالاصلية	الصفة العلمية
عز الدين عثماني	استاذ محاضر ـ أ ـ	جامعة تبسة	رئيسا
سايح بوساحيـة	استاذ محاضر ـ أ ـ	جامعة تبسة	مشرفا و مقررا
منير بوراس	استاذ محاضر ـ أ ـ	جامعة تبسة	عضوا مناقشا

السنة الجامعية: 2023/2022


بسم الله الرحمن الرحيم

﴿ وَمَا تَكُونُ فِي شَأْنٍ وَمَا تَتْلُو مِنْهُ مِنْ قُرْآنٍ وَلا تَعْمَلُونَ مِنْ عَمَلٍ إلا كُنَّا عَلَيْكُمْ شُهُودًا إِذْ تُفِيضُونَ فِيهِ وَمَا يَعْزُبُ عَنْ رَبِّكَ مِنْ مِثْقَالِ ذَرَّةٍ فِي الأَرْضِ وَلا فِي السَّمَاءِ وَلا أَصْغَرَ مِنْ ذَلِكَ وَلا أَكْبَرَ إلا فِي كِتَابٍ مُبِينٍ (61) أَلَا إِنَّ أَوْلِيَاءَ اللَّهِ لَا خَوْفٌ عَلَيْهِمْ وَلَا هُمْ يَحْزَنُونَ (62) الَّذِينَ آمَنُوا وَكَانُوا يَتَّقُونَ (63) لَهُمُ الْبُشْرَىٰ فِي الْحَيَاةِ الدُّنْيَا وَفِي الْآخِرَةِ ۚ لَا تَبْدِيلَ لِكَلِمَاتِ اللَّهِ ۚ ذَٰلِكَ هُوَ الْفَوْزُ الْعَظِيمُ (64) وَلَا يَحْزُنْكَ قَوْلُهُمْ ۘ إِنَّ الْعِزَّةَ لِلَّهِ جَمِيعًا ۚ هُوَ السَّمِيعُ الْعَلِيمُ(65) ﴾

الآيات من سورة يونس

شكر وعرفان

الشكر إلى بهجة العمر ونور الحياة والدتي يا من علمتني العطاء دون انتظار المقابل...

الشكر إلى ذلك الصرح العظيم الذي علمني أبي صاحب الفضل الكبير...

و لا يسعننا إلا أن نتقدم بوافر الشكر والتقدير

إلى الأستاذ المشرف الدكتور سايح بوساحية

الذي أكرمنا بالإشراف على هذا العمل، و أفاض علينا بعلمه وجهده وتصوياته القيمة والتي أنارت لنا الدرب في سبيل إتمام هذه المذكرة فكان خير معين وأفضل سند...

كما اتقدم بالشكر الخاص للجنة الموقرة التي انظمت تحت جناح هذا العمل العلمي لمناقشته و سهرت على تقديم الملاحظات القيمة

لتقويمه و دعمه...

الي الجوهرة الراقية القابعة تحت انوار الثرى

الى الحكمة الباقية في انفسنا وان تلاشت في الورى

الى الروح الزكية بمعالم اخلاقها الراقية في معالم السنى

الى طيبة الانوار الساطعة بظلالها الماحية لظلام الدجى

الى قدوة الصبر و الرضا بما سطرته مكامن السدى

الى الروح الزكية التي تقبع في جنة المأوى

الى الريحانة أخي سمير

مقدمة

المقدمة

أدي التطور الفكري و المعرفي بفضل الثورة العلمية التكنولوجية في مجال الاتصالات و المعلومات التي اقتحمت بقوة مختلف الابعاد الاقتصادية، الاجتماعية، الثقافية، و العلمية التي وفرت مناخا خصبا لنهضة علمية تكنولوجية شاملة تهاوت أمامها الحدود السياسية و الحواجز بين الدول ، بما تتميز به من عنصري السرعة والدقة في تجميع المعلومات، تخزينها ومعالجتها، ومن ثم نقلها او تبادلها.

و بالنظر الى أن عالم الجريمة المعلوماتية له خصوصيتها التي تميزها بالنظر للبيئة الرقمية التي تحيط بمقومات هذا النوع من الإجرام ، وله خطورته التي تصعب عملية الاكتشاف والإثبات، مما أدى بالمجتمع الدولي لإرساء نصوص دولية بهدف مكافحة الجريمة الإلكترونية، مع إدراك الصعوبة التي تطرحها المواجهة الإجرائية لأشكال الاجرام الجديد التي أفرزتها بيئة المعالجة الآلية للمعطيات، بدأت تحظى باهتمام المشرع الجزائري باستحداث تقنية التفتيش الالكتروني، و اصداره القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وكرس هيئات تقنية و خبراء في المجال المعلوماتي.

كما ساير المشرع الجرائم ذلك بوضع إستراتيجية شملت استحداث نصوص قانونية خاصة كفيلة بالحد من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من جهة، وتعديل النصوص القانونية السارية المفعول بما يتناسب مع هذا النوع من الجرائم ، مع إعطاء أهمية عملية لمكافحة الجريمة المعلوماتية عن طريق إرساء أجهزة وهيئات أسندت لها ذات المهمة، خاصة الهيئة الوطنية المكلفة بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، دون إغفال الدور الفعال للجهاز الأمني في هذا المجال، من خلال تسخر جهودهم و تجاربهم العملية لسد ثغرات الأنظمة الأمنية وتحسين و تطوير أساليب و ضمانات لمنع وقوع اعتداءات الاجرامية و تطبيق النصوص الاجرائية التي تمكن الجهات المختصة من البحث و التحقيق واستنباط دليل يتوافق مع الطبيعة التقنية للجرائم.

هذه تحولات ألزمت المشرع الجزائري بضبط التفتيش الالكتروني كأداة لمجابهة جرائم أنظمة المعلوماتية التي تعد آلية تقنية للمعالجة و الاتصال و فن تتجلي من خلاله التطورات التي عرفتها الدولة الجزائرية في مجال الجريمة المعلوماتية ، ونظرا لخصوصتها كونها ترتكب في بيئة افتراضية رقمية، فإنه بات من الضروري تطوير أساليب التحقيق الجنائي بصورة تتلاءم مع طبيعتها، وتمكن جهات التحقيق من كشف الجريمة.

و هذا ما سعى المشرع لتكريسه من خلال استحداث قواعد إجرائية تتفق و الطبيعة التقنية للجريمة المعلوماتية، و يعد التفتيش الالكتروني إحدى هذه الاجراءات التي حددها القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومن ثم تحقيق التوازن بين الضرورة الملحة للاستفادة من التقنيات وتكنولوجيات الحديثة، و بين الحاجة الفردية و الاجتماعية الى الحماية الجزائية من انعكاساتها الاجرامية.

الغرض من وراء البحث في الموضوع

تكمن أهداف البحث موضوع التفيش الالكتروني في الاطلاع على آليات و اجراءات المستحدثة لمواجهة الجرائم المعلوماتية ، لم تنل حظها من البحث والتحقيق والمحاكمة على المستوى الجزائي حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها، لاسيما أن هذا الموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها.

تتجلى اهداف التفتيش الالكتروني و التحقيق في مجال الإجرام السبيراني و كيفية اثباته في التشريع الجزائري بإصدر المشرع الجزائري للقانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال باعتباره قانون اجرائي خاص في مجال مكافحة هذا النوع من الجرائم و إيجاد طرق اجرائية ذات طبيعة تقنية تتلاءم معها.

ان الغرض من دراسة الموضوع معرفة الاسس آليات التحري الخاصة التي نص عليها المشرع في مجال التحقيق والإثبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من خلال تعديل قانون الاجراءات الجزائية.

تسعى هذه الدارسة إلى الوقوف على اغراض النصوص والأحكام القانونية المنظمة لإجراء التفتيش الالكتروني ومعرفة مدى فعاليتها في التصدي للجريمة المعلوماتية و الحد من خطورتها المتزايدة من خلال الكشف عن الأدلة و الوصول إلى مرتكبيها.

اهمية من وراء البحث في الموضوع

نظرا للأهمية البالغة التي تكتسيها مكافحة الجريمة المعلوماتية وما فرضته من تحديات خاصة في عصرنا الحالي الذي يعرف تطورا سريعا في مجال تكنولوجيات الإعلام والاتصال و ما تفرضه من مستلزمات تحدد الادوار التي تلعبها الجهات المختصة لحماية الامن و مكافحة الجرائم المعلوماتية.

تتمثل الاهمية من الدراسة الاجرائية في الوقوف على طرق التفيش الإلكتروني و آلياته القانونية في اطار التعاون الدولي للحد من الجرائم المعلوماتية و ضبط الاصول المرتبطة بتحديد نطاقه و الوظائف التي تقوم بها الجهات المعنية بعمليات التفتيش.

كما تتمثل اهمية دراسة موضوع التفتيش الالكتروني في الاطلاع على المستجدات المرتبطة بالجريمة المعلوماتية ودور التفتيش الالكتروني كدليل رقمي يقدم امام القضاء يحدد إجراءات المتابعة و يكشف الحقيقة و ينوير القاضي عند الفصل في النزاع القضائي.

الاطلاع على الجرائم المعلوماتية حديثة و امتداد تأثيرها إلى جميع الأصعدة المرتبطة بتطور تكنولوجيا الإعلام والاتصال ، الامر الذي يعقد اجراءات التفتيش الالكتروني إذ تجعل التعاملات معها صعبا مما يحتم إيجاد طرق جديدة للبحث في محل الجريمة.

معرفة إجراءات المعاينة والتفتيش الالكتروني والحجز داخل المنظومة المعلوماتية، ومراقبة الاتصالات الإلكترونية وحفظ المعطيات ، من خلال الوقوف على خصوصية الجريمة المعلوماتية من الناحية الإجرائية من خلال اعتمادنا على قانون الإجراءات الجزائية الجزائري، وكذا القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

المنهج المتبع في معالجة الموضوع

اعتمدنا في دراستنا هذه على المنهج التحليلي، الوصفي، كونها الأنسب لمثل هذه الدراسات من خلال تحليل مختلف المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة المعلوماتية من خلال معالجة النصوص والأحكام القانونية المنظمة لإجراء التفتيش الإلكتروني واختلافها عن النصوص الإجرائية التقليدية

كذا تم اعتماد المنهج الوصفي لمختلف الاتفاقيات الدولية والعربية من أجل مكافحة هذا النوع من الإجرام المعلوماتي و الهيئات المساعدة عل تكريس وظائف التفتيش الالكتروني، بالإضافة الى وصف الاجراءات التي تعتمدها الجهات المختصة لتنفيذ التفتيش الالكتروني.

الدوافع لاختيار البحث في الموضوع.

تتمثل الأسباب الشخصية لدراسة موضوع التفتيش الالكتروني في اهتمامي بمجال الجريمة المعلوماتية و ما ترتبه من آثار وكذا الاهتمام بمعرفة الإجراءات الخاصة للمتابعة التي تختلف عن إجراءات المتابعة في الجرائم التقليدية.

كما ان اهتماماتي تنصب حول تثمين حداثة موضوع الدراسة بالنظر لطابع الجدة ، ورغبتي الشديدة في التعمق المعرفي في مجال إجراءات التفتيش الالكتروني ، والوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحية الإجرائية.

أما الأسباب الموضوعية فتكمن فيما يطرحه موضوع التفتيش الالكتروني من ضمانات حماية إجرائية لمحل التفتيش و التزام السر المهني عند الاطلاع ، بالإضافة الى إشكاليات قانونية لا بد من الوقوف نظرا لحداثة الموضوع المتعلق بتجريم الافعال او الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات وفقا للقانون 04/09.

و من بين الأسباب الموضوعية لاختيار الموضوع محل الدراسة ظهور الإجرام المعلوماتي الذي أثار العديد من المشاكل خاصة الإجرائية في مجال الجريمة المعلوماتية باعتبار صعبة الكشف عنها و متابعة مرتكبها و لا يتم ذلك الا بمراعاة ضوابط التفتيش الالكتروني

الدراسات المرجعية السابقة.

سعى المشرع الجزائري لاتخاذ الخطوات التشريعية الضرورية لمواجهة الجرائم الالكتروني عن طريق سن نصوص قانونية تتوافق مع هذه الانشطة الإجرامية الحديثة، لقد تطرقت عدة دراسات السابقة الي الجرائم

المعلوماتية من الناحية الموضوعية فقط ،مع وجود بعض الدراسات التي تطرقت لها من الناحية الاجرائية لكن ليست بالتفصيل الامر الذي جعلها قاصرة ومن بين هذه الدراسات التي تم الاعتماد عليها في موضوع الدراسة.

الصعوبات العلمية في معالجة الموضوع

إن التفتيش الالكتروني يطرح العديد من الصعوبات بالنظر لمرونة الجريمة المعلوماتية الامر الذي يتطلب من السلطات بجميع مستوياتها تحديات قانونية خاصة خلال عملية البحث والتنقيب من اجل كشف الحقيقة، و بالنظر لجدة الموضوع لاحظنا قلة المراجع في هذا الجانب ، فنجد معظمها تتناول الجريمة المعلوماتية و اجراءات التحقيق ، وحاولنا من خلال المراجع استنباط الاحكام المتعلقة بالتفتيش الالكتروني و ضماناته و احكامه الاجرائية واهميته كدليل رقمي يقدم امام القضاء.

أصل التاريخي للموضوع.

ترجع الظروف التاريخية للموضوع و تطوره الى زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية فقد مكنت طرق المعالجة الآلية للمعطيات المجتمعات من تجاوز فكرة الحدود الإقليمية نظرا لكون التكنولوجية أو الجريمة هي عابرة للحدود، مما تطور معه الاجرام المعلوماتي الذي يفرض على الانظمة القانونية لإيجاد الفواصل التي تحول دون تطور الجريمة ، لذا يعد التفتيش الالكتروني آلية اجرائية لمواجهة الاجرام المعلوماتي وهذا ما كرسه القانون04/09.

الإشكالية.

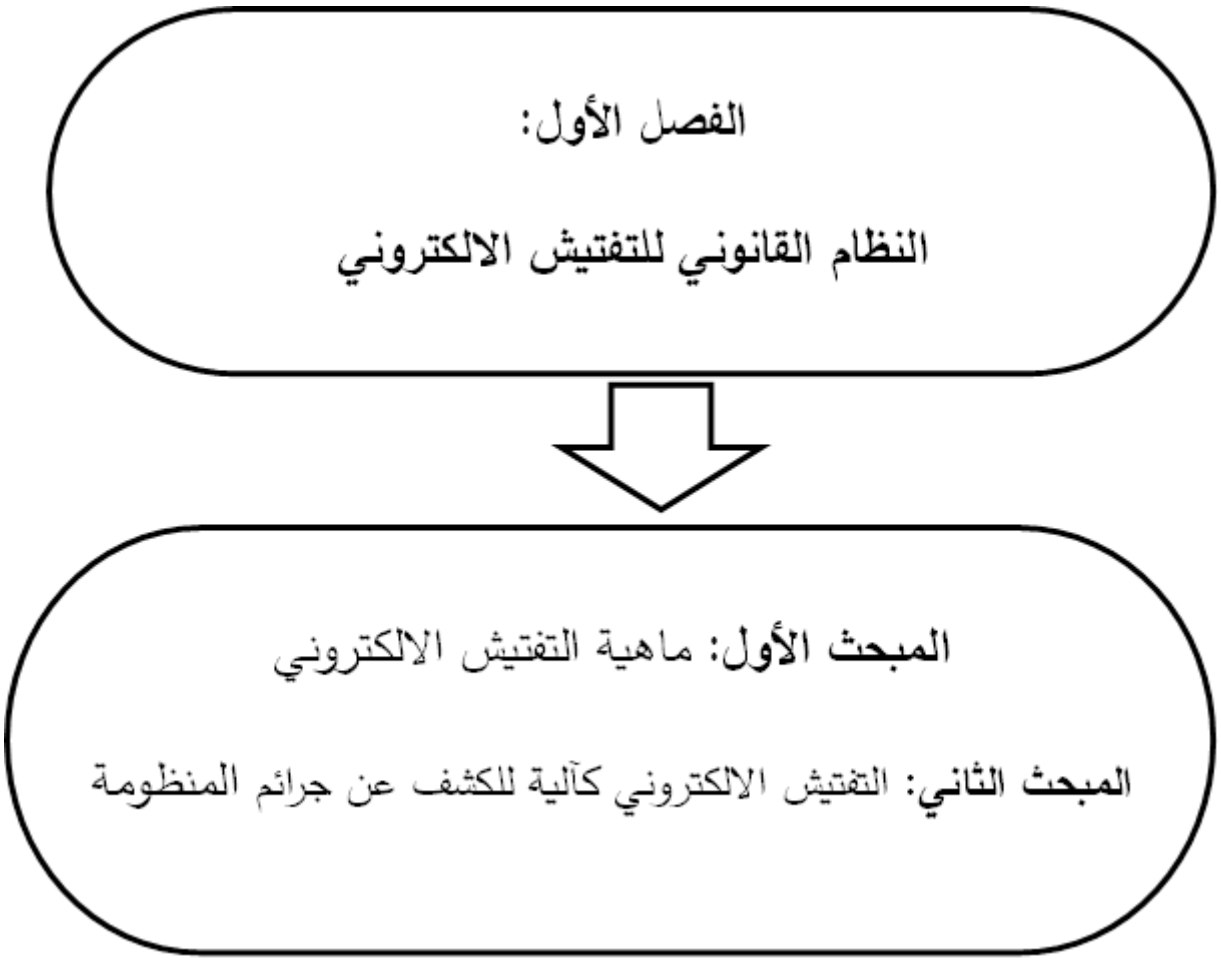
و بناءا على المعطيات السابقة لدراسة موضوع التفتيش الالكتروني تم الاعتماد على إشكالية يمكن صياغتهـا وفقا لمايلي

ما هي ضوابط وآليات تكريس التفتيش الالكتروني في الجرائم المعلوماتية ؟

الخطة المتبعة في موضوع الدراسة.

من خلال الفصلين تم الوقوف على الأحكام الموضوعية و الإجرائية الخاصة بالتفتيش الالكتروني من خلال قيام الجهات المختصة بالإجراءات التفتيشية لمتابعة مرتكبي الجرائم المعلوماتية من أجل إقرار هذه الحماية وفقا لخطة تضمنت في الفصل الاول: النظام القانوني للتفتيش الالكتروني مقسمة الى ابعاد ثنائية بحيث عالجت في المبحث الاول: ماهية التفتيش الالكتروني لحص مضمونه في ثلاثة مطالب ، المطلب الاول تناول مفهوم التفتيش الالكتروني و تناولنا في المطلب الثاني: الابعاد القانونية للتفتيش الالكتروني. اما المطلب الثالث فعالجنا المقتضيات المتعلقة بشروط التفتيش في البيئة الالكترونية. اما المبحث الثاني فتناول ثلاثة المطالب، تناولت في المطلب الاول: أنظمة التفتيش في المنظومة المعلوماتية، اما المطلب الثاني فعالجت فيه آليات التفتيش الدولية لمكافحة جرائم المنظومة المعلوماتية.

اما الفصل الثاني فخصصته للأحكام الاجرائية للتفتيش الالكتروني تضمن مبحثين ، تناولت في المبحث الاول: الجهات المختصة بالتفتيش الالكتروني وقسمته الي ثلاثة مطالب ، تناولت في المطلب الاول: الاختصاص النوعي للتفتيش الالكترونية ، اما المطلب الاول فعالجت فيه موضوع الاختصاص المكاني للتفتيش الالكتروني، كما تطرقت في المطلب الثالث الي التفتيش الالكتروني كآلية لحجز الادلة الرقمية وجمعها ، اما المبحث الثاني فخصصته لموضوع الضمانات القضائية للتفتيش الالكتروني، قسمته الى ثلاثة مطالب ، تناولت في المطلب الاول: الضمانات السابقة للتفتيش الإلكتروني، اما فيما يتعلق بالمطلب الثاني فعالجت فيه الضمانات اللاحقة للتفتيش الالكتروني، اما المطلب الثالث فخصصته لموضوع حجية الدليل المستخلص من التفتيش الالكتروني.


الفصل الأول:
النظام القانوني للتفتيش الالكتروني
المبحث الأول: ماهية التفتيش الالكتروني
المبحث الثاني: التفتيش الالكتروني كآلية للكشف عن جرائم المنظومة

الفصـل الاول:النظام القانوني للتفتيش الالكتروني.

ان التطورات الرقمية المتسارعة الحديثة اثرت على الجرائم المعلوماتية باعتبارهـاتعدي على حقوق و الحريات العامة، الا ان للجرائم الإلكترونية ميزة كونها جرائم لها آثارهـا على سلوك الجاني، والتعامل مع الجريمة الالكترونية التي تعد تحديا امام السلطات التحقيقية اثناء عمليات التفتيش الالكتروني على الرغم من قلة التجارب التحقيقية والوسائل البرمجية، باعتبار ان التفتيش الالكتروني آلية لكشف ملابساتها ومعالمها و لذا يتطلب وجود خبراء وفنيين في مجال الكشف عنهـا ، بتكريس ضوابط قانونية وتعاون دولي من اجل مواكبة التطورات الحاصلة في منظومة الجرائم المعلوماتية، وعليه سيتم معالجة الموضوع وفقا للخطة الآتية:

المبحث الأول: ماهية التفتيش الالكتروني.

المبحث الثاني: التفتيش الالكتروني كآلية للكشف عن جرائم المنظومة المعلوماتية.

المبحث الأول: ماهية التفتيش الالكتروني

يعد التفتيش الالكتروني من أخطر إجراءات التحقيق المقررة في الجرائم المعلوماتية وذلك لمساسه بالحريات الخاصة المكفولة دستوريا، وخطورة ما يسفر عنه من أدلة تؤدي إلى كشف الحقيقة عن الجريمة التي وقعت باستخدام إحدى الأنظمة المعلوماتية[1]، و بناءا عليه فإن دراستنا لإجراءات التفتيش الالكتروني تقتضي التطرق لتحديد مفهومه مقتضياته القانونية ، و عليه سيتم معالجة الموضوع وفقـا للخطة الآتيـة:

المطلب الأول: مفهـوم التفتيش الالكتروني.

المطلب الثاني:الابعاد القانونية للتفتيش الالكتروني.

المطلب الثالث: شروط التفتيش في البيئة الالكترونية.

المطلب الأول: مفهوم التفتيش الالكتروني.

نظم المشرع الجزائري إجراء التفتيش الذي لا يتلاءم وصور الجريمة التقليدية التي يمكن إدراكها بالحواس من خلال الآثار المادية المتروكة في مسرح الجريمة كالبصمات و الأوراق مزورة ....، إلا أن الأمر يختلف بالنسبة للجريمة المعلوماتية بالنظر لما يعترض التفتيش من مشكلات إجرائية تتمثل أساسا في البيئة التقنية التي ترتكب فيها الجريمة و التي لا تخلف آثارا مادية محسوسة بالإضافة إلى سهولة تدمير الدليل ومحوه.

الفرع الاول: تعريف التفتيش الالكتروني.

أمام العقبات و الإشكاليات التي تعترض إجراء التفتيش في البيئة الافتراضية تدخل المشرع من خلال القانون04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال

[1] – **د/أحمد السيد عفيفي** ،الاحكام العامة للعلانية في قانون العقوبات(دراسة مقارنة)، دار النهضة العربية، القاهرة، طبعة 2002،(ص).69

و محافحتها، لوضع ضوابط وإجراءات تتلاءم وطبيعة الجريمة المعلوماتية ، من هذا المنطلق جاءت هذه الدراسة لتسلط الضوء على التفتيش في البيئة الالكترونية، بتحديد مفهومه و أصوله التشريعية و التنظيمية لمعرفة حدوده و ضماناتـه.

اولا: تعريف التفتيش الالكتروني.

تتعدد و تختلف المفاهيم الفقهية للتفتيش الالكتروني بالنظر الى ابعاده المختلفة و تعدد مجالاته من حيث اختلاف الجرائم او تنوع مصادرها ، لذا استحدث المشرع الجزائري منظومة قانونية بمقتضى القانون رقم 04/09 ، اكتفى بتنظيم أحكامه وضوابطه تاركا تحديد مفهومه للفقه و القضاء، وبالرجوع إلى التعريفات الفقية فإنه يقصد بالتفتيش بوجه عام" البحث عن أشياء تفيد في الكشف عن جريمة وقعت ونسبتها إلى المتهمين و اعداد اجرءات التحقيق التي تهدف إلى البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المحددة"[1].

وبالنظر لاختلاف الاحكام التي تضبط التفتيش الالكتروني فقد عرفه بعض الفقهاء بأنه" الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، يستوي في ذلك أن يكون هذا المحل حيازة الحاسب الآلي أو أنظمة أو شبكة الانترنت"[2].

ثانيا : الاصول القانونية للتفتيش الالكتروني.

أحدثت التكنولوجيات في مجال تقنيات الحاسوب والاتصال تغييرات جذرية انعكست آثارها على تغيير نظام الجرائم المعلوماتية (Cyber Crimes) فهي جرائم يصعب حصرها، وتستهدف الاعتداء على البيانات والمعلومات والبرامج و نظم التشغيل و الأنظمة المعلوماتية، وشبكات الاتصال وقواعد البيانات[3]، مما يتطلب ضرورة توفيـر وسائل حديثة و إجراءات خاصة للجهات القضائية لمحاربة هذه النوع من الجرائم ومن ثمة ينصب التفتيش على الكيان المادي للحاسوب (Hardware) و هي الأشياء الملموسة من أجزائه التي

1- د/**أسامة عبد الله قايد**،الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، طبعة 1994،(ص).56.

2- **د/علي عدنان الفيل**، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، طبعة 2012،(ص).39.

3- **د/خالد ممدوح إبراهيم** ، الجرائم المعلوماتية ، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، طبعة 2009 ،(ص). 06.

تعد تقنية مادية تتكامل وظائفهاالآداء مهمة في المعالجة الآلية للبيانات، إذ يمكن ضبطها و حجزها وفقا للقواعد التقليدية للتفتيش[1].

ولكن تبرز الصعوبة حينما نكـون بصدد تفتيش وحجـز المكونات المعنويـة أو المنطقيـة للحاسوب (Software) كالبرامـج والمنظومات المعلوماتيـة وقواعد البيانات...الخ، وهذا ما عالجه المشرع الجزائري بموجب نصوص القانون رقم04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعـلام والاتصـال ومكافحتهـا، كمـا عـزز هذا الاتجاه بالمصادقة على نصوص الاتفاقية العربيـة لمكافحة جرائـم تقنية المعلومات المحـررة بالقاهـرة بتاريخ21 ديسمبر2010[2].

و يلاحظ ان المشرع الجزائري لم يضع تعريفا للتفتيش فقد اعتبره إجراء من اجراءات التحقيق الهدف منه الحصول على الأدلة لإثبات الجريمة للوصول للجاني، لكن بالمقابل أحاطه بجملة من الضوابط الصارمة لما يترتب عنه من مساس بحرية الأشخاص و كرامتهم و حرمة ممتلكاتهم[3]، وفقا لنص المادة 47 من التعديل الدستوري الجزائري" لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي".

يتضح من نص المادة ان المشرع يعاقب على كل انتهاك لهذه الحقوق و الحريات و هذا ما تؤكده المادة48 من التعديل الدستوري" تضمن الدولة عدم انتهاك حرمة المسكن. فلا تفتيش إلا بمقتضى القانون و في إطار احترامه.لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة". و هذا ما اكده المشرع في المـواد مـن 44 إلى47 و المادة 64 إضافة إلى المـادة 79 وما بعدها من قانون الإجراءات الجزائية، ولكن بالنظر لخطورة الجرائم المعلوماتية فان المشرع الجزائري اجاز تقييد الحقوق الدستورية بموجي تعديلات قانون الاجراءات الجزائية والقانون رقم 04/09 حتى لا يتحكم الجاني في تغيير الدليل و تظليل جهات التحقيق.

1- **د/علي حسن محمد الطوالبة**، التفتيش الجنائي عن نظم الحاسوب و الانترنيت، عالم الكتب الحديث الاردن، طبعة 2004،(ص).10.

2- راجع المرسوم الرئاسي رقم252/14 المؤرخ في 2014/09/08، الجريدة الرسمية رقم57، الصادرة بتاريخ 2014/09/28.

3 - **أ/ زيدان زيبحة**، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة، الجزائر، طبعة 2011 ،(ص).130.

الفرع الثاني : مميزات التفتيش في المنظومة المعلوماتية الالكترونية.

يعد التفتيش الالكتروني من اهم الاجراءات التي تباشرها سلطات البحث والتحقيق في مواجهة الجريمة المعلوماتية ، من خلال وضع المشرع آليات و اجراءات تتناسب و خصوصية الطبيعة المميزة للجريمة، من حيث ارتكابها على مسرح الكتروني يختلف عن المسرح التقليدي فالتفتيش اجراء صعب بالنظر الى طبيعة الدليل المتحصل منه ، و الذي يسهل اخفاءه و تدميره لذا التفتيش في الأنظمة الإلكترونية يحتاج الى معرفة علمية و فنية تتناسب مع خصوصيته.

ثانيا: خصائص التفتيش الالكتروني من حيث الابعاد القانونية.

بالنظر لخصوصية التفتيش الواقع على المنظومة المعلوماتية ، و تعقيده يستلزم الأمر توضيح خصائصه ومميزاته التي تعطيه نسقا وظيفيا خاصا التفتيش يتضمن تحديد ابعاده، و انظمته القانونية.

01- من حيث نطاق التفتيش الالكتروني.

بالنظر للظروف التي تقع فيها الجريمة المعلوماتية و حيزها اللامحدود فاضحى التفتيش ينطوي على قدر من الجبر والإكراه للاطلاع على البيانات والمعلومات الإلكترونية و كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام وسيلة تقنية المعلومات، وبوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات وغيرهـا.

و ما دام الإكراه عنصر أساسي في التفتيش لما يحمله من اكراه ولكنه مشروع من الناحية القانونية للكشف عن الجرائم ، فهو تعرض قانوني لحرية المتهم الشخصية و يشكل قيدا على حرمة أسراره الشخصية الموجودة على جهز حاسوبه الخاص او على برامج خاصة به او على بريده الالكتروني عبر شبكة الانترنت[1].

02- من حيث السلطات التي تباشر التفتيش الالكتروني.

لمصلحة المجتمع، تباشر الشرطة العلمية المتخصصة في حدود اختصاصها و جهات التحقيق القضائي مباشرة اجراءات التفتيش ، أو ما كلفها به القانون، مع تكريس الضمانات القانونية سواء رضي به من بوشر حياله، أم لا، فالسلطات المختصة تتخذ ما تضمن به تنفيذه عند عدم الاستجابة ، إذ أن تفتيش الشخص يستلزم تقييد حركته المدة اللازمة لإجراء التفتيش مما قد يستتبع الالزامية في الحدود القانونية ، من جانب الشخص المطلوب تفتيشه وللبحث عن الأدلة المادية للجريمة[2].

---

[1]- **د/ علي حسن الطوالبة**، المرجع السابق،ص.13

2- **د/أحسن بوسقيعة** ،التحقيق القضائي، الطبعة الثانية ، دار هومه، الجزائر ، طبعة 2012 ،(ص).83

03- من حيث مجال التفتيش الالكتروني.

ينطوي التفتيش على تعرضه لحرية المتهم الشخصية أو حرمة أسراره الموجودة على جهاز الكمبيوتر ذاته أو على برامج خاصة به أو على بريده الإلكتروني او على شبكة الأنترنت،لان الجريمة الإلكترونيـــة تتمثل في أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون.

ثانيا: خصائص التفتيش الالكتروني من حيث الاسس القانونية.

01- من حيث وسائل التفتيش الالكتروني.

يمتاز التفتيش الالكتروني بأنه وسيلة للبحث عن الأدلة المادية و المعنوية للجريمة و ضبطها كما يفيد الكشف عن الحقيقة باستخدام تقنية المعلومات، أي وسيلة مادية أو غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة ، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلت والمخرجات المرتبطة بها سلكية أو لاسلكية في نظام معلوماتي أو شبكة معلوماتية[1].

02- من حيث مجال التفتيش الالكتروني.

ينصب التفيش من حيث خصوصياته على الوظائف المعلوماتية ، فتعد الشبكة المعلوماتية ارتباط بين أكثر من وسيلة تقنية للمعلومات، للحصول عليها وتبادلها، بما في ذلك الشبكات الخاصة والعامة والشبكة العالمية "الإنترنت" و المواقع الإلكترونية باعتبارها مكان إتاحة أو معالجة البيانات أو المعلومات الإلكترونية على الشبكة المعلوماتية من أجل الكشف عن الادلة المادية والمعنوية للجريمة وضبطها[2].

و من خلال القانون رقم 04/09حاول المشرع تحديد الابعاد التي ينصب عليها التفتيش الالكتروني من خلال اعطاء بعض المفاهيم الاصطلاحية وفقا لنص المادة 02 منه" يقصد في مفهوم هذا القانون مايلي:

- الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال: جرائم المساس بانظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة اخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية.

---

[1] - يلاحظ في هذا المقام أن المشرع القطري توسع في ذكر المفاهيم المتعلقة بالجرائم الإلكترونية فكان أكثر دقة في التعبير عن المفاهيم و شرحها= انظر **د/طارق ابراهيم الدسوقي عطية،** الموسوعة الامنية الامن المعلوماتي،النظام القانونية لحماية المعلوماتية، دار الجامعة الجديدة للنشر،الاسكندرية، طبعة 2015 ،(ص).240

2 - **د/آمال عبد الرحيم عثمان،** شرح قانون الاجراءات الجنائية،دار النهضة العربية ، القاهرة، (بدون تاريخ الطبعة)،ص.62

– **منظومة معلوماتية:** أي نظام منفصل او مجموعة من الانظمة المتصلة ببعضها البعض او المرتبطة، يقوم واحد منها او اكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

– **معطيات معلوماتية:** أي عملية عرض للوقائع او المعلومات او المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

– **مقدمو الخدمات:**

– أي كيان عام او خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/او نظام للاتصالات.

– و أي كيان آخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال او لمستعمليها.

– **المعطيات المتعلقة بحركة السير:** أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الاخيرة باعتبارها جزءا من حلقة الاتصالات توضح مصدر الاتصال و الوجهة المرسل اليها و الطريق الذي يسلكه ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة.

– **الاتصالات الالكترونية:** أي تراسل او ارسال او استقبال او اشارات او كتابات او صور او معلومات مختلفة بواسطة أي وسيلة الكترونية.

03– من حيث طبيعة التفتيش الالكتروني.

إن التفتيش إجراء من إجراءات التحقيق و ليس من اجراءات الاستدلال و لانه يتم باذن لضبط الشرطة القضائية من جهات التحقيق المختصة و هذا ما اجمع على ذلك الفقه الجنائي كما أنه إجراء مفاجئ لا يحاط المتهم باجراء تفتيشه أو تفتيش منزله مسبقا لكي لا يبادر إلى التخلص من الادلة[1]، التي تتضمنها منظومة المعلومات ، فالتفتيش إجراء تحقيقي، وقد يباشر بهدف الحفاظ على الأدلـة.

الفرع الثالث: الطبيعة القانونية للتفتيش وصوره.

بالرغم من الاجماع الفقهي حول تكييف التفتيش الالكتروني بأنه إجراء تحقيقي يتضمن القيام بعمل معين من أجل الحصول على أدلة الجريمة الالكترونية تمهيدا لممارسة حق المجتمع في العقاب ، بوصفه عملا إجرائيا فهو واقعة قانونية يرتب عليها القانون آثارا إجرائية ، لذا فهو إجراء تقوم به السلطة القضائية بقصد الكشف الحقيقة.

1 – **د/ سامي الحسيني**، النظرية العامة للتفتيش في القانون المصري و المقارن ،دار النهضة العربية، القاهرة، طبعة 1980ص.85

أولا:التكييف القانوني للتفتيش الالكتروني.

تعددت آراء الفقهاء حول طبيعة التفتيش وظهرت أربعة اتجاهات مختلفة لتكييف الطبيعة القانونية للتفتيش الالكتروني:

1-الاتجاه الأول: يأخذ اصحابه في تحديد الطبيعة القانونية للتفتيش الهدف منه ، لانغاية الاجراء الحصول على الادلة و ضبطها و كشف حقيقتها و ازالة الغموض ، و ترجيح نسبتها الى شخص محدد مثل ضبط برامج غير مشروعة على جهاز حاسوب المتهم، و تقديمها ضده كألة اثبات أمام القضاء[1].

02- الاتجاه الثاني: ذهب أنصار هذا الرأي إلى وقت التفتيش، حسب المرحلة التي تكون فيها الدعوى الجزائية، فإذا ما تم التفتيش قبل فتح التحقيق كان من أعمال الاستدلال بينما يعد عملا من أعمال التحقيق إذا جرى بعد فتح التحقيق الابتدائي[2].

03- الاتجاه الثالث: وينظر أنصار هذا الاتجاه إلى التفتيش الالكتروني من زاوية صفة القائم به ، فيعتبر التفتيش من إجراءات التحقيق إذا قامت به سلطة التحقيق ، غير أن هذا الاتجاه تم انتقاده على أساس أن المشرع لا يعتد بصفة القائم بالإجراء خاصة في حالتي الندب والتلبس حيث يقوم به عناصر الضبطية القضائية ورغم ذلك يبقى من أعمال التحقيق[3].

04-الاتجاه الرابع: يأخذ هذا الاتجاه بالمعيار المختلط ، فيسعى اصحاب هذا الرأي الى التوفيق بين الاتجاهات السابقة، فيعد التفتيش من إجراءات التحقيق متى اتخذته سلطة التحقيق بعد تحريك الدعوى العمومية بقصد الكشف عن الحقيقة، وبالتالي يتضمن الإجراء ثلاثة معايير حسب الغاية، الوقت والقائم بالإجراءات[4].

وقد أخذ القضاء الجزائري بالمعيار المختلط وذلك حسب قرار الغرفة الجنائية بالمحكمة العليا في شأن التفتيش بقول" لأن الأمر بالتفتيش لا يمنع البحث واكتشاف أشياء أخرى ....، إن إجراء التفتيش يتم طبقا للمادة 47 من قانون الإجراءات الجزائية والمادة 64 من قانون الإجراءات الجزائية ، ان إبطال التفتيش وما تلاه من إجراءات خطأ ينجز عنه نقض القرار"[5].

