جامعة عمار ثليجي بالأغواط-

كليـة الحقوق والعلوم السياسية

قسم الحقوق

تخصص: قانون جنائي

بعنوان:

التفتيش الإلكتروني

مذكرة مقدمة من ضمن متطلبات نيل شهادة الماستر في القانون الجنائي

إعداد الطالبتان:

بن بريكة آسيا

بن سعيد نورالهدى

إشراف الدكتور:

خضرون عطاء الله

لجنة المناقشة

الدكتورة بركـــات بهـــيـــة	.....	**رئيســـــاً**
الدكتور خضرون عطاء الله	.....	**مشرفاً مقرراً**
الدكتورة بونـــاصر إيمان	.....	**عضواً مناقشاً**

السنة الجامعية 2024/2023

بسم الله الرحمن الرحيم

﴿ وفوق كل ذي علم عليم ﴾

الإهداء

إلى من رباني وعلمني إلى ابي الغالي.

إلى حضني الدافئ إلى أمي الحبيبة أدامها الله و بارك الله في عمرها.

إلى كل العائلة بفروعها الممتدة كبيرا وصغيرا.

إلى كل من وسعه قلبي ولم يسعه قلمي .

إلى كل من نكن لهم كل الاحترام والتقدير

نهدي هذا العمل المتواضع

أهدي عملي هذا

آسيا

الإهداء

بسم الله الرحمان الرحيم

{قل إن صلاتي ونسكي ومحياي ومماتي لله رب العالمين }
الأنعام :162

أهدي ثمرة جهدي المتواضة إلى أمي حفظها الله وأطال في عمرها

إلى أبي حفظه الله وأطال في عمره

وإلى إخوتي وأخواتي حفظهم الله ورعاهم

إلى جميع من ربطتني معهم رباط الأخوة في الله

و شكرا

نور الهدى

شكر وعرفان

كن عالما .. فإن لم تستطع فكن متعلما ، فإن لم تستطع فأحب العلماء ،فإن لم تستطع فلا تبغضهم"

بعد رحلة بحث و جهد و اجتهاد تكللت بإنجاز هذا البحث ، نحمد الله عز وجل على نعمه التي من بها علينا الذي أنار دربنا ويسر لنا السب لإنجاز هذا العمل المتواضع فهو العلي القدير. القائل في كتابه العزيز: (لئن شكرتم لأزيدنكم) سورة ابراهيم الآية 07.

كما لا يسعنا إلا أن نخص بأسمى عبارات الشكر و التقدير والامتنان إلى الأستاذ المشرف" الدكتور خضرون عطاء الله" لما قدمه لنا من جهد و نصح و معرفة طيلة إنجاز هذا البحث .

كما نتقدم بالشكر والامتنان إلى جميع أساتذة تخصص قانون جنائي وإلى كل أساتذة وإدارة قسم الحقوق. وإلى الذين كانوا عونا لنا في بحثنا هذا ونورا يضيء الظلمة التي كانت تقف أحيانا في طريقنا.إلى من زرعوا التفاؤل في دربنا وقدموا لنا المساعدات والتسهيلات والمعلومات، ولكل من ساهم من قريب أو بعيد لرفع معنوياتنا وكل من لم يبخل علينا بالنصيحة والتوجيه فلهم منا أسمى عبارات الشكر.

آسيا– نور الهدى

مقدمة

أحدثت التكنولوجيات في مجال تقنيات الحاسوب والاتصال تغييرات جذرية انعكست آثارها جليًّا، حيث أصبحت تكنولوجيا الاتصالات لما تميّزت به من سرعة نقل وتجميع وفرز المعلومات، ومن ثمة معالجتها والاستفادة منها، عالماً منفرداً بذاته اكْتسته أهمية جعلته غير بعيد عن أيادي الإجرام الذي امتاز هو الآخر بخصوصية نظراً للبيئة الرقمية التي تحيط بمقومات هذا النوع من الإجرام، وله من الخطورة ما يصعب عملية اكتشافه وإثباته كونه لا يعرف حدوداً سياسية ولا حواجز دولية. كما تستهدف الجرائم المعلوماتية (Cyber Crimes) الاعتداء على البيانات والمعلومات والبرامج ونُظم التشغيل والأنظمة المعلوماتية، وشبكات الاتصال وقواعد البيانات، مما يتطلب ضرورة توفير وسائل حديثة وإجراءات خاصة للجهات القضائية لمحاربة هذه النوع من الجرائم ومن ثمة ينْصبُّ التفتيش على الكيان المادي للحاسوب (Hardware) وهي الأشياء الملموسة من أجزائه التي تعد تقنية مادية تتكامل وظائفها لآداء مهمة في المعالجة الآلية للبيانات، إذ يمكن ضبطها وحجزها وفقا للقواعد التقليدية للتفتيش.

ولكن تبرز الصعوبة حينما نكون بصدد تفتيش وحجز المكونات المعنوية أو المنطقية للحاسوب (Software) كالبرامج والمنظومات المعلوماتية وقواعد البيانات...الخ. حيث كانت سياسة المشرّع في التعامل مع هذه الجرائم بوضع إستراتيجية شاملة لاستحداث 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 كبيرة لمكافحة الجريمة الالكترونية عن طريق هيكلة أجهزة وهيئات أسندت لها ذات المهمّة، خاصة الهيئة الوطنية المكلفة بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، دون تجاهل الدور الفعّال للجهاز الأمني في هذا المجال، من خلال تسخير جهوده وتجاربه العمليّة لسدّ ثغرات الأنظمة الأمنية وتحسين وتطوير أساليبه وضماناته لمنع

وقوع اعتداءات إجرامية وتطبيق النصوص الإجرائية التي تمكّن الجهات المختصّة من البحث والتحقيق واستنباط دليل يتوافق مع الطبيعة التقنية للجرائم.

ولعل نتيجة ذلك كانت استحداث قواعد إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية، ويعد التفتيش الالكتروني إحدى هذه الإجراءات التي حددها القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومن ثم تحقيق التوازن بين الضرورة الملحّة للاستفادة من التقنيات والتكنولوجيات الحديثة، وبين الحاجة الفردية والاجتماعية إلى الحماية القانونية من انعكاساتها الإجرامية.

تكمن أهداف بحث موضوع التفيش الالكتروني في محاولة التعرف على الأساليب والإجراءات المستحدثة لمواجهة الجرائم المعلوماتية، والتي لم تنل حظها بعد من البحث على المستوى الجزائي حيث نجد القواعد الإجرائية التقليدية التي لا يمكن أن تطبّق عليها، لاسيما أن هذا الموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها.