---

[1] - **د/هلالي عبد اللاه أحمد** ، حجية المخرجات الكمبيوترية في الاثبات الجنائي، الطبعة الاولى، دار النهضة العربية ، القاهرة، ص.46

[2] - **أ/فاروق الكيلاني**، محاضرات في قانون أصول المحاكمات الجزائيةالاردني و المقارن(الجزء الثاني)،دار الفارابي عمان ،طبعة 1980،ص398.

3 - **د/أحمد المهدي**، القبض والتفتيش والتلبس، الطبعة الأولى، دار العدالة، القاهرة،مصر، طبعة 2007،(ص).95

4 - **أ/يوسف دلاندة** ، قانون الإجراءات الجزائية، دار هومه، الجزائر، طبعة2001،(ص).46

5- قرار المحكمة العليا، رقم 165609، الصادر بتاريخ 1997/07/30، المجلة القضائية، العدد الثاني، لسنة 1997 ،(ص). 250

ثانيا: أسس الطبيعة القانونية للتفتيش الالكتروني المنصب على الجرائم المعلوماتية.

انطلاقا من التعريفات السابقة، يتبين لنا أن التفتيش الإلكتروني **هو إجراء تحقيقي** يستهدف ضبط أدلة الجريمة مثل البرامج الغير المشروعة والملفات المخزنة في الحواسيب والمعطيات المعلوماتية والاتصالات الالكترونية.

01-الاتجاه الأول يرى أن المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ، إلا في ضوء حقوق الملكية الفكرية، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة، ما لم تكن مسجلة على اسطوانة أو شريط ، تثور المشكلة عندما نكون أمام سرقة مال معلوماتي غير مادي[1].

02-الاتجاه الثاني يرى أن المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للستحواذ مستقلة عن دعامتها المادية ، على سند من القول أن المعلومات لها بيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وأنها ترتبط كما يقول الأستاذان "Catala و Vivant" أن المعلومات مال قابل للتملك أو الاستغلل على أساس بنيته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال[2].

وبالتالي فان الجرائم المعلوماتية لها خصوصية ترتكز على جوانب معنوية في البناء الوظيفي للانشطة الاجرامية و يجسده كيان مادي يمكن الاستحواذ عليه يتضمن البرنامج والمعلومات، واستطرد أصحاب هذا الاتجاه في القول بأنه طالما أن موضوع الحيازة غير مادي فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادية، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر[3] التي تتم بناءا عليها عمليات التفتيش الالكتروني.

و بالتالي فالتفتيش يرتبط ببيانات معالجة بصفة الكترونية و كيانات يصعب الكشف عنها ، و يثير التفتيش في مجال أنظمة الاتصال الإلكترونية ضرورة وضع ضوابط اجرائية تعمل على إقامة التوازن بين الحرية الفردية و حرمة الحياة الخاصة و تطبيق الفاعلية أثناء عملية التحقيق[4]. و عليه انقسم الفقه إلى اتجاهين لتحديد الطبيعة القانونية للجريمة الإلكترونية محل التفتيش.

---

[1]- **د/مفتاح بوبكر المطردي**، (الجريمة الإلكترونية)، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، مجلة القانون السودان العدد22، طبعة 2012، ص17، تم الدخول للموقع بتاريخ 2023/03/28 http://swideg-geography.blogspot.com/2017/08/blog-post_html على الساعى 15.30

[2]- **د/محمد عبد الله سلمة**، موسوعة الجرائم المعلوماتية، الطبعةالاولى، المكتب العربي الحديث،الاسكندرية، مصر، طبعة2007،ص.ص.43-44

3- **د/هدى حامد قشقوش**، جرائم الحاسب الالكتروني في التشريع المقارن ،دار النهضة العربية ، القاهرة،طبعة 1992، ص.ص.51-52

4 - **د/رضا هميسي**،(تفتيش المنظومات المعلوماتية في القانون الجزائري)، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، العدد 05، جوان 2012،(ص).159

المطلب الثاني: الابعاد القانونية للتفتيش الالكتروني.

إن 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.

الفرع الاول: الاساس القانوني للتفتيش الالكتروني.

تعد الجريمة المعلوماتية من الجرائم المستحدثة التي برزت في الوقت الراهن نتيجة تطور تقنية المعلومات واستغلالها على نحو غير مشروع وبوسائل من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، ونظرا لخصوصية هذه الجريمة كونها ترتكب في بيئة افتراضية رقمية، فإنه بات من الضروري تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن جهات التحقيق من كشف الجريمة والتعرف على مرتكبيهـا.

اولا:الاساس الدولي للتفتيش الالكتروني.

إن لامتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي أهمية في إمكانية الحصول على دليل عن بعد ، إلا أن بعض الفقه يتحفظ على القيام بذلك لأنه يعتبر انتهاك لسيادة الدولة الأجنبية، وإذا اقتضت ضرورة التحقيق القيام بذلك ينبغي مراعاة العديد من الضمانات يكون متفقا عليها سلفا عن طريق اتفاقيات ومعاهدات في هذا المجال، وهذا ما يؤكد أهمية التعاون الدولي في مكافحة الجرائم الإلكترونية[1].

و مع التطور التكنولوجي لثورة الاتصالات لم يعد نطاق الاتصالات محدودا في إقليم دولة واحدة، بل امتد ليشمل كل أرجاء العالم وذلك بعد ظهور شبكة الإنترنت وهي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعضها البعض بطريقة لا مركزية، ويدخل في تركيب هذه الشبكة ملايين الحواسب الموزعة عبر مختلف دول العالم.

وعليه يتضح أن طبيعة التكنولوجيا الرقمية عقدت التحدي أمام أعمال التفتيش والضبط، بسبب امتداد الأدلة الإلكترونية عبر شبكات الحاسوب[2] ، و في أماكن بعيدة عن الموقع المادي للتفتيش، وإن امكن الوصول إليها من خلال الحاسوب بعد أخذ إذن تفتيشه، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، وهو ما يزيد المسألة تعقيدا باعتبار أن الشبكة المعلوماتية ممتدة في أرجاء

---

1 - **Roger Merle et Andre Vitu**, traite de droit criminel, Tome2, quatrième édition, édition Cujas, Paris, 1989, p 57.

2 – **هلالي عبد اللاه احمد**، اتفاقية بودابست لمكافحة جرائم المعلوماتية ، الطبعة الاولى، دار النهضة العربية ، طبعة 2007،(ص). 76

العالم تقريبا. وبالتالي فإن الحاسوب الذي يمكن أن ترتكب عليه أو بواسطته الجريمة المعلوماتية يخضع للقانون الإجرائي الخاص بتلك المنطقة[1].

ثانيا: الاساس القانوني للتفتيش الالكتروني.

ان البحث في الاساس القانوني للتفتيش الالكتروني باعتباره اجراء من اجراءات التحقيق و احاطته بضوابط قانونية بالنظر الى اثره في الكشف عن الجريمة و اساس تستند عليه جهات التحقيق لكشف الجرائم وكما اوضحنا سابق يعد مبررا للمساس بحريات الاشخاص.

01- الاساس القانوني للتفتيش في القانون رقم 04/09

سعى المشرع الجزائري إلى محاربة الجرائم المعلوماتية من خلال استحداث نصوص قانونية جديدة أوجد جسد بمقتضاها قواعد إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية، ويعتبر التفتيش الالكتروني إحدى هذه الإجراءات التي حملها القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

كما نجد المشرع الجزائري أجاز تمديد التفتيش وذلك في نص المادة 05 الفقرة الثانية من القانون 04/09 " بأنه في حالة التفتيش 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 ، ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك ".

و يلاحظ ان المشرع الجزائري أخذ نفس مسار المشرع الفرنسي حيث أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، وهذا ما نصت عليه المادة 05 فقرة الثالثة من القانون رقم 04/09 "... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل".

02- الاساس القانوني للتفتيش في قانون الاجراءات الجزائية.

يلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم22/06 في المادة 45 الفقرة الخامسة منه، استغناؤه على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

---

[1]- **Vergucht Pascal**, La répression des délits informatiques dans une perspective internationale, thèse, Montpelier, 1996, p.63

والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني ، خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه حتى عن بعد. كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي تأخذ بنظام التفتيش عن بعد، أو ما يطلق عليه الفقه الفرنسي" التفتيش على المباشر"[1].

الفرع الثاني: الوظائف القانونية للتفتيش الالكتروني.

بالنظر للتطورات التي عرفتها الجريمة الالكترونية و تفاقم الظاهرة الاجرامية و ما رتبته من اعتداءات جعلت المشرع الجزائري ينظم آلية اجرائية تتناسب و طبيعة هذه الجرائم و تلعب دورا وظيفيا في متابعة الجرائم و البحث في مستودع الحقيقة عن أدلة الجريمة التي تتميز بنظامها الالكتروني،فإذا كان إجراء التفتيش لا يستهدف هذه الغاية فلا يعد تفتيشا بالمعنى المقصود في القانون و لا يؤدي الوظيفة التي حددها المشرع في حسن سيرورة اجراءات المتابعة ، و التفتيش بهذا المعنى تختلف صوره و تتعدد الوظائف التي يحققها.

اولا: الوظيفة الوقائية للتفتيش الالكتروني.

ترتبط عمليات التفتيش اللالكتروني بأسس وظيفية يرسم لها المشرع الجزائري من اجل تفعيل اجراءات المتابعة ودعم التعاون مع جهاز العدالة بالنظر الي الطبيعة الخاصة للجرائم المعلوماتية وصعوبة ضبط نطاقها من اتساع مجالاتها، باعتبار ان وسيلة الاعتداء مبرمجات الحواسيب و الشبكات الالكترونية.

01-وظائف التفتيش التقني الوقائي.

ضبط المشرع الجزائري نجاح اجراءات التفتيش الالكتروني بوظائف تدعيمية للنظام القضائي من خلال الرقابة الوقائية لبيئة الانترنت بحيث يتمتع بصفة الضبطية الادارية مزودي الدخول وخدمات الانترنت بحيث منحهم المشرع صلاحية الرقابة على سير حركة المنظومة المعلوماتية و اخضاعها للقانون و النظام من قبل المتعاملين مع الانترنت ، و تتم اجراءات التحفظ على الادلة الى غاية حضور رجال الضبطية القضائية[2].

و أكد المشرع الجزائري على أنه في حال الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس من الدولة، تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة لإعلام والاتصال ومكافحتها حصر إجراءات التفتيش. كذلك يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة أثناء ممارستهم لوظائفهم أو بمناسبتها، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، لا سيما قانون

1- **أ/عائشة بن قارة مصطفى**، حجية الدليل الإلكتروني في مجال الإثبات الجنائي (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، طبعة 2009،(ص). 54

2 - **د/هروال نبيلة هبة** ، الجوانب الاجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ،دار الفكر الجامعي، طبعة 2007،(ص).87

الإجراءات الجزائية ،تفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمها أنه يحوز و/أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية[1].

02- التفتيش بمقتضى النصوص القانونية.

قد يجبر القانون أحيانا إجراء تفتيش إداري لمنع وقوع الجريمة ، و هذا ما يمليه القوانين،كنص المادة 05 من القانون 04/09 الفقرة 04" يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث او التدبير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها و تزويدها بكل المعلومات الضرورية لانجاز مهمتها".

ومن ثمة تسهر الجهات المخصة على آداء التفتيش الالكتروني لوظائفه من خلال المعرفة التقنية للقائمين باعمال التحري و المباشرين للتحقيق في مجال الجرائم المعلوماتية من خلال التدريب على كيفية تشغيل الحواسيب و التدريب الجيد على نظمها الشبكية لاكتساب مهارات و معارف تتعلق بالبرمجة و المعالجة المعالجة الالكترونية للبيانات[2].

ثانيا وظائف التفتيش بحكم الضرورة.

ان النظم و الملفات تعد الوعاء الحقيقي لادلة الادانة او البراءة في الجرائم المعلوماتية ، و بالنظر لما تحتوية من تعقيدات معلوماتية الامر يستدعي التفتيش إذا كانت الضرورة الملحة تقتضي ذلك، جاز الاستناد إلى هذا الدليل في إدانة المتهم، حيث يعتبر دليل ناتج عن إجراء مشروع وهذا ما تؤكده المادة 03 من القانون رقم لقانون04/09" مع مراعاة الاحكام القانونية التي تضمن سرية المراسلات و الاتصالات ، يمكن لمقتضيات النظام العام او لمستلزمات التحريات او التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الاجراءات الجزائية و في هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام باجراءات التفتيش داخل منظومة معلوماتية".

المطلب الثالث: شروط التفتيش في البيئة الالكترونية.

ترتبط المتغيرات الخاصة بنظام المعلوماتية بميزات تجعل اجراءات المتابعة اكثر دقة و موضوعية بالنظر لاهميتها في كشف الادلة ، بحيث يتكون هذا الاخير من وحدات الإدخال والإخراج والذاكرة و أخرى غير معنوية وتتمثل في البرامج، البيانات والمعلومات ، و يعترض التفيش صعوبات ترتبط ببراعة الجاني في تغيير

---

[1] – راجع المرسوم الرئاسي رقم 261/15 المؤرخ في 8 أكتوبر سنة 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 53، الصادرة في 08 أكتوبر سنة 2015 .

2- **أ/علي عدنان الفيل**، اجراءات التحري و جمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية(دراسة مقارنة)،المكتب الجامعي الحديث العراق، طبعة 2011،(ص). 22

الادلة محل التفتيش او اذا النظام يتمع بحماية فنية تحول دون الولوج الي البيانات و تفتيشها، كما ان المشرع يسعى من خلال هذا الاجراء الى احترام الضمانات التي تكرسها القواعد الدستورية،لذا ضبطه بقيود.

الفرع الاول: سبب التفتيش في البيئة الإلكترونية.

ان الثورة التكنولوجية ادت الى تنوع وسائل الاتصال و تاثيرها على مجالات متعددة مما ادى الى اتساع نطاق العلاقات و كثرة الاجرام الذي يمثل سبب التفتيش في المنظومة المعلوماتية للوصول الى الحقائق محل التفتيش ، كما لم يعد نطاق الاتصالات محدودا في اقليم دولة واحدة بل امتد ليشمل كافة ارجاء العالم ،الامر الذي استلزم توقيع المشرع لاتفاقيات دولية لضبط الجرائم و مرتكبيها عبرشبكات الاتصال، و تحديد شروط التفتيش الالكتروني.

أولا: وقوع جريمة معلوماتية.

الجريمة المعلوماتية هي كل فعل غير مشروع مرتبط باستخدام حواسيب الكترونية لتحقيق اغراض غير مشروعة،ويعتبر التفتيش من الإجراءات الهامة في الدعوى الجزائية باعتباره إجراء من إجراءات التحقيق الابتدائي،الذي يساعد كدليل مادي مهم في الكشف الجرائم، و لا يتم ذلك الا وفقا لمراعاة القيود التي حددها المشرع و احترام خصوصيات محل التفتيش، مع التقيد بالاجراءات المرتبطة بالاذن القضائي .

و الجدير بالذكر أنه لا محل لإصدار الإذن بالتفتيش إلا إذا كان المشرع قد نص على الجرائم التي تشكل اعتداء على المعلومات في شكل نصوص التجريم و العقاب تطبيقا لمبدأ الشرعية ، وهذا ما دأبت عليه الكثير من التشريعات و منها التشريع الجزائري الذي حدد بموجب القانون04/21 المؤرخ في 28 ديسمبر2021 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات[1] الذي حدد بعض الجرائم المعلوماتية ، وعزز المشرع هذه الحماية بموجب القانون رقم 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها.

ثانيا: قيام الاتهام بارتكاب الجريمة المعلوماتية أو المشاركة فيها.

ينبغي ان تتوفر في حق الاشخاص المراد تفتيشهم دلائل كافية تدعو للاعتقاد بانهم ساهموا في ارتكاب الجريمة المعلوماتية سواءا بصفتهم فاعلين او شركاء، من خلال وجود دلائل كافية تمثل المضمون العقلي و المنطقي لملابسات الواقعة التي تؤدي الى نسبة الجريمة المعلوماتية اليهم بصفتهم فاعلين او شركاء[2].

ومن ثمة فالجرائم المعلوماتية يرتكبها الشخص بصفته فاعلا او شريكا ، و يكون محلها اجهزة حواسيب باعتبارها نظام معالجة كهربائي سريع و دقيق يستخدم في تداول البيانات و مصمم لتقبل و تخزين البيانات

---

[1] – راجع المواد من 394 مكرر الى غاية المادة 394 مكرر 08 من القانون 04/21 المؤرخ في 28 ديسمبر 2021 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات.

2 – **أ/ علي عدنان الفيل**، المرجع السابق،(ص). 50

ومعالجتها و اعطاء المعلومات وفقا لبرنامج التخزين الذي يتكون من مجموعة اوامر[1]، او يتم ارتكابها في شبكة الحواسيب التي تعرف على انها"مجموعة مكونة من اثنين او اكثر من اجهزة الحاسوب و المتصلة ببعضها اتصالا سلكيا او لا سلكيا"[2]

ثالثا : توافر إمارات وقرائن تفيد في كشف الحقيقة.

لا يوجد تفتيش الكتروني الا اذا توافرت لدى المحقق اسباب كافية على وجود جريمة معلوماتية او لدى الشخص المراد تفتيشه ادوات استخدمت في الجريمة،الامر الذي يتطلب إصدار سلطة التحقيق قرارها بالتفتيش ومباشرته بوقوع جريمة معلوماتية، و يتم بالانتقال الى مسكن امتهم او الاماكن التي تتواجد فيها الاجهزة المقصودة حال حيازة الحاسوب الآلي او احد مكوناته المادية كوسائط التخزين(الاقراص الصلبة او المرنة، الاشرطة الممغنطة...) ، و ايضا اجاز المشرع تفتيش المنظومة المعلوماتية عن بعد ، والولوج للكيان المنطقي للمنظومة المعلوماتية لأن هدف التفتيش ينصب على مسائل معنوية وفنية ليست مادية كالبرامج و قواعد البيانات باعتبارها وسيلة ارتكاب الجريمة او تخزين معلومات بشأنها[3].

و عليه فإن الدلائل الكافية شرط ضروري لاتخاذ إجراء التفتيش الذي يتضمن مساسا بحرمة الشخص أو مسكنه و هي الضمان الوحيد في التشريع الجزائري الذي يقي الأفراد من الوقوع كضحايا لإجراءات تعسفية. إذا اقتضت الضرورة اكتشاف جرائم أخرى عن طريق الصدفة بمناسبة تفتيش الملفات المخزنة ، و حتى لايغير الجاني الدليل تدخل المشرع الجزائري و نص على جواز التفتيش في كل الملفات الموجودة في النظام المعلوماتي[4].

رابعا: وجود إذن بالتفتيش الإلكتروني.

الاذن بالتفتيش الالكتروني يعد سببا لمباشرة اجراءات المتابعة والاطلاع على محل الجريمة يفيد في كشف الحقيقة وفقا للضوابط التي نص عليها المشرع عند التفتيش عن الأدلة الالكترونية في المنظومات المعلوماتية ، و يمنح من الجهات القضائية الى اجهزة ضبط الجرائم و المتمثلة في ضباط الشرطة القضائية و التي تتولى مهمة مباشرة جمع الاستدلالات و التحري في العالم الافتراضي[5].

و لا يتم تفتيش محل الجريمة إلا بمقتضى اذن تمنحه السلطات القضائية المختصة لتفتيش الاماكن و الحواسيب و الاطلاع على السجلات المستخدمة في عملية الولوج الى النظام الآلي لمعالجة البيانات مؤخوذ

---

1 – **د/هدى حامد قشقوش**، المرجع السابق،(ص). 18

2– د/**علي حسن محمد الطوالبة**، التفتيش الجنائي على نظم الحاسوب والانترنت(دراسة مقارنة)،عالم الكتاب الحديث،اربد، الاردن،طبعة 2004،(ص). 34

3– **أ/زيبحة زيدان** ، المرجع السابق، ص.ص.132–135

4 -**أ/نبيلة هبة هروال** ، المرجع السابق،(ص). 246

5 – المرجع نفســـه ،(ص). 90

من بيئة رقمية تعد مجالا حيويا ضخما يمكنها من تخزين مليارات المعلومات و الملفات ، وأمام كثرة الملفات فلا يعقل إصدار إذن بالتفتيش حسب عدد الملفات ، ومن ثمة فالإذن بالتفتيش لا يمكن أن يمتد إلى كافة الملفات لأنه ليس إذن مطلق بل هو مقيد بالغرض منه وهذا ما تؤكده معظم التشريعات الجزائية .

ويلاحظ انه لاجراءات اذن تنفيذ التفتيش الواقع على نظم الحاسوب والانترنت خصوصية تميزه عن الاجراءات التقليدية تنبع من دقة التعامل مع الاجهزة والبرامج التي يتضمنها،لذا يجب على الجهات المعنية باذن التفتيش اتخاذ اجراءات و تحريات دقيقة وفقالمايلي:

– تحديد نوع النظام المراد تفتيشـــه.

– الاعداد الجيد لعملية التفتيش من خلال التقييم العام للوضع الشامل حتى لا يتم افلات الدليل من التفتيش.

– يجب على الجهات القائمة بالتفتيش اخذ الاحتياطات اللازمة لقدرة المتهم على الدخول عن بعد الى النظام عن بعد من خلال جهاز الاتصال الوسيط.

– التحكم في عملية الدخولالى الاجهزة و الولوج الى الانظمة المعلوماتية و الحرص على عدم اتلاف الدليل و الحفاظ عليه، مع الاستعانة بعمليات التصوير لتوثيقعمليات التفتيش الالكتروني[1].

و يتبين من خلال موضوع الدراسة أن المشرع في جل القوانين التي نص فيها على اذن التفتيش حاول حماية خصوصية الأفراد بما فيها البيانات و المعلومات الشخصية و كذلك السجلات و الدفاتر أو الحاسبات الآلية والملحقات السرية بعدم جواز الإطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون، فالمعلومة التي يحظر الاطلاع عليها لا بد أن تتسم بالسرية، فإذا لم تكن كذلك، فهي مكشوفة و مجال حركتها غير محدد بمجموعة من الأشخاص ، وتكون قابلة للتداول ، فلا يمكن عندئذ الحديث عن الاعتداء عليها بالاطلاع عليها دون وجه حق[2].

الفرع الثاني: محل التفتيش في البيئة الالكترونية.

اشترط المشرع الجزائري لصحة التفتيش ان يكون مسببا ،باعتباره اجراء من إجراءات البحث والتحقيق ويهدف الى البحث عن ادلة مادية لجناية او جنحة تحقق وقوعها بمكان او شخص يتمتع بالحرمة، فلا تفتيش الا بمقتضى القانون.

و الغرض من محل الجريمة هو الحصول على الدليل وحجزه وفقا للمقتضيات القانونية و هذا ماتؤكده المادة 06 من القانون رقم04/09"عندما تكتشف السلطةالتي تباشرالتفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبها وانه ليس من الضروري حجز كل المنظومة،يتم نسخ

1 – **د/ علي حسن محمد الطوالبة**، المرجع السابق،،(ص). 59

2- **نجاة لوصيف، موسي مرمون**، (مبادئ و ضوابط المعالجة الآلية للمعطيات الشخصية)،مجلة العلوم الانسانية، جامعة بسكرة ، المجلد 33، عدد02 جوان 2022،(ص). 83

المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجزو الوضع في احراز وفقا للقواعد المقررة في قانون الاجراءات الجزائية".

اولا: تحديد محل التفتيش في البيئة التقنية.

بالنظر الى حداثة الجرائم المعلوماتية واتصالها بانظمة تكنولوجية معقدة من حيث الاساليب والادوات المستعملة في تنفيذها، الامر الذي استدعى تغييرأسلوب عمل أجهزة البحث و التحقيق، و إذ فرض عليه التعامل مع محل جريمة مسرحه غير معتاد يقع في عالم افتراضي، وفي بيئة تقنية تتطلب مهارات و قدرات و تقنيات خاصة قد لا تتوفر معظم هذه الأجهزة مما فرض عليها اعتماد فرق متخصصة و متكونة في مجال تقنيات المعلوميات ورصدها لمكافحة هذه الجرائم[1].

وعليه محل التفتيش يشمل كافة اجراءات التفتيش المنظومة المعلوماتية لكل ملف من الملفات المخزنة حتى وان كان الاجراء يحدث مساسا بالحريات الشخصية لذا احاطته التشريعات بضمانات ، و الهدف من ذلك تحقيق الموازنة بين مصلحة المجتمع في العقاب و بين حقوق الافراد و حرياتهم ، لذا اجاز خرق الخصوصية من خلال العمليات التفتيشية[2].

- ثانيا: الاشخاص كمحل للتفتيش في النظام المعلوماتي.

يساهم تفتيش الاشخاص في الاطلاع على المستودع الذي يحتفظ بسر الجريمة ، فالشخص المراد تفتيشه لديه او لدى غيره ادوات استخدمت في جريمة من جرائم الاعتداء على نظم المعالجة الآلية او اشياء متحصلة او مستندات او دعامات تفيد في كشف الحقيقة[3].

و على هذا الاساس تتعدد المحال و لا تكون قائمة بذاتها بل تكون موضوعة في مكان ما كالمسكن او المكتب او تكون صحبة مالكها او حائزها ، قد يكون من مالكي او مستخدمي الكمبيوتر أو من خبراء البرامج سواء كانت برامج نظام أو تطبيقات، وقد يكون من المحللين أو من مهندسي الصيانة و الاتصالات أو من مديري النظم المعلوماتية، أو أي أشخاص آخرين قد تكون بحوزتهم معدات و أجهزة معلوماتية أو أجهزة حاسب آلي محمولة متصلة بجهاز المودم، و أمتعته التي كانت في حوزته ، حتى و ان كان متنقلا بها باعتبارها من توابعـه[4].

1- **د/سعيد محمد**، الجرائم الإلكترونية و آليات الحصول على الدليل فيها، الطبعة الأولى ، دار النشر الذهبي ، الاردن ، طبعة 2005،(ص).53.

2- **د/ علي حسن الطوالبة**،المرجع السابق،(ص). 46

3- **أ/رشيدة بوكر**،جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن،الطبعة الاولى،منشورات الحلبي الحقوقية، بيروت،لبنان، طبعة 2012،(ص).208.

4- المرجع نفسه،(ص). 409

ثالثا: ضوابط تفتيش محل الجريمة المرتبط بالاشخاص.

ان اجراء التفتيش في الجريمة المعلوماتية تحتاج الى تقنيات خاصة تختلف عن حالات التفتيش التقليدية ،لان تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات الأجهزة وأماكن إخفاء المعلومات فيها لأنه يسهل اتلافها كليا او جزئيا ،كما يصعب تحديد مكان الدليل[1]، يلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش و الضبط فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة ومدى تبعيته للمجني عليه[2].

ويعد حضور أشخاص معنيين في أثناء إجراء التفتيش من قبل الضمانات المهمة التي تكفل إجراءه بشكل صحيح، و يبعد الشك حول إمكانية إخفاء الدليل من قبل القائمين به، ويقوم المفتش في إطار البحث عن الجرائم الماسة بأنظمة الإتصال والمعلوماتية بمجموعة من الإجراءات منهـا:

01- إجراءات تفتيش في النظام المعلوماتى الخاص بالمتهم.

تنصب اجراءات التفتيش حول محل ارتكاب الجريمة المرتبط بالنظام المعلومات الخاص بالمتهم ومحلها جرائم الحاسب الآلي الذي يعد بافذة التي يطل على عالم الانترنت،و الشبكة التي تشمل في مكوناتها الخادم والمزود الآلي...، وتجدر الإشارة هنا الى ان مثل هذا المحل لا يكون قائما بذاته، وانما يشمله مكان او عقار ما او يكون بصحبة مالكه او حائزه ولذلك وجب على ضابط الشرطة القضائية عند استصداره لاذن التفتيش ان يحدد محل ذلك الاجراء تحديدا دقيقا وكذلك الغرض منه والا كان التفتيش باطلا[3].

و عليه يحدد التفتيش الالكتروني دقة الاجراءات فمن خلاله يتم نقل البرنامج الداخلي من الوسائط المتعددة و بذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما يتم في جرائم النسخ و التقليد حيث يتم ضبط الوسائط المتعددة المحملة بالبرمج المنسوخة و الأجهزة المستخدمة في ذلك[4] .

02- إجراءات تفتيش في النظام المعلوماتي غير خاص بالمتهم.

تتعدد الوسائط الالكترونية وانظمتها المختلفة المرتبطة بالجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الأخرى المتصلة بالحاسب الذي ارتكبت في

---

1 - **نبيلة هبة هروال**،المرجع السابق،(ص). 234

2- **د/خالد ممدوح إبراهيم**، المرجع السابق،(ص). 228

1- د/عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي الإسكندرية،طبعة2009،(ص). 378

4- **د/كوثر سعيد عدنان خالد** ، حماية المستهلك الكتروني، الجامعة الجديدة (بدون ذكر مكان النشر)،طبعة 2012،(ص). 114

نظامه الجريمة المعلوماتية ، فهذا الفرض يؤكد فإن إجراءات التفتيش و الضبط تتطلب الدخول في نظام معلوماتي لشخص آخر[1].

يلاحظ أن الأمر يختلف من حيث صدور إذن بالتفتيش في النظام المعلوماتي لأحد الأشخاص عنه في الإذن بالتفتيش في الجرائم التقليدية الأخرى، لأن الإذن قد يصدر في حق شخص ارتكب جناية أو جنحة أو قامت قرائن قوية على ارتكابه للجريمة و عند القيام بتنفيذ إذن التفتيش، فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم، أو يمتد لأكثر من جهاز في أماكان مختلفة او تعدد المتهمين كأن يكون له شركاء في الأجهزة مما يتطلب الحصول على إذن آخر من وكيل الجهورية.

المبحث الثاني: التفتيش الالكتروني كآلية للكشف عن جرائم المنظومة المعلوماتية.

ان الجرائم الالكترونية تعد حدا فاصلا لقيام صفة الاجرام الذي يتميز باسخدامه تقنيات فنية لارتكاب اعتدءات ارتبطت بالنظم المعلوماتية استغلها مرتكبو الجرائم الإلكترونية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول ، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف التقليدية في القوانين الجنائية، لذا يرسم المشرع اجراءات التفيش الالكتروني كآلية للكشف عن الجرائم ومواجهة تطوراتها، وعليه سيتم معالجة الموضوع وفقا للخطة الآتية:

المطلب الأول: أنظمة التفتيش في المنظومة المعلوماتية.

المطلب الثاني: ضوابط التفتيش في المنظومة المعلوماتية.

المطلب الثالث: آليات التفتيش الدولية لمكافحة جرائم المنظومة المعلوماتية.

المطلب الأول: أنظمة التفتيش في المنظومة المعلوماتية.

يعتبر التفتيش عن الجريمة المعلوماتية في البيئة الرقمية من أصعب أنواع التفتيش، ويرجع ذلك إلى التطور المذهل في تكنولوجيا الإعلام والاتصال، و ارتباطه بخبرة المجرمين في التحكم في اثار الجريمة عن بعد ، الا ان التعاون الدولي يسعى للحد من الظاهرة الاجرامية، من خلال خلق انظمة يتسع مجالها لمواجهة للامحدودية الجريمة الالكترونية ،و خلق نسق تشريعي تكاملي ذو ابعاد وطنية ، لا يخضع للقواعد المتعارف عليها في التفتيش طبقا لقانون الإجراءات الجزائية، بالنظر لما يتميز به من خصوصية مرتبطة بطبيعة الجريمة المستهدفة وطبيعة مرتكبيها، فضلا عن مسرح الجريمة.

---

1 – **د/عز الدين عثماني**, (اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية), مجلة دائرة البحوث والدراسات القانونية والسياسية, جامعة الوادي, الجزائر, العدد الرابع , 2018،(ص). 60

الفرع الاول: ضبط المنظومة المعلوماتية الخاضعة للتفتيش الالكتروني .

ان نظام المعلومات نظام يتكون من أشخاص، وسجلات الكترونية، ويقوم هذا النظام بمعالجة البيانات والمعلومات في أي منظومة، أو هو مجموعة من العناصر المتداخلة التي تعمل مع بعضها البعض لجمع ومعالجة وتخزين وتوزيع المعلومات المتوفرة عن موضوع تتطلب من جهات التفتيش مهارات فنية غير متوافرة سوى لفئات متخصصة في مجال الحاسب الآلي ونظم تقنية المعلومات للتفتيش عنها بشكل منهجي من اجل الاطلاع على التنظيم والتحكم والتحليل في المنظومة المعلوماتية وفقا لتقنيات تفتيش الكتروني متطورة تجسيد مقتضيات معلوماتية تكرس الحصول على الدليل الالكتروني.

اولا: تفتيش الشبكات المتصلة بالحاسب الآلي " التفتيش عن بعد ".

إن سلبية التقنية الرقمية قد عقدت من التحدي أمام أعمال التفتيش و الضبط ، فالبيانات التي تحتوي على أدلة الإثبات قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش ، و إن كان من الممكن الوصول إليها من خلال حاسبات موجودة في الأبنية أو المواقع الجاري تفتيشها[1].

و قد يكون الموقع الفعلي للبيانات يدخل في اختصاص قضائي آخر أو حتى في بلد آخر، و إن كانت السلطات المختصة في دولة ما تسعى في كشف الحقيقة بشأن الجريمة المرتكبة ضد أحد أجهزتها فإن الأمر قد يكون خلاف ذلك بالنسبة لدولة آخرى ذلك ، وهذا ما يزيد من تعقيد الجريمة المعلوماتية العابرة للحدود وهو ما يستلزم وجود تعاون دولي[2]، و نستطيع أن نميز في هذه الصورة بين ثلاث احتمالات.

01– اتصال نظام المتهم بنظام آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة.

يثور الاشكال حول مدى إمكانية امتداد الحق في التفتيش إلى أجهزة أخرى غير جهاز المتهم إذ ان التشريعات الغربية قد تناولت في قوانينها الإجرائية حل هذه المشكلة كما هو الحال في التشريع الألماني من خلال القسم 103 من قانون الإجراءات الجزائية الألماني، التشريع البلجيكي من خلال المادة 88 من قانون تحقيق الجنايات[3]، و كذا المشرع الجزائري في المادة 05 الفقرة الاولى من القانون رقم 09/04" يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في اطار قانون الاجراءات الجزائية و في الحالات المنصوص عليها فيالمادة 04 اعلاه الدخول بغرض التفتيش و لو عن بعد الى:

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

– منظومة تخزين معلوماتية".

---

[1] – **د/خالد ممدوح ابراهيم** ، المرجع السابق،(ص). 202.

[2] – **أ/علي عدنان الفيل** ، المرجع السابق، ص44.

3– **د/خالد ممدوح ابراهيم** ، المرجع السابق،(ص). 203

02- اتصال نظام المتهم بنظام آخر خارج الدولة.

من المشاكل التي قد تثور في هذه المسألة قيام الجناة بتخزين بياناتهم في أنظمة معلوماتية خارج الدولة مستخدمين في ذلك شبكات الاتصال المعلوماتية وهذا لعرقلة جمع الأدلة و التحقيقات، وفي هذه الحالة فإن امتداد الإذن بالتفتيش إلى أقاليم دولة أخرى غير التي أصدرت إحدى جهاتها المختصة هذا الإذن وهو ما يسمى بالولوج أو التفتيش العابر للحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها[1].

وهذا ما يؤكده المشرع الجزائري في المادة 05 الفقرة الثالثة "اذا تبين مسبقا بان المعطيات المبحوث عنها و التي يمكن الدخول اليها انطلاقا من المنظومة الاولى ،مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل".

و بناءا عليه يتضح من الاتفاقية الأوروبية المتعلقة بجرائم تقنية المعلومات التي أجازت من خلال المادة 32 منه" إمكانية تمديد التفتيش لأجهزة و شبكات دولة أخرى حتى بدون إذنها في حالتين إذ تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، و الثانية إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش، وفقا لنص المادة 32 منه" يمكن لأي طرف دون تصريح من الطرف الآخر.

- أن يصل إلى البيانات المعلوماتية المخزنة و المتاحة للجمهور بغض النظر عن موقعها الجغرافي.

- أن يصل أو أن يتلقى عبر نظام معلوماتي يقع على إقليمه ، بيانات معلوماتية مخزنة في دولة أخرى ، إذا حصل هذا الطرف على موافقة قانونية و إرادية من شخص لديه السلطة القانونية للكشف عن هذه البيانات إلى هذا الطرف من خلال هذا النظام المعلوماتي"[2].

ثانيا: التنصت و المراقبة الالكترونية لشبكات الحاسب الآلي.

أمام صعوبة استخلاص الدليل التقنى وفقا للقواعد الإجرائية التقليدية ، مما ترتب عليه إفلات العديد من المجرمين من العقاب، فأصبح لزاما تطوير طرق الحصول على دليل يتماشى و الطبيعة التقنية للجرائم المعلوماتية لانها لاتترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية [3].

وبناءا عليه تفطن المشرع الجزائري بموجب قانون رقم 11/21 المؤرخ في 25 اوت 2021 المتعلق بالاجراءات الجزائية باستحداث الفصل الرابع من الباب الثاني من الكتاب الأول من المادة 65 مكرر إلى

---

[1]- **أ/علي عدنان الفيل** ، المرجع السابق ،(ص). 46

[2] - **د/هلالي عبد اللاه احمد**، المرجع السابق ،(ص). 378

[3]- **نعيم سعيداني** ،(آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري)، مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة باتنة ،سنة الجامعية 2012،(ص). 34

المادة 65 مكرر10 تحت عنوان" اعتراض المراسلات و تسجيل الأصوات و التقاط الصور، إذ بموجب هذا القانون يمكن لوكيل الجمهورية اعتراض الاتصالات السلكية و اللاسلكية ، كما تدخل المشرع مرة أخرى بموجب القانون04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و استحدث بموجبه إجراءين الأول يتمثل في المراقبة الالكترونية و الثاني حفظ المعطيات المتعلقة بحركة السير[1].

و بناءا عليه فان الدخول الى شبكة الانترنت و محاولة التنصت و المراقبة الالكترونية غير المشروعة ،شجعت الكثير من الدول على شبكة الانترنت ، و معرفة الاتصالات غير الصحيحة و محاولة منع وصولها الى النظم المعلوماتية ، واقرار صحة وسائل الرقابة و متابعة حركة المرور للمعطيات التقنية[2].

الفرع الثاني: اصول نظام تفتيش المعطيات المعلوماتية .

يعتمد التفتيش الالكتروني على انظمة لمجابهة الجرائم المعلوماتية و تكنولوجيا الحاسبات الآلية ووسائل الإتصال و شبكات الربط ليحمل مصطلح تقنيات المعلومات ليعبر عن النظم كوسيلة لارتكاب جرائم آخرى الناشئ في البيئة الرقمية التي اخضعها المشرع للتفتيش الالكتروني ، من خلال الاطلاع على الدعامات ، البرامج والمعطيات، وحدات الإدخال والإخراج، أسلاك الاتصال ، البرامج والمعلومات المشفرة في شكل معطيات، وعليه فإنه أيا من الأجهزة الحديثة التي ينطبق عليها هذا الوصف تعتبرا نظاما و يرتبط من الناحية الواقعية ببرامج و أنظمة تكشف عن المعطيات انثاء عمليات التفتيش.

اولا: برنامج مالتيجو" Maltego " المستخدم أثناء المعاينة والتفتيش.

وجب على الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين استخدام بعض البرامج التي تساعدهم في الكشف عن الجريمة المعلوماتية في جانبها التقني ،من خلال تحليل البيانات والمعطيات الموجودة في الملفات وكشف جميع جوانبها وجذورها مع إظهار المخفية منها وفك التشفير عن المشفرة واسترجاع المخلفات ، من أجل الوصول إلى دلائل أخرى باعتبار الجريمة المعلوماتية تقع في عالم افتراضي لا تخلف أي آثار مادية محسوسة[3].

و منه يتضح ان هذا البرنامج من أفضل وأقوى البرامج الخاصة بجمع المعلومات عن الهدف الذي نريد معرفة بعض المعلومات عنه، وله قدرة كبيرة على جمع المعلومات المتعلقة بشخص أو عدة أشخاص بالإضافة

---

[1] – **أ/رشيدة بوكر** ، المرجع السابق،(ص). 440-441

2 – **أ/خالد عياد الحلبي**،اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر والتوزيع ، عمان،الاردن، طبعة 2011،(ص). 164

[3] – **نعيم سعيداني**، المرجع السابق،(ص). 140

إلى صلة الوصل بينهم بالاعتماد على الايميل، الشبكات الاجتماعية، الموقع الالكتروني وحتى رقم الهاتف والكثير الكثير من الأمور الأخرى[1].

فهو عبارة عن أداة تفاعلية لاستخراج البيانات والمعلومات حيث تقدم رسومات بيانية توضيحية موضحة تسلسل ارتباط البيانات والمعلومات ببعضهاالبعض، مما يعني أنها تساعد في إيجاد الأمور المشتركة بين أجزاء مختلفة من المعلومات التي يمكن الحصول عليها من الشبكة العنكبوتية، ويستخدم في التحقيقات عبر هذه الشبكة للعثور على العلاقات بين أجزاء المعلومات من مصادر مختلفة موجودة على الانترنت.

ثانيا: برنامج فورنسيك " Forensic " المستخدم أثناء المعاينة والتفتيش.

هذا البرنامج مفهومه الشامل هو الجرائم، لكن هذه الجرائم يتم تقسيمها حسب أصناف معينة، منها الخاصة بالقتل و منها الخاصة بالسرقة والجنايات وما إلى ذلك، لكن خصص قسم خاص بالجرائم الإلكترونية، وهو ما يطلق عليه بـ Digital Forensic، وهو المتعلق بموضوعنا اليوم، بحيث يقوم على تعقب وحجز الأعمال والمهمات غير المشروعة و غير القانونية والتي يتم ممارستها باستخدام الشبكة العنكبوتية أو الأجهزة الإلكترونية

يقوم مجموعة من المحترفين في مجال المعلوماتية بالسهر على عمل النظام ، هؤلاء الأشخاص لديهم خبرات كافية و قوية من أجل المساهمة في كشف وإبطال الأعمالغير القانونية السائرة ضمن الشبكات العنكبوتية ، كما يقوم برنامج بتصوير القرص بواسطة حزم برمجيات ونظرا إلى أن هذه الحزم مصممة للمحققين الجنائيين، فإنها تتضمن أدوات لتجميع ملف كامل من بيانات مجزأة ، كما أنه يقوم بأعمال التحري والفحص للأدلة الرقمية و أخذ نسخ منها وتجميعها وتحليلها وفك التشفير واستعادة الملفات المحذوفة وكلمات المرور وتحليل البريد الالكتروني والبحث المتقدم، وتوليد تقارير لاستخدامها امام الجهات الجنائية المختصة[2].

المطلب الثاني: ضوابط التفتيش في المنظومة المعلوماتية.

التفتيش الالكتروني عبارة عن بناء اجرائي يتضمن فعالية تنفيذية لمجموعة من الوظائف المرتبطة بالبحث عن ادلة لجريمة ارتكبت يعاقب عليها القانون سواءا اخذت وصف جناية او جنحة تحقق وقوعها في محل من اجل تحصيل الادلة و نسبتها الى مرتكبيها وفقا لما هو مقرر قانونا.في مسرح الجريمة يتميز بيئته افتراضية، ومن اجل ضمان صحة التفتيش الالكتروني يجب من الناحية الواقعية وجود روابط موضوعية يستند عليها لضمان التقيد بالاجراءات التفتيشية.

1- **أ/نضال أدمين،** منتدى برامج الكمبيوتر والأنترنيت، موجود على الرابط http://nidhal-technologie.own0.com/t60-topic تم الدخول بتاريخ بتاريخ 2023/04/18.

2- أ/**إيناس محمد راضي،** الأجهزة التحليلية الحديثة في كلية علوم الأدلة الجنائية، على الرابط http://www.uobabylon.edu.iq/uobColeges/service_showrest.aspx?fid ، تم الدخول للموقع و الاطلاع بتاريخ 2023/04/16 على الساعة 12.00

الفرع الاول: ركائز ارتكاب الجريمة المعلوماتية.

إن المنطق القانوني و العقلي يتطلب وقوع جريمة معلوماتية لأجل القيام بإجراءات التفتيش الالكتروني باعتباره وسيلة إجرائية تهدف إلى الحصول على دليل المادي ، باعتبارها كل سلوك غير مشروع موجه للمساس و الاعتداء على المكونات غير مادية للنظام المعلوماتي في وفرتها و إتاحتها أو في سلامتها و تكاملها.

اولا: وجود جريمة الإلكترونية.

يسعى ضبط الشرطة و القضائية والمحققون الى اثبات قياماركان و عناصر الجريمة المعلوماتية حسبما يحدده القانون ، و الى ايجاد العلاقة بين تلك الاركان و الشخص المتهم بتنفيذها باعتبارها نشاط اجرامي تستخدم فيه تقنيات حديثة ، لذلك صعب وضع تعريف عام و شامل لها، فعرفت بأنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية او داخل نظام حاسوب و تشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية"[1]

أما المشرع الجزائري فتبنى حديثا تعريفا لجرائم تقنية المعلومات بموجب المادة 02 من القانون رقم 04/09"الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال:جرائم المساسبانظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة اخري يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية" اعتبر المشرع أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة[2]، اما قانون العقوبات الجزائري المعدل والمتمم لم يعرف جرائم الانترنت،بل اكتفى بالعقاب على بعض الأفعال ، تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات".

ثانيا: قيام اركان الجريمة المعلوماتية.

تتمثل أركان الجريمة الإلكترونية مثل الجريمة العادية في الركن الشرعي و المادي والمعنوي:

01- الركن الشرعي لقيام الجريمة المعلوماتية.

حدد قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص جرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات . فينطلقون أنصار هذا الاتجاه من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة ، وبالتالي تعرف على أنها " فعل إجرامي لا يعرف الحدود الجغرافية ، و التي يتم ارتكابها بأدة هي الحاسب الآلي عن طريق شبكة الانترنت و بواسطة

[1] - أ/**محمد امين احمد الشوابكة**،جرائم الحاسوب و الانترنت ، الطبعة الاولى ،دار الثقافة ،عمان ، الاردن،طبعة 2004،(ص).10.

[2] - **أ/حملاوي عبد الرحمان** ، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية ، منشورة بمجلة الحقوق جامعة بسكرة كلية الحقوق ، العدد 33 ، طبعة2016،(ص). 45

شخص له دراية فائقة بها"[1] فيستخدم الكمبيوتر في ارتكابه كأداة فهي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا

نصت على مبدا الشرعية المادة الأولى من قانون العقوبات الجزائري ، ومن الانتقادات الملاحظة أن المشرع لا يستطيع أن يحصر مسبقا كل ما يصلح من الأفعال لتجريم الاعتداءات المعلوماتية ، وأن تطور الحياة وتقدم وسائل التقنية الحديثة ومهارة بعض الأفراد في إساءة استخدامها يخلق كل يوم مخاطر جديدة للجرائم الالكترونية، يضمن مبدأ الشرعية لمرتكبيها الإفلات من العقاب لمجرد أن المشرع قد أغفل النص على تجريم كل الافعال الماسة بشبكة الانترنت و الكمبيوتر.

و لتفادي الاشكالات القانونية دعم المشرع الجزائري مبدأ شرعية التفتيش الالكتروني لتتلاءم مع طبيعة الجرائم المرتكبة في هذا العالم الافتراضي المعلوماتي بخصوصية تجعل من الصعب تطبيق القواعد الموضوعية التقليدية عليها عند ارتكاب هذا النوع من الجرائم، من خلال استدرك المشرع الجزائري الأمر بإصداره للقانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وخص التفتيش والحجز بإجراءات مستحدثة تكمل تلك المنصوص عليها في قانون الإجراءات الجزائية الجزائري نص على الأحكام العامة التي تبين الأهداف المتوخاة من هذا القانون وتحديد مفهوم المصطلحات التقنية ومجال تطبيق أحكامه، وتضمن الأشخاص أو الكيانات العامة أو الخاصة التي تقدم خدمات للاتصالات بواسطة المنظومة المعلومة أو لنظام الاتصال.

- جسد الأحكام الخاصة بمراقبة الاتصالات الالكترونية إذ يراعى فيها التهديدات المحتملة وأهميته للمصالح المحمية، إذ نص القانون على أربعة حالات يسمح فيها للسلطات الأمنية مراقبة الاتصالات والمراسلات الالكترونية وجاءت على سبيل الحصر .
- تضمن القواعد الإجرائية الخاصة بالتفتيش والحرز في مجال الجرائم الالكترونية، وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن، مع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة إلا أن المشرع الجزائري بإحالته إلى هذا الأخير قضى على مبدأ من مبادئ القانون والتي تنص على أن القاعدة الخاصة تقيد العامة في جميع الأحوال، إذا أصبح القانون 04/09 السالف الذكر يتقيد بالقواعد العامة لقانون الإجراءات الجزائية وقانون العقوبات.
- تطرق فيه إلى التزامات المتعاملين في مجال المعلوماتية بتحديد هذه الالتزامات لاسيما إلزامية حفظ المعطيات المتعلقة بحركة سير، والتي من شانها المساعد في الكشف عن الجرائم المعلوماتية.

1 – **أ/رشيدة بوكر**،المرجع السابق،(ص).40

02- الركن المادي لقيام الجريمة المعلوماتية.

يتكون الركن المادي للجريمة الالكترونية من السلوك الاجرامي و النتيجة و العلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها ، انشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة الا أنه لا مناص من معاقبة الفاعل و يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل ايجابي مرتكب مثال جريمة الغش المعلوماتي، الركن المادي فيها هو تغيير الحقيقة في التسجيلات الكترونية أو المحررات الإلكترونية[1]، جرائم المساس بنظم المعلوماتية او المعطيات المعلوماتية،جرائم الاعتداء على حرمة الحياة الخاصة و المعطيات الشخصية ، جرائم الاحتيال باستخدام بطاقة الائتمان، جرائم المساس بالملكية الفكرية، و تتمثل الامثلة التي سيتم اعطاؤها في نماذج عن الجرائم محل المتابعة و التفتيش الالكتروني ، و يكون محلها المنظومة او النظام المعلوماتية[2].

الجرائم الواقعة عل الاشخاص

- جرائم التهديد عبر مواقع الانترنت.
- جرائم انتحال الشخصية عبر المواقع الالكترونية.
- جرائم التشهير و تشويه السمعة عبر المواقع الالكترونية.

الجرائم الواقعة على الاموال

- جرائم الاحتيال المالي باستخدام وسائل معلوماتية.
- اختلاس البيانات المالية للمجني عليه واستغلالها.
- الاستعمال الغير القانوني لبطاقات الائتمان.

الجرائم الواقعة على امن و مؤسسات الدولة

- جرائم الارهاب باستخدام المعلومات لتسهيل العمليات الارهابية.
- التجسس عبر المراقع الالكترونية.
- التنصت من خلال الدخول لقواعد بيانات الحكومة من خلال استخدام برامج الاختراق.

03- الركن المعنوي لقيام الجريمة المعلوماتية.

لما كانت جرائم المعلوماتية من الجرائم التقنية العالية و التي تتطلب المعرفة و الخبرة من قبل الجهات التي تمارس عمليات التفتيش، و من ثمة فهي جرائم عمدية، بمعنى وجود نية التخطيط و التدبير لارتكاب

---

[1]- **د/محمود نجيب حسني**، شرح قانون العقوبات (القسم الخاص)، دار النهضة العربية،القاهرة، طبعة 1990،(ص).158.

[2]- **د/علي ابراهيم توفيق**، دور المحقق في الجرائم الالكترونية ، الطبعة الثالثة ، دار المدى للنشر و التوزيع، العراق ، طبعة 2000،(ص). 141

الجريمة المعلوماتية، فالأصل إن الفاعل المعلوماتي في الجريمة الالكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به، و لكن هذا لا يمنع أن بعض الجرائم الالكترونية تتوافر فيها القصد الجنائي الخاص مثال جرائم تشويه السمعة عبر الانترنيت ، و جرائم نشر الفيروسات عبر الشبكات وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي[1].

وعليه حتى يتمكن الفاعل او الشريك المعلوماتي من تنفيذ جريمتهم الإلكترونية يستلزم ذلك توفر أدوات عدة وأبرزهـا:الاتصال بشبكة الإنترنت، توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب، وسائل التجسس، ومنها ربط الكاميرات بخطوط الاتصال الهاتفي، البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز، طابعات ،هواتف رقمية ونقالة[2].

الفرع الثاني: صور التفتيش الالكتروني في المنظومة المعلوماتية.

بظهور الاعتداءات المعلوماتية وانتشارها الواسع اصبحت تشكل جرائم واسعة النكطاق لذا اقر المشرع الجزائري حماية جنائية لكل المعطيات الداخلية او خارجية، مع منح السلطات المختصة حق الاطلاع و الولوج لاجراء عمليات التفتيش الالكتروني التي تختلف صوره و حالاته حسب القواعد المحددة .

اولا: التفتيش الالكتروني للمكونات المادية للحاسوب (Computer Hardware)

يتكون الحاسوب من مجموعة الوحدات لكل منها وظيفة محددة تتصل هذه الاخيرة ببعضهابشكل يجعلهاتعمل كنظام متكامل ، ومجموع الوحدات تشكل ما يسمى بنظام الحاسوب[3]، وينصب إجراء التفتيش على الكيان المادي للحاسوب و إظهـار نتائج التشغيل كالشاشة والطابعة والسماعـات و الراسـم و الاقراص المرنـة و الصلبة وحدة الذاكرة التي تعتبر من أشهر تخزين البيانات و المحافظة عليها[4].

من خلال ماسبق يتبين بوضوح أن التفتيش إذا تعلق بالمكونات المادية للحاسوب لا مشكل في ذلك ويتم وفقا لأحكام المادة 44 من قانون الاجراءات الجزائية ، وعليه يجب الانتقال إلى مكان تواجد الحاسوب أو أحـد مكوناته المادية بضبط جهـاز الحاسوب ومكـوناته أو ملحقاته وحجزها وتقديمها كدليل لإدانة المتهم يخضع للإجراءات التقليدية للتفتيـش كتحديد طبيعة المكان الموجودة فيه تلك المكونات سواء كان عامـا أو خاصا إضافة إلى حضور المعني أو من ينوب عنه.

---

[1] – **د/عبد الفتاح بيومي حجازي** ، المرجع السـابق،(ص). 101

[2]– **د/هدى قشقوش** ، المرجع السابق،(ص). 20

3– **د/علي حسن محمد الطوالبة**، المرجع السابق،ص.19

4– **د/طارق إبراهيم الدسوقي عطية**،الأمن المعلوماتي، دار الجامعة الجديدة للنشر، الاسكندرية، طبعة 2009 ،(ص). 88

ثانيا: التفتيش الالكتروني للمكونات المنطقية للحاسوب (Computer Software).

يقصد بالكيان المنطقي مجموعة البرامج و الاساليب والقواعد و عند الاقتضاء الوثائق الالكترونية المتعلقة بتشغيل وحدة معالجة البيانات اذ يشتمل الجانب الافتراضي البرامج ، الكيانات التطبيقية مثل برامج معالجة النصوص، جداول البيانات الالكترونية.

و يطلق أيضا على المكونات المعنوية للحاسوب بالبرمجيات، فهي بمثابة عصب عمل الكمبيوتر إذ توفر إمكانات و سرعة فائقة في إنجاز المهام المطلوبة، كما يعرف الكيان المنطقي للحاسوب لغة بأنه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسوب كنظم التشغيل و برامج التطبيقات. تقسيم برامج الحاسوب إلى نوعين: يسمى الأول برامج النظام والثاني برامج التطبيقات

وعليه فإجراء التفتيش على المكونات المعنوية للحاسوب، ومنها تفتيش المنظومة المعلوماتية سواء كانت في حاسوب واحد، أو مرتبطة عن طريق شبكة اتصال سلكي أو لاسلكي كالأنترنيت ، بالنظر الى ترابطها على مستويات متعددة وطنية وعالمية ، نظرا للطبيعة المعنوية الخاصة لهذه المعطيات المخزنة إلكترونيا، اضافة الى أنها تتم في بيئة افتراضية يتطلب الكشف عنها استخدام رجال القضاء قدرات فنية و تقنية ذات جودة وتكنولوجيات فائقة وسائل تقنية للكشف عن الرقم السري أو الكود(Code)، أو كلمة السر(Password)[1] ، أو نظام التشفير أو ترميز البيانات للولوج إلى مختلف الملفات لتقديمها كدليل ضد المتهم.

ثالثا: دعائم تفتيش المنظومة المعلوماتية.

تفادى المشرع الجزائري النشاط الاجرامي المعلوماتي بتعديل قانون العقوبات بإضافة قسم سابع مكرر عنوانه" المساس بأنظمة المعالجة الآلية للمعطيات" بموجب القانون الاجراءات الجزائية بوضع دعائم اجرائية تتناسب و طبيعة الجرائم المستحدثة حيث يهدف المشرع الى حماية نظام المعالجة الآلية للمعطيات الذي خضع لتطورات متلاحقة في مجال صناعة الكمبيوتر و ملحقاته و برامجه[2].

بالنرجوع الي القوانين الاجرائية يلاحظ ان المشرع عدل المواعيد و الاحكام الاجرائية المتعلقة بالتفتيش بالاضافة الي استحداث القانون قم 04/09 في هذه الجرائم حيث عرفت المادة 02 الفقرة 02 منه المنظومة المعلومات بأنها" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين..." .

---

[1] – **أ/نبيلة هبة هروال**، المرجع السابق ،(ص). 355

[2]– **قارة آمال**،(الجريمة المعلوماتية)، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، تاريخ المناقشة2002،(ص). 100

رابعا: أثر التفتيش الالكتروني.

تعد الجريمة المعلوماتية اثرا مرتبا لقيام جهات التحقيق القضائي بعمليات التفتيش الالكتروني بشكل متطور و سريع من خلال قيامهم بابعاد الجناة و العاملين على الاجهزة عن المكان ليتم تفتيش الاجهزة و الشبكات لمعرفة المعطيات المخزنة و معرفة رقم الاتصال و الاطلاع الجيد على مسرح الجريمة و نقل المعطيات المعلومات و نسخها[1].

– الدور الوقائي للتفتيش الالكتروني في الكشف عن الجرائم.

خرج المشرع الجزائري المبدأ العام فجعل من إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة المعلوماتية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة 03 من القانون04/09 "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات،يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون ، بوضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع وتسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية"، كما نصت المادة04 الفقرة 02 من نفس القانون على أنه" في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني..."[2].

– منع المجرم المعلوماتي من تدمير أو إخفاء الدليل.

أدرج المشرع إجراء التفتيش في مجال الجرائم المعلوماتية في قانون الإجراءات الجزائية، فأجاز الدخول بغرض التفتيش و لو عن بعد إلى المنطومة المعلوماتية دون إذن صاحبها، وهذا برغم اعتبار برامج الحاسوب من بين المصنفات الأدبية المحمية بموجب مجموعة من النصوص الخاصة[3].

ونظرا لما تتطلبه العملية من جانب تقني معقد أجاز المشرع نسخ و إفراغ المعطيات على دعامة تخزين الكترونية تكون قابلة للحجز مثل الأقراص المرنة والأقراص المضغوطة والذاكرة الومضية...إلخ وهذا بموجب نص المادة 06 من القانون 04/09 "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها.

---

[1]– **أ/خالد عياد الحلبي**،المرجع السابق،ص.154

[2] – راجع المادة 04 من القانون رقم 04/09 المؤرخ في 05 اوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

[3]– د/**عبد الهادي بن زيطة**، حماية برامج الحاسوب في التشريع الجزائري، الطبعة الأولى ، دار الخلدونية، الجزائر، طبعة 2007،(ص).35

– حجز المعطيات المعلوماتية.

في بعض الاحيان يستحيل نسخ المعطيات لاسباب تقنية كما لو كانت المعطيات مخزنة بانظمة التشغيل التي يمكن نسخها ، فيتعين على السلطة المكلفة استخدام التقنيات المناسبة لمنع الوصول الى المعطيات التي تحتويها المنظومة المعلوماتية الموضوعة تحت تصرف الاشخاص المرخص لها باستخدام المنظومة المعلوماتية وفقا للمادة 07 من القانون رقم 04/09 و الهدف من الاجراء الاحترازي هو الحفاظ على الادلة في محيطها الالكتروني[1].

– منع الوصول الى المعطيات المعلوماتية .

يتم الحجز وفقا لآليات ومتطلبات تحكمها قواعد وجوانب تقنية للمعلوماتية تتماشى مع البيئة الرقمية التي ترتكب بها الجرائم، و المشرع الجزائري أكد امكانية نسخ البيانات المعالجة آليات و ضبطها، كما اجاز حجز المعطيات المخزنة داخل نظم المعلوماتية اذا كانت تفيد في كشف الجرائم او مرتكبيها ، اما طريقة حجز المعطيات فتتم عن طريق نسخ المعطيات محل البحث على دعامات تخزين الكترونية قابلة للحجز، وفقا للمادة 06 من القانون رقم 04/09 و تمتد عمليات النسخ الى المعطيات اللازمة لفهم المعطيات محل التفتيش.

المطلب الثالث: آليات التفتيش الالكتروني الدولي لمكافحة جرائم المنظومة المعلوماتية.

أدى سوء استخدام الفضاء السبيراني إلى بروز جرائم مستحدثة، تطلبت نوعا جديدا من الأدلة تسمى الأدلة الرقمية، أو الأدلة الإلكترونية، تتفق وطبيعة الوسط الافتراضي الذي ارتكبت فيه الجريمة. فكان التحدي دوليا بالنظر الى استخدام الشبكات المعلوماتية كآلية لتنفيذالاجرام فإن خبراء الأمن المعلوماتي وصانعي السياسات الحكومية يرون انها مشكلة عالمية، تتطلب تعاونا في جميع القطاعات لمكافحة الجريمة.

الفرع الاول: الجهود الدولية و الإقليمية لمكافحة الجرائم الالكترونية.

عمل المجتمع الدولي من أجل وضع نصوص قانونية تتناسب مع التطور الحاصل في جانب الاجرام المعلوماتي إذ كان لابد من إيجاد القواعد القانونية لمسألة منع الاعتداء على النظم المعلوماتية أو الاستخدام غير المشروع لها من خلال عديد الاتفاقيات و الآليات القانونية والقضائية كاساليب لمجاهة الجريمة المعلوماتية.

اولا:ضرورة التعاون الأمني و القضائي الدولي في مجال دعم التفتيش الالكتروني.

تعد الجرائم الإلكترونية من أخطر التحديات الأمنية التي تواجه أعضاء المجتمع الدولي ، فهي جرائم معقدة ترتكب بوسائل تقنية حديثة ومتطورة من قبل مجرمين على مستوى عال من الذكاء و الخبرة مما يجعل الإثبات والتحقيق فيها صعب ، بحيث أن الصورة التقليدية أ لإجراءات التحقيق التي تقوم بها الجهات المكلفة بالبحث والتحري عن الجريمة لا تتماشى و طبيعة الجرائم الإلكترونية يرى بضرورة التعاون الدولي في هذا المجال

[1] – **د/رضا هميسي**، المرجع السابق،(ص). 175

الذي يكون في إطار اتفاقيات خاصة ثنائية أو متعددة الأطراف تجيز هذا الامتداد و التنسيق بين الدول ، ودعم التعاون الشرطوي باستخدام تقنيات عالية التقدم لدعم التفتيش الالكتروني.

وحتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام ، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، نتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوع من الجرائم المعلوماتية ، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب ، بل تعدت إلى أمن البنى الأساسية[1].

بالنظر الى الاساليب الحديثة التي يستخدمها المجرمون حديثا لتنفيذ عملياتهم الاجرامية اصبحت عابرة للحدود و مكافحتها لا يتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها لتسهيل عمليات التفتيش الالكتروني ، من خلال خلق كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة[2].

و غير انه يلاحظ من الناحية العملة صعوبة تنفيذ هذا التعاون الدولي بالنظر الاختلافات التشريعية و التنظيمية و هذا ما يؤكده الدكتور عادل عبد العال ابراهيم خراشي"ان التعاونالدوليف مجال الجرائم المعلوماتية يعد من اهم الانجازات لتوسيع دائرة المتابة و القضاء على الظاهرة الاجرامية وتسهيل عمليات التفتيش الا انها تلقى اشكالات تنفيذها اهمها القضور التشريعي و التعارض بين مصالحها ، التنوع و اختلاف النظم القانونية الاجرائية، صعوبة تنفيذ الانابات القضائية الدولية..."[3].

ورغم الانتقادات التي تم توجيهها لهذه الاتفاقيات فإنها مع ذلك تبقى مبادرة محمودة لاسيما وأن المجهودات التي قامت بها كل من المنظمتين العالميتين للملكية الفكرية والتجارة الدولية من أجل توفير حماية برامج الحاسب الآلي من الاعتداءات والأخطار التي تتعرض لها و منع الاعتداءات الاجرامية سواء على

---

[1] – **د/جميل عبد الباقي الصغير** ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، طبعة 1998،(ص). 75

[2] – **د/يونس عرب**، جرائم الكمبيوتر و النترنت ، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، (الجزء الأول)،الطبعة الأولى، منشورات اتحاد المصارف العربية، (بدون مكان نشر)، طبعة2002 ، ،(ص). 150

[3] - **د/ عادل عبد العال ابراهيم خراشي**، اشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية و سبل التغلب عليها، دار الجامعة الجديدة، الاسكندرية، مصر، طبعة2005،(ص).96

مستوى القرصنة بمظاهرها المختلفة أو على مستوى الفيروسات التي تخترق النظم و البرامج و تمنع تنفذ أهدافها.

ثانيا:جهود المنظمة الدولية للشرطة الجنائية.

انتشرت ظاهرة الإجرام وتعقدت أساليبها وتنوعت آثارها لتتحول إلى ظاهرة دولية تشغل بال المجتمع الدولي بجميع عناصره من دول ومنظمات وهيئات حكومية وغير حكومية. كما برزت الجريمة المنظمة العابرة للحدود الوطنية والتي تشكل خطرا على جميع الدول والمجتمعات، وخصوص ما يتعلق بارتكاب الجرائم المعلوماتية ، وهكذا كانت الحاجة الماسة إلى ضرورة إنشاء آلية دولية لمكافحة الجريمة وتحقيق التعاون المثمر بين الأجهزة الأمنية التابعة لدول مختلفة تمثلت في المنظمة الدولية للشرطة الجنائية (الانتربول) من خلال دعم الاجراءات المرتبطة بالتحرى حول الجرائم الالكترونية ، و أن تتخذ خطوات محددة نحو تحقيق الاهداف الآتية:

- ابرام اتفاقيات تنطوي على نصوص و تنظيمات لتحديث اجرات التفتيش الالكتروني و الضبط المباشر و تمكين قوى الشرطة في سائر أنحاء العالم من مواجهة التحديات الإجرامية.
- اتخاذ تدابير ملائمة لحل اشكاليات الاختصاص القضائي في مجال الانابات القضائية الدولية لتسهيل اجراءات التفتيش الالكتروني.
- ايجاد آليات حديثة لتسهيلالدخول للمواقع و اللولوج الى الانظمة المعلوماتية بتقنيات رقمية حديثة
- تحقيق معايير الامن المعلومات للبيانات.
- حماية الانظمة المتصلة بالمعلوماتية و عبر المواقع الالكترونية[1].

بالاضافة الى جهود الأمم المتحدة من خلال مؤتمرها الخاص بمنع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية أو الجرائم الحاسب الآلي. أما على المستوى العربي نجد أن مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية ، بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين, في حدود القوانين والأنظمة المعمول بها في كل دولة.

و منه يتضح انه يتم تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء، و ملاحقة مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، عن طريق تعقب الأدلة الرقمية وضبطها, والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم ووضع حد لهـــا[2].

1- **د/عادل عبد العال ابراهيم الخرشي**، المرجع السابق،(ص).72

2- **د/جميل عبد الباقي الصغير** ، المرجع السابق ،(ص).101

ثالثا: الجهود المبذولة على مستوى الاقليمي

في ظل شيوع شبكات المعلومات وفي ظل التوسع والنماء الكبير لأنظمة الحواسيب المفتوحة ونقل وتدفق المعلومات إضافة إلى التشديد على أهمية مكافحة كافة الأنشطة التي تستهدف العناصر الثلاثة لامن المعلومات وتضم الكمبيوتر وهي السرية وسلامة المحتوى وتوفر المعلومات والنظم، برزت على المستوي الاقليمي عدة جهود لمكافحة جرائم المعلوماتية من اجل وضع قواعد لمنع الجرائم المرتكبة عبر الانترنت وردع مرتكبيها.

و تظهر الجهود الدولية في هذا المجال تعلق باتفاقية بودابست، والتي تم التوقيع عليها في العاصمة المجرية بودابست(المجر) سنة 2001 ، وذلك لمواجهة الاستخدام الغير مشروع للحاسب من خلال الاتفاقيات التي صادقت عليها الجزائر، و الاتفاقية العربية سنة 2010 و اتفاقية الاتحاد الإفريقي للتعاون الدولي و القضائي لمكافحة الجريمة العابرة للحدود .

كما عملت الاجهزة الاقليمية للمجلس الأوربي، الذي يحاول تكريس وجوب التعاون بين أعضاء الاتحاد لمواجهة هذا النمط المستحدث من الإجرام سواء فيما بينهم أو بالتنسيق مع هيئات ومنظمات دولية أخرى[1]، الحرص على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات, وذلك من خلال العديد من الجهود التي بذلت في هذا الشأن.

و تجلت الاهتمامات الاقليمية للمجلس بالمعلوماتية بشكل عام وما يحيطها من مشكلات لتصدي للاستخدام الغير المشروع للحواسيب و شبكة الانترنت ، وقد اتجه الى الاهتمام بداية إلى العمل على حماية البيانات الشخصية حتى لا تؤدي الرغبة في زيادة فاعلية عمل الحاسبات الآلية لخدمة المجتمع في تهديد حق الأفراد في الخصوصية, ففي عام 1981 تم التوقيع على الاتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيا، وقد تضمنت تلك الاتفاقية عدة مبادئ تمثلت في الحد الأدنى من الاحتياطات التي يجب أن تتضمنها التشريعات الداخلية للدول أطراف المعاهدة لحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيا[2].

الفرع الثاني: السياسة الوطنية في مجال ضمان فعالية التفتيش الالكتروني.

ان الهدف من التفنيش الالكتروني تمكين جهات التحقيق من كشف الجريمة والتعرف على مرتكبيها، وهو الأمر الذي سعى المشرع الجزائري إلى تجسيده من خلال استحداث نصوص قانونية جديدة أوجد بموجبها قواعد إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية، ويعتبر التفتيش الالكتروني إحدى هذه الإجراءات التي

---

[1]- **د/محمد امين الشوابكة** ،جرائم الحاسوب والانترنت الجريمة المعلوماتية، الطبعة الاولى، دار الثقافة للنشر والتوزيع،(بدون مكان النشر)، طبعة2007،(ص). 73

2- **د/ عادل عبد العال ابراهيم خراشي**،المرجع السابق،(ص).82

حملها القانون رقم 04/09 المؤرخ في05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

اولا: تصنيف الجرائم المعلوماتية محل التفتيش الالكتروني.

كثيرة هي التصنيفات المرتبطة بالجريمة الالكترونية في المنظور الفقهي، نظرا للاعتبارات الكثيرة التي ينظر لها، أما من ناحية التشريع فسنعتمد على تصنيف قانون العقوبات الجزائري إياها في تعديله بالقانون 14/21 المؤرخ في 28 ديسمبر 2021 فقد جاء في المادة 12 من هذا القانون المعدل و المتمم بالفصل الثالث من الباب الثاني من الكتاب الثالث بالقسم السابع مكرر عنوانه " المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى 394 مكرر 07... .

– فقد أضيف في هذا القسم ثماني مواد جاء في المادة الأولى394 مكرر جريمة الدخول أو البقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

– وفي المادة 394مكرر01 نص على جريمة إدخال معطيات في نظام للمعالجة الآلية للمعطيات، أو إزالة أو تعديل معطيات موجودة فيه، إذا كان ذلك عن طريق الغش.

– وفي المادة 394 مكرر02 نص على القيام عن طريق الغش بـ:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

أما في المادتين (394 مكرر03 و394 مكرر 04) فإنه أورد فيهما تشديد العقوبة إذا ارتكبت الجرائم المنصوص عليها في هذا القسم ضد الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام أو ارتكبت من طرف شخص معنوي.

– وفي المادة 394 مكرر05 نص على أن المشاركة في مجموعة هدفها الإعداد لإحدى هاته الجرائم المنصوص عليها في هذا القسم، يعاقب المشارك بنفس العقوبة المقررة للجريمة ذاتها.

– وفي المادة 394 مكرر06 نص على أن الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم يعد كارتكاب الجريمة ذاتها.

وعند التأمل في هذه الجرائم يمكن أن نحصرها في أربع جرائم

- الدخول أو البقاء غير المشروع في منظومة للمعالجة الآلية للمعطيات، سواء لمجرد الدخول أو البقاء أو ترتب على ذلك الحذف أو التغيير لمعطيات المنظومة، أو ترتب عليه تخريب نظام اشتغال المنظومة.
- إدخال معطيات في نظام المعالجة الآلية للمعطيات، أو إزالة أو تعديل معطيات موجودة في ذلك النظام.

- استحداث أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال معطيات متحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

وقد وضع المشرع هذا القسم (المساس بأنظمة المعالجة الآلية للمعطيات) بعد القسم السابع المعنون(التعدي على الملكية الأدبية والفنية) من الفصل الثالث المعنون (الجنايات والجنح ضد الأموال) من الباب الثاني المعنون (الجنايات والجنح ضد الأفراد).

ووضع لتلك الجرائم عقوبات لا تزيد مدة الحبس فيها عن ثلاث سنوات باستثناء الحالات التي تشدد فيها العقوبة، مما يفهم منه أنها مندرجة في قسم الجنح.

ثانيا: صعوبة تصنيف الجرائم المعلوماتية محل التفتيش الالكتروني.

من خلال ما سبق يتضح أنه من الصعوبة تماما حصر الجريمة الالكترونية محل التفتيش ، لعدة أسباب أهمها:

– إن أشكالها متعددة متنوعة، مما يصعب حصر الأفعال المكونة لها، وهي تزداد تنوعا وتعدادا كلما أوغل العالم في استخدام الحاسب الآلي وشبكة الانترنت، فمن مجرد الدخول إلى أنظمة معلوماتية بطريقة غير شرعية، إلى البقاء في تلك الأنظمة، إلى تخريبها وتغيير محتوياتها، أو انتحال شخصية فيها، ومن تواصل بين المجرمين، إلى تنظيم العمل الإجرامي عن طريق الانترنيت.

– كثرة الأهداف في الجريمة الالكترونية، فمن مجرد التحدي للأنظمة المعلوماتية، إلى مجرد العبث بالمعطيات الإلكترونية، إلى هدف إيقاع الضحايا في خسائر مادية أو معنوية ،إلى هدف الكسب المادي غير المشروع، وغير ذلك من الأهداف[1].

– الاختلاف في حجم الأضرار التي تتركها تلك الجرائم، فمن مجرد الاطلاع على معلومات سرية، إلى إفشائها إلى الخسارة المادية، أو الخسارة المعنوية.

– تنوع الجهة المستهدفة بتلك الجرائم، فقد يكون المستهدف منها شخصا عاديا، وقد يكون مؤسسة خاصة أو عمومية، وقد تكون الدولة بحد ذاتها هي المستهدفة منها.