وتظهر جليّا أهداف التفتيش الالكتروني والتحقيق في مجال الإجرام السيبراني وكيفية إثباته في التشريع الجزائري بإصدر المشرّع الجزائري للقانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال باعتباره قانون إجرائي خاص في ميدان مكافحة هذا النوع من الجرائم وإيجاد طرق إجرائية ذات طبيعة تقنية تتلاءم معها.

كما عزّز هذا الاتجاه بالمصادقة على نصوص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 مع إدراكه الصعوبة التي تطرحها المواجهة الإجرائية لأشكال الإجرام الجديد التي أفرزتها بيئة المعالجة الآلية للمعطيات ،استحدث تقنية التفتيش الالكتروني في القانون رقم 04/09 وخلق هيئات تقنية وخبراء في المجال المعلوماتي.

غرضنا من دراسة الموضوع معرفة ضوابط التحرّي الخاصة التي نص عليها المشرّع في مجال التحقيق والإثبات في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من خلال تعديل قانون الإجراءات الجزائية .

حيث نسعى في هذه الدراسة إلى النظر في غاية النصوص والأحكام القانونية المتعلّقة بتنظيم إجراء التفتيش الالكتروني والوقوف على مدى فعاليتها في ردع الجريمة المعلوماتية والحد من خطورتها المتزايدة من خلال الكشف عن الأدلة والوصول إلى مرتكبيها وما تفرضه من تحديات خاصة في عصرنا الحالي الذي يشهد قفزة رهيبة في مجال تكنولوجيات الإعلام والاتصال وما تفرضه من مسؤوليات تقع على عاتق الجهات المختصة لحماية الأمن ومكافحة الجرائم المعلوماتية.

تتمثل أهمية دراسة موضوع التفتيش الالكتروني في الاطلاع على المستجدات المرتبطة بالجريمة المعلوماتية ودور التفتيش الالكتروني كدليل رقمي يقدم أمام القضاء يحدد إجراءات المتابعة ويكشف الحقيقة ويساعد القضاء على الفصل في النزاع.

الاطلاع على الجرائم المعلوماتية الحديثة، ومدى تأثيرها على القواعد التقليدية في التحري معرفة إجراءات المعاينة والتفتيش الالكتروني والحجز داخل المنظومة المعلوماتية ،ومراقبة الاتصالات الالكترونية 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.

اعتمدنا في دراستنا هذه على المنهج التحليلي، الوصفي، كونها الأنسب لمثل هذه الدراسات من خلال تحليل المواد القانونية التي تتضمن إجراءات المتابعة في الجريمة المعلوماتية من خلال النصوص والأحكام القانونية المنظمة لإجراء التفتيش الالكتروني ومهامه، بالإضافة إلى وصف الإجراءات التي تعتمدها الجهات المختصة لتنفيذ التفتيش الالكتروني.

كانت أسبابنا الشخصية لدراسة موضوع التفتيش الالكتروني نتيجة اهتمامنا بمجال الجريمة المعلوماتية وما ترتبه من آثار وكذا الفضول لمعرفة الإجراءات الخاصة للمتابعة التي تختلف عن إجراءات المتابعة في الجرائم التقليدية.

وانصبّ اهتمامنا حول موضوع الدراسة كونه حديثا، لا يزال يتطلب التعمّق المعرفي فيه، للوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحية الإجرائية.

وأسبابنا الموضوعية تمحورت فيما يطرحه موضوع التفتيش الالكتروني من ضمانات حماية إجرائية لمحل التفتيش من جهة والالتزام بالسر المهني عند الاطلاع، بالإضافة إلى المعوقات القانونية التي لا بد من وضعها بالحسبان نظراً لحداثة الموضوع المتعلق بتجريم الأفعال أو الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات وفقا للقانون 04/09.

يطرح موضوع التفتيش الالكتروني صعوبات عدّة نظرا لمرونة الجريمة المعلوماتية ،الأمر الذي يتطلب من السلطات بجميع مستوياتها تحديات قانونية خاصة خلال عملية البحث من أجل الكشف عنها. و نظراً لحداثة الموضوع واجهتنا عراقيل تتعلق بقلة المراجع في هذا الجانب، فنجد معظمها تتناول الجريمة المعلوماتية وإجراءات التحقيق، وحاولنا من خلالها تحليل الأحكام المتعلقة بالتفتيش الالكتروني وضماناته وأحكامه الإجرائية وأهميته كدليل رقمي يقدم أمام القضاء.

و بناءا على المعطيات السابقة لدراسة موضوع التفتيش الالكتروني تم الاعتماد على إشكالية يمكن صياغتها وفقا لما يلي:

كيف نظم المشرع الجزائري إجراء التفتيش الالكتروني على الجرائم المعلوماتية ؟ وهل كرس نفس الضوابط والآليات القانونية للتفتيش أم تعامل مع خصوصية مسرح الجريمة في الفضاء الرقمي ؟

ومن أجل الإجابة على الإشكالية السابقة تم الوقوف على الأحكام الموضوعية والإجرائية الخاصة بالتفتيش الالكتروني لإقرار الحماية القانونية للفضاء الرقمي وفقاً لخطة تضمنت في (الفصل الأول) الأحكام القانونية لإجراء اللتفتيش الالكتروني في مبحثين تعرضنا في (المبحث الأول) الإطار المفاهيمي لإجراء التفتيش الالكتروني. ومن ثم يلي (المبحث الثاني) موسوماً بالضوابط القانونية للتفتيش الإلكتروني.

أما (الفصل الثاني) فجاء موسوماً بالأحكام الإجرائية للتفتيش الالكتروني في مبحثين يتعلق (المبحث الأول) بالجهات المختصة بالتفتيش الالكتروني، أما (المبحث الثاني) فخصصناه لموضوع آثار للتفتيش الالكتروني وكيفية التعامل معها.

واختتمنا دراستنا هاته بخاتمة تضمنت بعض التوصيات والاقتراحات التي بدت لنا من خلال تطرقنا لموضوع الدراسة والتشريع الخاص به.

الفصل الأول الأحكام القانونية لإجراء لتفتيش الالكتروني

بالنظر إلى ما يحمله التطور التكنولوجي الرقمي من منافع جمّة للحياة البشرية اليوم ،إلا أنّ بين طيّاته الكثير من المخاطر التي تتجلّى في ما يُعرَف اليوم بجرائم المنظومة المعلوماتية وما تتسبّب فيه من انتهاكات لخصوصية وحقوق الأفراد والحريات العامة، الأمر الذي يعتبر إشكالاً أمام السلطات التحقيقية للقيام بعملية التفتيش الالكتروني نظراً لقلة الخبرة في هذا الميدان كونه مستجدّاً يتسارع تطوّره كل يوم، وبما أن التفتيش الالكتروني من مضامين الكشف عن ملابسات الجريمة المعلوماتية ومعالمها فهو يستدعي توافر خبراء وفنيين في مجال الكشف عنها، بتكريس تعاون دولي وضوابط قانونية من أجل مواكبة هاته التطورات الحاصلة في منظومة الجرائم المعلوماتية، وعليه تم التطرق في هذا الفصل إلى مبحثين، هما كالتالي:

المبحث الأول: الإطار المفاهيمي لإجراء التفتيش الالكتروني.