وعليه فإن الجرائم الالكترونية في الدول التي لم تسن لها قوانين خاصة يجد مرتكبوها إفلاتا من العقاب بسبب عدم النص عليها، وحتى الدول التي سنت لها قوانين فإنه نظرا لطبيعة هذه الجرائم المتكاثرة والمسرعة

[1] – **د/ وردة شرف الدين** ، (الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري) ، مجلة المنار للبحوث والدراسات القانونية والسياسية ، العدد الثالث ، ديسمبر 2017 ، الصادرة عن كلية الحقوق والعلوم السياسية جامعة يحي فارس المدية ،(ص). 33

في التطور تبعا لتطور التقنيات الالكترونية تواجه فيها تلك الجرائم الإلكترونية غير المشمولة في القانون صعوبة في تطبيقها.

كما أطلق المشرع الجزائري على الجرائم المعلوماتية مصطلحي: "جرائم المساس نظمة المعالجة الآلية للمعطيات" و" الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، وقد عرفها ضمن القانون رقم 04/09 في المادة 02 منه على أنه يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال: (جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[1].

و بالرغم من كل الاحكام القانونية الموضوعية والاجرائية فان اجراءات التفتيش الالكتروني لا تتم الا وفقا للضمانات القانونية الا ما استثني بنصوص خاصة، وهذا ما يؤكده القانون رقم 07/18 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المؤرخ في 10 جوان 2018 وفقا للمادة 12 منه "ما لم يوجد نص يقضي بخلاف ذلك تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية او لترخص منها طبقا للاحكام المنصوص عليها في هذا القانون".

كما قيد المشرع والاتصال بضرورة مراعاة حرمة الحياة الخاصة بحيث منح المشرع الجزائري للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته العديد من الامتيازات و قيده من جهة آخرى احتراما للضمانات الدستورية وهذا ما اكده المشرع الجزائري في المادة 49 من القانون رقم 07/18 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"يمكن السلطة الوطنية القيام بالتحريات المطلوبة و معاينة المحلات و الاماكن التي تتم فيها المعالجة ، باستثناء محلات السكن و يمكنها للقيام بمهامها الولوج للمعطيات المعالجة و جمع المعلومات و الوثائق أيا كانت دعامتها".

وتظهر عدة عراقيل وصعوبات لجهات التحري في الكشف عن هذه الجرائم ومتابعة مرتكبيها بالنظر الى اتساع نظام الشبكات المعلوماتية و تطور التقنيات الفنية للأنترنت ، الأمر الذي دفع بالمشرع إلى إيجاد وحدات متخصصة تعمل في هذا المجال، مزودة بالخبراء والتقنيين وتنظيم دورات متخصصة لهم في مجال مكافحة الجريمة المعلوماتية، وذلك بتلقيهم المعلومات الخاصة بتقنية أجهزة النظام المعلوماتي والجوانب الفنية لها، حتى تسهل عليهم عملية الكشف عن الجرائم ومنع وقوعها بإحكام الرقابة التي فعل المشرع الجزائري آلياتها القانونية.

[1] – يقصد بالاتصالات الإلكترونية حسب المادة 02 الفقرة الثانية من قانون رقم 04/09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها(أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتاب أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية)أنظر قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

و لدعم الاجراءات التفتيشية تلعب الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها دور فعال، إذ تعتبر سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وأساسا أعضاء من الحكومة ، معززا ذلك بالمرسوم الرئاسي رقم 261/15[1] وكلفت الهيئة بتنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها[2]،بالاضافة الى صدور المرسوم الرئاسي رقم 05/20 المؤرخ في 20 جانفي سنة 2020 بوضع منظومة وطنية لأمن الأنظمة المعلوماتية ، تدعم اجراءات التفتيش الالكتروني.

ومن خلال ما تقدم يتضح ان المنظومة تعد أداة الدولة في مجال أمن الأنظمة المعلوماتية وتشمل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمنها وتنسيقها و تنفيذها، وتشمل المنظومة الموضوعة لدى وازرة الدفاع الوطني مـايأتي:

– مجلس وطني لأمن الأنظمة المعلوماتية، ويدعي في صلب النص المجلس إعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، الموافقة عليها وتوجيهها .

– وكالة لأمن الأنظمة المعلوماتية تدعى في صلب النص الوكالة وتكلف بتنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

و عليه تتمثل مهام المجلس الوطني لأمن الأنظمة المعلوماتية:

- البث في عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.
- د ارسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما .
- د ارسة التقارير المتعلقة بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، و الموافقة عليها .
- الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.
- الموافقة على تصنيف الأنظمة المعلوماتية .
- يبدي المجلس رأيـا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية[3].

---

[1]- راجع المرسوم الرئاسي رقم 261/15 المؤرخ في 8 أكتوبر سنة 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية ، العدد رقم53 الصادرة في 08 أكتوبر سنة 2015 .

[2] – **نورة صرشي** ، (مكافحة الجريمة المعلوماتية)، مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق جامعة الجزائر ،سنة 2012،(ص). 65.

[3] – **منصورية بلعيد**،(النظام الاجرائي للجريمة المعلوماتية)،مذكرة لنيل الماستر في تخصص القانون القضائي، جامعة بن باديس مستغانم ، السنة الجامعية2020،(ص). 95

ملخص الفصل الاول

تعد الجريمة المعلوماتية نمط للاعتداء بمقتضى أفعال جنائية غير مشروعة تتضمن كافة الاركان التي يشترطها المشرع، لتكون محلا للمتابعة الجنائية، بمقتضى النصوص التشريعية والتنظيمية ، الا ان مرونة هذه الجرائم يقتضي تدخل المشرع بآليات تتميز بالسرعة و التقنيات الفنية لتلاءم طبيعة الاجرام الحديث و مقتضياته التي فرضت على المشرع الجزائري الدخول في اتفاقيات دولية على اساس الاستفادة من خبرات الدول في هذا المجال و الحصول على الدعم الدولي في مجال التفتيش الالكتروني الذي يعد آلية للمتابعة الجنائية.

و عليه يتميز التفتيش الالكتروني بحداثته بالنظر الى ما تطرحه الجرائم المعلوماتية من قضايا واقعية تتضمن الاعتداء على منظومة معلوماتية تحمل اسرار وخصوصية يتم الاعتداء عليه بحسب طبيعة الجرم الجنائي اثر التقدم العلمي في مجال الاتصال و استخدام التكنولوجيات المتقدمة على مجالات الحياة المتعددة بحيث اصبح بؤرة لارتكاب العديد من الجرائم ، في وسط إفتراضي غير متعارف عليه ، مما دفع المشرع الجزائري الى تعديل بعض احكام قانون 2006 المتعلق بقانون العقوبات، بالإضافة إلى تعديله لقانون الإجراءات الجزائية إلا أن كل هذا لم يغطي الصرح الكبير الذي تسميه الجريمة المعلوماتية في العالم المعلوماتية.

و على هذا الاساس يعد التفتيش الالكتروني إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات و تخزين و مخرجات لأجل البحث فيها عن أفعال غير مشروعة تشكل جناية أو جنحة و التوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة و نسبتها الى المتهم بارتكابها، وفقا لشروط و ضوابط قانونية حددها المشرع الجزائري تضمن نسبة الجريمة الى الجاني ، و تعطي صلاحيات للجهات المختصة للقيام بعمليات التفتيش الالكتروني.

الفصل الثاني:

الاحكام الاجرائيـة للتفتيش الالكتروني

المبحث الأول: الجهات المختصة بالتفتيش الالكتروني

المبحث الثاني: الضمانات القضائية للتفتيش الالكتروني

الفصل الثاني: الاحكام الاجرائية للتفتيش الالكتروني.

إن استعمال تكنولوجيا المعلوماتية مرتبط باستخدام شبكة الأنترنت، فأدمجت معظم دول العالم تقنية المعلومات لتعبر على مدى التقدم في الثورة التكنولوجية الا انها استخدمت من جهة آخرى كأداة اجرامية من خلال استغلال الأنظمة المعلوماتية وتطبيقاتها المتعددة بروز عدة جرائم حديثة إلى بروز عدة أثرت على الجانب التشريعي في الجزائر، وعلى هذا الاساس لابد من وجود مبرر اجرائي للتفتيش الالكتروني، بهدف كشف الحقيقة سواء أكانت الأدلة المراد البحث عنها لإثبات التهمة او نفيها. وعليه سيتم معالجة الموضوع وفقا للخطة الآتيـــة:

المبحث الاول: الجهات المختصـة بالتفتيش الالكتروني.

المبحث الثاني: الضمانات القضائية للتفتيش الالكتروني.

المبحث الاول: الجهات المختصة بالتفتيش الالكتروني.

يعد التفتيش الالكتروني من بين الأساليب والإجراءات التي تتماشى و خصوصية الجرائم الالكترونية لأنه ينصب على محل جريمة يتميز ببيئة رقمية افتراضية ، و حتى يكون التفتيش مشروعا لا بد من وقوع جريمة من الجرائم المعلوماتية واتهام شخص أو أشخاص معينين بارتكـاب هذه الجريمة أو المشاركة فيها و توافر أمارات أو دلائل على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره بمقتضى ضبط قواعد اجرائية خاصة من الناحية القانونية و العملية، والتي سنسلط عليها ضوء المعالجة الاجرائية، و عليه سيتم معالجة الموضوع وفقا للخطة الآتية:

المطلب الاول: الاختصاص النوعي للتفتيش الالكترونية.

المطلب الثاني: الاختصاص المكـاني للتفتيش الالكتروني.

المطلب الثالث: القواعد الاجرائية للحجز الالكتروني و التفتيش عن الادلة الرقمية وجمعها .

المطلب الاول: الاختصاص النوعي للتفتيش الالكترونية.

تسمح إجراءات التفتيش الالكتروني بتسهيل مكافحة الجرائم المعلوماتية، إذ الاثر المترتب على التفتيش المنصب على المنظومة المعلوماتية هو منع المجرم المعلوماتي من تدمير أو إخفاء الدليل للإفلات من العقوبة وذلك بموجب نصوص القانون 04/09 السالف الذكر وتطبيقا لنصوص الاتفاقية العربية لمكافحة جرائـم تقنيـة المعلومـات خاصة المادتـان 26 و27 المتعلقتـان بتفتيـش المعلومـات المخزنـة و ضبطها.

الفرع الاول: اجراءات التحري في التفتيش الالكتروني للمنظومة المعلوماتية.

لا يكفي قيام جريمة معلوماتية فقط لقيام سبب التفتيش الالكتروني بل لا بد أن يوجه الاتهام إلى شخص أو أشخاص معينين تقوم دلائل كافية للاعتقاد أنهم من ساهموا في ارتكاب الجريمة سواء كانوا فاعلين أصلين أو شركاء فيها، حتى تكون اسباب التفتيش صحيحة و قانونية، ووفقا للإجراءات التي حددها المشرع.

اولا: السلطات المختصة بالتفتيش الالكتروني.

ان اجراءات التفتيش الالكتروني لا تعد صحيحة ومنتجة لآثارهـا إلا إذا تم القيام به من طرف الأشخاص أو الجهات المخول لها قانونا صلاحيات إجرائه، وقد اختلفت التشريعات الإجرائية في هذا الشأن، فمنها من أسند هذه المهمة إلى المدعي العام وهناك من منحها إلى قاضي التحقيق أو ضباط الشرطة القضائية، وبالنسبة للمشرع الجزائري فقد أوكل صلاحية إجراء التفتيش إلى السلطات القضائية الممثلة في النيابة أو التحقيق وكذا ضباط الشرطة القضائية وفقا لأحكام المادة 05 من القانون رقم 11/21 ق.إج.ج[1].

ومن الملاحظ ان المشرع اجاز لوكيل الجمهورية و لقاضي التحقيق او ضباط الشرطة القضائية في اجراءات التفتيش الالكتروني تسخير كل عون مؤهل له إلى المهارات الفنية التي تتطلبها الجريمة المعلوماتية فقد أجاز المشرع الجزائري للسلطات المكلفة بالتفتيش الاستعانة بخبير له دراية بالمعلوماتية محل البحث أو التدابير المتخذة من اجل المحافظة على الدليل، طبقا لمقتضيات المادة 05 الفقرة الرابعة من الأمر رقم 04/09 ،و تقديم التوضيحات و كيفية التفتيش بطرق صحيحة عليه للطرق التقنية الحديثة[2].

و بالنظر لخصوصية التفتيش الالكتروني فانه يخضع من حيث الاجراءات و الضبط للأحكام المتعلقة بالجرائم الماسـة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم المنصوص عليها على سبيل الحصر في المادة 03/47 ق.إ.ج.ج، فتخضع لقواعد خاصة تختلف عن القواعد العامـة المقررة في البندين 01 و 02 من المادة 01/45 ق.إ.ج.ج[3]، و تتباين القواعد حسب حالتين:

01- الحالة الأول تتعلق بالجرائم الخاصة.

إذا تعلق الأمر بالتحقيق التمهيدي في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة أنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، فإن ضابط الشرطة القضائية بموجب الفقرة الأخيرة من المادة 45 إ.ج.ج لم يعد مقيدا عند إجراء تفتيش المساكن والمحلات لشرط المتعلق بضرورة حضور المشتبه فيه أو من ينوبه أو شاهدين إذا حصل التفتيش

---

[1]- **د/ رضا هميسي**، المرجع السابق ،(ص).162.

[2] - **زبيحة زيدان**، المرجع السابق،(ص).160.

[3] - راجع المادة 45 الفقرتين الاولى و الثانية من الامر رقم 11/21 المؤرخ في 25 اوت 2021 المتعلق بقانون الاجراءات الجزائية الجزائري.

في مسكن المتهم وفقا للمادة 82ق.إ.ج.ج "...غير انه يجوز له وحده في مواد الجنايات ان يقوم بتفتيش مسكن المتهم في غير الساعات المحددة في المادة 47 بشرط ان يباشر التفتيش بنفسه و ان يكون ذلك بحضور وكيل الجمهورية "، و يختلف الأمر إذا حصل التفتيش في مسكن غير المتهم او شخص آخر يشتبه فيه يحوز أوراقا أو أشياء لها علاقة بالجريمة[1].

02- الحالة الثانية تتعلق بالجرائم المعلوماتية.

أصبح من صلاحيات ضابط الشرطة القضائية إذا تعلق التحقيق التمهيدي الذي يجريه بجريمة متلبسا بها أو تحقيق متعلق بإحدى الجرائم المعلوماتية المرتبطة بتفتيش مساكن التي توجد بها أجهزة حواسيب آلية ، يمكنه بموجب المادة 47 مكرر المستحدثة في قانون الإجراءات الجزائية أن يجري التفتيش بعد الموافقة المسبقة من وكيل الجمهورية بحضور شاهدين مسخرين من غير الموظفين الخاضعين لسلطته أو بحضور ممثل يعينه صاحب المسكن محل التفتيش، إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا في مكان آخر وأن الحال يقتضي عدم نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس لنظام العام أو لاحتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله.

و يقوم على آداء وظائف التفتيش ضباط شرطة متخصصين بناءا على اذن بالتفتيش من الجهات القضائية ، فتقوم بحكم موقعها الوظيفي بالبحث و التحري حول الجرائم المعلوماتية من خلال ما تكرسه شرطة الانترنت من ضمانات عند توليها مباشرة الاجراءات في العالم الافتراضي، بشرط ان تكون الجهات القائمة التفتيش الالكتروني على كفاءة تدريبية في مجال الجرائم المعلوماتية[2].

لذلك دعم المشرع الجزائري الجهاز الشرطوي بأنظمة تسهر على مواكبة الجرائم الحديثة وتشرف عليها في هذا المجال الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، فهناك هيئات تابعة للجهاز الأمني، مكلفة بالتدخل للمواجهة العملية على المستوى التطبيقي للجرائم المعلوماتية، وتصنف الهيئات التابعة للجهاز الأمني والمكلف بمكافحة الجرائم المعلوماتية، تابعة لسلك الأمن الوطني[3]، بحث يوجد على مستو ى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي:

- المخبر المركز ي للشرطة العلمية.
- المخبر الجهوي للشرطة العلمية بقسنطينة.
- المخبر الجهوي للشرطة العلمية بوهران.

---

[1]- راجع المادتين 83 من الامر رقم 11/21 المؤرخ في 25 اوت 2021 المتعلق بقانون الاجراءات الجزائية الجزائري.

2 - **أ/نبيلة هبة هروال**، المرجع السابق،(ص). 100

[3] - **سعاد رابح**، المرجع السابق،(ص).281

ثانيا: ضوابط التحري في مجال الالكتروني.

01- التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في مرحلة التحقيق الابتدائي.

ترتبط الجريمة الرقمية بالمنظومة المعلوماتية باعتبارها نظام منفصل او مجموعة من الانظمة المتصلة ببعضها البعض او المرتبطة يقوم واحد منها او اكثر بمعالجة آلية للمعطيات لتنفيذ برنامج معين إذ يتم تطبيقه وفقا لقواعد مرتبطة بحواسيب و ادوات تعمل بشكل متكامل لأداء مهمة في معالجة البيانات آليا[1].

و على هذا الاساس يؤكد الفقهاء ضرورة تماشي اجراءات التفتيش مع خصوصية هذه الجرائم ، لذا وضع المشرع الجزائر الاستثناء في قانون الاجراءات الجزائية ، فلا يطبق في التفتيش الالكتروني المرتبط بالجرائم المعلوماتية القيود المنصوص عليها في المادة 47 الفقرة الاولى من ق.إج.ج ، و تؤكد الاستثناء الفقرة الثانية من نفس المادة المتعلقة بالميعاد القانوني "غير انه يجوز اجراء التفتيش و المعاينة و الحجز في كل ساعة من ساعات النهار او الليل في الجرائم المعاقب عليها في المواد 342الى 348 من قانون العقوبات...و عندما يتعلق الامر بجرائم المعالجة الالية للمعطيات ..."، و ترجع أسباب هذا الاستثناء الى الظروف الآتية:

- التفتيش الالكتروني يحتاج الى جهات متخصصة في عمليات البحث الرقمي و كل ما يفيد في كشف الحقيقة مما تتلاشى معه مسألة احترام الزمن المحدد للتفتيش في الاجراءات العادية.
- الخروج عن الاحكام العامة في قانون الاجراءات مرده الى قوة تدفق المعلومات و سهولة التحكم في المعطيات، مما يفسح المجال للجناة للتحكم في الدليل الجنائي.
- الخوف من تحكم الجناة في المعلومات و طمس الشاهد الالكتروني ، لذا اجاز المشرع التفتيش الالكتروني في المنظومة المعلوماتية عن بعد، لمواجهة آثار تغيير الدليل.
- احترام الميعاد القانوني يؤدي الى عدم جدوى التفتيش الالكتروني، و يفسح المجال للجناة للتلاعب بالأدلة.

02- التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في مرحلة التحقيق القضائي.

تنص المادة 79 إ.ج.ج على أنه يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات، على أن يباشر التفتيش وفقا للمادة 81 إ.ج.ج في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا الحقيقة.

03- بالنسبة للميقات القانوني للتفتيش والضبط في الجرائم الماسة أنظمة المعالجة الآلية للمعطيات.

باستقراء المادة 83 ق.إ.ج.ج و التي تحيلان إلى المادة 47 ق.إ.ج.ج الخاصة بميقات التفتيش القانوني، وفي إطار وضع الأسس القانونية الكفيلة بمحاربة بعض الظواهر الإجرامية الحديثة، كجرائم الإرهاب والمخدرات

1- **د/بلال أمين زين الدين**، "جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن"، دار الفكر الجامعي، الإسكندرية 2008طبعة،(ص). 22

والجريمة المنظمة عبر الوطنية والجرائم الماسة الانظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والجرائم المتعلقة التشريع الخاص لصرف، يقرر قانون الإجراءات الجزائية لقاضي التحقيق دخول المساكن وتفتيشها في أي وقت خارج الميقات القانوني المقرر في المادة 01/47 ق.إ.ج.ج متى تعلق الأمر بتلك الجرائم، وله أن يأمر ضابط الشرطة القضائية المختص مكانيا للقيام بتلك الإجراءات.

04- بالنسبة لضبط أدلة الجريمة:

يترتب على اجراءات التفتيش الإلكتروني وصول جهات التحري الى نتائج التفتيش ،فيتم حجزها وفقا للمقتضيات القانونية ، إذ تنص المادة 84 ق.إ.ج.ج على أنه إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات الكترونية فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوبة عنه وحدهما الحق في الإطلاع عليها قبل ضبطها، وعلى قاضي التحقيق أن يتخذ مقدما جميع الإجراءات لضمان احترام كتمان سر المهنة و ضمان حقوق الدفاع، ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة.

ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا كما يستدعى أيضا كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء ولا يجوز لقاضي التحقيق أن يضبط غير الأشيـاء والوثائق النافعة في إظهار الحقيقـة أو التي قد يضر إفشاؤها بسير التحقيق ، ويجوز لمن يعنيهم الامر الحصول على نفقتهم، وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تخل بمقتضيات التحقيق[1].

05- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

حدد قانون 11/21 المتعلق بالإجراءات الجزائية الجزائري في الباب الثاني من الكتاب الأول الفصل رابع بعنوان " اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" ويشمل المواد من 65 مكرر05 إلى 65 مكرر10 حيث اجاز لرجال الشرطة القضائية إذا اقتضت ضرورات التحري في الجريمة المتلبس بهـا أو التحقيق الابتدائي، القيام اعتراض المراسلات، تسجيل الأصوات والتقاط الصور لكنه قيدهم بجملة من الشروط لتكون الإجراءات صحيحة ومنتجة لآثارها وهي:

- أن يقوم الضباط بهذه الأعمال سعيا للكشف عن جرائم حددها المشرع في المادة 65 مكرر05 وهي: جرائم المخدرات، الجرائم المنظمة العابرة للحدود الوطنية، الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة لتشريع الخاص لصرف، جرائم الفساد.

[1] - **د/أحمد عبد الحكيم عثمان**، المرجع السابق،(ص). 221.

ما يلاحظ أن المشرع الجزائري عدد هذه الجرائم على سبيل الحصر وقد يرجع هذا للخطورة الإجرامية لهذه الأفعال وأثرها على السياسة العامة في الدولة واقتصادها، المقصود بالتحقيق الابتدائي، هو التحريات الأولية للضبطية ، أما إذا كانت هذه الأعمال في غير هذه الجرائم فإجراؤها باطل[1].

– أن يصدر الإذن إلى ضباط الشرطة القضائية للقيام لأعمال المحددة في المادة 65 مكرر05، و ان يكون من وكيل الجمهورية أو قاضي التحقيق المختصين[2] وفقا لمـــايلي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية:
- وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

ثالثا: مقتضيات اجراءات التفتيش الإلكتروني.

يعد التفتيش الإلكتروني إجراء تحققي في الجرائم المعلوماتية ، يستهدف ضبط أدلة الجريمة مثل البرامج الغير المشروعة والملفات المخزنة في الحواسيب و المعطيات المعلوماتية والاتصالات الالكترونية قد يتطلب التحقيق تفتيش شخص المتهم أو منزله قصد ضبط الاشياء المحصلة من الجريمة، يخضع للقواعد الخاصة لاذن التفتيش، وتختلف معطياته بحسب نوع كل جريمة.

01– ضوابط الاذن بالتفتيش الالكتروني

ان الإذن المسلم يسمح بوضع الترتيبات التقنية لدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن. فتنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص و في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة، وفقا للمقتضيات الآتيـة:

– ضابط الشرطة القضائية مقيد أثناء قيامه لعمليات المحددة في المادة 65 مكرر05 للحفاظ على السر المهني ، وهذا راجع لخطورة هذه الأفعال الإجرامية التي تنفذ على مستوى من الاحتراف والسرية ، وإذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة.

---

[1] – **د/نصر الدين هنوني، دارين يقدح**، الضبطية القضائية في القانون الجزائري، الطبعة الثانية، دار هومة، الجزائر، طبعة 2011،(ص). 78.

[2] – يلاحظ انه قبل تعديل القانون رقم 22/06 لا يجوز اتخاذ هذا الاجراء و اللجوء إليه خلال مرحلة التحريات الأولية حتى ولو تعلق الأمر بحالة تلبس، ثم استحدث المشرع اللجوء إلى هذه الأساليب بموجب تعديل القانون رقم 22/06 لتتماشى مع التطورات الحديثة التي تشهدها المنظومة الجنائية.

– يجب أن يتضمن الإذن المذكور، كل العناصر التي تسمح لتعرف على الاتصالات المطلوب التقاطها كتحديد رقم الهاتف واسم المشترك، وتحديد الأماكن المقصودة سكنية أو غيرهـــــا، وتحديد نوع الجريمة التي تبرر اللجوء إلى هذه التدابير[1].

– يسلم الإذن مكتوب لمدة أقصاها أربعة (04) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

– يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالاتصالات السلكية واللاسلكية للتكفل لجوانب التقنية للعمليات الذكورة في المادة 65 مكرر05.

– يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

– يصف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات والصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع لملف، وتنسخ وتترجم المكالمات التي تتم للغات الأجنبية، عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض.

02– ضبط اجراءات التفتيش الالكتروني وفقا للقانون رقم 04/09

نص المشرع الجزائري في القانون رقم 04/09 على جملة من الإجراءات المستحدثة و الخاصة لتحري والتحقيق عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومنها الجرائم الماسة بالتوقيع الإلكتروني،كمراقبة الاتصالات الإلكترونية، تفتيش النظم المعلوماتية، حجز المعطيات المعلوماتية، جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، التحفظ العاجل للبيانات المعلوماتية المخزنة كل إجراء فيما يلي:

– اجراءات مراقبة الاتصالات الإلكترونية.

يقصد بالاتصالات الالكترونية حسب المادة 02 ومن قانون 04/09 أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية. وقد نص المشرع الجزائري في المادة 04 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سابق الذكر، على مراقبة الاتصالات الالكترونية، ونظم الحالات التي تسمح للجوء إلى هذا الإجراء وهي:

[1] – **د/محمد حزيط** ، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة التاسعة، دار هومة، الجزائر، طبعة 2014،(ص). 113

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

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

– لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة م الأبحاث الجارية.

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

و لا يجوز إجراء عمليات المراقبة في الحالات المذكورة سابقا إلا بإذن مكتوب من السلطات القضائية المختصة. عندما يتعلق الأمر بالحالة الاولى يختص النائب العام لدى مجلس قضاء الجزائر يمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته المنصوص عليها في المادة 13 من نفس القانون، إذ لمدة ستة (06) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[2].

و على هذا الاساس تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الحالة الاولى ، موجهة حصرا لتجميع وتسجيل معطيات ذات صلة للوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير[3].

ولقد أوكل المشرع الجزائري بموجب المادة 04 فقرة 03 من قانون 04/09 ،والمادة 04 فقرة 02 بند 04 من المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر سنة 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مهمة مراقبة الاتصالات الالكترونية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تحت سلطة القاضي المختص.

– اجراءات تفتيش الالكتروني للنظم المعلوماتية.

نص المشرع الجزائري في المادة 05 من القانون رقم 04/09 على ضرورة توافر حالات على سبيل الحصر، تجيز للسلطات القضائية وضباط الشرطة القضائية القيام بتفتيش المنظومة المعلوماتية في إطار قانون الإجراءات الجزائية وهي الحالات المذكورة في المادة 04 منه حيث نصت المادة05 منه" يجوز للسلطات القضائية المختصة

---

[1] – **د/أحمد حزيط** ، المرجع السابق،(ص). 78

[2] – **د/محمد معمر الصغير**، الوافي في الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الحديث، الجزائر ، طبعة 2010،(ص). 88

[3] – راجع القانون رقم 04/09 المؤرخ في 05 اوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

وكذا ضباط الشرطة القضائية ، في اطار قانون الاجراءات الجزائية و في الحالات المنصوص عليها في المادة 04 اعلاه الدخول ولو عن بعد الى

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

– منظومة تخزين معلوماتية.

يلاحظ ان المشرع الجزائري عند وضعه للقانون رقم 04/09 ادرك مدى الصعوبة التي تواجه المحققين و القضاة في البحث عن الدليل الالكتروني و في رصده و حجز المعطيات محل التفتيش و في الدخول الى المنظومة المعلوماتية[1] فنص في المادة 05 منه" يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث او بالتدبير المتخذة لحماية المعطيات التي تتضمنها .قصد مساعدتها و تزويدها بالمعلومات الضرورية لإنجاز المهمة".

– اجراءات حجز المعطيات المعلوماتية.

يرتب التفتيش الالكتروني اثر يتمثل في حجز المعطيات ، يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع علي المعطيات التي يشكل محتواها جريمة لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك ، وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به لا يجوز استعمال المعلومات المتحصل عليها عن طريق عملية المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية[2].

و هذا ما نظمه المشرع الجزائري في نص المادة 06 و07 من القانون04/09.

وتتمثل شروط إجراء الحجز فيمـايلي:

– عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

– يجب على السلطة التي تقوم لتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري العملية على اساسها.

– غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

---

[1] – **أ/ زيبحة زيدان** ، المرجع السابق ،(ص).168

[2] – **أ/عبد القادر عدو**، الجريمة الإلكترونية إجرائيا، الطبعة الثانية، دار هومة، الجزائر ، طبعة ،2016،ص.109

و يلاحظ انه إذا استحال إجراء الحجز وفقا لما هو منصوص عليه فيما سبق، لأسباب تقنية، لذا يتعين على السلطة التي تقوم لتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم إستعمال هذه المنظومة.

– على السلطة التي تباشر التفتيش أن تامر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل استعمال الوسائل التقنية المناسبة لذلك.

– تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز إستعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

– في حال الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس من الدولة، تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة لإعلام والاتصال ومكافحتها حصر إجراءات الحجز[1].

– اجراءات جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات.

نظم المشرع الجزائري ضمن قانون 04/09 سابق الذكر، إجراء جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وجعله من التزامات مقدمي الخدمات في مساعدة السلطات، حيث تنص المادة 10 على أنه" في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة لتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرفات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وكذلك المعلومات المتصلة وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

و يعزز المشرع الجزائري هذا الاجراء بالرقابة التي تقوم بها الجهات المعنية وفقا لنص المادة 12 على أنه: "زيادة على الالتزامات المنصوص عليها في المادة 11 من قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يتعين على مقدمي خدمات " الانترنت" ما يلي:

أ– التدخل الفوري لسحب المحتو ت التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب– وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

[1]– راجع المادة 21 من مرسوم رئاسي رقم 261/15 مؤرخ في 08 أكتوبر سنة 2015، المحدد لتشكيلة و تنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– جمع الأدلة من خلال اعتراض رسائل البريد الالكتروني.

وذلك من خلال الاستعانة ببرامج مصممة للبحث في مضمون الرسائل الالكترونية المتبادلة على شاكلة برنامج كارنيفور و1000 DCS الذي طورته المباحث الفيدرالية لأمريكية FBI الذي يتعقب ويفحص رسائل البريد الالكتروني المرسلة والواردة عبر أي حاسوب خادم تستخدمه أي شركة توفر خدمة الانترنت وهو برنامج مستخدم في التحقيق في قضايا الأمن القومي الأمريكي.

كل هذه الأساليب والبرامج والأنظمة هي وسائل تساعد ضباط الشرطة القضائية في أعمال البحث والتحري و تنفيذ الاذن القضائي بالتفتيش ، ولكن يبقى أمر استخلاص نتائجها أمرا مرهونا بمدى التزام مقدم خدمة الانترنت بمد يد العون لأجل تحديد مكان ارتكاب الجريمة وهوية مرتكبها[1].

ومن ثمة تنصب الاجراءات على مراقبة اتصالاته الإلكترونية التي تتم عن طريق الانترنت بما في ذلك مراسلات البريد الالكتروني ،و يؤكد الفقه ان التقنية المستخدمة في المراقبة ذات طابع الكتروني تتم طريق مجموعة الاجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات المتعلقة بالمجرمين وفق برنامج موضوع مسبقا لتحديدهم من اجل ضبطهم[2].

– اجراءات التحفظ العاجل للبيانات المعلوماتية المخزنة.

تشوب اجراءات التفتيش الالكتروني أثناء عملية التحقيق عيوب تلحق بالمحقق الجنائي في جرائم المعلوماتية و قد تتعلق بأسلوب التحقيق وصعوبته ، وقد ترجع إلى عوائق تحول دون الحصول على الدليل[3] لذا نظم المشرع الجزائري إجراء التحفظ العاجل للبيانات المعلوماتية المخزنة، ضمن قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كالتزام من التزامات مقدمي خدمات الإنترنت.

كما نظمه المشرع الجزائري بأحكام تمنح الهيئة الوطنية سلطة الاشراف و مساعدة السلطات القضائية و مصالح الشرطة في التحريات التي تجريها ، ونظم احكامها ضمن مرسوم رئاسي رقم 261/15 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال وذلك بجعل القيام بهذا الإجراء كمهمة من المهام الموكلة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته[4].

---

[1] – **رابح مباركية** ، المرجع السابق ،(ص).24

[2]– **نبيلة هبة هروال**، المرجع السابق،(ص).168

[3] - **د/خالد ممدوح إبراهيم**، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق،(ص). 128.

[4]– راجع نص المادة 13 من القانون رقم 04/09 منه:" تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته . تحدد تشكيلة الهيئة و تنظيمها و كيفيات سيرها عن طريق التنظيم".

- **الحفظ العاجل للبيانات المعلوماتية المخزنة ضمن قانون 04/09.**

تحدث المشرع الجزائري في الفصل الرابع من قانون المتضمن القواعد الخاصة للوقاية عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سابق الذكر، على أنه من بين التزامات مقدمي الخدمات مساعدة السلطات المكلفة بالتحريات بحفظ المعطيات.

و اكد ذلك المشرع في نص المادة 10 من القانون رقم 04/09 على أنه في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ... وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11منه(**حفظ المعطيات المتعلقة بحركة السير المعلومات**) تحت تصرف السلطات المذكورة. ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزوا بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

بينما فصلت المادة 11 في إجراء حفظ المعطيات المتعلقة بخط السير حيث نصت على أنه: مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:

-المعطيـــات التي تسمح لتعرف على مستعملي الخدمــة،

- المعطيات المتعلقة لتجهيزات الطرفية المستعملة للاتصال،

- الخصـــائص التقنيــة وكذا ريخ ووقت ومدة كل اتصال،

- المعطيات المتعلقة لخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

- المعطيات التي تسمح لتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة، وكذا تلك التي تسمح لتعرف على مصدر الاتصال وتحديد مكانه، تحدد مدة حفظ المعطيات المذكورة، بسنة واحدة ابتداء من تاريخ التسجيل.

- **الحفظ العاجل للبيانات المعلوماتية المخزنة ضمن مرسوم رئاسي رقم 261/15.**

نص المشرع الجزائري في المادة 04 من المرسوم الرئاسي رقم 261/15 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على مهام الهيئة و نظامها ، فمن بين المهام الموكلة للهيئة الوطنية حفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية. إلا أنه لم يحدد المدة القصوى التي تلتزم الهيئة لحفظ هذه المعطيات كما فعل لنسبة لحفظ المعطيات المتعلقة بخط السير على مستوى مقدمي خدمات الانترنت بمقتضى المادة 11 من قانون04/09 .

– اجراءات التسرب الرقمي (طرق التسرب في مجال الجريمة المعلوماتية)

يمكن تصور التسرب في نطاق الجرائم المعلوماتية في دخول ضابط شرطة قضائية او عون شرطة القضائية الى العالم الافتراضي (شبكة الانترنت) وذلك بتسجيله على مواقع معينة كمواقع التواصل الاجتماعي و اشتراكه في

محادثات عبر غرف الدردشة او حلقات الاتصال المباشر لرفع ومعاينة الجرائم او ربط الاتصال مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء او صفات مستعارة ووهمية سعيا منه للتعرف عليهم وتحديد أماكنهم[1].

ويلاحظ ان المشرع الجزائر يدعم اجراءات التفتيش الالكتروني من خلال الوظائف التي تقوم بها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته مساندة بذلك الجهات المختصة بإجراءات التحري و التحقيق وفقا للمهام الآتية:

– تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته.

– مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الاعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية.

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و تحديد مكان تواجدهم.

الفرع الثاني: الاذن و القيام بعمليات التفتيش الالكتروني.

يمتاز التفتيش الالكتروني بأنه وسيلة للبحث عن الأدلة المادية المعنوية للجريمة و ضبطها كما يفيد الكشف عن الحقيقة باستخدام تقنية المعلومات، أي وسيلة مادية أو غير مادية أو مجموعة وسائل مترابطة أو غير مترابطة ، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها. ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكية أو لاسلكية في نظام معلوماتي أو شبكة معلوماتية، و لا تتم اجراءات التفتيش و لا تثبت صحتها الا بإذن من الجهات القضائية المختصة و لا تتم الا وفقا لمعطيات يحددها القانون.

اولا: الاحكام القانونية للإذن بالتفتيش في البيئة الالكترونية.

وفقا للأحكام التنظيمية يشترط في التفتيش الالكتروني لضمان صحته الاذن القضائي الذي يحتاج إلى تقدير فني لأجل التأكد من مدي صحة قواعده واتخاذ تقرير الاجراءات الكفيلة بمتابعة مرتكبيها واثبات الأدلة في مواجهتهم، ويتم الانتقال إلى مسرح الجريمة تنفيذا عادة لأوامر وكيل الجمهورية في إطار إتمام إجراءات البحث و التحري، أو تنفيذا لأوامر قاضي التحقيق ويشترط احترام الشروط المتعلقة بالإذن المكتوب[2].

و من ثمة تتعدد و تختلف صور الاذن بالتفتيش فغالبا ما يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يتواجد في المسكن، ومن ثم هل يجوز بمقتضى هذا الإذن لضباط الشرطة القضائية الولوج إلى

---

[1] – **نعيم سعيداني**، المرجع السابق،(ص).177

2 – **رابح مباركة**، (اجراءات التحري والتحقيق في الجريمة الالكترونية)،مذكرة لنيل الماستر في تخصص قانون الاعلام الالي و الانترنت ، جامعة محمد الابراهيمي ، جامعة برج بوعريريج، السنة الجامعية 2022/2021،ص66

البيئة الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن أدلة إثبات التي يمكن أن تكون محل الضبط[1]. وقد نص التشريع الإجرائي الجنائي الجزائري على إمكانية الوضع تحت المراقبة الالكترونية في مجال مكافحة الجرائم المعلوماتية حسب نصوص المواد65 مكرر05 إلى مكرر10قانون22/06، وذلك تحت الفصل الرابع الموسوم باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بحيث يجوز لوكيل الجمهورية وكذلك لقاضي التحقيق في حال فتح تحقيق قضائي، منح إذن لضابط الشرطة القضائية المكلفين بالبحث والتحري عن الجرائم المعلوماتية، يتضمن اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية دون موافقة المعنيين بها.

ويشترط في الإذن أن يكون مكتوبا ومتضمنا لكافة العناصر الأساسية التي تسمح بالتعرف على الاتصالات المطلوب التقاطها وذلك لمدة أقصاها 04 أشهر قابلة للتجديد، ولصاحب الإذن الحق في تسخير أي عون عمومي أو خاص لدى هيئة الاتصالات السلكية أو اللاسلكية من أجل التكفل بالجوانب التقنية المتعلقة بالعملية، وتختتم العملية بإعداد محضر من قبل ضابط الشرطة القضائية يتضمن مضمون العملية مع توضيح تاريخ وساعة بداية العملية وانتهائها.

ثانيا: دعائم الاذن بالتفتيش الإلكتروني.

يقصد سعى المشرع الجزائري الى ضبط الجانب الاجرائي للتفتيش الالكتروني من خلال توزيع المهام و تكليف الجهات المختصة بإذن التفتيش فهو ذلك التفويض الموجه من سلطة التفتيش المختصة إلى أحد مأموري الضبط القضائي متضمنا تخويله إياه إجراء التفتيش الذي تختص به تلك السلطة [2]وعليه يجب أن يحدد في الإذن الندب بالتفتيش المكان و الشخص و الأشياء المراد تفتيشها و ضبطها كتحديد الحاسوب ، برامج الاختراق برامج الفيروسات .

دعم المشرع الجزائري الاذن بالتفتيش الالكتروني بتدخل الهيئة الوطنية للوقاية من الجرائم المتصل بتكنولوجيا الاعلام و الاتصال و مكافحته بالنظر الى الجوانب الفنية و التقنية التي يتميز بها التفتيش الالكتروني لذا لجأ إلى هذا الأسلوب سنة 2009 بموجب نص كل من المادتين 03 و04 الواردتين ضمن فصول القانون04/09 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال الهيئة المختصة بتنفيذ عمليات المراقبة الإلكترونية للإتصالات.

و تم تعزيز ذلك من خلال إستحداث مديرية المراقبة الوقائية واليقظة الإلكترونية التي يدخل في صميم إختصاصاتها القيام بمهام المراقبة الإلكترونية للإتصالات من أجل الكشف عن الجرائم المعلوماتية بناء على

---

1 – **د/علي حسن طوالبة**، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة، الطبعة الأولى ،2004،(ص).31.

2 – **أ/ رشيدة بوكر**، المرجع السابق،(ص).374.

رخصة مكتوبة من السلطة القضائية وتحت مراقبتها، حسب ما تقره المادة 11 من المرسوم الرئاسي 261/15 كما منحها القانون حسب نص المادة 21 من المرسوم السالف الذكر الصفة الحصرية لتولي مهام المراقبة الإلكترونية في حال تصنيف الجريمة المعلوماتية ضمن الجرائم الإرهابية والتخريبية والماسة بأمن الدولة دون سواها من الهيئات الوطنية الأخرى وذلك تحت سلطة قاض مختص[1].

ثالثا: التقنيات والوسائل الفنية المستخدمة في اذن التفتيش الالكتروني.

ينفذ التفتيش الالكتروني باستخدام تقنيات حديثة تتلاءم و طبيعة الجرائم المرتكبة من خلال عملية المراقبة والتتبع الإلكتروني في مجال الجرائم المعلوماتية و بالنظر لصعوبات التفتيش في المنظومة والنظام المعلوماتي يتم الاستعانة ببعض الوسائل التقنية نذكر منها:

01– تقنية تتبع عنوان: (TCP –IP)

عنوان IP هو العنصر المسؤول عن تراسل الحزم البيانية عبر شبكة الانترنت وتوجيهها إلى أهدافها، ويعتبر بمثابة عنوان الحاسوب المتصل بالشبكة ويتكون من شفرة رقمية تتكون من أربع 04 أجزاء ، يشير الأول إلى المنطقة الجغرافية والثاني لرمز مقدم الخدمة، والثالث لمجموعة الحواسيب المرتبطة و الرابع يخص الحاسوب الذي يتم الاتصال منه[2].

ففي حالة وجود جريمة معلوماتية فإن ضباط الشرطة القضائية يسلطون ضوء عمليات التفتيش على فضاء الاتصالات الإلكترونية التي يقصد بها كل تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعته عن طريق أي وسيلة إلكترونية ، و تعمل الهيئة الوطنية للوقاية من جرائم الاتصال على مساعدة السلطات القضائية وفقا لنص المادة 05 فقرة 01 من المرسوم الرئاسي 261/15، فتعمل مصالح الشرطة القضائية في مجال التحريات الالكترونية ، ضمن فريق تحقيق يقومون بتتبع عنوان IP للجهاز مصدر الجريمة وتحديد موقعه[3].

02– استخدام تقنية فحص البروكسي برنامج (PROXY).

البروكسي هو الوسيط العامل بين الشبكة والمستخدم، تستخدمه الشركات المقدمة لخدمة الاتصال لأجل إدارة الشبكة ،وضمان أمنها وتوفير حزمة الذاكرة الجاهزة Memory يعمل البروكسي على تلقي طلب المستخدم للبحث عن صفحة ما فيتحقق ضمن الذاكرة الجاهزة عما إذا جرى تنزيل الطلب من قبل فيقوم بإعادة إرسالها للمستخدم دون الحاجة إلى طلبها من الشبكة العالمية للمعلوماتweb من أجل تزويد المستخدم بها، ومن

---

[1] – **رابح مباركية**، المرجع السابق،(ص).53

[2] - المرجع نفسه ،(ص).21

[3] – **د/عبد الله بن سعود محمد السراني**، فاعلية الاساليب المستخدمة في اثبات جريمة التزوير الالكتروني ، جامعة نايف العربية للعلوم الامنية (بدون ذكر مكان النشر)، طبعة 2011،(ص).51

مزاياه أن ذاكرته هذه يمكن أن تحتفظ بتلك المعلومات والعمليات، وهو ما يمنح لضباط الشرطة القضائية فحصها واستخلاص الدلائل ضد المتهم بمساعدة مزود الخدمات[1].

03- استعمال برامج التتبع المعلوماتي برنامج (HACK- TRACER)

يمكن لبرامج التتبع ان تقوم بالتعرف على محاولات الاختراق و من قام بها، واشعار الجهة المتضررة بذلك، وهذه البرامج عادة ما تكون ٍ بالتعرف على محاولات ساكنة في خلفية المكتب، عندما ترصد أي محاولة للقرصنة أو الاختراق وتسارع بغلق منافذ الدخول للمخترق، ثم تبدأ بعملية مطاردته واقتفاء أثره وصولا إلى تحديد عنوانه الإلكتروني (IP) واسم الشركة المزودة بخدمة الانترنت ومعلومات أخرى، يتكون من شاشة رئيسية تقدم للمستخدم بيانا بعمليات الاختراق ، فيستعين بها ضباط الشرطة القضائية للوصول الى الجنـاة[2].

04- الاستعانة بنظام كشف الاختراق (System Detection Intrusion)

هو النظام الذي يرمز له بـ S.D.I وهو نظام يعتمد على مجموعة من البرامج التي تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الشبكة مع تحليلها بحثا عن أي إشارة قد تدل على وجود مشكلة تهدد أمن الحاسوب والشبكة ، و يتم ذلك من خلال تحليل رزم البيانات اثناء انتقالها عبر الشبكة، و مراقبة بعض ملفات التشغيل فيستعين بها ضباط الشرطة القضائية بتسجيل الاحداث فور وقوعها في الحاسوب او الشبكة[3].

05- العمل بنظام التمويه.

هو نظام حاسوبي مخصص لكي يتعرض للهجمات الإلكترونية عبر الشبكة، من خلال خداع من يقوم بذلك وذلك بإبداء سهولة في الاعتداء عليه وذلك لإغرائه، وذلك حتى يتمكن من جمع أكبر قدر من المعلومات عن أسلوب الهجوم وتحليله وهو ما يسمح لجهات التحري و التحقيق إتخاذ الإجراءات الوقائية التي تزود فريق التحقيق بالمعطيات اللازمة، والعديد من البيانات التي توضح معالم الجريمة[4].

ثالثا: الاذن بالتفتيش الالكتروني و التزامات مقدمي خدمات الانترنت

يقصد بمزود الخدمات أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات لأجل التواصل بواسطة تقنية المعلوماتية، ويقوم بتخزين ومعالجة المعطيات بما فيها المعلومات الخاصة بالمشترك كنوع خدمة الاتصالات المستخدمة لديه، هويته، عنوانه البريدي، رقم هاتفه وذلك بناء على اتفاق ترتيب الخدمة القائم بينهما ، **يقدمون** المساعدة في مجال أعمال البحث والتحري وفقا للمادة 12 من القانون04/09

---

[1]- **أ/خالد عياد الحلبي**، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، الطبعة الاولى ، دار الثقافة للنشر والتوزيع ، عمان، الاردن، طبعة 2011،(ص).206.

[2] - **رابح مباركية** ، المرجع السابق ،(ص).36.

[3] - **أ/ خالد عياد الحلبي**، المرجع السابق،(ص). 209

[4] - **د/عبد الله بن سعود محمد السراني** ، المرجع السابق،(ص).51.

و منه نستنتج أن القانون قد سمح للسلطات المختصة بمتابعة الجرائم المعلوماتية حق طلب التحفظ على البيانات المخزنة لديها وحق كذلك تزويدها بالمعلومات الخاصة بالمشترك ونشاطه في إطار عملها المتعلق بأعمال البحث والتحري عن الجرائم المعلوماتية.

و بالرجوع الى النصوص الدولية نجد انه إجراء و التزام المستوى الدولي حسب ما تقرره أحكام المادتين 16 و17 من اتفاقية بودابست لمكافحة الجرائم المعلوماتية[1]، وقد وردت هذه الالتزامات على المستوى الوطني حسب ما جاء في نص المادة 10 من القانون رقم 04/09، التي توجب على مقدمي خدمة الانترنت مساعدة السلطات في إطار التحريات القضائية من خلال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ، ووضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات المذكورة وكل ذلك تحت غطاء السرية ، كما ألزمت المادة 11 من نفس القانون مقدمي الخدمات حفظ المعطيات التالية:

- المعطيات التي تسمح بالتعرف على مستخدمي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة.
- المعطيات التي تسمح بالتعرف على المرسل إليه وعناوين المواقع المطلع عليها.

ولضباط الشرطة القضائية تسهيلا لعمليات التفتيش الإلكتروني إمكانية تقديم طلبات لمزودي الخدمة بالانترنت لأجل تزويدهم بالمعلومات المخزنة ومن ضمن هذه الطلبات:

- طلب التحفظ المعجل على البيانات المخزنة ليتفادى المزود شطب التسجيلات و القضاء على الدليل.
- طلب تقديم بيانات معلوماتية خاصة بالمشترك.
- طلب اعتراض على الاتصـــالات الالكترونيـة.

إذن تعتبر هذه الإجراءات ذات الطابع الإجرائي الفني والمعلوماتي في مجال أعمال البحث والتحري عن الجرائم المعلوماتية التي يباشرها ضباط الشرطة القضائية تنفيذا للاذن القضائي بالتفتيش و الخضوع لتعليمات وكيل الجمهورية أو قاضي التحقيق أو اختصاصا منهم، وذلك من خلال ممارسة مهامهم بعيدا عن مسرح الجريمة أي في مرحلة تسبق التنقل للمعاينة والتفتيش المادي وضبط الأدلة الالكترونية والمادية وهي الإجراءات التي تختلف نوعا ما من حيث الوسائل والطرق بالنسبة للإجراءات الفنية الخاصة بمعاينة مسرح الجريمة المعلوماتية[2].

و بناءا عليه حدد المشرع الجزائري إجراءات البحث و التحري الأولية بشأن الجريمة المعلوماتية و التي يبادر إليها ضباط الشرطة القضائية، بمجرد الوصول إلى علمهم بوقوع الجريمة، تنتقل إلى تفصيل المسائل

---

[1] – أ.**د/ هلالي عبد اللاه احمد**، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)،(ص).191.

[2] – **د/خالد عياد الحلبي** ، المرجع السابق ،(ص).197.

الخاصة بالإجراءات العملية ذات الطابع الخاص المتعلقة بمرحلة المعاينة والتفتيش والتي يتم عادة على مسرح الجريمة، والتي تقتضي تنقل الجهات المختصة من أجل تحقيق الهدف الرئيسي وهو إحراز الادلة المادية والإلكترونية، والتي من شأنها إثبات الادانة أو براءة المتهم، وعادة ما يتولى مهمة الانتقال إلى مسرح الجريمة المعلوماتية، الفرقة الخاصة بالبحث والتحقيق في مسائل الجرائم المعلوماتية، نظرا لتوفرهم على معارف تسمح لهم بالتعامل الصحيح مع أدلتها، ولا يتم الانتقال إلى مسرح الجريمة إلا لفرضيتين اثنتان:

- فرضية مداهمة مسرح الجريمة المتلبس بها ، وهو أمر مستبعد جدا إذا لم نقل نادر ، نظرا لخصوصية الجريمة و المجرم المعلوماتي، اللذان يتميزان بالخفاء و السرية في تنفيذ الجريمة إضافة إلى صعوبة كشفها.
- فرضية تنفيذ المهام الموكلة لهم إما من تلقاء أنفسهم بناء على بلاغ أو شكوى بشأن جريمة معلوماتية، أو تنفيذا لأوامر وكيل الجمهورية أو قاضي التحقيق، وهي الفرضية الأقرب للتجسيد نظرا إلى ضرورة تضافر الجهود الفنية والقانونية لأجل مكافحة الجرائم المعلوماتية.

رابعا: شروط تنفيذ الاذن بالتفتيش الالكتروني.

لحماية الحريات الفردية من التعسف و الانحراف في استعمال السلطة فان الشروط الموضوعية غير كافية ، فلا بد من وجود شروط شكلية لصحة إجراء التفتيش في الجرائم المعلوماتيـــة وتتمثل هذه الشروط في الشروط الشكلية للاذن بالتفتيش الالكتروني.

01-الحضور الضروري لبعض الأشخاص أثناء التفتيش في البيئة التقنية.

يعد هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط ، و بالرجوع إلى النصوص القانونية فإن الأصل هو حضور المتهم، وهذا الشرط مسلم به بالنسبة لتفتيش الأشخاص لأنه يقع عليهم ، أما بالنسبة لتفتيش المسكن فقد يتصور غياب المتهم في ذلك ، ولهذا قضت معظم التشريعات بأن يكون التفتيش بحضور المتهم أو من ينوب عنه[1]وهو ما أقره المشرع الجزائري صراحة بموجب المادة 45 من قانون الإجراءات الجزائية ، إذ اشترط في تفتيش المنازل و ما في حكمها سواء من طرف الضبطية القضائية أو قاضي التحقيق أن يتم في حضور المتهم أو من ينوبه ، و في حالة غيابه يجب أن يكون ذلك بحضور شاهدين شرط أن لا يكونا من الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش .

و لصحة الضبط أن يتم التفتيش في حضور المتهم أو من ينوبه و في حالة غيابه يعين شاهدين[2] إلا أن المشرع الجزائري و بموجب الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية التي تنص على انه " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة

---

[1] - **أ/رشيدة بوكر** ، المرجع السابق ، ص.ص. 413- 414

[2] - **أ/نبيلة هبة هروال** ، مرجع سابق،(ص).252.

بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف باستثناء الأحكام المتعلقة بالحفاظ على السر المهني ..." استبعد هذا الشرط و العلة في ذلك هي الطبيعة الخاصة لهذه الجرائم كونها ذات طبيعة تقنية محضة ترتكب في بيئة تقنية ، وهذه الخصوصية امتدت للأدلة المعتمدة في إثباتها التي تتميز بسرعة تعديلها و التلاعب فيها مما يستدعي سرعة استخلاصها قبل فقدانها[1].

02- الميقات الزمني لإجراء التفتيش في الجرائم المعلوماتية.

يقصد بضمانة الميقات الزمني في التفتيش أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع و العلة في ذلك هو تضييق نطاق الاعتداء على الحريات الفردية و حرمة المسكن إلا أن هناك من التشريعات من تركت مسألة تحديد ميقات التفتيش للقائم به و بالتالي يجوز له القيام به ليلا أو نهارا ومن بين هذه التشريعات نجد التشريع الإجرائي المصري[2].

و على العكس من ذلك فان المشرع الجزائري و كذا المشرع الفرنسي ذهب إلى حظر تفتيش المنازل و ما في حكمها في وقت معين ، فقد حدد المشرع الجزائري حسب أحكام المادة 47 الفقرة الأولى 68 من قانون الإجراءات الجزائية ميقات التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا ، أما القانون الفرنسي فقد حدد ميقات التفتيش من الساعة السادسة صباحا إلى الساعة التاسعة مساءا و هذا من خلال المادة 59ق.إ.ج.ج[3].

إلا أن هناك حالات استثنائية يجوز فيها إجراء التفتيش في كل وقت ليلا أو نهارا و أهمها :

. حالة رضا صاحب المنزل رضا حرا ، و صريحا و عن علم بالسبب .

. حالة الضرورة و المتمثلة في الاستغاثة من داخل المنزل كالحريق مثلا.

و يلاحظ أن المشرع الجزائري استثنى الميعاد القانوني من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من حظر التفتيش ليلا ، قد أدرك الطبيعة المميزة لهذه الجريمة و خصوصيتها من حيث إمكانية ارتكابها في أي وقت و أن أدلة الإدانة فيها سهلة المحو و التدمير و أنها غير مرئية و عليه فإن تأخير إجراء التفتيش قد يحفز على ارتكاب العديد من الجرائم و يعرقل السير الطبيعي لمجريات التحقيق ، و من جهة ثانية فان هذه الضمانة

---

[1] – **أ/نبيلة هبة هروال** ، المرجع و الموضع نفسه،(ص).252

[2] – **د/أشرف عبد القادر قنديل** ، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة للنشر، الإسكندرية ، مصر ، طبعة 2015،(ص).152

[3] - ART 59 Code de procédure pénale français dispose que "les perquisitions et les visites domiciliaires ne peuvent être commence avant 6 heure et après 21 heure ".

بدأت أهميتها تتضاءل مع ظهور ما يعرف بالتفتيش عن بعد أو ما يطلق عليه في الفقه الفرنسي مصطلح التفتيش على المباشر و الذي يمكن أن يتم في أي وقت[1].

المطلب الثاني: الاختصاص المكاني للتفتيش الالكتروني.

يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في البحث والتحري الالكتروني عن الجريمة المعلوماتية، و يتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة وهو الاختصاص القضائي لنظر في الجرائم المعلوماتية والقانون الواجب تطبيقه على الفعل ، و بالنظر لخصوصية الجريمة المعلوماتية فغالبية الأفعال ترتكب من قبل أشخاص خارج الحدود أو تمر عبر شبكات معلوماتية وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها. وهو ما يبرز أهمية معرفة ما إذا كانت القواعد المعتمدة في مجال تحديد الاختصاص القضائي والقانون الواجب التطبيق في الجرائم العادية يمكن تطبيقها على هذه الجرائم أم يتعين إفراد قواعد خاصة في ضوء خصوصيتها وما تثيره من مشكلات في حقل الاختصاص القضائي.

الفرع الاول: شروط تفتيش المنظومة المعلوماتية.

يجب أن يحدد في الإذن الندب بالتفتيش المكان و الشخص و الأشياء المراد تفتيشها و ضبطها كتحديد الحاسوب ، برامج الاختراق برامج الفيروسات ، و لا شك أن في تحديد إذن التفتيش تحديد دقيقا بالنسبة لجرائم الغش المعلوماتي قد يخلق بعض الصعوبات و العراقيل أثناء الممارسة العملية للتفتيش، ويرجع ذلك إلى الطبيعة الخاصة للنظام المعلوماتي.

اولا: الطبيعة القانونية للاختصاص المكاني للتفتيش الالكتروني.

يعد الاختصاص المحلي الاطار المكاني الذي يمارس فيه ضباط الشرطة القضائية الوظائف المرتبطة بمهام التي يتضمنها اذن التفتيش بحيث اشترط المشرع الجزائري مراعاة قواعد الاختصاص حتى يضمن صحة التفتيش الالكتروني[2]، و بالرغم من ذلك يرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود، وما يتطلبه ذلك من تعاون دولي للموازنة بين موجبات مكافحة الجريمة المعلوماتية ووجوب حماية السيادة الوطنية.

01- تحديد القانون الواجب التطبيق (في نطاق مبدأ إقليمية النص الجنائي)

تختص المحاكم الجزائرية بالنظر في الجرائم التي تقع كلها أو جزء منها على إقليمها أيا كانت صفة الشخص المتهم وبغض النظر عن جنسيته ، ويرتبط قانون العقوبات في أية دولة ارتباطا وثيقا بسيادتها بل في الحقيقة اهم مظهر

---

[1] – **أ/رشيدة بوكر** ، المرجع السابق ،(ص).417

[2] -**زبيحة زيدان**، المرجع السابق،(ص).163

للدولة على اقليمها، فيعد مبدأ إقليمية النص الجنائي معتمد في التشريعات الجنائية ومن مبادئ قوانين كل دول العـالم.

و عليه تبنى القانون الجزائري هذا المبدأ فتنصت المادة03 من القانون رقم 14/21 المتعلق بقانون العقوبات "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما تطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية"[1] ،كما نصت المادة15من القانون04/09 "زيادة عن قواعد الاختصاص المنصوص عليها في قانون الاجراءات الجزائية ، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الإقليم الوطني،عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية او الدفاع الوطني أو المصالح الاستراتيجية للإقتصاد الوطني".

أما في نطاق تطبيق مبدأ العينية للفعل المجرم بالنص الجنائي ليطبق على بعض الجرائم بعينها والعقاب عليها رغم عدم وقوعها على الإقليم الوطني التي ترتكب في الخارج بصرف النظر عن جنسية مرتكبها وبالعودة إلى صورة الجريمة الالكترونية واركانها التي نص عليها المشرع الجزائري سواء تعلق الأمر بجريمة الدخول غير المشروع في نظام المعالجة الآلية للمعطيات أو إعاقة أو تحريف تشغيل نظم المعالجة عن طريق التعطيل أو التوقيف لنظم المعالجة الآلية للمعطيات باستخدام فيروسات او عن طريق إدخال أو محو أو تعديل بيانات نظم المعالجة الآلية للمعطيات قد تمت بالجزائر[2].

02-دعم التبليغ عن الجرائم المعلوماتية.

حدد المشرع الجزائري الضوابط المكانية للجرام المعلوماتية وفقا لقانون العقوبات و قانون الاجراءات الجزائية و اعتبرها جرائم مرتكبة بالجزائر و إن كانت النتيجة لم تقع بالجزائر، قد يكون التبليغ من خلال ملء المبلغ لإستمارة رقمية على الموقع المخصص لتلقي البلاغات او من خلال الخدمة التي أصبحت متاحة منذ 07 أفريل2015 المتعلقة بإيداع الشكاوى أو المعلومات المتعلقة بالجرائم عبر الموقع الالكتروني المستحدث[3] لمتابعة جرائم الجنح او جنايات وذلك بهدف تشجيع الغير على التبليغ عن الجرائم بمـا فيها المعلوماتية.

وتظهر أهمية تلقي البلاغات في أنها تساعد رجال البحث والتحري على تحديد نوع الجريمة المبلغ عنها ان كانت تندرج ضمن الجرائم المعلوماتية، وكذلك وضع تصور مبدئي لخطة العمل المناسبة للبحث والتحري بشأن الجريمة، وبالتالي تحديد نوع الخبرة المطلوبة لأجل المعاينة وتحريز الأدلة.

---

[1] – و هذا ما اكده المشرع الجزائري في المادة 586 من القانون رقم 11/21 من قانون الاجراءات الجزائية المؤرخ في 25 اوت2021.

[2] – **أ/ نبيلة هبة هروال** ، المرجع السابق،(ص).134

[3]– تم انشاء موقع من قبل هيئة الدرك الوطني على العنوان التاليhttps://ppgn.mdn.dz ، وهو ما يوفره موقع المديرية العامة للأمن الوطني على موقعه www.dgsn.dz الذي يمكن لأي شخص من التبليغ وبصفة تضمن سرية

و منه نستنتج ان اجراءات التفتيش الالكتروني تخضع لأعمال التحقيق باعتبارها من الاعمال الإجرائية لتنظيم القانون من حيث شروط صحتها و آثارها ،و أي اجراء مخالف للقواعد الاجرائية يترتب عنه جزاء يتمثل في البطلان، و لا يقبل الدفع ببطلان التفتيش الا ممن شرع البطلان لمصلحته ، كحائز جهاز الحاسوب او البرنامج الذي جرى تفتيشه ، وإذا تعلق بطلان التفتيش بالنظام فيجوز الاحتجاج به في اية مرحلة من مراحل الدعوى الجزائية[1].

ثانيا: ضوابط الاختصاص المكاني للتفتيش الالكتروني.

01- حدود الاختصاص الإقليمي للشرطة القضائية.

يقصد بالاختصاص الإقليمي النطاق الجغرافي الذي يمارس فيه ضباط الشرطة القضائية صلاحياتهم، و يتحدد بالدائرة الإقليمية التي يباشرون فيها أعمالهم.

02- الاختصاص الإقليمي لضباط للشرطة القضائية في الجريمة المعلوماتية.

مدد المشرع الجزائري من اختصاص ضباط الشرطة القضائية و جعلته يشمل كامل الإقليم الوطني في اطار البحث و معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بعدما كان هذا الأمر مقتصرا في البداية على الجرائم المتعلقة بالإرهاب حسب التعديل الذي جاء به القانون11/21المتعلق بالإجراءات الجزائية و تم توسيع ذلك إلى جرائم أخرى منها الجريمة المعلوماتية، و في هذه الحالة يعمل ضباط الشرطة القضائية تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا و يعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات، و يرفع ضباط الشرطة القضائية ايديهم عن اجراءات التفتيش الالكتروني في حال وصول وكيل الجمهورية ، ويقوم بإتمام جميع اعمال الضبط القضائي أو يكلف كل ضابط للشرطة القضائية بمتابعة اجراءات التفتيش وفقا لنص المادة 56 ق.إ.ج.ج.

03- الصلاحيات الممنوحة للنائب العام في قضايا الجرائم المعلوماتية.

طبقا لأحكام المادة 40 مكرر01 من ق.إ.ج.ج فإن ملف القضية التي يؤول الاختصاص فيها إلى المحكمة المختصة القطب الجزائي يصل إلى النائب العام التابعة له هذه المحكمة عن طريق وكيل الجمهورية التابع للمحكمة التي وقعت بها الجريمة حسب ما جاء به المرسوم التنفيذي348/06 المتعلق بتعيين و تحديد المحاكم ذات الاختصاص الإقليمي الموسع، و طبقا للمادة 40 مكرر03 من ق.إ.ج.ج ، فإنه للنائب العام التابعة له المحكمة المختصة المطالبة بالإجراءات في جميع مراحل الدعوى.

[1] - **د/ علي حسن محمد الطوالبة**، المرجع السابق، ص.177

04- اختصاصات و صلاحيات وكيل الجمهورية في الجرائم المعلوماتية.

لقد تناول قانون الاجراءات الجزائية اختصاصات و صلاحيات السيد و كيل الجمهورية و منحه سلطات و صلاحيات اخرى ، تنص المادة 35 من ق.إ.ج.ج على أنه" يمثل وكيل الجمهورية النائب العام لدى المحكمة بنفسه أو بواسطة أحد مساعديه و هو يباشر الدعوى العمومية في دائرة المحكمة التي بها مقر عمله" كما حددت المادة 36 من نفس القانون اختصاصات وكيل الجمهورية، و ذكرت المادة 36مكرر مهام و صلاحيات أخرى تندرج ضمن مهام و صلاحيات وكيل الجمهورية.

05- توسيع صلاحيات وكيل الجمهورية و قاضي التحقيق في الجرائم المعلوماتية:

تجسد هذا التوسيع في الصلاحيات من خلال منح وكيل الجمهورية سلطة الإذن بالتفتيش ، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور و هذا ما نصت عليه المادة 65مكرر05 من القانون 22/06 و يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها و لو خارج المواعيد المحددة في المادة 47 من هذا القانون و بغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن[1].

كما نلاحظ توسيع الصلاحيات من خلال التعديلات التي جاء بها القانون رقم 11/21صلاحيات قاضي التحقيق ومنحته صلاحيات إضافية لم يكن يتمتع بها من قبل، و هذه الصلاحيات يمارسها عند التحقيق في نوع معين من الجرائم وردت على سبيل الحصر، منها اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و إجراء عملية التسرب الرقمي[2].

07- توسيع الولاية القضائية للمحاكم الجزائية في الجرائم المعلوماتية.

يعد البعد الدولي من اهم مميزات الجريمة المعلوماتية لكونها جريمة عابرة للحدود و لا تعرف حدودا تمنع انتشارها فيمكن ارتكابها من عدة أفراد ينتمون لجنسيات مختلفة، كما يمكن أن يرتكب الفعل في بلد معين و تكون النتيجة في بلد أخر مما أثار خلافا فقهيا حول تحديد الجهات المختصة بعمليات التفتيش و الفصل في

---

[1]- **د/عبد الله أوهايبية** ، ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي، الاستدلال، الطبعة الأولى، الديوان الوطني للأشغال التربوية ، طبعة 2004،(ص).300

[2] - حدد المشرع الجزائري في قانون الوقاية من الفساد ومكافحته 01/06 المؤرخ في 20 فيفري 2006 والقانون 04/09 حالات تطبيقية بخصوص قواعد الاختصاص المحلي بإجراءات المراقبة الالكترونية ،التسرب الرقمي ....، مع ذكر الحالات التي يمكن اللجوء فيها إلى المراقبة الالكترونية.

النزاع القضائي، لإتاحة الفرصة للاطلاع على مدة التخزين في اقاليم متعددة ، والسماح لمزودي الخدمات الاطلاع على محتوى الرسائل و تعاونهم مع رجال القضاء[1].

فذهب فريق من الفقه إلى القول بان الاختصاص يؤول إلى محاكم الدولة التي تم فيها تحميل البيانات لكونها دولة المصدر إلا أن هذا الرأي تعرض للانتقاد لكون بعض الأفعال لا تكون معاقبا عليها في دولة التحميل و بالتالي فهي فعلا مباحا و لا يعاقب عليه القانون، و هذا ما دفع لظهور رأي أخر يرى بان الاختصاص للنظر في هذه الجرائم يؤول لمكان تحقق النتيجة لاحتمال تعدد الدول التي تم فيها التحميل مما يؤدي إلى إفلات المجرم من العقاب، و هذا ال أري أيضا لاقى انتقادا لكونه لم يأخذ بعين الاعتبار بانه مصلحة المتهم تقتضي تطبيق قانون الدولة الحامل لجنسيتها و ليس قانون دولة أخرى[2].

08- توسيع الإجراءات الخاصة بالاختصاص الإقليمي.

بالرجوع إلى قانون الإجراءات الجزائية نجده يجيز تمديد الاختصاص المحلي والنوعي للمحاكم الجزائرية من خلال نص المادة 329 الفقرة الأخيرة حيث تجيز تمديد الاختصاص المحلي للمحاكم ليشمل اختصاص محاكم أخرى، وذلك عن طريق التنظيم في الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات وفقا للمرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 حيث أنشئت الأقطاب القضائية المتخصصة بموجب القانون 114/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية من بين الجرائم المعلوماتية التي تختص المحاكم وذلك حسب المواد 37، 40 و329 من قانون الإجراءات الجزائية[3].

كذلك نظم المشرع الجزائري في القانون 04/09 المؤرخ في 5 أوت 2009 أحكام جديدة خاصة بالاختصاص في مجال الجريمة المعلوماتية والتي تتماشى والتطور الذي لحق هذه الجريمة، ومن بين هذه القواعد ما نصت علية المادة الثالثة التي تتضمن الإجراءات الجديدة حول التحريات والتحقيقات من ترتيبات تقنية بالإضافة إلى نص المادة 15 من القانون 04/09 التي نصت على أنه" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبي وتستهدف مؤسسة الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

1- **د/ غنام محمد غنام**، دور قانون العقوبات في مكافحة جرائم الكمبيوتر و الانترنت و جرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون ، المنصورة ، مصر، طبعة 2010،(ص).180.

2 - **د/محمد عوض محمد**، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، بحث مقدم في المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، طبعة1993،(ص).43 تم الدخول الى الموقع academia- araria.com:// https و تصفحه بتاريخ 2023/05/02 على الساعة 16.00.

3 - **د/محمد معمر الصغير**، المرجع السابق،(ص).22.

ثالثا: معيار تحديد الاختصاص الإقليمي في الجريمة المعلوماتية.

إن تطبيق الإجراءات التقليدية في الجرائم المعلوماتية أصبح لا يتماشى مع طبيعة الجريمة و ما تتميز به من خصائص أهمها البعد الدولي و وقوعها في عالم افتراضي غير محدد الحدود الإقليمية، و هو ما جعل المشرع الجزائري يحسم هذه النقطة الإجرائية بتوسيع ولاية متابعة الجرائم الالكترونية و يحدد الوظائف الاجرائية لعمليات التفتيش الالكتروني التي تقوم بها الجهات المختصة ، بالنظر للاعتداءات التي تخلفها الجريمة المعلوماتية من اعتداءات، خاصة اذا كانت تستهدف المؤسسات و امن الدولة و هيئات الدفاع الوطني، أو المصالح الاستراتيجية للاقتصاد الوطني.

01اختصاص تمديد التفتيش الالكتروني الى منظومة معلوماتية اخرى.

انصبت اهتمامات المشرع الجزائري بالمنظومة المعلوماتية و انشاء العديد من الأجهزة و الهيئات الرقابية التي تساهم في مكافحة الجريمة الالكترونية، بالإضافة الى اعتماد العديد من الاليات التي تساهم في التصدي للإجرام الالكتروني من خلال متابعة الارتباط بين شبكات الحواسيب سواءا كانت شبكة محلية او شبكات دولية الامر الذي يستدعي سرعة متابعة الجناة ، من خلال تمديد التفتيش الى منظومة معلوماتية اخرى ، ففي هذه الحالة يختص النائب العام لدى مجلس قضاء الجزائر بمنح النائب العام بمنتح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 من القانون04/09، و في غير هذه الحالة نطبق القواعد العامة التي رسمها قانون الاجراءات الجزائية يرجع الاختصاص لوكيل الجمهورية وقاضي التحقيق بمنح الاذن بالتفتيش[1].

02– إختصاص تمديد الانابات القضائية خارج الجزائر.

يقصد بالإنابة القضائية ذلك الاذن او التكليف الصادر من الجهات المختصة من او انابة للقيام بالاجراء المطلوب فهو كل تصرف اجرائي يصدر ممن له سلطة التحقيق بموجبه يفوض احد مأموري الضبط القضائي ليقوم بدلا منه باجراء[2]، و حدد المشرع الجزائري سبل في مجال ملاحقة الجرائم المعلوماتية من خلال تمديد الانابات القضائية ، والسماح لضبط الشرطة القضائية بتتبع المعلومات المخزنة في منظومة معلوماتية تقع خارج الاقليم الوطني في اطار المساعدة القضائية[3].

---

[1] – **أ/ زيبحة زيدان** ،المرجع السابق ،(ص).142.

[2]– **د/ احمد فتحي سرور** ، الوسيط في قانون الاجراءات الجنائية ، دار النهضة العربية(دون مكان النشر)،(دون تاريخ الطبعة)،(ص).507.

[3]– **أ/زيبحة زيدان** ،المرجع السابق،(ص).144.

03– الاختصاص الإقليمي في الجريمة المعلوماتية في الاتفاقيات و في القوانين المقارنة.

– الاختصاص الإقليمي في اتفاقية بودابست.

نظمت المادة 22 من الباب 03 من اتفاقية بودابست الاختصاص القضائي في الجرائم المعلوماتية مؤكدة على ضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية و تدابير أخرى لإقرار الاختصاص القضائي على الجرائم الواردة في الاتفاقية، فالمادة السالفة الذكر وضعت مجموعة من المعايير و التي بمقتضاها تنسق الأطراف المتعاقدة حدود صلاحياتها المتعلقة بالجرائم المتعلقة بالاتفاقية و ذلك عندما ترتكب الجريمة في إقليمه، أو على متن احدى السفن التي ترفع علم ذلك الطرف، أو على متن احدى الطائرات المسجلة بموجب قوانين ذلك الطرف من جانب أحد مواطنيه اذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي مكان ارتكابها، أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأية دولة.

كما نصت الاتفاقية على عدم استبعاد الاختصاص الجنائي الذي ينص عليه أحد الأطراف وفقا لقانونه الوطني و مطالبة الدول الأطراف في الاتفاقية بالتشاور حول الاختصاص القضائي الأكثر ملائمة لمحاكمة مرتكبي الجرائم المعلوماتية في حالة تعدد المطالبة من طرف الأطراف باختصاصه القضائي حول واقعة معينة[1].

– الاختصاص الإقليمي في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

لم تخرج الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عن الضوابط و المبادئ التي رسمتها اتفاقية بودابيست فيما يتعلق بالاختصاص في الجرائم المعلوماتية، و تناولت مسالة الاختصاص في المادة 30 منها التي نصت على التزام كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في هذه الاتفاقية و ذلك اذا ارتكبت الجريمة كليا أو جزئيا أو تحققت في إقليم الدولة الطرف، على متن احدى السفن التي ترفع علم ذلك الطرف، أو على متن احدى الطائرات المسجلة تحت قوانين الدولة الطرف من قبل مواطني الدولة الطرف اذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها ، أو اذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة اذا كانت الجريمة تمس المصالح العليا للدولة[2].

رابعا: التعاون الدولي في مواجهة امتداد إجراءات التفتيش والضبط خارج حدود الدولة.