المبحث الثاني: الضوابط القانونية لإجراء التفتيش الالكتروني.

المبحث الأول: الإطار المفاهيمي لإجراء 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].

ولإلقاء نظرة عامة على إجراءات التفتيش الالكتروني يجب التطرق لمفهومه وسائله ومتطلباته القانونية، ولزاماً لذلك جاء تقسيم هذا المبحث كالتالي:

المطلب الأول: مفهوم التفتيش الالكتروني

يتعرض التفتيش على الجريمة المعلوماتية لمشكلات إجرائية تتمثل أساساً في البيئة التقنية التي تُرتكب فيها الجريمة والتي لا تخلِّف آثاراً مادية ملموسة بالإضافة إلى القدرة على محو الدليل والتخلّص منه، لذلك نظم المشرّع الجزائري إجراء التفتيش الذي لا يتلاءم وهاته الظروف.

الفرع الأول: تعريف التفتيش الالكتروني وأنظمته

أولا : تعريف التفتيش الالكتروني

تطرق المشرّع من خلال القانون 04/09[2] المتعلّق بالقواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الاعلام والاتصال ومكافحتها لوضع ضوابط وإجراءات تتلاءم وطبيعة الجريمة المعلوماتية، تاركاً تحديد مفهومه للفقه والقضاء من هنا وجب تسليط الضوء على التفتيش في البيئة الالكترونية وتحديد مفهومه وأصوله ، وبالرجوع إلى التعريفات الفقهية نجدها اختلفت بالنظر إلى أبعاده المختلفة وتعدّد مجالاته من ومن حيث اختلاف الجرائم أو تنوّع مصادرها.

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

[2] – القانون 04/09 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47.

وباختلاف الأحكام التي تحدد التفتيش الالكتروني فقد عرفه بعض الفقهاء بأنه "الاطلاع على محلٍ منحهُ القانون حماية خاصة باعتباره مستودع سرِّ صاحبهِ، يستوي في ذلك أن يكون هذا المحل حيازة الحاسب الآلي أو أنظمة أو شبكة الأنترنت"[1].

يقصد بالتفتيش بوجه عام "البحث عن أشياء تفيد في الكشف عن جريمة وقعت ونسبتِها إلى المتهمين وإعداد إجراءات التحقيق التي تهدف إلى البحث عن الأدلّة المادية لجناية أو جنحة تحقّقَ وقوعها في محلٍ يتمتّع بحرمة المسكن أو الشخص، وذلك بهدف ارتكابها أو نسبتها إلى المتّهم وفقا للإجراءات القانونية المحددة"[2].

إن التفتيش إجراء من إجراءات التحقيق وليس من إجراءات الاستدلال ولأنه يتم بإذن لضابط الشرطة القضائية من جهات التحقيق المختصة وهذا ما أجمع على ذلك الفقه الجنائي كما أنه إجراء مفاجئ لا يحاط المتهم بإجراء تفتيشه أو تفتيش منزله مسبقاً لكي لا يبادر إلى التخلص من الأدلة[3]، التي تتضمنها منظومة المعلومات، فالتفتيش إجراء تحقيقي ،وقد يباشر بهدف الحفاظ على الأدلة.

ثانيا: وسائل تفتيش المعطيات المعلوماتية

يعتمد التفتيش الالكتروني على أنظمة لمجابهة الجرائم المعلوماتية وتكنولوجيا الحاسبات الآلية ووسائل الإتصال وشبكات الربط ليحمل مصطلح تقنيات المعلومات ليعبر عن النظم كوسيلة لارتكاب جرائم آخرى الناشئ في البيئة الرقمية التي أخضعها المشرّع 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 ويرتبط من الناحية الواقعية ببرامج وأنظمة تكشف عن المعطيات أثناء عمليات التفتيش.

[1] – د/ علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، مصر، 2012، ص 39.

[2] – د/أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994، ص 56.

[3] – د/هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في الاثبات الجنائي، ط1، دار النهضة العربية، القاهرة، ص 46.

1- 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[1].

حيث يعتبر 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 إلى صلة الوصل بينهم بالاعتماد على الإيميل ،الشبكات الاجتماعية، الموقع الالكتروني وحتى رقم الهاتف والكثير من الأمور الأخرى[2].

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 الأنترنت.

2- برنامج فورنسيك " Forensic " المستخدم أثناء المعاينة والتفتيش.

هذا البرنامج مفهومه الشامل هو الجرائم، لكن هذه الجرائم يتم تقسيمها حسب أصناف معينة، منها الخاصة بالقتل ومنها الخاصة بالسرقة والجنايات وما إلى ذلك، لكن خصص قسم خاص بالجرائم الالكترونية، وهو ما يطلق عليه ب Digital Forensic، وهو المتعلق

[1] – نعيم سعيدان، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة باتنة، السنة الجامعية 2012، ص 140.

[2] – أ/نضال أدمين، منتدى برامج الكمبيوتر والأنترنيت، منشور على الرابط – http://nidhal-technologie.own0.com/t60-topic تم الاطلاع عليه بتاريخ 2024/04/12

بموضوعنا اليوم، بحيث يقوم على تعقب وحجز الأعمال والمهمات غير المشروعة وغير القانونية والتي يتم ممارستها باستخدام الشبكة العنكبوتية أو الأجهزة الالكترونية، حيث يقوم مجموعة من المحترفين في مجال المعلوماتية بالسهر على عمل النظام، هؤلاء الأشخاص لديهم خبرات كافية وعالية من أجل المساهمة في كشف وإبطال الأعمال غير القانونية السائرة ضمن الشبكات العنكبوتية، كما يقوم برنامج بتصوير القرص بواسطة حزم برمجيات ونظراً إلى أن هذه الحزم مصمّمة للمحققين الجنائيين، فإنها تتضمن أدوات لتجميع ملف كامل من بيانات مجزأة، كما أنه يقوم بأعمال التحري والفحص للأدلة الرقمية وأخذ نسخ منها وتجميعها وتحليلها وفك التشفير واستعادة الملفات المحذوفة وكلمات المرور وتحليل البريد الالكتروني والبحث المتقدم، وتوليد تقارير لاستخدامها أمام الجهات الجنائية المختصة[1].

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

3- تقنية تتبع عنوان: (TCP –IP)

عنوان IP هو العنصر المسؤول عن تراسل الحزم البيانية عبر شبكة الأنترنت وتوجيهها إلى أهدافها، ويعتبر بمثابة عنوان الحاسوب المتصل بالشبكة ويتكون من شفرة رقمية تتكون من أربع (04) أجزاء، يشير الأول إلى المنطقة الجغرافية والثان 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 الالكترونية التي يقصد بها كل تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعته عن

[1] – أ/ إيناس محمد راضي، الأجهزة التحليلية الحديثة في كلية علوم الأدلة الجنائية، منشور على الرابط : http://www.uobabylon.edu.iq/uobColeges/service_showrest.aspx?fid ، تم الاطلاع عليه بتاريخ 2023/04/16 على الساعة 20:00سا.

[2] – المرجع نفسه.

طريق أي وسيلة إلكترونية، وتعمل الهيئة الوطنية للوقاية من جرائم الاتصال على مساعدة السلطات القضائية وفقا لنص المادة 05 فقرة 01 من المرسوم الرئاسي 261/15[1]، فتعمل مصالح الشرطة القضائية في مجال التحريات الالكترونية، ضمن فريق تحقيق يقومون بتتبع عنوان IP للجهاز مصدر الجريمة وتحديد موقعه[2].

4- 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 للمعلومات web من أجل تزويد المستخدم بها، ومن مزاياه أن ذاكرته هذه يمكن أن تحتفظ بتلك المعلومات والعمليات، وهو ما يمنح لضباط الشرطة القضائية فحصها واستخلاص الدلائل ضد المتهم بمساعدة مزود الخدمات[3].

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

يمكن لبرامج التتبع أن تقوم بالتعرف على محاولات الاختراق ومن قام بها، وإشعار 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 الالكتروني (IP) واسم الشركة

[1] – 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، الصادرة في 08 أكتوبر سنة 2015.

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

[3] – أ/خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة ط1، دار الثقافة للنشر والتوزيع ، عمان – الأردن، 2011 ، ص 206.

المزودة بخدمة الأنترنت ومعلومات أخرى، يتكون من شاشة رئيسية تقدم للمستخدم بيانا بعمليات الاختراق، فيستعين بها ضباط الشرطة القضائية للوصول إلى الجناة.[1]

6- الاستعانة بنظام كشف الاختراق (Detection Intrusion System)

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، ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة، ومراقبة بعض ملفات التشغيل فيستعين بها ضباط الشرطة القضائية بتسجيل الاحداث فور وقوعها في الحاسوب أو الشبكة[2].

7- العمل بنظام التمويه:

هو نظام حاسوبي مخصص لكي يتعرض للهجمات الالكترونية 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 والتحقيق إتخاذ الإجراءات الوقائية التي تزود فريق التحقيق بالمعطيات اللازمة، والعديد من البيانات التي توضح معالم الجريمة[3].

الفرع الثاني: التكييف القانوني للتفتيش الالكتروني

تتعدد آراء الفقهاء حول طبيعة التفتيش حيث تظهر أربعة اتجاهات مختلفة لتكييف الطبيعة القانونية للتفتيش الالكتروني:

الاتجاه الأول: يأخذ اصحابه في تحديد الطبيعة القانونية للتفتيش الهدف منه، لغاية إجراء الحصول على الأدلة وضبطها وكشف حقيقتها وإزالة الغموض، وترجيح نسبتها إلى شخص

[1] – رابح مباركية ، مذكرة مكملة لنيل شهادة الماستر حقوق تخصص قانون الإعلام الآلي والإنترنت بكلية الحقوق والعلوم السياسية جامعة محمد البشير الإبراهيمي برج بوعريريج ، ص 36.

[2] – أ/ خالد عياد الحلبي، المرجع السابق، ص 209.

[3] – د/عبد الله بن سعود محمد السراني ، المرجع السابق، ص 51.

محدد مثل ضبط برامج غير مشروعة على جهاز حاسوب المتهم، وتقديمها ضده كأدلة اثبات أمام القضاء[1].

الاتجاه الثاني: يستند أصحاب 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 عملاً من أعمال التحقيق إذا جرى بعد فتح التحقيق الابتدائي.

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 المشرّع لا يعتدّ بصفة القائم ب الإجراء خاصة في حالتي الندب والتلبّس حيث يقوم به عناصر الضبطية القضائية، ورغم ذلك يبقى من أعمال التحقيق[2].

الاتجاه الرابع: يأخذ هذا الاتجاه بالمعيار المختلط، فيسعى أصحاب هذا الرأي إلى 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[3].

بالرغم من الإجماع 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 آثاراً إجرائية، لذا فهو إجراء تقوم به السلطة القضائية بقصد الكشف الحقيقة.

وقد ارتأى القضاء الجزائري العمل 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

[1] – أ/فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الأردني والمقارن، ج2، دار الفارابي، عمان، 1980، ص 398.

[2] – د/ أحمد المهدي، القبض والتفتيش والتلبس، ط1، دار العدالة، القاهرة، مصر، 2007، ص 95.

[3] – أ/ يوسف دلاندة، قانون الإجراءات الجزائية، دار هومه، الجزائر، 2001، ص 46.

من قانون الإجراءات الجزائية، أن إبطال التفتيش وما تلاه من إجراءات خطأ ينجز عنه نقض القرار".[1]

الفرع الثالث: خصائص التفتيش الالكتروني

بالرجوع لخصوصية التفتيش الواقع على المنظومة المعلوماتية، وتعقيده يستلزم الأمر توضيح خصائصه ومميزاته التي تعطيه نسقاً وظيفيّاً خاصاً للتفتيش.

أولا- من حيث نطاق التفتيش الالكتروني:

إن الظروف التي ترتكب فيها الجريمة المعلوماتية وحيزها اللامحدود أضحى التفتيش ينطوي على قدر من الجبر والإكراه للاطلاع على البيانات والمعلومات الالكترونية وكل 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 وغيرها.

و ما دام الإكراه عنصر أساسي في التفتيش لما يحمله من إكراه، إلا أنه مشروع من الناحية القانونية للكشف عن الجرائم، فهو تعرّضُ قانونٍ لحريةِ المتّهم الشخصية ويشكل قيداً على حرمة أسراره الشخصية الموجودة على جهاز حاسوبه الخاص أو على برامج خاصة به أو على بريده الالكتروني عبر شبكة الأنترنت[2].