يعد التفتيش بوصفه إجراءا تحقيقيا تنص عليه التشريعات لأن فيه مساسا بحرية الأفراد و حرية أماكنهم و التي تكفل القانون بحمايتها من أي انتهاك، فالتفتيش يشكل انتهاكا قانونيا لهذه الحرية و الجريمة التي كفلها المشرع و ذلك بهدف تحقيق مصلحة أهم و أعم من مصلحة الأفراد و هي المصلحة العليا

[1] – **أد/ هلالي عبد اللاه احمد** ، المرجع السابق،(ص).210

[2] – **نعيم سعيداني** ، المرجع السابق،(ص).223

للمجتمع، التي تتمثل في كشف الحقيقة في جريمة وقعت، حيث أنه بهدف إيصال الجاني إلى العدالة قد تستدعي مصلحة التحقيق اتخاذ هذا الإجراء للحصول على الأدلة التي تفيد في كشف الجريمة[1].

ولكون الجرائم الماسة بأنظمة الإتصال والمعلوماتية ظاهرة مستحدثة على الساحة الإجرامية داخل الجزائر لم ينص قانون العقوبات عليها صراحة بل ذكرها في القسم السابع مكرر03 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وبين كذلك أن تعقب مرتكب الجريمة و تتبع أثاره و ضبط الأدلة المعلوماتية الدالة على ارتكابه للجريمة قد لا يتقيد بحدود الدولة وإنما يمتد إلى خارجها و هذا مرجعه إلى قوة انتشار شبكات الإنترنت التي ربطت جميع الدول ببعضها البعض و أصبح لا يحدها فاصل، لتحقيق الصالح العام أبرمت الجزائر العديد من الإتفاقيات الدولية لمكافحة هذه الظاهرة، مع فرض الضمانات التي أقرتها المواثيق الدولية، مع مراعاة مبدأ المعاملة بالمثل[2].

المطلب الثالث: القواعد الاجرائية للحجز الالكتروني و التفتيش عن الادلة الرقمية وجمعها.

إن التطور المدهش للإنترنيت أدى إلى نشوء جرائم ناتجة عن ذلك الاستخدام الإنترنيت بحيث أصبحت أداة في يد الجاني يستخدمها ليحقق أغراضه الإجرامية ، و نظرا لظهور مشكلة جرائم الكمبيوتر باعتبارها تمثل معلومات تبرز في بيانات و نصوص، الصور والأشكال والرموز، وقواعد البيانات وبرامج الحاسوب، كما أنها مجموعة من البيانات والمعطيات التي قد تمت معالجتها وتحليلها وتلخيصها وتجريبها لتحقيق الأهداف المرجوة منها واستخدامها في المجالات المختلفة، أي أنها البيانات المجهزة في شكل منظم ومفيد بتسلسل منطقي ختي يسهل تتبعها وكشف الدليل[3].

الفرع الاول: طرق التعامل مع الدليل الرقمي اثناء التفتيش و الحجز.

بما ان الضبط بطبيعته القانوني لا يقع الا على اشياء المادة المنقولة , وهذا لا خلاف في ضبطه اما النظام المعلوماتي تفتيشه يتميز بالتعقيد لمعالجة الآلية للبيانات الرقمية، وهو يشتمل على وسائل الإدخال والإخراج و تخزين البيانات، وهذا قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة الكترونية متباينة الحدود الوطنية والدولية.

كل هذه المعطيات عقدت اجراءات التفتيش الالكتروني ، مما جعل المشرع الجزائري يكرس اجراءات وقائية الغاية منها الحيلولة دون وقوع الجريمة الإلكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة 03 من القانون رقم04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام

---

[1] – **د/سامي جلال فقي حسين**، المرجع السابق،(ص).09

[2] – **د/خالد ممدوح إبراهيم**، المرجع السابق،(ص).235

[3] –**عزيزة رابحي**،(الأسرار المعلوماتية وحمايتها الجزائية) ،أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق و العلوم السياسية ، جامعة أبو بكر بلقايد تلمسان السنة الجامعية 2018/2017،ص.25

و الاتصال و مكافحتهما، من جهة أخرى يهدف التفتيش المنصب على المنظومة المعلوماتية إلى استخلاص الدليل الإلكتروني، قبل قيام المجرم المعلوماتي بتدميره أو إخفائه للإفلات من العقوبة.

أولا: الإلتزام بضوابط التفتيش الإلكتروني اثناء تفتيش موقع الجريمة المعلوماتي.

إن الإنتقال الى مسرح الجريمة الإلكتروني من أجل إجراء المعاينة يعتبر أول إجراء من إجراءات البحث والتحري، فهو الإجراء الأكثر أهمية لآنه يسمح بالمعاينة المادية للوقائع المشكلة للجريمة، و الإنطلاق بشكل سريع ومباشر في عملية البحث وضبط الأدلة، التي تساعد على معرفة وقت وكيفية إرتكاب الجريمة وهوية فاعلها، وعادة ما تسند هذه المهمة لأفراد الشرطة العلمية والتقنية، نظرا لضرورة التدخل بسرعة وبطريقة مدروسة تتلاءم وطبيعة الجريمة محل المعاينة، من خلال القيام بسلسلة من العمليات التي تستلزم خبرة ميدانية[1].

وفي الحالة وجود أسباب تدعو للاعتقاد أن 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 ، كما انه إذا تبين مسبقا من المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

01- الإجراءات الخاصة المتعلقة بالمعاينة

ذهب جانب من الفقه بأن البيانات لها طابع مادي على أساس النبضات أو الذبذبات إلكترونية و الإرشادات أو الموجات كهرومغناطيسية القابلة لأن تسجل وتخزين على وسائط متعددة و يمكن قياسها[2] و من ثمة التفتيش إلى ضبط الأدلة الرقمية التي تفيد في كشف الحقيقة، و الضبط غاية التفتيش، ولا يتم ذلك الامر الا من خلال عمليات المعاينة.

- قبل الانتقال إلى إجراء المعاينة.

يجب إتباع الخطوات التالية من قبل رجال البحث والتحقيق قبل التحرك إلى مسرح الجريمة المعلوماتية لإجراء المعاينة وهي :

- توفير معلومات مسبقة عن مكان الجريمة، وكذلك عن نوع وعدد الأجهزة المتوقع مداهمتها، ونوع الشبكات المتصلة بها، وذلك لتحديد خطة التعامل معها.

- إعداد خريطة الموقع الذي سيتم الانتقال إليه مع ضرورة وضع خطة وتقسيم الأدوار على فريق التحقيق وتحديد المهام واختصاص كل واحد منهم حتى لا تتداخل الاختصاصات.

---

[1] - **Charle Diaz**, La Police Techenique et Scientifique, 2eme Edition, Edition Presse universitaire de France, France – 2006 - p54

[2] – **د/خالد ممدوح إبراهيم**، المرجع السابق،(ص). 331

– الحصول على الاحتياجات الضرورية من الأجهزة والبرامج الحاسوبية للاستعانة بها في الفحص.

– تأمين مصدر التيار الكهربائي حتى لا يتم التلاعب به عن طريق قطعه أو تعديله بهدف تعطيل عمل فريق المعاينـــة.

– مراجعة الخطة واستحضار الإذن القضائي[1].

02– عند معاينة مسرح الجريمة.

المعاينة إجراء من أهم إجراءات التحقيق الجنائي لأهمية الأدلة المستقاة منها التي تكون غالبا ذات دلالة قاطعة في الإثبات، وقد أكدت المعاينة الفنية في كثير من الأحيان فعاليتها في إظهار حقيقة الجريمة ومعرفة كيفية وأسباب وقوعها وهوية مرتكبيها، لذلك يترتب على المحقق مراعاة الدقة والترتيب وبذل أقصى ما يمكن من العناية و الإهتمام عند إجراء ، للحيلولة دون فقدان ما يمكن إستخلاصه من معلومات قيمة قد تفيد في تنوير التحقيق، ويرى الفقه الجنائي ضروة إتباع ضوابط خاصة لأجل معاينة مسرح الجريمة المعلوماتية هي:

– تحديد أجهزة الحواسيب الموجودة وتحديد مواقعها بأسرع وقت ممكن، إضافة إلى البحث عن النهاية الطرفية المزود للخدمة بالانترنت Modeme من أجل قطع الاتصالات الخارجية التي يمكن أن تخرب الأدلة أو تمحوها من على ذاكرة الحاسوب، كما يراعي ضرورة تصوير الأجهزة الموجودة وخاصة الأجراء الخلفية التي تحمل الأرقام التعريفية للأجهزة.

– ضرورة وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة، مع رصد الاتصالات الهاتفية من و إلى مسرح الجريمة مع إبطال مفعول الهواتف النقالة التي تساعد عن طريق تقنية الجيل الثالث في تدمير الأدلة من خلال اتصالها بالأجهزة محل المعاينة.

– ملاحظة واثبات الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال وطريقة الولوج للنظـام إضافة إلى ملاحظة واثبـات حالـــة التوصيلات والكابلات المتصلة بالنظام حتى يمنح فرصة لإجراء المقارنة حين يعرض الأمر على القضاء[2].

–عدم التسرع في نقل أي "مادة معلوماتية" من مسرح الجريمة وذلك قبل إجراء اختبار اليقين من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي والتي قد تؤدي إلى إتلاف البيانات المخزنة مباشرة في حالة تعرضها لهـــا.

–حفظ ما تحتويه سلة المهملات من أوارق ممزقة أو كربون نسخ أو أقراص ممغنطة سليمة أو محطمة مع فحصها ورفع البصمات عنها وكذلك التحفظ على مستندات الإدخال والمخرجات الورقية والتي عادة ما تكون ذات صلة بالجريمة.

---

[1] – **أ/ علي عدنان الفيل**، المرجع السابق،(ص). 33

2 – **منصورية بلعيد**، المرجع السابق،ص.ص.47–48

-حصر عملية المعاينة في فئة المختصين والمحققين الذين يتوافرون على الكفاءة العلمية والخبرة الفنية في مجال النظم المعلوماتية، والذين تلقوا تدريبا فنيا كافيا على التعامل مع الأدلة الإلكترونية، ففي فرنسا مثلا يقوم فريق التحقيق المتكون من ثلاث عشر شرطيا بالإشراف على تنفيذ المهام التي يأمر بها وكيل الجمهورية أو قاضي التحقيق، أثناء عمليات المعاينة ويعملون على فحص الأجهزة ونسخ محتوياتها والتحقيق واعداد تقارير فنية ترسل إلى قاضي المختص[1].

إذن تعتبر هذه مجموعة من الإجراءات والتدابير العملية الفنية ذات الطابع الخاص بمسائل المعاينة والتي تجري على مسرح الجرائم المعلوماتية والتي تعتبر ضرورية لأجل إتمام أعمال التفتيش والضبط اللاحقة.

ثانيا: الإجراءات الخاصة بالتفتيش وضبط الأدلة.

الضبط هو الأثر المباشر للتفتيش الالكتروني ، وباعتباره أحد إجراءات التحقيق فتنطبق عليه القواعد التي تنطبق على التفتيش فإذا بطل التفتيش بطل الضبط، و التفتيش يعتبر وسيلة تهدف للوصول إلى الحقيقة وليس غاية في حد ذاته، ولعل أن الشكل الذي يتبادر إلى الذهن في هذه الحالة هو مدى قابلية النظم المعلوماتية للتفتيش باعتبارها بيانات مادية[2].

01- جمع الدليل و الحصول عليه

الخطوة الأولى في عملية التحقيق الجنائي هي تحديد مصدر الدليل الرقمي المتوقع حتى يتم الحصول عليه بصورة رقمية تمهيدية لفحصه و تحليل مصادر البيانات تختلف فقد تكون أقراص و يمكن القيام بهذه العملية عن طريق مقارنة توقيع الحاوية الأصلية و البيانات المنسوخة، بالإضافة إلى عمل نسخ آخرى من البيانات مع التأكد من سلامتها بنفس الخطوة السابقة و حفظها في مكان آمن في حالة حدوث أي عطب في البيانات المستخدمة[3].

و للحصول على البيانات يجب المرور بعدد من الخطوات للتأكد من صحة الدليل، قبل و بعد تفتيش المنظومة و بتحديد الأدوات و كيفية استخدامها و المنهج المتبع للحصول على الدليل من الحاوية مع الحرص على عدم تعديل الدليل أو المساس به بأي شكل من الأشكال من خلال عملية تحويل أو نسخ جزء من المنظومة أو البيانات[4].

---

[1] - **د/على حسن محمد الطوالبة**، المرجع السابق،(ص). 135

[2]- **د/حسن طاهر داود**، المرجع السابق ،(ص). 228

[3]- **نعيم سعيداني**، المرجع السابق ،(ص). 124.

[4]- **فاطمة الزهراء خبازي**، الجريمة الإلكترونية في ظل الجرائم المرتبطة بتكنولوجيات المعلومات على الخط الالكتروني،http:// salahgardafi.eb2a.com.content تم الدخول الى الموقع بتاريخ 2023/04/28، على الساعة 10.00

02- فحص البيانات الرقمية

يقوم المحقق الجنائي في عملية فحص البيانات بفصل الأدلة المتعلقة بالقضية و استخراج البيانات التي تم الحصول عليها من الخطوة السابقة حسب نوع الحاوية للبيانات، و يجب على المحقق مراعاة استخدام نوع الأدلة المناسبة لاستخراج الدليل الرقمي.

03- تحليل و مراجعة الأدلة.

تتم عملية التحليل على البيانات التي تم استخراجها في عملية الفحص، حيث يتم تحديد الاستنتاجات من خلال عملية التحليل، في هذه المرحلة سوف يتم تحديد و ربط الأحداث المشتبه بهم و من المستحسن أن يقوم بعملية التحليل أكثر من محقق حيث كل شخص قد يكون له طريقته الخاصة في البحث و التحليل و بالتالي الحصول على عدد أكبر من الأدلة لدعم ملف القضية ، كما يقوم المحقق الجنائي بتدوين عملية التحقيق منذ البداية إلى غاية نهايتها، على محاضر و تقارير ترفق كملف مجمل لأجل إثبات الدليل الناتج عن عملية التفتيش الالكتروني الذي تم نقله من مصدر مسرح الجريمة المعلوماتية[1].

الفرع الثاني: الحجز بمنع الوصول إلى المعطيات و حدود استعمالـه.

حجز المعطيات المعلوماتية يظل الهدف الأساس لعملية تفتيش المنظومة المعلوماتية، هو وضع اليد على الأدلة الرقمية لإدانة المجرم الإلكتروني، فإذا كان حجز الأشياء المادية كالمعدات (المكونات المادية للحاسوب) و الأوراق والمستندات...الخ، لا يعد مشكلة ويتم وفق القواعد الإجرائية التقليدية ، غير أن الأمر يختلف تماما، إذ ليس من السهل توقيع الحجز على المنظومة المعلوماتية التي هي في الأصل شيء معنوي غير ملموس.

و يلاحظ ان المشرع الجزائري يؤكد ضمانات الحجز وحفظ الدليل وفقا لنص المادة 06 من القانون رقم 04/09 التي تنص على "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأن وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية".

اولا: طرق الحصول والتعامل مع الدليل الرقمي أثناء التفتيش الالكتروني والحجز.

يجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري بها العملية ، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشغيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات ، و يتم الحجز عن طريق منع الوصول إليها حيث نص المشرع الجزائري في المادة 07 من القانون

[1] - **حسني ثابت**، الجريمة الإلكترونية في ظل تطور تكنولوجيات المعلومات على الخط : http//:kenona online. com تاريخ الاطلاع بتاريخ 2023/04/30، على الساعة 19.00.

رقم04/09" إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها ...".

والملاحظ أن المشرع لم يحدد الأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه[1]، لذلك نص على ضرورة إجراء تدابير احترازية من طرف المختصين باستعمال الوسائل التقنية المناسبة القصد منه عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية.

01- حدود استعمال المعطيات الناتجة عن اجراءات التفتيش الالكتروني.

تطرقنا فيما سبق إلى أن إجراء مراقبة الاتصالات الالكترونية يمس بحق الأشخاص في سرية المراسلات الالكترونية، وهو حق مكفول دستوريا، لذا نص المشرع الجزائري تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة ، إلا فيما تتطلبه التحريات والتحقيقات القضائية وهذا بموجب نص المادة 09 من القانون رقم 04/09 السالف الذكر التي تنص على"تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية".

بعد عملية التفتيش تتم عملية التحقيق من الأدلة الرقمية بحيث يجب أن يمر الدليل الرقمي المراد حجزه بمراحل حتى يتم اعتباره دليل رقمي معتمد كدليل للإثبات ويمكن حصر هذه المراحل فيما يلي:

- الاسراع في الكشف يجب على المحقق السرعة في الانتقال الى مسرح الجريمة.

- اتباع الخطوات اصولية المستحدثة في السيطرة على أجهزة و الحواسيب المستخدمة في الجريمة.

الاستعانة بخبراء الحواسيب والبرامج لمنع فقدان أو تلف أو تلوث الأدلة.

- الحفاظ على مسرح الجريمة وتأمينه ومنع العبث به[2].

02-احتياطات الكشف عن الدليل الالكتروني وتشتمل على الاجراءات التالية التي ينبغي على الفريق مسرح الجريمة من المحققين وأعضاء الضبط القضائي، ذوي الاختصاص من الخبراء والجنائيين وفق المواد(41 و42 و43 , 44, 49 , 52)، و على هذا الاساس يتم القيام بمايلي:

---

[1] - أما بالنسبة للمشروع قانون المعاملات الإلكترونية ، فقد تضمن تعريفات لعدد من المصطلحات، حيث عرف البيانات الإلكترونية بأنها بيانات مماثلة أو حزمة إلكترونية سواء على شكل نص أو رمز أو صوت أو صور .... كما عرف السجل الإلكتروني بأنه مجموعة المعلومات التي تشكل في مجملها وصفا لحالة تتعمق بشخص أو شيء ما والتي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية.

[2] - **د/طارق ابراهيم الدسوقي عطية** ، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية" الأنترنت" (بدون مكان النشر)، طبعة 2014،(ص). 89

_ فتح محضر الخاص بالمضبوطات الجرمية عند اول لحظة الوصول وعند المغادرة مسرح الجريمة

_ تصوير مسرح الجريمة من قبل فريق الأدلة الجنائية قبل الدخول وبعد الخروج منها .

_ اجراء الكشف والمخطط على محل الحادث بشكل اصولي دقيق .

_ خبير بصمات يتولى رفع البصمات من مسرح الجريمة .

_ خبير حاسبة الإلكترونية وشبكات يتولى رفع وتحريز الأدلة الرقمية بالطرق الفنية مزودا ببرامج عرض الصور وبرامج فك الملفات المضغوطة مثل winrar ,winzip

_ الحفاظ على الأجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الاشياء التي يعتقد ان لها صلة بالجريمة.

_ تحديد وتوثيق اسم جهاز الكمبيوتر والأجهزة الملحقة به من خلال ما يتم التي العثور عليه في مسرح الجريمة حيث أن رمز بروتوكول الإنترنت يلعب دورا مهما في تحديد موقع ومكان المشتبه به.

_ اثبات الطريقة التي تم بواسطتها اعداد النظام والعمليات الالكترونية، وخاصة ما تحتويه السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام.

_ عدم نقل أي مادة متحفظ عليها من مسرح الجريمة قبل التأكد من خلو المحيط الخارجي بموقع الحاسب الآلي من أي مجالات لقوة مغناطيسية يمكن أن تسبب في محو البيانات المسجلة عليها. واثبات حالة التوصيلات والكابلات المتصلة بمكونات النظام كله، وذلك لأجراء مقارنة لدى عرض الأمر على القضاء.

_ إنتداب خبير القضائي في مسائل الجرائم الالكترونية مع المحقق عند اجراء الكشف على مسرح الجريمة ورفع البصمات من خلال التعاون بين خبراء ادلة الجنائية من خلال انشاء مكتب التنسيق بين المؤسسات المشار اليها انفـا بصورة مستمر ومتواصل[1].

ثانيا: تحديد تقنية الرقابة وحدود استعمال المعطيات المتحصل عليها.

تكون الترتيبات التقنية الموضوعة لأغراض المراقبة الإلكترونية الموجهة حصريا لتجميع وتسجيل المعطيات ذات الصلة بالحالات الواردة على سبيل الحصر للمادة الرابعة من قانون 04/09 السالف الذكر على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة، أما التقنيات التكنولوجية التي تستعمل في إطار المراقبة فهي تتمثل في اعتراض المراسلات الإلكترونية والتقاط الصور وكذلك الشأن بالنسبة لتفتيش المنظومة المعلوماتية وحجزها كليا أو جزئيا وفق ما نصت عليه المواد 05 و 07 من القانون سالف الذكر 04/09.

إلا أن مصير المعلومات المتحصل عليها جراء التفتيش نصت عليه المادة 09 من نفس القانون المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها

[1] – **نعيم سعيداني**، المرجع الســـابق،(ص). 156

عن طريق عملية المراقبة إلا في الحدود الضرورية للتحريات والتحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الالكترونية يتحدد بحدود ضرورة التحقيقات وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار[1].

المبحث الثاني: الضمانات القضائية للتفتيش الالكتروني.

أجاز المشرع الجزائري التفتيش الإلكتروني ليتماشى مع تقنية الجرائم المعلوماتية، والإجراء يشمل فحص الأجهزة المحمولة والحواسب والدخول على البرامج بأمر مسبب و يوضح الجهات المنوط بها التفتيش ، و تلعب الضبطية القضائية في مجال مكافحة جريمة واقعة داخل بيئة غير محسوسة كمسرح لارتكاب الجريمة، مما يقتضي سعى الجهات المكلفة للحصول على مشروعية الدليل الجنائي الإلكتروني باستصدار أمر أو إذن قضائي بتفتيش مقتنيات المتهم الإلكترونية ، من أجل الحصول على المعلومات اللازمة، وعليه سيتم معالجة الموضوع وفقا للخطـة الآتية:

المطلب الاول: الضمانات السابقـة للتفتيش الإلكتروني.

المطلب الثاني: الضمانات اللاحقة للتفتيش الالكتروني.

المطلب الثالث: حجية الدليل المستخلص من الوسائل الالكترونية بالتفتيش الالكتروني.

المطلب الاول: الضمانات السابقـة للتفتيش الإلكتروني.

إن من أهم الأمور التي يرمي إليها التفتيش هو البحث عما يظهر حقيقة الجريمة، سواء بإثبات وقوعها وربطها بالجاني، وضبط متحصلات التفتيش الالكتروني كأدلة يمكن الاستفادة منها في أثناء التحقيق أو بإثبات عدم علاقته بها من خلال الوسيلة الالكترونية التي جرى التفتيش فيها. ويطلق على هذه الأدلة المستخلصة من التفتيش الالكتروني بالأدلة الرقمية أو الأدلة الالكترونية[2]، و يستخلص الدليل من الوسيلة الالكترونية أو الواسطة الالكترونية تبعا لحركات الجاني وسلوكه، وبالتالي قد تؤثر في مقدار العقوبة التي تقررها المحكمة، لذا يضبط المشرع عمليات التفتيش الالكتروني بضمانات.

الفرع الاول: مراقبة الادلة الالكترونية و تجميعها.

تلعب الأدلة الرقمية الناتجة عن التفتيش الالكتروني دورا في إثبات الجرائم وتثمين اجراءات متابعتها ومع إزدياد استعمال الكمبيوتر والإنترنت، تنامت الحاجة لإدخال أنواع جديدة من الأدلة الرقمية، و عليه بدأ المشرع بسن تشريعات جديدة أو تعديل تشريعات سارية المفعول، كما أن البحث عن الحقيقة القضائية لا ينبغي أن يكون مطلقا دون أي قيد ، بل لابد أن يخضع لضوابط معينة حتى لا يتعسف من يسعى للحصول

---

[1] – **د/ أمنة امحمدي بوزينة** ، المرجع السابق ،(ص). 74

[2] – يطلق بعض الفقه على عملية البحث عن أدلة الجريمة في العالم الرقمي مصطلح الولوج أو النقاذ باعتباره أكثر دقة من التفتيش الالكتروني الذي يعني البحث و الفحص و التدقيق في البيانات.

عليها لخرق القوانين، وهذه الضوابط تأتي في العادة سابقة لإجراء التفتيش لضمان مشروعية الاطلاع على محل تفتيش النظام المعلوماتي.

اولا: ضمانات الرقابة القانونية لموضوع التفتيش في الجرائم المعلوماتية.

إن القاعدة العامة تقضي بأن الأصل في الإنسان هو البراءة ، وهذا يتطلب أن يكون الدليل قريبا من الحقيقة الواقعة وأن يكون بعيدا عن الظن، فلا مجال لدحض القاعدة العامة القاضية بان الأصل في الإنسان البراءة إلا بدليل يقيني ثابت، وهذا يخلق نتيجة مفادها إن جميع الأدلة ومنها المستخلصة من وسائل التفتيش الالكتروني تخضع لتقدير القاضي الذي يقدر مدى اقتناعه بها بعد التثبت من صحة وسلامة الإجراء الذي اتبع في استخلاصها تؤسس حكمه على الأدلة اليقينية الجازمة والتي تخضع في نهاية الأمر لتكون محلا للطعن.

وبالنظر للصعوبات يستلزم التطرق للتفتيش على المكونات المادية والمنطقية للنظام المعلوماتي وشبكات الاتصال بعدية سلكية ولا سلكية محلية ودولية حدد المشرع الجزائري ضمانات قانونية وقضائية لضمان حسن سير اجراءات التفتيش الإلكتروني و في نفس الوقت حماية حقوق و حريات المتهم المحمية بقواعد دستورية وتنظيمية.

01- تمديد الآجال في الإجراءات المتعلقة التوقيف تحت النظر في الجرائم المعلوماتية.

ان التوقيف تحت النظر إجراء خطير يمس الحرية الشخصية للأفراد في الجرائم المعلوماتية ، لكنه في نفس الوقت ضروريا في بعض الأحيان لإجراء التحريات التي يقوم بها المحققون لإظهار الحقيقة و معرفة ملابسات و مرتكبي الجرائم ، و نظرا لهذه الخطورة فان الدستور الجزائري أعطى أهمية خاصة لهذا الإجراء و أخضعه لرقابة القضاء، ضمانا لصحة اجراءات التفتيش الالكتروني و منع تغيير أدلة الجريمة[1].

و على هذا الاساس تعد الجريمة المعلوماتية من بين الجرائم التي أعطى المشرع فيها للشرطة القضائية صلاحية طلب التمديد لأجال التوقيف للنظر بسبب تعقيداتها و تعدد المتورطين فيها و هذا يعد خروجا عن القواعد العامة، و للبحث في هذا الأمر و تفصيله ارتأينا التعرض للحالات التي يمكن فيها توقيف الشخص المشتبه فيه تحت النظر و الحالات التي سمح فيها القانون بتمديد فترة الوضع تحت النظر باختصار و هي:

قيد المشرع الجزائري ضباط الشرطة القضائية و لم يترك لهم السلطة التقديرية لتقرير التوقيف للنظر و حصر ذلك في الحالات التاليـة:

- حالـة التلبس بجناية أو جنحة: و قد نصت على هذه الحالة في المادة 51 ق.إ.ج.ج.
- حالـة التحقيق الابتدائي: هذه الحالة منصوص عليها في المادة 65 ق.إ.ج.ج
- حالـة تنفيذ الإنابة: هذه الحالة نصت عليها المادة 141 ق.إ.ج.ج و هي الحالة التي تتطلبها ضرورة تنفيذ الإنابة القضائية.

---

[1] - **أ/علي عدنان الفيل**، المرجع السابق،(ص). 145

02- السلطة المختصة بتفتيش النظام المعلوماتي.

إن التفتيش الالكتروني إجراء من إجراءات التحقيق التي تمس بحقوق الأفراد و حرياتهم ، و نتيجة لذلك حرص المشرع الجزائي الجزائري إلى إسنادها لجهة قضائية تكفل حماية الحقوق و الحريات و تضمنها و قد حددها بقاضي التحقيق الذي يقوم بها بنفسه إلا أنه يمكن لضباط الشرطة القضائية القيام بذلك بصفة استثنائية في ظل دراسة التفتيش في البيئة الرقمية ، سوف نعرض إلى هذا الإجراء في تلك البيئة ، وهذا بالإشارة إلى دور سلطة التحقيق الأصلية ثم التحقيق بصفة استثنائية.

و عليه يتضح أن إجراء التفتيش في العالم الافتراضي بمعرفة سلطة التحقيق يعد ضمانة، فلا بد أن تكون هذه السلطة وفقا للقواعد العامة مختصة أصلا بالتحقيق اختصاصا محليا ، لذا مدد المشرع الجزائري الاختصاص لقاضي التحقيق في الجرائم المعلوماتية بعد أن كان يحدده بمكان وقوع الجريمة أو بمحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو مكان القبض على أحد الأشخاص المشار إليهم ولو كان لسبب آخر طبقا للمادة 40 من قانون الإجراءات الجزائية.

و على هذا الاساس فإن المادة 40 من الامر رقم 11/21 ق.إ.ج.ج[1] تجير تمديد الاختصاص المحلي من اجل التحكم في الدليل و ضمان نجاح عملية التفتيش الالكتروني " كما يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم ، في جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف" و الملاحظ أن تمديد اختصاص المحلي لقاضي التحقيق مشمولا كما هو الشأن بالنسبة للنيابة بأحكام المرسوم التنفيذي رقم 348/06 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[2] .

و أمام كثرة و تنوع مهام السلطة الأصلية في التحقيق خاصة في حالة التفتيش الالكتروني التي تتعدد فيها الأماكن و المتهمين المراد تفتيشهم ، يمكن لهذه الأخيرة تفويض سلطاتها في التفتيش للضبطية القضائية عن طريق الندب أو الإذن لها وهذا بعد توافر دلائل كافية قبل المتهم من اجل ضمان متابعة الأدلة عبر الشبكات وسرعة الحجز عليها ومنع تغيير معالم الجريمة المعلوماتية أو طمس آثارهـا.

---

[1] - عدلت المادة 40 من الامر رقم 11/21 المعدل و المتمم الفقرة الاولى أصبحت تنص على أنه " يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشبه في مساهمتهم في اختراقها أو بمحل القبض على أحد هؤلاء الأشخاص حتى و لو كان هذا القبض قد حصل لسبب آخر".

[2] – راجع المادة الأولى الى غاية المادة الخامسة من المرسوم التنفيذي المؤرخ في 05 أكتوبر سنة 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

03- إجراء التفتيش في العالم الافتراضي بمعرفة الضبطية القضائية.

قد يمنح القانون صلاحية استثنائية لضباط الشرطة القضائية القيام بإجراء التفتيش و هذا بتوافر حالة من الحالات التالية وهي:

- الندب أو صدور الإذن من سلطات التحقيق بناء على توافر دلائل كافية قبل المتهم .
- القبض على المتهم بناء على دلائل كافية .
- حالة التلبس بالجريمة.
- بناء على رضا المتهم وعليه سوف نفصل كل حالة على النحو التالي:

ثانيا: الإنابة بالتفتيش في مجال التفتيش الالكتروني.

الأصل أن سلطة التحقيق هي صاحبة الاختصاص في القيام بالإجراءات المنصوص عليها قانونا ، إلا أنه قد تستدعي ضرورات عملية مردها الحرص على تسهيل أعمال التحقيق و سرعة الإنجاز و الاستفادة من قدرات الضبطية القضائية في تنفيذ بعض الإجراءات التي تفوض بعض هذه الأعمال وهذا بتوافر شروط معينة عنها ضرورة صدور إذن بذلك.

و يقصد بالأذن بالتفتيش الالكتروني" ذلك التفويض الموجه من سلطة التفتيش المختصة إلى أحد مأموري الضبط القضائي متضمنا تخويله إياه إجراء التفتيش الذي تختص به تلك السلطة "[1]، ويكرس المشرع الجزائري ايضا ضمانة التفتيش عن بعد وفقا للقانون رقم 04/09 في المادة 05 منه "يجوز للسلطات القضائية و كذا ضباط الشرطة القضائية في اطار قانون الاجراءات الجزائية و في الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش و لو عن بعد..."، و لا يختلف الأمر بالنسبة لجرائم الغش المعلوماتي فيما يتعلق بالقواعد الإجرائية المنظمة للإذن في جرائم التقليدية المنصوص في قانون الإجراءات الجزائية خاصة المواد من 138 إلى المادة 142 منه.

01- تمديد التفتيش خارج الإقليم و شروط المساعدة القضائية.

يضمن نشاط السلطات القضائية ومصالح الشرطة القضائية في ظل التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال وضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم التي تمس بأمن الدولة ذلك تحت سلطة القاضي المختص سلامة اجراءات التفتيش الالكتروني ، ودعم المشرع الجزائري ذلك بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته ، أما فيما يخص تطبيق الوقاية من الجرائم مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات كالاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات

[1] - **د/طارق ابراهيم الدسوقي عطية** ، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية" الأنترنت ، المرجع السابق، ص. 193

التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات وتسهيل تجميع وتسجيل محتواها في حينها و مساعدة السلطات القضائية في القيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية[1].

و يلاحظ ان التفتيش الالكتروني يتميز بتعقيده فغالبا ما يتم على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وقد يتجاوز أحيانا النظام المشتبه به إلى أنظمة أخرى مرتبطة به داخل الوطن أو خارجه،لشيوع التشابك بين الحواسيب وانتشار الشبكة الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول، وامتداد التفتيش إلى نظم غير النظام محل الاشتباه يثير تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

وعليه ضمن المشرع الجزائري عند مصادقته على الاتفاقيات الدولية تهيئة الارضية الملاءمة لتفعيل عمليات التفتيش الالكتروني من خلال من خلال تبادل المعلومات مع نظيراتها في الخارج و ضمان إستجابة الدول للطلبات الرامية للمساعدة القضائية بشأن التفتيش الالكتروني. و لقد نص القانون رقم 04/09 على التعاون والمساعدة القضائية الدولية وتناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام[2].

02- الميقات الزمني لإجراء التفتيش في الجرائم المعلوماتية.

يقصد بضمانة الميقات الزمني في التفتيش أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع لاى و العلة في ذلك هو تضييق نطاق الاعتداء على الحريات الفردية و حرمة المسكن ، ويلاحظ أن المشرع الجزائري باستثنائه للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من الميعاد القانوني، اعطى ضمانة لتطويق الدليل الإلكتروني و منع تغييره او التصرف فيه ،كما أدرك الطبيعة المميزة لهذه الجريمة و خصوصيتها من حيث إمكانية ارتكابها في أي وقت و أن أدلة الإدانة فيها سهلة المحو و التدمير و أنها غير مرئية و عليه فإن تأخير إجراء التفتيش قد يحفز على ارتكاب العديد من الجرائم و يعرقل السير الطبيعي لمجريات التحقيق .

و من جهة ثانية فان هذه الضمانة المقررة لحماية الحقوق والحريات الشخصية بدأت أهميتها تتضاءل مع ظهور ما يعرف بالتفتيش عن بعد أو ما يطلق عليه في الفقه الفرنسي مصطلح التفتيش على المباشر و الذي يمكن أن يتم في أي وقت[3]، أما التشريعات التي لم تنص على أحكام خاصة تتعلق بالتفتيش في الجريمة

---

[1] – **أ/يوسف مناصرة** ، الدليل الإلكتروني في القانون الجزائي، دار الخلدونية الجزائر، طبعة 2021،(ص). 86

[2]– يلاحظ فيما يخص الاختصاص القضائي تم توسيع اختصاص المحاكم الجزائية للنظر في هذه الجرائم ولو ارتكبت من طرف الرعايا الأجانب عندما تكون المصالح الإستراتيجية للجزائر مستهدفة.

[3]– **أ/رشيدة بوكر** ، المرجع السابق ،(ص). 417

المعلوماتية، فإنها تطبق بشأنها الأحكام العامة تسري عليها قواعد العامة الخاصة بالجرائم التقليدية المحددة للفترة الزمنية المقررة لإجراء التفتيش مع مراعاة الاستثناءات الواردة على القاعدة[1].

ومنه نستنتج ان المشرع الجزائري يكرس الضمانات من خلال اشتراط اقتران الإذن بالتفتيش الالكتروني قيام قرائن قوية على ارتكابه للجريمة عند التنفيذ ، لأن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم، أو أن للمتهم أكثر من جهاز في أماكن مختلفة كأن يكون المتهم مالكا لجهاز في منزله و جهاز أخر في عمله، أو أن يكون الشخص له شريك في الأجهزة مما يتطلب الحصول على إذن آخر من وكيل الجهورية. ويتم ذلك عن طريق تحديد مجال هذا التفتيش وما يستتبعه بالضرورة من تتبع لشبكات المعلومات، و يخضع ذلك للسلطة التقديرية للقاضي من حيث توافر حالة الضرورة أو عدم توافرها.

و هذا النظام إتبعته بعض الدول مثل الولايات المتحدة الأمريكية و كندا، حيث نصتا على أن يكون إذن التفتيش متضمنا مـايلي:

- البحث عن أدلة محصلة من كيان الحساب المنطقي و التي يدخل فيها برامج التطبيق ونظم التشغيل.
- البيات المستخدمة بواسطة برمج الكمبيوتر أو كيانه المنطقي.
- السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات[2].

لا شك أن تحديد إذن التفتيش تحديد دقيقا بالنسبة لجرائم الغش المعلوماتي قد يخلق بعض الصعوبات و العراقيل أثناء الممارسة العملية للتفتيش ، ويرجع ذلك إلى الطبيعة الخاصة للنظام المعلوماتي الذي قد يحتوي على العديد من الملفات[3] و بالتالي يثور التساؤل حول ما إذا كان كل ملف مفرد يعامل معاملة الحاوية المغلقة المنفردة التي تتطلب وجود إذن قضائي مستقل عن الآخر، خاصة إذا عمد المتهم إلى وضع أسماء مستعارة لملفات تحتوي على مواد غير مشروعة[4].

لذا حدد المشرع الجزائري هذه الاحكام وضبطها في القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة في قانون رقم 04/09 ومن ثم لا نجده يتحدث عن هذا الشرط ، كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى[5].