ثانيا- من حيث السلطات التي تباشر التفتيش الالكتروني:

تباشر الشرطة العلمية المتخصصة في حدود اختصاصها وجهات التحقيق القضائي مباشرة إجراءات التفتيش، أو ما كلّفها به القانون، مع تكريس الضمانات القانونية سواء رضي به من بُوشِر حياله، أم لا، فالسلطات المختصة تتخذ ما تضمن به تنفيذه عند عدم الاستجابة، إذ أن تفتيش الشخص يستلزم تقييد حركته المدّة اللازمة لإجراء التفتيش مما قد

[1] – قرار المحكمة العليا، رقم: 165609، الصادر بتاريخ 1997/07/30، المجلة القضائية، العدد 2، لسنة 1997، ص 250.

[2] – د/ علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنت/ دراسة مقارنة، عالم الكتب الحديث، ط1، 2004، ص 13.

يستتبع الإلزامية في الحدود القانونية، من جانب الشخص المطلوب تفتيشه وللبحث عن الأدلة المادية للجريمة[1].

ثالثا- من حيث وسائل التفتيش الالكتروني:

يمتاز التفتيش الالكتروني بأنه وسيلة للبحث عن الأدلة المادية والمعنوية للجريمة وضبطها 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[2]. ومنه 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 "الأنترنت" والمواقع الالكترونية باعتبارها مكان إتاحة أو معالجة البيانات أو المعلومات إلا لكترونية على الشبكة المعلوماتية من أجل الكشف عن الأدلة المادية والمعنوية للجريمة وضبطها[3].

و من خلال القانون رقم 04/09 حاول المشرّع تحديد الأبعاد التي ينصب عليها التفتيش الالكتروني من خلال إعطاء بعض المفاهيم الاصطلاحية وفقا لنص المادة 02 منه " يقصد في مفهوم هذا القانون ما يلي:

الجرائم 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 الالكترونية[4]...

[1] – د/أحسن بوسقيعة، التحقيق القضائي، ط2، دار هومه، الجزائر، 2012، ص 83.

[2] – د/طارق ابراهيم الدسوقي عطية، الموسوعة الامنية الامن المعلوماتي،النظام القانونية لحماية المعلوماتية، دار الجامعة الجديدة للنشر ،الاسكندرية، 2015، ص 240.

[3] – د/آمال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ب ت ط، ص 62.

[4] – د/ سامي الحسيني، النظرية العامة للتفتيش في القانون المصري و المقارن ،دار النهضة العربية، القاهرة، 1980، ص. 85

المطلب الثاني: الوظائف القانونية للتفتيش الالكتروني

يستهدف التفتيش البحث والاستقصاء في محلّ له حرمة من أجل البحث عن الحقيقة وكشف أدلة الجريمة وبيان فاعلها سواء بالبحث عن أوراق أو أشياء تفيد التحقيق وحدها أو بالاشتراك مع غيرها في وقوع الجريمة، وفي نسبتها إلى من نسبت إليه، ولا ينصرف التفتيش إلى الأشياء المعلنة التي يمكن للكافة الاطلاع عليها فهو يمس مستودع السر سواء وقع على الشخص المتهم أو مسكنه. وذلك بهدف ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة باعتباره إجراء من إجراءات التحقيق.

إذا كان إجراء التفتيش لا يستهدف الغاية المرجوة منه فلا يعد تفتيشاً بالمعنى المقصود في القانون ولا يؤدي الوظيفة التي حددها المشرّع في حسن سيرورة إجراءات المتابعة، والتفتيش بهذا المعنى تختلف صوره وتتعدد الوظائف التي يحققها.

الفرع الأول: الوظيفة الوقائية للتفتيش الالكتروني

أقرّ المشرّع 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 القانون "04/09" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحرّيات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، بوضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"، كما نصت المادة 04 الفقرة 02 من نفس القانون على أنه " في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو الدفاع الو طني أو مؤسسات الدولة أو الاقتصاد الوطني...".[1]

[1] – المادة 04 من القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

1- منع المجرم المعلوماتي من تدمير أو إخفاء الدليل:

أدرج المشرّع إجراء التفتيش في مجال الجرائم المعلوماتية في قانون الإجراءات الجزائية، فأجاز الدخول بغرض التفتيش ولو عن بعد إلى المنطومة المعلوماتية دون إذن صاحبها، وهذا برغم اعتبار برامج الحاسوب من بين المصنّفات الأدبية المحميّة بموجب مجموعة من النصوص الخاصة.[1]

ونظرا لما تتطلبه العملية من جانب تقني معقد أجاز المشرّع نسخ وإفراغ المعطيات على دعامة تخزين إلكترونية 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.

2- حجز المعطيات المعلوماتية:

في بعض الأحيان يستحيل نسخ المعطيات لأسباب تقنية كما لو كانت المعطيات مخزنة بأنظمة التشغيل التي يمكن نسخها، فيتعين على السلطة المكلفة استخدام التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية الموضوعة تحت تصرف الأشخاص المرخّص لها باستخدام المنظومة المعلوماتية وفقا للمادة 07 من القانون رقم 04/09 والهدف من الإجراء الاحترازي هو الحفاظ على الأدلة في محيطها الالكتروني.[2]

3- منع الوصول إلى المعطيات المعلوماتية:

يتم الحجز وفقا لآليات ومتطلبات تحكمها قواعد وجوانب تقنية للمعلوماتية تتماشى مع البيئة الرقمية التي ترتكب بها الجرائم، والمشرّع الجزائري أكّد إمكانية نسخ البيانات المعالجة آليات وضبطها، كما أجاز حجز المعطيات المخزّنة داخل نظم المعلوماتية إذا كانت تفيد في

[1] – د/ عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري، ط1، دار الخلدونية، الجزائر، 2007، ص 35.

[2] – القانون 04/09 المؤرخ في 05 أوت 2009، المرجع السابق، أنظر د/ رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، عدد 05، 2012، ص 175.

كشف الجرائم أو مرتكبيها، أما طريقة حجز المعطيات فتتم عن طريق نسخ المعطيات محل البحث على دعامات تخزين إلكترونية قابلة للحجز، وفقا للمادة 06 من القانون رقم 04/09 وتمتد عمليات النسخ إلى المعطيات اللازمة لفهم المعطيات محل التفتيش.

تقتضي عمليات التفتيش الالكتروني أسس وظيفية يرسّم لها المشرّع الجزائري من أجل تفعيل إجراءات المتابعة ودعم التعاون مع جهاز العدالة بالنظر إلى الطبيعة الخاصة للجرائم المعلوماتية وصعوبة ضبط نطاقها من اتساع مجالاتها، باعتبار أن وسيلة الاعتداء برامج الحواسيب والشبكات الالكترونية.

ضبط المشرّع الجزائري نجاح إجراءات التفتيش الالكتروني بوظائف تدعيمية للنظام القضائي من خلال الرقابة الوقائية لبيئة الأنترنت بحيث يتمتع بصفة الضبطية الإدارية مزودي الدخول وخدمات الأنترنت بحيث منحهم المشرّع صلاحية الرقابة على سير حركة المنظومة المعلوماتية وإخضاعها للقانون والنظام من قبل المتعاملين مع الأنترنت، وتتم إجراءات التحفظ على الأدلة إلى غاية حضور رجال الضبطية القضائية.[1]

و أكد المشرّع 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، طبقاً للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، لا سيما قانون الإجراءات الجزائية ،تفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمها أنه يحوز و/أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية.[2]

يفرض القانون أحياناً إجراء تفتيش إداري لمنع وقوع الجريمة، وهذا ما تمليه القوانين ،كنصّ المادة 05 من القانون 04/09 الفقرة 04 "يمكن السلطات المكلفة بالتفتيش تسخير

[1] – د/ هروال نبيلة هبة، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، 2007، ص 87.

[2] – المرسوم الرئاسي رقم 261/15 المؤرخ في 8 أكتوبر سنة 2015، المرجع السابق.

كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدبير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها"، ومن ثمة تسهر الجهات المخصة على آداء التفتيش الالكتروني لوظائفه من خلال المعرفة التقنية للقائمين بأعمال التحري والمباشرين للتحقيق في مجال الجرائم المعلوماتية من خلال التدريب على كيفية تشغيل الحواسيب والتدريب الجيد على نظمها الشبكية لاكتساب مهارات ومعارف تتعلق بالبرمجة والمعالجة المعالجة الالكترونية للبيانات[1].

الفرع الثاني: وظائف التفتيش لمستلزمات التحري والتحقيق

إن النظم والملفات تعد الوعاء الحقيقي لأدلة الإدانة أو البراءة في الجرائم المعلوماتية ،وبالنظر لما تحتوية من تعقيدات معلوماتية يستدعي الأمر 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 لقانون 04/09 "مع مراعاة الأحكام القانونية التي تضمن سرّية المراسلات والاتصالات، يمكن لمقتضيات النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش داخل منظومة معلوماتية".

المطلب الثالث: صور التفتيش الالكتروني في المنظومة المعلوماتية.

بظهور الاعتداءات المعلوماتية وانتشارها الواسع أصبحت تشكل جرائم واسعة النطاق لذا أقر المشرّع الجزائري حماية جنائية لكل المعطيات الداخلية أو الخارجية، مع منح السلطات المختصّة حق الاطلاع والولوج لإجراء عمليات التفتيش الالكتروني التي تختلف صوره وحالاته حسب القواعد المحددة.

[1] – أ/ علي عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث العراق، 2011، ص 22.

أولا: التفتيش الالكتروني للمكونات المادية للحاسوب (Hardware Computer)

يتكون الحاسوب من مجموعة الوحدات لكل منها وظيفة محددة تتصل هذه الأخيرة ببعضها بشكل يجعلهاتعمل كنظام متكامل، ومجموع الوحدات تشكل ما يسمى بنظام الحاسوب[1]، وينصب إجراء التفتيش على الكيان المادي للحاسوب وإظهار نتائج التشغيل كالشاشة والطابعة والسماعات والراسم والأقراص المرنة والصلبة ووحدة الذاكرة التي تعتبر من أشهر تخزين البيانات والمحافظة عليها.[2]

من خلال ماسبق يتبين بوضوح أن التفتيش إذا تعلق بالمكوّنات المادية للحاسوب لا مشكل في ذلك ويتم وفقا لأحكام المادة 44 من قانون الإجراءات الجزائية، وعليه يجب الانتقال إلى مكان تواجد الحاسوب أو أحد مكوناته المادية بضبط جهاز الحاسوب ومكوناته أو ملحقاته وحجزها وتقديمها كدليل لإدانة المتهم يخضع للإجراءات التقليدية للتفتيش كتحديد طبيعة المكان الموجودة فيه تلك المكونات سواء كان عامّاً أو خاصّاً إضافة إلى حضور المعني أو من ينوب عنه.

ثانيا: التفتيش الالكتروني للمكونات المنطقية للحاسوب (Computer Software)

يقصد بالكيان المنطقي مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق الالكترونية المتعلقة بتشغيل وحدة معالجة البيانات إذ يشتمل الجانب الافتراضي على البرامج، الكيانات التطبيقية مثل برامج معالجة النصوص، جداول البيانات الالكترونية.

ويطلق أيضا على المكونات المعنوية للحاسوب بالبرمجيات، فهي بمثابة عصب عمل الكمبيوتر إذ توفر إمكانات وسرعة فائقة في إنجاز المهام المطلوبة، كما يعرف الكيان المنطقي للحاسوب لغة بأنه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسوب كنظم التشغيل وبرامج التطبيقات.

[1] – د/ علي حسن محمد الطوالبة، المرجع السابق، ص 19.

[2] – د/ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة للنشر، الاسكندرية، 2009، 88.

تنقسم 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 كالأنترنت، بالنظر إلى ترابطها على مستويات متعددة وطنية وعالمية، نظرا للطبيعة المعنوية الخاصة لهذه المعطيات المخزنة إلكترونيا، إضافة إلى أنها تتم في بيئة افتراضية يتطلب الكشف عنها استخدام رجال القضاء قدرات فنية وتقنية ذات جودة وتكنولوجيات فائقة ووسائل 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- التفتيش عن بعد:

إن البيانات التي تحتوي على أدلة الإثبات قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، وإن كان من الممكن الوصول إليها من خلال حاسبات موجودة في الأبنية أو المواقع الجاري تفتيشها[2].

و قد يكون الموقع الفعلي للبيانات يدخل في اختصاص قضائي آخر أو حتى في بلد آخر وإن كانت السلطات المختصة في دولة ما تسعى في كشف الحقيقة بشأن الجريمة المرتكبة ضد أحد أجهزتها فإن الأمر قد يكون خلاف ذلك بالنسبة لدولة أخرى ذلك، وهذا ما يزيد من تعقيد الجريمة المعلوماتية العابرة للحدود وهو ما يستلزم وجود تعاون دولي[3] ،ونستطيع أن نميّز في هذه الصورة بين ثلاث احتمالات:

1- اتصال نظام المتهم بنظام آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة:

يثور الإشكال حول مدى إمكانية امتداد الحق في التفتيش إلى أجهزة أخرى غير جهاز المتهم إذ أن التشريعات الغربية قد تناولت في قوانينها الإجرائية حل هذه المشكلة كما

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

[2] – د/ خالد ممدوح ابراهيم، امن المعلومات الالكترونية، الدار الجامعية، الاسكندرية، 2008. ، ص 202.