و من ثمة نستنتج ان المشرع الجزائري حاول كباقي التشريعات المقارنة توفير الحماية والوقاية الجنائية اللازمة لمنع المساس بالأنظمة المعالجة الآلية للمعطيات، لكن تخوفه من هذا التطور الذي اقتحم المجال المعلوماتي ادى الى ارتكاب جرائم ماسة بالنظام و الأمن لذلك دعم التفتيش الالكتروني بآليات قانونية و تقنيات فنية لمواكبة

---

[1]– راجع المادة 47 مكرر من الامر رقم11/21 المتعلق بقانون الإجراءات الجزائية.

[2] – **د/سامي جلال فقي حسين**، المرجع السابق،(ص). 09

[3] – **د/ خالد حازم إبراهيم**، المرجع السابق ،(ص). 294

[4]– **أ/رشيدة بوكر** ، المرجع السابق ،(ص). 411

[5] – **رابح مباركية** ، المرجع السابق ،(ص). 35

التطور الحاصل في مجال الجرائم الالكترونية ، بوضع مجموعة من القواعد الموضوعية لحماية المتعاملين في هذا المجال من جهة والمنظومة المعلوماتية من جهة أخرى.

الفرع الثاني: القيود المفروضة على اجراءات التفتيش الالكتروني.

أما قانون الإجراءات الجزائية فقد نص على أن تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات إلا إذا نص القانون على طريقة معينة للإثبات. وهذا يعني أن الإثبات بالوثائق الإلكترونية جائز في الدعاوى الجزائية طالما لم ينص القانون على طريقة معينة للإثبات، وطالما اقتنع القاضي بالدليل. وعلى الرغم من ذلك، فإن معظم القضاة و أعضاء النيابة العامة يجمعون المعلومات الأساسية الضرورية المتعلقة بالجرائم الإلكترونية و كيفية التحقيق فيها و اثباتها وبالتالي يترددون في الأخذ بالأدلة الرقمية لإثبات الجرائم الإلكترونية.

اولا: قواعد التفتيش داخل المنظومة المعلوماتية.

بالرجوع إلى القانون 04/09 في المادة 05 نجد أن المشرع أجاز للسلطات القضائية المختصة، وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 الدخول بغرض التفتيش ولو عن بعد إلى:

– منظومة معلوماتية أو جزء منها وكذلك المعطيات المخزنة فيها ومنظومة تخزين معلوماتية.

– في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وان 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".

01– التفتيش بناءا على احكام الأمر 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل ونأخذ المثال في هذا الشأن بالمساعدة القضائية الدولية كإجراء جديد لتتبع مجرمي المعلوماتية.

المشرع الجزائري من خلال نص المادة 05 من القانون رقم 04/09 نص على التفتيش المنصوص عليه في قانون الإجراءات الجزائية وهذا بالإحالة التي تضمنتها المادة 04 منه، غير أن القانون 04/09 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد، وهذا الإجراء يمكن من الدخول إليه دون إذن او حضور صاحبها، و يتم ذلك بالدخول في الكيان المنطقي للحاسوب والتفتيش عن الأدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية

أو نسخها للبحث عن الدليل فيها، وهذه القاعدة تعد استثناء على القواعد التي رسمها المشرع في قانون الاجراءات الجزائية طبق للقاعدة الفقهية الخاص يقيد العام.

02- التفتيش بناء على امر القبض.

يترتب على القبض الصحيح تفتيش شخص المتهم عموما و المتهم المعلوماتي خاصة وهذا ما نصت عليه بعض التشريعات المقارنة كقانون إساءة استخدام الحاسب الآلي[1]، و على ذلك فإن التفتيش الشخص يجيز تفتيش نظام الحاسب الذي يحمله معه خارج مسكنه و كذا الأجهزة المعلوماتية التي في حوزته وقت تفتيشه سواء كانت ملكا له أو لغيره[2]، و يقصد بشخص المتهم المعلوماتي كمحل للتفتيش " تحسس جسمه و ملابسه و فحصه بدقة و إخراج ما يخفيه فيها من متحصلات الجريمة المعلوماتية وإذا كانت معه أمتعة جاز تفتيشها بحثا عن أي جزئيات تتعلق بالوحدات المعلوماتية محل البحث ، سواء كانت بين يديه أو يضعها أمامه في الطريق العام أو يضعها في سيارته "[3].

03- التفتيش في البيئة التقنية على حالة التلبس بالجريمة.

تتفق معظم التشريعات الإجرائية على أن حالة التلبس تعد إحدى الحالات التي تتوسع فيها اختصاصات الضبطية القضائية ، إذ بإمكانها مباشرة بعض الاختصاصات التي في أصلها من اختصاص سلطة التحقيق ومنها تحديدا التفتيش وهذا للبحث عن الأدلة التي تثبت الجريمة وتحديد فاعلها سواء تعلق الأمر بتفتيش المساكن أو الأشخاص.

ومن مظاهر التفتيش في حالة التلبس في الجرائم المعلوماتية، كأن يكون الجاني بصدد اختراق النظام المعلوماتي لمصرف أو مؤسسة مالية لأجل التزوير في البيانات الخاصة بأحد العملاء حتى يتمكن من تحويل مبالغ مالية إلى جهة أخرى ، فيتم مطاردته عن طريق الانترنت وبعد فترة قصيرة من ارتكاب جريمة التزوير المعلوماتي يتم تحديد هويته خاصة إذا كان الحاسوب المستعمل ملكا له ، ففي هذه الحالة تعد الجريمة جريمة متلبس بها حتى وإن تم القبض على الفاعل لاحقا لكونه في حالة تتبع ما لم يكن قد فات وقت طويل على ارتكابه الجريمة ، وإن كانت الصعوبة تكمن في رصد مرتكب الجريمة في شخصه[4].

ثانيا: قيود التفتيش في البيئة الالكترونية.

لحماية الحريات الفردية من التعسف و الانحراف في استعمال السلطة فان الشروط الموضوعية غير كافية ، فلا بد من وجود شروط شكلية لصحة إجراء التفتيش في الجرائم المعلوماتية وتتمثل هذه الشروط في :

---

[1] - **أ/رشيدة بوكر**، المرجع السابق،(ص). 413

[2] - **د/خالد حازم ابراهيم** ، المرجع السابق،(ص). 319

[3] - **أ/نبيلة هبة هروال** ، المرجع السابق،(ص). 246

[4] - **أ/رشيدة بوكر**، المرجع السابق، ص.ص. 409-410

01- الحضور الضروري لبعض الأشخاص أثناء التفتيش في البيئة التقنية.

يعد هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط ، إلا أن المشرع الجزائري و بموجب الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية التي تنص على انه" لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف باستثناء الأحكام المتعلقة بالحفاظ على السر المهني ..." استبعد هذا الشرط و العلة في ذلك هي الطبيعة الخاصة لهذه الجرائم كونها ذات طبيعة تقنية محضة ترتكب في بيئة تقنية ، وهذه الخصوصية امتدت للأدلة المعتمدة في إثباتها التي تتميز بسرعة تعديلها و التلاعب فيها و هو ما يستدعي سرعة استخلاصها قبل فقدانها[1].

بالإضافة الى ان الخطوة الأولى في عملية التحقيق الجنائي هي تحديد مصدر الدليل الرقمي المتوقع حتى يتم الحصول عليه بصورة رقمية تمهيدية لفحصه وتحليل مصادر البيانات المختلفة ، فقد تكون أقراص صلبة، ذاكرة عشوائية، أقراص خارجية وغيرها، وللحصول على البيانات يجب المرور بعدد من الخطوات للتأكد من صحة الدليل، و بالتالي الحضور يؤثر سلبيا على جمع الادلة ، فقبل وبعد تفتيش المنظومة يجب على الشخص المسؤول على مسرح الجريمة رسم خطة قبل الوصول أو الحصول على البيانات أي يجب عليه تحديد مسبقا الطريقة التي سوف يقوم باتخاذها، وما هي الأدوات وكيفية استخدامها والمنهج المتبع للحصول على الدليل من الحاوية مع الحرص على عدم تعديل الدليل أو المساس به بأي شكل من الأشكال من خلال عملية تحويل أو نسخ جزء من المنظومة أو البيانات.

بناءا على الخطوة السابقة، يجب على القائم بعملية التفتيش للمنظومة المعلوماتية أو الحجز عليها البدء في عملية استخراج البيانات من المنظومة، مع التأكد من سلامة البيانات بعد تحويلها و ضمان عدم وجود تغيير، ويمكن القيام بهذه العملية عن طريق مقارنة توقيع الحاوية[2].

02- وجود ضرورة للتفتيش الالكتروني.

يتم اللجوء إلى إجراء مراقبة الاتصالات الالكترونية في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد

---

[1] - **أ/رشيدة بوكر**، المرجع السابق،(ص). 415

[2] - **أ/عفيفي كامل عفيفي**، جرائم الكمبيوتر، منشورات الحلبي الحقوقية (بدون مكان النشر)، طبعة 2003 ، ص.475

الوطني[1]، أو لمقتضيات التحريات كالتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية[2].

03- الجهة القضائية المختصة بذلك.

بالرجوع إلى المادة 04/أ من القانون رقم 04/09 السالفة الذكر و المتعلقة بالوقاية من الافعال الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في المادة نفسها الفقرة الأخيرة إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضابط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها المنصوص عليها بموجب المادة 13 من القانون نفسه إذنا لمدة 06 ستة أشهر قابلة للتجديد، وذلك على أساس طبيعة ونوعية الترتيبات التقنية المراد أخذها بخصوص الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية".

المطلب الثاني: الضمانات اللاحقة للتفتيش الالكتروني.

إن التفتيش في الجرائم المعلوماتية ينصب على مكونات مادية للنظام المعلوماتي والتي تخضع للقواعد العامة في التفتيش باعتبارها أشياء مادية ملموسة ، أما المكونات المعنوية للنظام المعلوماتي فأخضع المشرع تفتيشها لقواعد خاصة تضمنها القانون رقم 09/04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحته ، إذ نصت المادة الخامسة منه على إمكانية التفتيش عن بعد في منظومة معلوماتية .

الفرع الاول: متابعة اجراءات التفتيش والحجز داخل المنظومة المعلوماتية.

حرصت معظم التشريعات على إحاطة التفتيش بشروط لازمة لصحته ، لما يتضمنه من تقييد للحريات الفردية ، و اعتداء على حرمة الحياة الخاصة ، ومن الشروط و الضمانات الواجب توافرها في إجراء التفتيش ما هو شكلي ومنها ما هو موضوعي ، وعليه سوف تقسم عليه الشروط إلى شروط موضوعية للتفتيش و شروط شكلية .

اولا: ابعاد اجراءات التفتيش والحجز داخل المنظومة المعلوماتية

01- ضمانات تفتيش المكونات المادية لجهاز الكمبيوتر.

لا يقوم الاختلاف في أن الولوج إلى المكونات المادية للنظام المعلوماتي للبحث عن شيء يتصل بالجريمة المعلوماتية المرتكبة مما يفيد في الاطلاع على الدليل الذي سيساهم في الكشف عن الحقيقة و معرفة

---

[1]- تعرف المعطيات المعلوماتية بانها "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين". راجع **د/سامي جلال فقي حسين**، المرجع السابق،(ص). 99

[2]- **نورة صرشي** ، المرجع السابق ،(ص). 65.

مرتكبيها، لذا يخضع التفتيش الالكتروني لضمانات إجراءات قانونية خاصة ، بمعنى أن تفتيش المكونات المادية في المنازل، فإذا كان الشخص يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها في إحدى الأماكن العامة ، أو الأماكن العامة بطبيعتها فإن تفتيشها يكون وفقا للقواعد و الضمانات المقررة بتفتيش الأشخاص في هذا المجال.

أما إذا كان المكان الموجود به المكونات المادية من الأماكن الخاصة كأن توجد في مسكن المتهم أو أحد ملحقاته فتطبق عليها الأحكام و الضمانات المتعلقة بتفتيش المساكن[1] ، مع المراعاة التمييز بين ما إذا كانت المكونات المراد تفتيشها متصلة أو منعزلة عن حاسبات أخرى في مكان آخر غير مكان المتهم مثلا ، و ما إذا كانت المعلومات المخزنة في أوعية هذا النظام الآخر من شأنها كشف الحقيقة تعين هنا مراعاة القيود و الضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن[2].

ولضابط الشرطة القضائية وحده مع الأشخاص الحاضرين عملية التفتيش الحق في الاطلاع على منظومة البيانات المعلوماتية قبل حجزها، غير أنه عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني و اتخاذ جميع التدابير اللازمة لضمان احترام ذلك السر، وتغلق المستندات المنسوخة ويختم عليها إذا أمكن ذلك، فإذا تعذرت الكتابة عليها، ويحرر جرد الأشياء والمستندات المحجوزة.

و عليه يتم التفتيش دون التقيد بالإجراءات الواردة في المادة 47 ق.ع.ج، وحدد الاستثناء بموجب تعديل قانون الإجراءات الجزائية في الفقرة الثالثة من ذات المادة التي تنص على أنه"و عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبيض الأموال و الإرهاب و كذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل و ذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

02- ضمانات تفتيش الالكتروني للمكونات المعنوية.

ينصب التفتيش على الجانب الغير مادي المتمثل في المعلومات المعالجة ، ولعل الصورة المعتادة و المثال العلمي الذي يمكن تقريره هنا هو فحص البرمجيات الذي يعد من الوسائل الرئيسية في الكشف عن أكثر الجرائم المعلوماتية ، مثل جرائم الدخول غير المصرح به فإن وجود برمجيات غير مصنفة تعمل في بيئة الاختراق أو تساعد عليه.

---

[1] - **د/الشحات إبراهيم محمد منصور** ،المرجع السابق،(ص). 196 .

[2]- **د/خالد ممدوح إبراهيم** ، المرجع سابق ،(ص). 195.

– إجراءات تفتيش في الجرائم الماسة بالمعطيات الرقمية الخاصة بالمتهم.

إذا كان محل ارتكاب الجريمة ينصب على نظام المعلومات الخاص بالمتهم دون لزوم التدخل في نظام معلوماتي لشخص آخر، و في هذا الفرض إذا كانت الشروط الإجرائية للتفتيش صحيحة وفقا لما نص عليه القانون فإن التفتيش و ما يسفر عنه من ضبط أي من الأدلة، سواء أكانت هذه الأدلة هي أجهزة الكمبيوتر أم أحد الوسائط المتعددة، يكون مشروعا، وهذا الحال يكثر في جرائم التزوير و التزييف حيث يتم التفتيش و ملحقاته من طباعات ملونة أو أجهزة ماسح ضوئي، و يتم نقل البرنامج الداخلي الذي يوجد عن طريق إتمام عملية التزوير أو التزييف في أي من الوسائط المتعددة و بذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما يتم أيضا في الجرائم النسخ و التقليد حيث يتم ضبط الوسائط المتعددة المحملة بالبرامج المنسوخة أو الأجهزة المستخدمة في ذلك[1].

- **إجراءات تفتيش في نظام معلوماتي غير خاص بالمتهم.**

يظهر هذا الفرض في الجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الآخرى المتصلة بالحاسب الذي ارتكبت في نظامه المعلوماتي الجريمة و في هذا الفرض فإن إجراءات التفتيش و الضبط تتطلب الدخول في نظام معلوماتي لشخص آخر.

ويلاحظ أن قانون الإجراءات الجزائية نص على أنه لا يجوز لرجال الشرطة القضائية الدخول في أي محل مسكون إلا في الأحوال المبينة في القانون، وهو ما دعا المشرع إلى مد تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن و كذلك السيارة الخاصة إذا كانت توجد في مسكن المتهم، أما إذا وجدت في الطريق العام فلها نفس حرمة الشخص بحيث لا يجوز تفتيشها إلا إذا جاز تفتيش الشخص قانون[2].

ثانيا: اصول القانونية للتعامل مع الدليل الرقمي اثناء التفتيش الالكتروني و الحجز.

ان الضبط الناتج عن عمليات التفتيش الالكتروني محله في مجال الجرائم الإلكترونية، البيانات المعالجة إلكترونيا، فهنا ثار الجدل حول مدى صلاحية البيانات الإلكترونية البيانات لأن يكون محلا للضبط , انقسم الفقه إلى اتجاهين:

01– الاتجاه الاول: الاتجاه المعارض لإمكانية خضوع مكونات الحاسوب المنطقية للتفتيش.

يرى هذا الاتجاه ان تفتيش المنظومة المعلوماتية كما عرفت المادة 02/02 من القانون رقم04/09 سالف الذكر المنظومة المعلوماتية" أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، كما عرف أيضا النظام المعلوماتي على أنه "جهاز يتكون من مكونات مادية ومكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية، وهو

[1] – **د/خالد ممدوح إبراهيم**، المرجع نفسه،(ص). 229.

[2] – **د/عز الدين عثماني**، المرجع الســابق،(ص). 64

يشتمل على وسائل الإدخال والإخراج كتخزين البيانات، وهذا قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة ".

و إذا كان إخضاع المكونات المادية للتفتيش لا يثير أي إشكال أو اختلاف فقهي ، فإن الأمر على خلاف ذلك بالنسبة للمكونات المعنوية أو الغير المادية إذ ثار جدل فقهي حول إمكانية خضوعها للتفتيش تمهيدا لضبط الأدلة ،إذ ذهب رأي إلى جواز خضوع هذه المكونات للتفتيش و يستندون أنصار هذا الرأي إلى أن القوانين الإجرائية تنص على إصدار الإذن بضبط " أي شيء" فإن ذلك يفسر تفسيرا واسعا بحيث يشمل معلومات و بيانات الحاسب المحسوسة و غير محسوسة[1].

02- الاتجاه الثاني: الاتجاه المؤيد لخضوع الكيانات أو مكونات الحاسوب المنطقية للتفتيش

و على النقض من الرأي الأول فإن أنصار الرأي الثاني يرون أن المكونات المعنوية أو الغير مادية لا تصلح بطبيعتها بأن تكون محلا للتفتيش ، لأن التفتيش يهدف أساسا إلى ضبط أدلة مادية ، وهو ما ينتفي في المعلومات ذات الطبيعة الغير محسوسة مما يستلزم وجود أحكام خاصة تتلاءم وهذه الطبيعة.

و في مقابل هاذين الرأيين هناك رأي ثالث الذي يستبعد عبارة كل شيء للقول بقابلية أو عدم قابلية المكونات المعنوية للتفتش و يعتمد في رأيه على الواقع العملي الذي يتطلب أن يقع الضبط على معلومات الحاسب الآلي إذا اتخذت شكلا ماديـا، لذلك يرى أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، و بالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره[2].

و من ثمة تتعزز هذه الآراء بالجانب الذي يرى ان بيانات المنطقية للحاسوب لا تصلح لأن تكون محلا للضبط ، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي أو بنقلها على دعامة أو غيرها من الوسائل المادية، ويستند هذا الرأي إلى ان النصوص التشريعية المتعلقة بالضبط محل تطبيقها الاشياء المادية الملموسة[3].

03- موقف المشرع الجزائري.

إن إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة الإلكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة 03 من القانون رقم04/09 ، التي تنص على "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا

---

[1] - **أ/علي عدنان الفيل** ، المرجع السابق ،(ص). 42

[2] - المرجع نفسه،(ص). 58

[3] - **د/عز الدين عثماني**, المرجع السابق , ص.ص. 49-50

القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش كالحجز داخل منظومة معلوماتية".

إلا أن المشرع الجزائري ومن خلال القانون 04/09 المادة الخامسة منه، يتضح أنه سار في اتجاه الرأي الثاني الذي رأى بضرورة وجود قواعد خاصة تحكم التفتيش و هذا بالنظر إلى طبيعة المعلومات التي لا تتماشى و النصوص التقليدية التي تعتبر قيدا على الحرية الفردية ، ومن ثم يصبح القياس على الأشياء المادية محضورا لمنافاته الشرعية الإجرائية ، فبالرجوع للمادة 05 من قانون 04/09 نجد أنها أجازت للسلطات القضائية و المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش و لو عن بعد إلى:

. منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها.

. منظومة معلوماتية.

أما الاتفاقية الأوربية المتعلقة بجرائم تقنية المعلومات فتنص في فقرتها الأولى من المادة 19 من الفصل الرابع على أنه " يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مشابهة :

. لنظام معلوماتي أو لجزء منه و كذلك للبيانات المعلوماتية المخزنة فيه و على أرضه.

. لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية"[1].

ثالثا: الجزاء المترتب على عدم مراعاة أحكام و ضوابط التفتيش الالكتروني.

إن القواعد التي وضعها المشرع للتفتيش الالكتروني راعى فيها التوفيق بين حماية الحرية الفردية للأشخاص و حرمة حياتهم الخاصة في العالم الإفتراضي و بين المصلحة العامة في الكشف عن الحقيقة و الوصول بالتحقيق إلى غايته المنشودة.

و تثير مسألة البطلان إشكالات عديدة، فيما يتعلق بطبيعة البطلان اذا كان يتعلق بالنظام العام أم بمصلحة جوهرية للخصوم، و كذلك الشأن فيما يخص حالات البطلان فهل هذا يعني أن احترام تلك الضمانات واجب في التفتيش طبقا للقانون يترتب على مخالفتها البطلان او تكون إجراءات التحقيق صحيحة و منتجة لآثارها القانونية ، فيقع التفتيش باطلا الذي يتم بدون الحصول على إذن من السلطة القضائية المختصة طبقا لنص المادة 44 ق.إ.ج.ج بالإضافة إلى أنه يقع التفتيش باطلا إذا أجراه عضو الضبطية القضائية الذي لا يحمل صفة ضابط الشرطة القضائية لأن هذه الصفة تعتبر من أهم الضمانات المقررة حماية للحرية الشخصية للفرد أو يبادر به خارج حدود اختصاصه الإقليمي.

[1] – **أ.د/هلالي عبد اللاه أحمد** ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،(دارسة مقارنة)، الطبعة الاولى ، دار النهضة العربية، (بدون مكان النشر)، طبعة 1997،(ص). 180

ومن ثمة فإن وجود الدلائل و القرائن القوية يتوفق على جدية التحريات المرتبطة بإجراءات التفتيش الالكتروني و ما ينتج عنها من ادلة تعد من المسائل الموضوعية التي تخضع لقاضي الموضوع ، ومن ثم فإذا أراد المتهم الدفع ببطلان التفتيش لعدم جدية التحريات التي سبقته فهذا الدفع يقدم أمام محكمة الموضوع ، و لا يجوز إثارته أمام المحكمة العليا باعتبارها محكمة قانون .

الفرع الثاني: الحصول على البيانات و التعامل مع الدليل الرقمي اثناء التفتيش.

عمل المشرع الجزائري على وصف الافعال الاجرامية المعلوماتية بدقة الأفعال بدقة، حتي يضمن صحة الادلة الناجمة عن عمليات التفتيش الالكتروني ، و إيجاد حلول للمشتملات المتعلقة بالدليل الالكتروني من حيث الوسائل المستعملة في الحصول عليه و مدى تأثير مشتملات الدليل الالكتروني على الاقتناع الشخصي للقاضي.

اولا: الركائز القانونية للحصول على البيانات الرقمية.

تباينت الآراء الفقهية حول مدى امكانية إجبار المشتبه فيه او المتهم على تقديم معلومات للولوج للأنظمة المعلوماتية ،إذ ذهب رأي إلى أنه لا يمكن إجبار المتهم على تقديم المعلومات اللازمة لتسهيل الدخول أو الولوج للنظام المعلوماتي و يستندون في ذلك إلى القاعدة العامة التي مفادها عدم جواز أو إمكانية إجبار المتهم على الإجابة على الأسئلة التي من شأنها أن تؤدي إلى إدانته ، و لا يمكن أن يفسر سكوته أو صمته ضد مصلحته وهو ما يمكن استنتاجه من نص المادة 100ق.إ.ج.ج التي نص على أنه" يتحقق قاضي التحقيق حين مثول المتهم لديه لأول مرة من هويته و يحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه و ينبهه بأنه حر في عدم الإدلاء بأي إقرار و ينوه عن ذلك التنبيه في المحضر".

و في المقابل يرى رأي آخر أنه و إن كان لا يجوز إجبار الشخص الإدلاء بأقوال ضد نفسه ، إلا أن ذلك لا يمكن أن يكون حائلا ضد إلزام المتهم بتقديم معلومات للسلطة المختصة لأجل الدخول أو الولوج للنظام المعلوماتي[1] متى كانت هذه المعلومات بحوزته قياسا على إجبار الشخص على تسليم مفتاح الخزانة التي بحوزته و قد رد أنصار الرأي الأول على ذلك أن كلمة السر و ما في حكمها هي أمر معنوي (بخلاف المفتاح الذي يعد شيء مادي) تكتنفه عدة صعوبات كإدعاء المتهم نسيانها[2].

إلا أن المشرع الجزائري حسم المسألة بإمكانية إجبار غير المتهم على تقديم المعلومة للسلطات المختصة و التي تمكن من الولوج للنظام المعلوماتي كما هو الحال بالنسبة لمقدم الخدمة مثلا وهو ما نصت عليه المادة 10 18، 11 19 من القانون رقم 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

---

[1]- **نوارة حسين،**(آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا) ، منشور في مجلة الدراسات القانونية لأعمال ملتقى آليات مكافحة الجرائم الإلكترونية ، كلية الحقوق جامعة الجزائر،(ص). 107

[2] - **أ/رشيدة بوكر،** المرجع السابق ، ص.ص. 399-400 .

و الاتصال و مكافحتها ، لأن الإكراه الواقع على غير المتهم لا يمس بحقوق الدفاع وهو ما حثت عليه الاتفاقية الأوروبية المتعلقة بجرائم تقنية المعلومات من خلال المادة 19 الفقرة الرابعة اذ نصت على أنه" يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل تحويل سلطاته المختصة سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من أجل حماية البيانات المعلوماتية التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار إليها الفقرتين الأولى والثانية"[1].

و من ثمة بين المشرع الحل في الحالة التي يكون فيها النظام المعلوماتي مزود بحماية فنية ككلمة السر، فالمشرع من خلال القانون المذكور أعلاه تناول إجراءات تحري خاصة و المتمثلة في المراقبة التقنية وحفظ المعطيات المتعلقة بحركة السير، ونظرا لخصوصية الجريمة المعلوماتية وسهولة تدمير الأدلة فإن المشرع حدد ضمانات لسلامة التفتيش الالكتروني و صحة الحصول على الدليل الرقمي و حجزه[2].

و في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم مساعدات إلى السلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوي الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من القانون 04/09 تحت تصرف السلطات المذكورة وذلك لتمكين سلطات التحقيق من الحصول على البيانات و التعامل مع الدليل الرقمي اثناء التفتيش.

كما يتعين علي مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق، كما حدد القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب من خلال المادة 12 من قانون رقم 04/09 على مقدمي الخدمات التزامات خاصة وهي:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية و تقنية.

- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام و أن يخبروا المشتركين لديهم بوجودها[3].

---

[1] – المادة 11 من القانون رقم 04/09 " مع مراعاة طبيعة و نوعية الخدمات يلتزم مقدمو الخدمات بحفظ أ . المعطيات التي تسمح بالتعرف على مستعملي الخدمة ، ب . المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال . الخصائص التقنية و كذا تاريخ ووقت ومدة كل اتصال ، د . المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها، هـ . المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال و كذا عناوين الموقع المطلع عليها ...".

[2] – **أ/عبد القادر عدو**، المرجع السابق،(ص). 109

[3] – **نورة صرشي** ، المرجع السابق ،(ص). 63

بالإضافة الى دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحته في دعم الحصول على الدليل الرقمي ، حيث تتشكل هذه الهيئة من لجنة مديرة يرأسها الوزير المكلف بالعدل و ثلاثة مديريات ومركز العمليات التقنية وملحقات جهوية، كما يتمثل أعضاؤها في الوزير المكلف بالداخلية الوزير المكلف بالبريد وتكنولوجيا الاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني ممثل عن الرئاسة الجمهورية، ممثل عن وزارة الدفاع، قاضيان من المحكمة العليا، وبهذا ضمت الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكري والدرك الوطني و الأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية[1].

كما يتمثل دور هذه الهيئة في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهي تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية[1]

ثانيا: اسس حجر البيانات و تحصيلها اثناء التفتيش الالكتروني.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها، كما اقر المشرع في نفس القانون 04/09 إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 05 وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كخبراء وتقنيين مختصين في الإعلام الآلي وفن الحاسوب لإجراء عملية التفتيش على المنظومة المعلوماتية وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات لتسهيل عمليات التفتيش الالكتروني ، و حجز الأدلة وفقا لما يتلاءم و المقتضيات القانونية [2].

01- قواعد الحجز داخل المنظومة المعلوماتية.

نص القانون 04/09 في المادة السادسة على أنه عندما تكتشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مقيدة للكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

كما يجب في كل الأحوال على السلطات التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري فيها التفتيش، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلي

---

[1] - **أ/يوسف مناصرة** ، المرجع السابق ،(ص). 115

[2]- **د/أمنة امحمدي بوزينة** ، المرجع السـابق،(ص). 75

المساس بالمعطيات، وإذا استحال إجراء الحجز وفق ما هو منصوص عليه في أحكام المادة السادسة من نفس القانون لأسباب تقنية، يتعين علي السلطات المعنية التي تقوم بالتفتيش باستعمال التقنيات المناسبة لمنع الوصول إلي المعطيات التي تحتويها المنظومة المعلوماتية والتي تم نسخها، الموضوعة تحت تصرف الأشخاص المرخص لها باستعمال هذه المنظومة[1].

02- محضر التفتيش الالكتروني في الجرائم المعلوماتية.

لما كان التفتيش عملا من أعمال التحقيق فيستلزم تحرير محضر يدون ويثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة ، و القانون لم يتطلب شكلا خاصا في محضر التفتيش ، وبالتالي لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما[2] كأن يكون المحضر مكتوب باللغة العربية للدولة ، وأن يحمل تاريخ تحريره و توقيع محرره ، كما يجب أن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[3].

المطلب الثالث: حجية الدليل المستخلص من الوسائل الالكترونية بالتفتيش الالكتروني.

أدلة الإدانة في الجرائم المعلوماتية ذات نوعية مختلفة، فهي معنوية الطبيعة كسجلات الكمبيوتر ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، وقد أدت هذه الأدلة الرقمية وتثير أمام القضاء مشكلات كبيرة من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية.

الفرع الاول: مراجعة و تحليل الدليل الرقمي اثناء التفتيش الالكتروني.

الدليل الرقمي هو الدليل الكامن في العالم الافتراضي ، و يعرف بأنه المعلومات و البيانات ذات القيمة في أي تحقيقات جارية و مخزنة أو منقولة أو المعالجة بواسطة الأجهزة الإلكترونية، و يتكون الدليل الرقمي من دوائر و حقول مغناطيسية، و نبضات كهربائية غير ملموسة، و للاستفادة من الدليل الموجود على الوسائط المعلوماتية، و حتى يصبح مستندا إلكترونيا، يجب تعريفه ،توثيقه، طباعته، تخزين نسخة منه، و تحريزه بالقدر الذي يوفر المصداقية، و يحمي الدليل من أي طعن بسبب سوء التعامل معه ، وقبول الدليل الرقمي المستخلص منها.

أولا: الحجز على الادلة الرقمية الناشئة عن التفتيش الالكتروني.

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق يهدف إلى البحث عن الأدلة لإثبات وقوع جريمة ما في مكان معين، و نظرا لخطورته تشترط أغلب التشريعات الحصول عمى رخصة التفتيش من الجهة القضائية المختصة للحجز على المنظومة المعلوماتية، لان نظم المعالجة في الجرائم الإلكترونية تتميز بانها معالجة

---

[1]- **نورة صرشي** ، المرجع السابق،(ص). 65

[2] - **د/أشرف عبد القادر قنديل** ، المرجع السابق،(ص). 154

[3]- **أ/نبيلة هبة هرول** ، المرجع السابق ،(ص). 263

الآلية تكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال متطورة ، فيتم الحجز عن طريق التنفيذ و الاستعانة بخبراء من اجل الحفاظ على الدليل الرقمي [1].

و هذا ما اكده المشرع الجزائري لتسهيل عمليات الضبط و الحجز داخل المنظومة المعلوماتية بموجب القانون 40/90 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال حيث قررها آليات خاصة منها، وفقا لنص المادة 06 منه "عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها و انه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز و الوضع في احراز وقفا للقواعد المقررة في قانون الاجراءات الجزائية .

01- ضبط عمليات حجز الادلة.

يقصد المشرع بحجز المعلومات المخزنة تلك المعطيات المفرغة في دعامة مادية خارج النظام، كالأقراص أو تلك المخزنة داخل النظام ذاته، مثل الذاكرة، بينما يقصد بالمعطيات المعالجة التي أصبحت جزء من النظام بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة، أو تلك المعطيات المرسلة عن طريق منظومة معلوماتية، مثل تبادل المعلومات بين أجهزة المنظومة المعلوماتية فالأولى تعتبر معطيات داخلية للنظام، أما الثانية فتعتبر معطيات خارجية للنظم المعلوماتية .

و يجب في كل الاحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية"

- حجز المعطيات المعلوماتية عندما تكتشف السلطة التي تباشر في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها وانه ليس من الضروري حجز كل منظومة، يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز.
- حجز هذه المعطيات عن طريق منع الوصول اليها، ويتم ذلك عادة عن طريق الترميز او بتقييد الدخول الى تلك المنظومة، او عن طريق اية وسيلة الكترونية.
- حجز المعطيـــات ذات المحتوى الجرمي للمجرم.

وتقع تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به في قانون العقوبات وقانون الإجراءات الجزائية الجزائري، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات والتحقيقات القضائية.

1- **عبد الصديق شيخ**، (الوقاية من الجرائم الإلكترونية في ظل القانون رقم **04/09**) ، مجلة معالم الدراسات القانونية والسياسية، كلية الحقوق والعموم السياسية، جامعة المدية، الجزائر ، المجلد04، العدد 01، 2020،(ص). **199.**

02– أنواع الأدلة الرقمية الناجمة عن التفتيش الالكتروني.

من بين الأشياء او الأدلة التي تضبط وتحتفظ بها في الجرائم المتعلقة بالجريمة المعلوماتية[1] والتي لها قيمة في اثبات تلك الجريمة وتنسبها الى المتهم.

– ضبط جهاز الكمبيوتر وملحقاته: أي ان وجوده وضبطه امر مهم جد للقول بأن الجريمة الواقعة هي جريمة معلوماتية او انها مرتبطة بالمكان او الشخص الحائز على الجهاز[2]، و لأجهزة الكمبيوتر أشكال وأنواع مختلفة الامر الذي يتطلب على ضباط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه ومواصفاته بسرعة فائقة اما بنفسه او بواسطة خبير.

– **البرمجيات**:**software** إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بالتثبيت وتنصيب هذا البرنامج امر في غاية الأهمية عند فحص الدليل.

– **وسائل التخزين المتحركة**: كالأقراص المدمجة "أقراص الليزر، والاقراص المرئية والاشرطة المغناطيسية وغيرها".

– **المودم**:**modem** وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف[3]

– **ضبط البريد الالكتروني**: عن طريق تحديد صندوق البريد الخاص بالمتهم محل التفتيش بعد معرفة اسم المستخدم والرقم السري للدخول وفتح البريد الالكتروني عن طريق البريد الوارداو الصادر او الحفظ او المهملات او ضبط الرسائل الالكترونية عن طريق تشغيل برامج البريد الالكتروني في جهاز المتهم ومراجعة قائمة الرسائل الجديدة ليلتقط الرسالة المطلوبة[4]، و توجد جملة من الصعوبات التي تواجه المحقق في ضبط الدليل:

ان عملية ضبط البيانات المعالجة آليا تواجه عدة صعوبات أهمها:

– ضخامة البيانات التي من الواجب فحصها

– الضبط في مجال المعلوماتية قد يمثل أحيانا اعتداء على حقوق الغير او على حرمة حياتهم الخاصة مما يستوجب اتخاذ ضمانات لازمة لحماية هذه الحقوق.

– قد توجد هذه البيانات والمعطيات في شبكات وأجهزة تابعة لدولة اجنبية مما يستدعي تعاونها مع جهات التحقيق الوطنية.

---

[1]– **د/محمود إبراهيم غازي**، الحماية الجنائية للصوصية والتجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، طبعة 2013،(ص). 256

2– د/خالد عياد الحلبي ، المرجع السابق ،(ص). 176

3– **د/ نهلا عبد القادر المومني**، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع ، عمان، الاردن، طبعة 2010 ، (ص (42).

[4] – **د/خالد عياد الحلبي**، المرجع السابق،(ص). 170

و يلاحظ ان المشرع الجزائري يؤكد ضمانات الحجز وحفظ الدليل وفقا لنص المادة 06 من القانون رقم 04/09 التي تنص على "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأن وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية". قواعد التفتيش و الحجز في النظم المعلوماتية.

ثانيـــا: محضر التفتيش الإلكتروني.

01- افتتاح محضر التفتيش الالكتروني.

إن لافتتاح المحضر أهمية بالغة وتقدير الدليل الذي يستخلص من الأوراق، فهي أول بيانات تقع عليها العين هي من المقدمة الذي تعتبر ملخص عن الواقعة ، حتى تكون الافتتاحية صحيحة لا بد أن يتضمن مجموعة من البيانات نوردها فيما يلي:

- الرقم القضائي للواقعة والتكييف القانوني لها:

إن أول ما يتصدر المحضر جمع الاستدلالات هو الرقم القضائي الخاص بالواقعة حسب ترتيب القيد بدفتر القضايا مقترن بالوصف القانوني والتكييف القانوني للواقعة (جناية، جنحة...).

وتجدر الإشارة إلى أن الرقم المقيد من قبل الشرطة هو رقم مؤقت، وذلك لحين صدور قرار نهائي من النيابة العامة في التحقيق، إما بمواصلة قيد الأوراق بذات القيد أو تقييدها برقم قضائي آخر، مع إخطار الشرطة المختصة بقرار التغيير[1].