[3] – أ/ علي عدنان الفيل، المرجع السابق، ص 44.

هو الحال في التشريع الألماني من خلال القسم 103 من قانون الإجراءات الجزائية الألماني، والتشريع البلجيكي من خلال المادة 88 من قانون تحقيق الجنايات[1]، وكذا المشرّع الجزائري في المادة 05 الفقرة الأولى من القانون رقم 09/04 " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية.

2- 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 والتحقيقات، 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[2].

وهذا ما يؤكده المشرّع الجزائري في المادة 05 الفقرة الثالثة "إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول اليها 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".

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

[1] – د/ خالد ممدوح ابراهيم، المرجع السابق، ص 203.

[2] – أ/ علي عدنان الفيل، المرجع السابق، ص 46.

طرف دون تصريح من الطرف الآخر أن يصل إلى البيانات المعلوماتية المخزنة والمتاحة 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 وإدارية من شخص لديه السلطة القانونية للكشف عن هذه البيانات إلى هذا الطرف من خلال هذا النظام المعلوماتي"[1].

[1] – د/ هلالي عبد الإله أحمد، المرجع السابق، ص 378.

المبحث الثاني: الضوابط القانونية لإجراء التفتيش 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 الالكترونية يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الشرطة والمحققين والقضاة، 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 الالكترونية.[1]

المطلب الأول: الأسباب القانونية لإجراء التفتيش الالكتروني

يتجلى مفهوم التفتيش الالكتروني في كونه عبارة عن بناء إجرائي يتضمن فعالية تنفيذية لمجموعة من الوظائف المرتبطة بالبحث عن أدلة لجريمة ارتكبت يعاقب عليها القانون سواءا أخذت وصف جناية أو جنحة تحقّق وقوعها في محل من أجل تحصيل الأدلة ونسبتها إلى مرتكبيها وفقا لما هو مقرر قانوناً. في مسرح الجريمة يتميز ببيئته الافتراضية ،ومن أجل ضمان صحة التفتيش الالكتروني يجب من الناحية الواقعية وجود روابط موضوعية يستند عليها لضمان التقيد بالإجراءات التفتيشية.

الفرع الأول: وجود جريمة الالكترونية

إن المنطق القانوني والعقلي 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 والاعتداء على المكونات غير مادية للنظام المعلوماتي في وفرتها وإتاحتها أو في سلامتها وتكاملها.

[1] – Roger Merle et Andre Vitu, traite de droit criminel, Tome2, 4eme édition, édition Cujas, Paris, 1989, p 57.

يسعى ضباط الشرطة القضائية والمحققون إلى إثبات قيام أركان وعناصر الجريمة المعلوماتية حسب ما يحدده القانون، وإلى ايجاد العلاقة بين تلك الأركان والشخص المتهم بتنفيذها باعتبارها نشاط إجرامي تستخدم فيه تقنيات حديثة، لذلك صعب وضع تعريف عام وشامل لها، فعرفت بأنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية".[1]

اعتبر المشرّع 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]، أما قانون العقوبات الجزائري المعدل والمتمم لم يعرّف جرائم الأنترنت، بل اكتفى بالعقاب على بعض الأفعال، تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات".

تتمثل أركان الجريمة الالكترونية مثل الجريمة العادية في الركن الشرعي والمادي والمعنوي:

أولا- الركن الشرعي لقيام الجريمة المعلوماتية:

حدد قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص جرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات.

حيث يرى أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكاب الجريمة، وبالتالي تعرف على أنها " فعل إجرامي لا يعرف الحدود الجغرافية، والتي يتم ارتكابها بأدة هي الحاسب الآلي عن طريق شبكة الأنترنت وبواسطة شخص له دراية فائقة بها"[3] فيستخدم

[1] – أ/ محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، ط1، دار الثقافة، عمان- الأردن، 2004، ص 10.

[2] – أ/ حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، منشورة بمجلة الحقوق لكلية الحقوق جامعة بسكرة، العدد 33، 2016، ص 45.

[3] – أ/ رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص 40.

الكمبيوتر في ارتكابه كأداة. إذا فهي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا نصت على مبدأ الشرعية المادة 01 من قانون العقوبات الجزائري، ومن الانتقادات الملاحظة أن المشرّع لا يستطيع أن يحصر مسبقاً 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 المشرّع قد أغفل النص على تجريم كل الأفعال الماسة بشبكة الأنترنت والكمبيوتر.

و لتفادي الإشكالات القانونية دعم المشرّع 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 المشرّع الجزائري الأمر بإصداره للقانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وخصّ التفتيش والحجز بإجراءات مستحدثة تكمّل تلك المنصوص عليها في قانون الإجراءات الجزائية الجزائري كما نص على الأحكام العامة التي تبين الأهداف المتوخّاة 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 المحميّة، 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 المشرّع 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.

- تطرّق فيه إلى التزامات المتعاملين في مجال المعلوماتية بتحديد هذه الالتزامات لاسيما إلزامية حفظ المعطيات المتعلقة بحركة سير، والتي من شأنها المساعدة في الكشف عن الجرائم المعلوماتية.

ثانيا- الركن المادي لقيام الجريمة المعلوماتية:

يتكون الركن المادي للجريمة الالكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها، إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل ويتخذ الركن المادي في هذه الجريمة عدّة صور بحسب كل فعل إيجابي مرتكب، مثال جريمة الغش المعلوماتي، الركن المادي فيها هو تغيير الحقيقة في التسجيلات الالكترونية أو المحرّرات الالكترونية[1]، جرائم المساس بنظم المعلوماتية أو المعطيات المعلوماتية، جرائم الاعتداء على حرمة الحياة الخاصة والمعطيات الشخصية ،جرائم الاحتيال باستخدام بطاقة الائتمان، جرائم المساس بالملكية الفكرية، وتتمثل الأمثلة التي سيتم إعطاؤها في نماذج عن الجرائم محل المتابعة والتفتيش الالكتروني، ويكون محلها المنظومة أو النظام المعلوماتية[2].

1- الجرائم الواقعة عل الاشخاص:

- جرائم التهدي د عبر مواقع الأنترنت.
- جرائم انتحال الشخصية عبر المواقع الالكترونية.

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

[2] – د/علي ابراهيم توفيق، دور المحقق في الجرائم الإلكترونية، ط3، دار المدى للنشر والتوزيع، العراق، 2000، ص 141.

- جرائم التشهير وتشويه السمعة عبر المواقع الالكترونية.