ويكتب الرقم القضائي بمداد مغير للون المداد المسطر به المحضر ويفضل أن يكون باللون الأحمر حتى يكون واضحا ضمانا لسهولة الحصول عليه. ومعرفته ومنع تكرار القيد. وبالتالي لا بد أن يكون جميع الجنح والجنايات أو مخالفة أو شكوى عن وقوع جريمة معلوماتية لا بد أن تكون مقيدة برقم قضائي.

- عنوان المحضر التفتيش الالكتروني.

يتضمن عنوان المحضر تاريخ ووقت ومكان افتتاحه، وبيانات المحقق والإجراءات التي قام بها قبل بدء التحقيق، ونتناولها على النحو التالي:

- تاريخ ووقت افتتاح المحضر التفتيش الالكتروني.

إن أول ما يكون في المحضر هو تاريخ افتتاحه ووقته، والتاريخ يثبت فيه أي أيام الأسبوع قد جرى التحقيق فيها واليوم والشهر والسنة بالتقويمين، الميلادي والهجري. وهذا التاريخ كثيرا ما يفيد في معرفة وقت حدوث الجريمة.

---

1 - لكي يعتبر محضر التحقيق صحيحا لا بد له أن يقيد برقم يميزه عن غيره من المحاضر مع ضرورة إخطار الشرطة المختصة في حالة صدور قرار من النيابة العامة تغيير الرقم القضائي للمحضر الذي سجلته الشرطة في مرحلة جمع الاستدلالات.

– مكان تحرير المحضر التحقيق.

تتمثل في بيانات يدونها المحقق بحيث يثبت عند تحرير المحضر اسمه وصفته وأهمية هذا البيان في تحديد ما إذا كان للمحقق حق مباشرة التحقيق من عدمه، ويتلو بيان اسم كتب التحقيق ، سواء كان كاتب النيابة أو آخر انتدبه المحقق بعد أداء اليمين، مع إثبات الحلف على ما سبق بيانه[1].

02– الإجراءات السابقة على بدء التحقيق.

ويقصد به إثبات جل وكل الإجراءات السابقة على بدء ومباشرة التحقيق من تلقيه للبلاغ وانتقاله إن انتقل ومضمون محضر الاستدلالات إن وجد، فيجب على المحقق إثبات البلاغ الذي تلقاه عن الحادث على الصورة التي وردت إليه، كساعة وصول البلاغ إليه وتأشيرة بذلك عليه.

– مقدمة المحضر

هي عبارة عن ملحص وافي عن الواقعة، ويراعى في مقدمة المحضر إثبات ذلك:

– طريقة تلقي البلاغ.

– ملخص بسيط عن الواقعة.

ويكون بعد ذلك إثبات ورود الأخبار عن الواقعة للمحقق كما بينا سابقا على المحقق أن يقوم بإثبات محضر مضمون الواقعة وكيفية حدوثها، ومناقشة الأطراف شفاهة.

03– موضوع المحضر

هو ما يتضمنه المحضر من إثبات جميع ما قام به المحقق من إجراءات قانونية وفنية من أجل كشف الغموض عن الواقعة، قبض على مرتكبي (المجرم المعلوماتي) الفعل، وضبط الأدلة من أجل إسناد الواقعة[2].

ويمكن تقسيم هذه الإجراءات إلى قسمين:

– الإجراءات التي قام بها المحقق ويطلق عليها الأدلة المحسوسة أو المادية.

– الإجراءات المتعلقة بأطراف الواقعة

يقصد بها الحجج والبراهين التي تشير إليها دلالة العثور على الآثار والأجسام المتعلقة بالجريمة ومعاينتها، وفحصها والتي يمكن إدراكها بالحواس أو عن طريق استعمال أي وسيلة من الوسائل العلمية التي تستعمل لضبط الأدلة وخاصة الإلكترونية منها[3].

---

1 – لا بد عند كتابة المحضر ذكر جميع بيانات المحقق الذي قام بالتحقيق ليميز بينه وبين محاضر الشرطة.

2 – **د/عبد الفتاح بيومي الحجازي**، المرجع السابق،(ص). 74

3 – تتمثل الضوابط في كل ما يتوصل إليه المحقق من حجج والبراهين والادلة التي يتركها الجاني في محل الجريمة المعلوماتية

وتتمثل هذه الإجراءات لضبط الأدلة المادية من خلال قيام المحقق الانتقال إلى مكان ارتكاب الجريمة ومعاينتها ومن أسفرت ونتج عنه من آثار ومدلولات بالإضافة إلى وضع خطة من فريق البحث من أجل تنفيذها من خلال القبض على المتهم تفتشه من خلال الإجراءات المتعلقة بأطراف الواقعة.

تتمثل الواقعة (الجريمة) من المبلغ، المجنى عليه، الشاهد المتهم المضبوطات.

ولذلك يجب أن يقتصر مناقشة المتهم على أحد المحققين ذوي الخبرة وليس أعوانهم وأن يكون ذلك في غرفة التحقيق.

- يجب على المحقق تقديم إيضاحات من المتهم عن تفاصيل وجزيئات الواقعة.
- مواجهة المتهم بأقوال أطراف الواقعة الآخرين كالشهود أو المجني عليه أو متهم آخر.
- مواجهة المتهم بالدلة التي تم العثور عليها بمسرح الجريمة أو في حيازته.
- يجب أن يحدد المحقق مدى تعارض وتناقض واختلاف أقول المتهم ويقوم بمواجهته بهذا التناقض[1].

04- توقيع المحقق على المحضر

أوجب القانون على المحقق أن يوقع على المحاضر وكذلك الحال بالنسبة إلى الكاتب ويجب أن يتم التوقيع على كل صفحة من صفحات التحقيق.

هذا وفضلا عن نهاية المحضر وذلك إبعاد لأية شبهة كالتزوير على أنه بالنسبة للكاتب يكفي توقيعه مع المحقق في نهاية محضر التحقيق، لأن الثقافة القائمة بالمحضر مستمدة من توقيع عضو النيابة العامة.

الفرع الثاني: مدى مشروعية الأخذ بالدليل الرقمي المستخلص من التفتيش الالكتروني.

يترتب عمليات التفتيش آثار متعددة اهمها حجز كل المنظومة و يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهما على دعامة تخزين الكترونية تكون قابلة للوضع و الحجز في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، مع إمكانية الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، كما ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية[2].

أولا: مشروعية الدليل المستخلص من التفتيش الالكتروني.

لما كانت مخرجات وهدف التفتيش هو البحث عن مجموعة من الأدلة التي تتعلق بجريمة معينة، هو ما مدى مشروعية الأدلة المستخلصة من الوسائل الالكترونية وهل لها قيمة قانونية أمام المحاكم خاصة أنها تعتبر على غير الأدلة التي اعتادت المحكمة عليها من أدلة مادية.

---

[1] - أ/**عفيفي كامل عفيفي**، المرجع السابق ،(ص). 154

[2] – **د/الشحات إبراهيم محمد منصور**، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية، دار الفكر الجامعي الاسكندرية، طبعة 2011،(ص). 197

01- شروط صحة الدليل المستخلص من التفتيش الالكتروني.

ومن ثمة لابد من التعرف على الشروط الواجب توافرها في الدليل الالكتروني حتى يقال بأنه دليل مشروع وحتى يمكن للقاضي الأخذ به، وطالما أن التفتيش هو إجراء مطلوب من النيابة العامة[1] في خضم تحرياتها وتحقيقها حول حقيقة الجريمة، وهذه الشروط هي:

- أن يكون الحصول على الدليل المستخلص من الوسائل الالكترونية قد تم بطريقة مشروعة.

مقتضى هذا الشرط أن لا تكون العملية أو الإجراء الذي تم الحصول من خلاله على الدليل الالكتروني إجراء غير مشروع أو مخالفا لأحكام الدستور والقانون وعلى ذلك فلا يجوز التعدي على تلك الحرمات فلا يتعرض لها إلا وفقا لما تقتضيه القوانين، وهذا يقود إلى نتيجة مفادها إن الحصول على الدليل الرقمي لابد أن يتم ضمن إجراء صحيح، فلابد للتفتيش أن يتم وفقا لشروط التفتيش، و إلا اعتبر التفتيش باطلا ، كاستخدام التدليس والخداع للحصول على الدليل المستخلص من الوسائل الالكترونية

ويرى الباحثون أن المشرع استجاب للمتطلبات العملية عندما سن قوانين تواجه جرائم أنظمة المعلومات ، من حيث تجريم التعدي على حريات الأفراد المتوافرة في الحواسيب والانترنت، محيط هذه الحريات بالحماية وكما احاط التفتيش الالكتروني بضمانات قانونية وقضائية[2].

- أن **يكون الدليل المستخلص من الوسائل الالكترونية يقينيا**

ومفاد ذلك أن لا يكون الدليل قابلاً للشك، و إذا كان ذلك فإن الشك يفسر لصالح المتهم ، وهنا يأتي دور القائم على التفتيش وخبرته في مجال يقينية الدليل ونوعية البرامج والأجهزة المستخدمة ، إن تطلب الأمر ذلك.

02- خضوع الدليل المستخلص من التفتيش الالكتروني للمناقشة.

ان الدليل المستخلص من الوسائل الالكترونية لا يمكن الاعتداد به إلا بعدما يطرح للمناقشة أمام المحكمة، والتي يكون لها تقدير قيمة هذا الدليل ولاشك أن للمناقشة و إظهار واستجلاء جوانب الدليل بحد ذاته والإجراء المستخلص من خلاله اجراءات التفتيش الالكتروني دور بارز في تشكيل قناعة المحكمة في الاعتماد على هذا الدليل من عدمه.

وذلك لما لهذه المناقشة من دور هام في تشكيل المحكمة لقناعتها على ضوء ما طرح أمامها وعلى مسامعها من أدلة تخللها العديد من المناقشات، ولا يكفي في ذلك مجرد الاطلاع على محاضر التفتيش

---

[1] - **د/غنام محمد غنام**، دور قانون العقوبات في مكافحة جرائم الكمبيوتر و الانترنت ، دار الفكر والقانون المنصورة(بدون مكان النشر)، طبعة 2010،(ص). 211

[2]- **أ.د/عبد اللاه هلالي احمد** ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،(دارسة مقارنة)، الطبعة الاولى ، دار النهضة العربية، (بدون مكان النشر)، طبعة 1997،(ص). 180

الالكتروني، ويمتد الأمر إلى أن المحكمة التي لم تستمع لمناقشة الدليل المستخلص من الوسائل الالكترونية لا تملك الحكم بالدعوى لأنه لا تستطيع تقدير قيمة هذا الدليل[1].

ثانيا: حجية الدليل المستخلص وسائل التفتيش الالكتروني

اشترط المشرع الجزائري الحصول على الدليل الرقمي بصورة مشروعة فلا يجوز للقاضي الجنائي أن يسند في حكمه الا على دليل تم الحصول عليه قانونية، ولابد أن يكون الدليل صحيحا لا يشوبه بطلان يتقرر بمخالفة إجراءات القانونية ، لأن مشروعية الخصومة الأدلة تعتبر حدا لا يمكن للقاضي أن يتجاوزه، نظرا لما تقوم عليه الخصومة الجنائية من تعزيز لقرينة البراءة ومن جهة اخرى مراعاة حرية القاضي في الإثبات باعتباره ممثلا لسلطة الدولة في العقاب[2].

اما بالنسبة لموقف المشرع الجزائري من الدليل الالكتروني في ظل التشريع الجزائري نصت المادة 212 ق.إ.ج.ج الفقرة الأولى "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص في القانون على غير ذلك، و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"، و القاضي الجزائري عند الفصل في النزاع المتعلق بالجريمة المعلوماتية يجد بين يديه المحضر الخاص بالتفتيش الالكتروني ، هذا الاخير يرجع للسلطة التقديرية للقاضي الجنائي للأخذ به داعما هذه السلطة ببقية الادلة المقدمة ، بالإضافة الى السلطات التي منحها له المشرع في مجال التحقيق القضائي[3].

---

[1] – **د/ مصطفى محمد موسى** ، التحقيق الجنائي في الجرائم الكترونية ، مطابع الشرطة القاهرة، طبعة 2008 ،(ص). 259

1– **آمال قارة** ، المرجع السابق،(ص).196.

[3]-راجع المـادة307 من الامر رقم 11/21 المؤرخ في 25 اوت 2021 المتعلق بقانون الاجراءات الجزائية الجزائري.

ملخص الفصل الثاني

مع التطور التكنولوجي للاتصالات الذي يشهده العالم الحالي والذي استفاد منه عالم الإجرام، وجدت جرائم حديثة يطلق عليها مصطلح الجرائم المعلوماتية والتي أثارت العديد من الاعتداءات على الاشخاص، الاموال و امن الدولة...، لذا كرس المشرع الجزائري التفتيش الالكتروني كضابط للكشف عن الاعتداءات الإجرامية.

ولما كانت الضبطية القضائية مقيدة في الدعوى الجزائية بمبدأ الشرعية الجنائية والإجرائية، فإن هذه الأخيرة لا يمكنها اتخاذ اجراء التفتيش الالكتروني دون الرجوع إلى القواعد المنصوص عليها في قانون الإجراءات الجزائية، حتى لو كانت هذه الأفعال الغير مشروعة ولها درجة عالية من الخطورة الإجرامية، كل هذه التغيرات ونظرا لحداثة الجريمة المعلوماتية.

و على هذا الاساس يعد التفتيش الالكتروني في الجريمة المعلوماتية إجراء صعب بالنظر إلى طبيعة الدليل المتحصل منه والذي يسهل 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.

و عليه ساير المشرع الجزائري في ذلك المجتمع الدولي من اجل مكافحة الجريمة المعلوماتية حيث بادر إلى وضع استراتيجية شملت استحداث نصوص قانونية خاصة بمقتضى القانون04/09 كفيلة بالحد من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من جهة، وتعديل النصوص القانونية السارية المفعول بما يتناسب مع هذا النوع من الجرائم، مع إعطاء أهمية عملية لمكافحة الجريمة المعلوماتية عن طريق إرساء أجهزة وهيئات أسندت لها ذات المهمة.

بحيث يبرز الدور الايجابي للهيئة الوطنية المكلفة بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال دون إغفال الدور الفعال للجهاز الأمني في هذا المجال، التي تساهم مع السلطات المختصة في جمع الأدلة المتعلقة بالجريمة المعلوماتية، التي تخضع لمبدأ حرية القاضي الجنائي في الإقناع وصولا إلى الحقيقة الموضوعية بشأن الجريمة والمجرم ،أما في الجرائم المعلوماتية فيتسم إجراء التفتيش من أهم إجراءات التحقيق بمقتضى المعاينة الأولية للاستدلال على ملابسات الجريمة، والغاية من الاجراءات ضبط ما استعمل في ارتكاب الجريمة أو نتج عنها.

خاتمة

خاتمـــة

إن التطور الهائل الذي شهده كل من مجال تقنية المعلومات ومجال الاتصالات والاندماج المذهل الذي حدث بينهما، إذ أصبحت جميع القطاعات تعتمد في آداء عملها على استخدام الأنظمة الالكترونية ، مما وسع في مجال الاجرام المعلوماتي ليمس الجرائم الواقعة على الاشخاص، الجرائم الواقعة على الاموال ، الجرائم الماسة بأمن الدولة.

و على هذا الاساس حدد المشرع الجزائري القواعد الاجرائية التي تتناسب ومتطلبات الحماية القضائية للحقوق محل الاعتداء متابعة الجرائم لمعلوماتية ، وتجسيد التفتيش الالكتروني كآلية لضبط الدليل الرقمي، و دعم هذه الضوابط من خلال الانضمام الى العديد من الاتفاقيات الدولية ، كما نص تعديل قانون الاجراءات الجزائية سنة 2006 ، بالإضافة للإجراءات المستحدثة الخاصة بالجريمة الالكترونية وفقا للقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبالرغم من وجود النصوص القانونية لمكافحة الجريمة الالكترونية.

نتائج الدراسة.

إن الانعكاسات السلبية الناجمة عن الاستخدام الغير المشروع الذي ألحق الضرر بالفرد والمجتمع في اطار الجريمة المعلوماتية أثارت العديد من الاشكالات في موضوع دراستنا، بالتالي سنستعرض اهم النتائج التي ت م استخلاصها من دراسة موضوع التفتيش الالكتروني

عدم تناسب احكام لتي في نطاق قانون الاجراءات الجزائية الذي وضعت نصوصه لتحكم الجرائم التقليدية ، وعدم توافقه مع احكام الجرائم المعلوماتية المستحدثة لتميزها بالمرونة و لا تلاءم تطبيقات قانون الاجراءات الجزائية و خصوصية أحكامه لذا استحدث المشرع القانون رقم 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها

الا ان الاشكالات الاجرائية في مجال المتابعات تعد أول عائق في غياب التأهيل الفني لجهات التحقيق الذي يؤدي الى اتلاف الدليل وإفلات مرتكبي هذه الجرائم من العقاب، و بالنظر الى ان التفتيش الالكتروني لم يعد قادرا على استيعاب كافة الجرائم المعلوماتية لاستخدامها اساليب متطورة و متحولة ، مما ساهم في خلق اشكالات على صعيد الملاحقة الجنائية في إطار القوانين و الدولية

مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، حتى يضمن التفتيش الالكتروني احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى ، وتتكامل فيه الدوار و الاهداف بعد المصادقة على المعاهدات الدولية.

و بالنظر الى تطور معطيات الجرائم الالكترونية و قلة المعلومات الخاصة بالنواحي الفنية التي تستخدمها الجهات المختصة بالتفتيش الالكتروني، و الاجهزة والبرامج الدقيقة وضعف الاجهزة المختصة بالتحري في هذا النوع من الجرائم وعدم التنسيق بين المحققين في هيئات التحقيق والمبرمجين في مجال تقنية المعلومات والانظمة الالكترونية والشبكات ذات المستويات التي حددها القانون رقم 04/09.

و في ختام نتائج دراسة موضوع التفتيش الالكتروني، وتأسيسا على معطيات النتائج أعلاه لاحظنا أن المشرع الجزائري قد عمل جاهدا على سن نصوص عقابية موضوعية وإجرائية لمكافحة الجريمة المعلوماتية مواكبا بذلك التشريعات المتطورة، الا انه تبقي العديد من الثغرات التي تحول دون التطبيق الجيد للنصوص و المراسيم التي استحدثها المشرع.

اقتراحات الدراسة

على هذا الاساس نقترح الأخذ ببعض التعديلات في أحكام المتعلقة بالتفتيش الالكتروني حتى يصل المشرع إلى مكافحة أكثر فعالية لهذا النوع المستحدث و المتطور من الإجرام المعلوماتي وتقديم المقترحات والحلول البديلة لتتناسب و الوسائل الاجرامية الحديثة.

لتدارك النقص المتمثل في عدم وجود قانون خاص للجرائم الالكترونية، لذا سنحدد جملة الاقتراحات و الحلول البديلة لتتناسب ووسائل الاجرامية الحديثة التي ستساهم بشكل فعال لتزويد الجهات التشريعية بكل المستجدات في مجال تقنية المعلومات و تطوير التفتيش الالكتروني

ضرورة تفعيل التفتيش الالكتروني من خلال سد الثغرات في مجال التشريعات الالكترونية ، من خلال إصدار تشريع خاص ومستقل للجرائم الإلكترونية بوضع إجراءات جنائية تنسجم مع طبيعة هذا النمط من الجرائم ، و تحديد ضوابط التفتيش الالكتروني و احكامه الاجرائية المختلفة.

عقد دورات مكثفة للإطارات العاملة في حقل التحري الشرطوي و التحقيق في مجال جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب، والجرائم المرتبطة بها والنظر في مضامين منهاج التحقيق و الاستفادة من تجارب أو خبرات الدول المتطورة في مجال التفتيش الالكتروني و استغلال الاجراءات الوقائية لمنع وقوع الجريمة.

ضرورة مواكبة القوانين للتطورات واستيعابها ، بالنظر الى التطور المتلاحق في مجال تقنية المعلومات والاتصالات و ما يقابله من استغلال الجناة لهذه التقنية المتطورة بابتكار أساليب جديدة لارتكاب الجرائم الإلكترونية، استحداث شعبة خاصة لمكافحة الجرائم الالكترونية

تحسين التكوين المستمر للعناصر المكلفة بمكافحة الجريمة المعلوماتية، من أجل الرفع من الكفاءة لمختلف الفئات من رجال الأمن ومهندسي الإعلام، ورجال القانون، من اجل القيام بإجراءات التفتيش الالكتروني من خلال خلق إخصائيين تقنيين في مجال تسهيل عمليات التفتيش الالكتروني.

إلغاء المادة 47 مكرر إ ج إذ من شأن ضرورة تفتيش ضابط الشرطة القضائية مسكن المشتبه فيه الموضوع تحت النظر أو المحبوس، بحضور شاهدين غير بعين لسلطته أو ممثل يعينه صاحب المسكن، عرقلة سرعة الحصول على الدليل الرقمي، و لتالي من الأحسن الأخذ بما جاء في أحكام المادة 45 فقرة أخيرة إجراءات جزائية، من عدم ضرورة حضور صاحب المسكن أو من ينوبه، عند تفتيش مسكنه في الجرائم المحددة في هذه الفقرة، منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

العمل على ايجاد ادلة اثبات جديدة تتلاءم مع طبيعة الجرائم الإلكترونية، أو التوسيع من اختصاص الجهات التي حددها القانون 04/09 في مواجهة الجريمة الإلكترونية ، كما يجب على الصعيد الدولي إزالة العقبات فيما يتعلق بموضوع الجرائم الإلكترونية من خلال الإنضمام الى الاتفاقيات الجماعية ذات العلاقة بالجرائم الإلكترونية او الاتفاقيات الخاصة بالمساعدة القضائية بشكل عام على أن يكون مرجعهم في كل هذا المبادئ التي وضعيا الاتحاد الدولي للاتصالات باعتباره الجهة المختصة ونقطة المحور الذي تعود إليها حكومات الدول في موضوع تقنية المعلومات، و متابعة الجرائم الالكترونية.

التوصيات.

و عليه يمكننا تلخيص التوصيات في النقاط التالية:

ضرورة إيجاد وسائل مناسبة للتعاون الدولي لمكافحة من الناحية الإجرائية في مجال التفتيش الالكتروني وتمديد الاختصاص ، والتطبيق الفعلي لمواد القانون 04/09 في مجال التوفيق بين التشريع الخاص بهذه الجرائم والتعاون الدولي القائم على تبادل المعلومات، وقبول أي دولة للأدلة المجموعة في دولة أخرى لضمان الحماية العالمية الفعلية لبرنامج المعطيات وشبكة الانترنت ككل.

ضرورة قيام ضباط الشرطة القضائية وأعوان الضبط القضائي بمعاينة وتفتيش وحجز تقني للأجهزة في المكان الذي تم فيه ضبط الأجهزة قبل الحجز عليها، تفاديا لأي حذف أو تغيير للمعطيات والبيانات خاصة منها المتصلة بالإنترنت من جهة وعدم المساس بممتلكات الأشخاص من جهة أخرى في حالة ما إذا كان التفتيش سلبي .

إعادة تسمية قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بقانون الوقاية من جرائم تقنية المعلومات ومكافحتها، أو بقانون الوقاية من جرائم أنظمة المعلومات ومكافحتها، لخلق توازي في الاشكال لان المشرع الجزائري يطلق على الافعال الغير المشروعة في المجال الالكتروني تسمية الجرائم المعلوماتية.

التزام المشرع الجزائر أي بسن قانون مستقل جديد كامل ، يبين فيه جميع الآليات الموضوعية و الإجرائية الخاصة بالجرائم الإلكترونية، مع استحداث شعبة متخصصة في الجهات القضائية للتحقيق في الجرائم الالكترونية تتكون من خبراء و مبرمجين في مجال مكافحة الجرائم الالكترونية تتولى عمليات التدريب والتأهيل للمحققين في مجال التحقيق و التفتيش في الجرائم المعلوماتية.

يجب النص على ضرورة حضور المتهم أو محاميه إجراءات الإطلاع على نتائج التفتيش الإلكتروني لتأكيد سلامة الإجراء وضمان حقوق الدفاع أيضا، و احترام الضمانات التي يكرسها الدستور و القوانين الاجرائية.

– النص على أنه إذا اقتضت ضرورات التحري والتحقيق في جرائم المساس أنظمة المعالجة الآلية للمعطيات، فإنه يجوز للسلطة القضائية. أن تأمر مقدمي الخدمات، بحفظ المعطيات المتعلقة بحركة السير، المخزنة والموجودة بحيازته أو تحت سيطرته وصيانة سلامة تلك المعلومات.

ضرورة التعاون الدولي لمكافحة الجرائم الإلكترونية من خلال انشاء وحدات متخصصة على المستوى الدولي و العربي ، تهتم بالتنسيق المني بين الدول في مجال متابعة و معاقبة مرتكبي الجرائم الإلكترونية

عدم ملائمة نصوص قانون الإجراءات الجزائية للتماشي مع اجراءات التفتيش الالكتروني و جمع أدلة الجرائم المعلوماتية، مع ضرورة مراجعة التشريعات الوطنية من خلال تقنين خاص يحدد الإطار الإجرامي لخصوصية هذه الجرائم ، مع تشديد الوصف الجنائي والعقوبات المقررة لأنماطها الإجرامية، مع تحديد الإجراءات المتخذة بدقة.

قائمة المراجع و المصادر

قائمة المراجع و المصادر.

أولا: المراجع باللغة العربية.

أ. الكتب:

✓ **الكتب العامة:**

- أحمد السيد عفيفي ،الاحكام العامة للعلانية في قانون العقوبات(دراسة مقارنة)، دار النهضة العربية، القاهرة، طبعة 2002.

-أحمد عبد الحكيم عثمان، تفتيش الأشخاص وحالات بطلانه، منشأة المعارف، الاسكندرية، طبعة2002.

-أحمد المهدي ، القبض والتفتيش والتلبس، الطبعة الأولى ، دار العدالة، القاهرة ، طبعة 2007.

-أحسن بوسقيعة ،التحقيق القضائي، الطبعة الثانية ، دار هومه، الجزائر ، طبعة 2012.

-أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، طبعة 1994.

- يوسف دلاندة ، قانون الإجراءات الجزائية، دار هومه، الجزائر، طبعة2001.

✓ **الكتب الخاصة:**

-الشحات إبراهيم محمد منصور، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية، دار الفكر الجامعي الاسكندرية، طبعة 2011.

-أمال عبد الرحيم عثمان ، شرح قانون الاجراءات الجنائية،دار النهضة العربية ، القاهرة، (بدون تاريخ الطبعة).

-بلال أمين زين الدين، "جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن"، دار الفكر الجامعي، الإسكندرية 2008طبعة.

-هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الاولى، دار النهضة العربية، القاهرة، مصر، طبعة 1992

– هلالي عبد اللاه أحمد.

- تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي،(دارسة مقارنة)، الطبعة الاولى ، دار النهضة العربية، (بدون مكان النشر)، طبعة 1997،(ص). 180
- حجية المخرجات الكمبيوترية في الاثبات الجنائي، الطبعة الاولى، دار النهضة العربية، القاهرة(بدون تاريخ نشر)
- اتفاقية بودابست لمكافحة جرائم المعلوماتية ، الطبعة الاولى، دار النهضة العربية ، طبعة 2007

– زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، طبعة 2011.

-كوثر سعيد عدنان خالد ، حماية المستهلك الكتروني ، الجامعة الجديدة (بدون ذكر مكان النشر)،طبعة .

- محمد امين احمد الشوابكة ،جرائم الحاسوب و الانترنت ، الطبعة الاولى ،دار الثقافة ،عمان ، الاردن ،طبعة 2004

-محمد عبد الله سلمة، موسوعة الجرائم المعلوماتية، الطبعة الاولى، المكتب العربي الحديث ،الاسكندرية، مصر، طبعة2007.

-محمود إبراهيم غازي، الحماية الجنائية للصوصية والتجارة الالكترونية، الطبعة الأولى، مكتبة الوفاء القانونيـــة الاسكندرية، طبعة 2013.

- مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الكترونية ، مطابع الشرطة القاهرة، طبعة 2008 .

– نهلا عبد القادر المومني، الجرائم المعلوماتية ، دار الثقافة للنشر و التوزيع ، عمان، الاردن، طبعة 2010 .

-سامي الحسيني، النظرية العامة للتفتيش في القانون المصري و المقارن ،دار النهضة العربية، القاهرة ، طبعة 1980

-سعيد محمد، الجرائم الإلكترونية و آليات الحصول على الدليل فيها، الطبعة الأولى ، دار النشر الذهبي، الاردن، طبعة 2005.

-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي)دراسة مقارنة(، دار الجامعة الجديدة، الإسكندرية، طبعة 2009.

-عبد الله بن سعود محمد السراني، فاعلية الاساليب المستخدمة في اثبات جريمة التزوير الالكتروني ، جامعة نايف العربية للعلوم الامنية (بدون ذكر مكان النشر)، طبعة 2011.

-عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي الإسكندرية،طبعة2009.

– علي عدنان الفيل

- إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث مصر، طبعة 2012.
- اجراءات التحري و جمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية) دراسة مقارنة(،المكتب الجامعي الحديث العراق، طبعة 2011.

- علي ابراهيم توفيق، دور المحقق في الجرائم الالكترونية ، الطبعة الثالثة ، دار المدى للنشر و التوزيع، العراق، طبعة 2000.

- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت) دراسة مقارنة(،عالم الكتاب الحديث ، اربد، الاردن، طبعة 2004.

- علي حسن طوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة، الطبعة الأولى ،2004.

-فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الاردني و المقارن)الجزء الثاني(،دار الفارابي عمان ،طبعة 1980.

-رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الاولى ،منشورات الحلبي الحقوقية ،بيروت، لبنان ،طبعة 2012.

-خالد عياد الحلبي، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، دار الثقافة للنشر والتوزيع ، عمان، الاردن،طبعة 2011.

- **غنام محمد غنام**، دور قانون العقوبات في مكافحة جرائم الكمبيوتر و الانترنت و جرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون ، المنصورة ، مصر، طبعة 2010،(ص).180

ب. الرسائل والمذكرات.

✓ **الرسائل الجامعيــة.**

-عزيزة رابحي،(الأسرار المعلوماتية وحمايتها الجزائية)،أطروحة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق و العلوم السياسية ، جامعة أبو بكر بلقايد تلمسان السنة الجامعية 2018/2017.

✓ **مذكرات الماجستير**

-نعيم سعيداني،(آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري)، مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة باتنة ،سنة الجامعية 2012.

- قارة أمال، (الجريمة المعلوماتية)، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، تاريخ المناقشة2002

- نورة صرشي،(مكافحة الجريمة المعلوماتية)، مذكرة من اجل الحصول على شهادة الماجستير في القانون الجنائي كلية الحقوق جامعة الجزائر ،سنة 2012

✓ **مذكرات الماستر.**

- منصورية بلعيد،(النظام الاجرائي للجريمة المعلوماتية)،مذكرة لنيل الماستر في تخصص القانون القضائي، جامعة بن باديس مستغانم ، السنة الجامعية2020

- رابح مباركة ، (اجراءات التحري والتحقيق في الجريمة الالكترونية)،مذكرة لنيل الماستر في تخصص قانون الاعلام الالي و الانترنت ، جامعة محمد الابراهيمي ، جامعة برج بوعريريج، السنة الجامعية 2022/2021.

ت. المجلات العلمية.

-(اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية) ، عز الدين عثماني, مجلة دائرة البحوث والدراسات القانونية والسياسية , جامعة الوادي، الجزائر , العدد الرابع , 2018.

-(تفتيش المنظومات المعلوماتية في القانون الجزائري)، رضا هميسي، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، العدد 05، جوان 2012

- (مبادئ و ضوابط المعالجة الآلية للمعطيات الشخصية) ،نجاة لوصيف، موسي مرمون، ،مجلة العلوم الانسانية، جامعة بسكرة ، المجلد 33، عدد02 جوان 2022.

-(ضوابط مكافحة الجريمة المعلوماتية ،)، سعاد رابح، مجلة القانون العام الجزائري ،المجلد السابع، كلية الحقوق الجزائر، العدد01،جوان 2000.

-(الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري) ، **وردة شرف الدين** ،مجلة المنار للبحوث والدراسات القانونية والسياسية ، العدد الثالث ، ديسمبر 2017 ، الصادرة عن كلية الحقوق والعلوم السياسية جامعة يحي فارس المدية.

-(آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا) ، **نوارة حسين**، منشور في مجلة الدراسات القانونية لأعمال ملتقى آليات مكافحة الجرائم الإلكترونية ، كلية الحقوق جامعة الجزائر

-(الوقاية من الجرائم الإلكترونية في ظل القانون رقم 04/09) عبد الصديق شيخ، مجلة معالم الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة المدية، الجزائر ، المجلد04، العدد 01، 2020

- (عربوز فاطمة الزهراء، التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية) ، مجلة العلوم و الدراسات القانونية كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس،الجزائر،العدد10.

ج.الملتقيات و الاعمال الدراسية

✓ **الملتقيات**

-مفتاح بوبكر المطردي،(الجريمة الإلكترونية)، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، مجلة القانون السودان العدد22، طبعة 2012،

- حملاوي عبد الرحمان،(مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية) منشورة بمجلة الحقوق جامعة بسكرة كلية الحقوق ، العدد 33 ، طبعة2016.

ح. النصوص القانونية.

✓ **الاتفاقيات.**

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات محررة بالقاهرة في2010/12/21 صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم252/14 المؤرخ في 2014/09/08، الجريدة الرسمية رقم57، الصادرة بتاريخ 2014/09/28.

الدساتير.

- المرسوم الرئاسي 251/20 المؤرخ في 15 سبتمبر سنة 2020 المتضمن التعديل الدستوري ، الجريدة الرسمية رقم 98.

✓ **النصوص التشريعية.**

- القانون04/09 المؤرخ في 05 اوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية رقم 47.

- القانون04/21 المؤرخ في 28 ديسمبر2021 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات ، الجريدة الرسمية رقم 102/21، الجريدة الرسمية رقم 18.

- القانون 01/06 المؤرخ في 20 فيفري سنة 2006، المتعلق بالوقاية من الفساد ومكافحة الجريدة الرسمية رقم 37.

- القانون رقم 07/18 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المؤرخ في 10 جوان 2018 الجريدة الرسمية رقم 50.

- القانون رقم 07/18 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الجريدة الرسمية رقم .44

✓ **النصوص التنظيمية.**

- المرسوم الرئاسي رقم 261/15 المؤرخ في 8 أكتوبر سنة 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية ، العدد 53، السنة الثانية والخمسون، الصادرة في 08 أكتوبر سنة 2015 .

- تعديل المرسوم التنفيذي348/06 المؤرخ في5 أكتوبر سنة 2006المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق الجريدة الرسمية رقم 13.

خ الاحكام القضائية.

✓ **القرارات القضائية.**

- قرار المحكمة العليا بتاريخ 1997/07/30 ، ملف رقم 165609 ، المجلة القضائية لسنة 1997 العدد الثاني.

✓ **مواقع الانترنت.**

-http://swideg-geography.blogspot.com/2017/08/blog-post_html-

- www.cybercrime.gov/coedraft.html

- http://nidhal technologie.own0.com/t60-topic

-http://www.uobabylon.edu.iq/uobColeges/service_showrest.aspx?fid
- http:// salahgardafi.eb2a.com.content.
- http//:kenona online. com

ثالثا: المراجع باللغة الفرنسية

- **Roger Merle** et Andre Vitu, traite de droit criminel, Tome2, quatrième édition,
édition Cujas, Paris, 1989.
- **Vergucht Pascal**, La répression des délits informatiques dans une perspective internationale, thèse, Montpelier, 1996.
- **Charle Diaz**, La Police Techenique et Scientifique, 2eme Edition, Edition Presse .universitaire de France, France 2006.

الفهرس

الفهرس.

الملخص باللغة العربية

يشهد العالم المعاصر ثورة في مجال تكنولوجيا الإعلام والاتصال، حيث عرف الإنترنت انتشار واسعا ومعه انتشرت الاعتداءات الإلكترونية، نتيجة للاستخدام غير المشروع للتقنيات الحديثة، هو ما استدعى تدخل المشرع لوضع حد لهذا التنامي الخطير في ميدان الإجرام المعلوماتي، عن طريق سن نصوص قانونية موضوعية دولية وحتى داخلية، تنظم و تضبط التفتيش الالكتروني الذي يواجه الجرائم التي تشكل اعتداء أو تهديدا للأمن المعلوماتي، مع استحداث هيئات تعمل على المستوى الميداني من أجل مكافحة الاجرام المعلوماتي

وأمام تزايد الجريمة المعلوماتية، كرس المشرع الجزائري التفتيش الالكتروني بمقتضى عدة انظمة موضوعية وإجرائية للكشف عن الادلة الرقمية و المساهمة في كشف الحقيقة نتيجة الاستخدام الواسع للتقنيات الرقمية بمختلف أنواعها الأمر الذي ألزم فعالية النصوص و الآليات القانونية الواضحة لمكافحة الجريمة المعلوماتية، من أجل ذلك بادر المشرع الجزائري في ظل الجهود الدولية الى ابرام العديد من الاتفاقيات الدولية فيما بين الدول لوضع قواعد قانونية دولية استراتيجيات متكاملة، يستفيد منها المشرع لتطوير تقنيات التفتيش الالكتروني و إصدار وتعديل العديد من القوانين بما يتلاءم مع التطور الملحوظ في هذا المجال.

Abstract in English

The contemporary world is witnessing a revolution in the field of information and communication technology, where the Internet has known as widespread and with it the spread of electronic attacks, as a result of the illegal use of modern technologies, which necessitated the intervention of the legislator to put an end to this dangerous growth in the field of cybercrime, by enacting international and even internal.

In the face of the increase in information crime, the Algerian legislator devoted electronic inspection under several objective and procedural systems to detect digital evidence and contribute to the disclosure of the truth as a result of the wide use of digital technologies of various kinds, which obliged the effectiveness of clear legal texts and mechanisms to combat cybercrime, For this reason, the Algerian legislator, in light of international efforts, initiated the conclusion of many international agreements among countries to develop international legal rules and integrated strategies, benefitting the legislator to develop electronic inspection techniques. Issuing and amending many laws in line with the remarkable development in this field.