2- الجرائم الواقعة على الأموال:

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

3- الجرائم الواقعة على أمن ومؤسسات الدولة:

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

ثالثا- الركن المعنوي لقيام الجريمة المعلوماتية:

لما كانت جرائم المعلوماتية من الجرائم التقنية العالية والتي تتطلب المعرفة والخبرة من قبل الجهات التي تمارس عمليات التفتيش، ومن ثمة فهي جرائم عمدية، بمعنى وجود نية التخطيط والتدبير لارتكاب الجريمة المعلوماتية، فالأصل إن الفاعل المعلوماتي في الجريمة الالكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به، ولكن هذا لا يمنع أن بعض الجرائم الالكترونية تتوافر فيها القصد الجنائي الخاص مثال جرائم تشويه السمعة عبر الأنترنت، وجرائم نشر الفيروسات عبر الشبكات وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.[1]

وعليه حتى يتمكن الفاعل أو الشريك المعلوماتي من تنفيذ جريمتهم الالكترونية يستلزم ذلك توفر أدوات عدة وأبرزها الاتصال بشبكة الأنترنت، توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب، وسائل التجسس، ومنها ربط

[1] – د/ عبد الفتاح بيومي حجازي، الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2009، ، ص 101.

الكاميرات بخطوط الاتصال الهاتفي، البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز، طابعات ،هواتف رقمية ونقالة.[1]

كما رأينا سابقا أن الجريمة المعلوماتية هي كل فعل غير مشروع مرتبط باستخدام حواسيب إلكترونية لتحقيق أغراض غير مشروعة، ويعتبر التفتيش من الإجراءات الهامة في الدعوى الجزائية باعتباره إجراء من إجراءات التحقيق الابتدائي، الذي يساعد كدليل مادي مهم في الكشف الجرائم، ولا يتم ذلك إلا وفقاً لمراعاة القيود التي حددها المشرّع مع احترام خصوصيات محل التفتيش والتقيّد بالإجراءات المرتبطة بالإذن القضائي.

الفرع الثاني: قيام الاتهام بارتكاب الجريمة المعلوماتية أو المشاركة فيها.

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

ومن ثمة فالجرائم المعلوماتية يرتكبها الشخص بصفته فاعلا أو شريكا، ويكون محلها أجهزة حواسيب باعتبارها نظام معالجة كهربائي سريع ودقيق يستخدم في تداول البيانات ومصمّم لتقبل وتخزين البيانات ومعالجتها وإعطاء المعلومات وفقا لبرنامج التخزين الذي يتكون من مجموعة أوامر[3]، أو يتم ارتكابها في شبكة الحواسيب التي تعرّف على أنها "مجموعة مكونة من اثنين أو اكثر من أجهزة الحاسوب والمتصلة ببعضها اتصالا سلكيا أو لا سلكيا".[4]

[1] – د/ هدى حامد قشقوش، هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، ط1، دار النهضة العربية، القاهرة، مصر، طبعة 1992، ص 20.

[2] – أ/ علي عدنان الفيل، المرجع السابق، ص 50.

[3] – د/ هدى حامد قشقوش، المرجع السابق، ص 18.

[4] – د/ علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت (دراسة مقارنة)، عالم الكتاب الحديث، أربد – الاردن، 2004، ص 34.

الفرع الثالث : توافر أدلة وقرائن تفيد في كشف الحقيقة.

لا يوجد تفتيش إلكتروني إلا إذا توافرت لدى المحقق أسباب كافية على وجود جريمة معلوماتية أو لدى الشخص المراد تفتيشه أدوات استخدمت في الجريمة، الأمر الذي يتطلب إصدار سلطة التحقيق قرارها بالتفتيش ومباشرته بوقوع جريمة معلوماتية، ويتم بالانتقال إلى مسكن المتهم أو الأماكن التي تتواجد فيها الأجهزة المقصودة حال حيازة الحاسوب الآلي أو أحد مكوناته المادية كوسائط التخزين (الاقراص الصلبة أو المرنة، الأشرطة الممغنطة ...)، أيضا أجاز المشرّع تفتيش المنظومة المعلوماتية عن بعد، والولوج للكيان المنطقي للمنظومة المعلوماتية لأن هدف التفتيش ينصبّ على مسائل معنوية وفنية ليست مادية كالبرامج وقواعد البيانات باعتبارها وسيلة ارتكاب الجريمة أو تخزين معلومات بشأنها[1].

و عليه فإن الدلائل الكافية شرط ضروري لاتخاذ إجراء التفتيش الذي يتضمن مساسا بحرمة الشخص أو مسكنه وهي 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، وحتى لا يغيّر الجاني الدليل تدخل المشرّع الجزائري ونص على جواز التفتيش في كل الملفات الموجودة في النظام المعلوماتي[2].

الفرع الرابع: وجود إذن بالتفتيش الالكتروني

الإذن بالتفتيش الالكتروني يعد سبباً لمباشرة إجراءات المتابعة والاطلاع على محل الجريمة يفيد في كشف الحقيقة وفقا للضوابط التي نص عليها المشرّع عند التفتيش عن الأدلة الالكترونية في المنظومات المعلوماتية، ويمنح من الجهات القضائية إلى أجهزة ضبط الجرائم والمتمثلة في ضباط الشرطة القضائية والتي تتولى مهمة مباشرة جمع الاستدلالات والتحري في العالم الافتراضي[3].

[1] – أ/ زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص ص 132 – 135.

[2] – أ/ نبيلة هبة هروال، المرجع السابق، ص 246.

[3] – نبيلة هبة هروال، المرجع السابق، ص 90.

و لا يتم تفتيش محل الجريمة إلا بمقتضى إذن تمنحه السلطات القضائية المختصة لتفتيش الأماكن والحواسيب والاطلاع على السجلات المستخدمة في عملية الولوج إلى النظام الآلي لمعالجة البيانات مؤخوذ من بيئة رقمية تعد مجالاً حيويا ضخماً يمكّنها من تخزين مليارات المعلومات والملفات، 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.

والجدير بالذكر أنه لا محل لإصدار الإذن بالتفتيش إلا إذا كان المشرّع قد نص على الجرائم التي تشكل اعتداء على المعلومات في شكل نصوص التجريم والعقاب تطبيقا لمبدأ الشرعية، وهذا ما دأبت عليه الكثير من التشريعات ومنها التشريع الجزائري الذي حدد بموجب القانون 04/21 المؤرخ في 28 ديسمبر 2021 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات[1]، الذي حدد بعض الجرائم المعلوماتية، وعزز المشرّع هذه الحماية بموجب القانون رقم 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ويلاحظ أنه لإجراءات إذن تنفيذ التفتيش الواقع على نظم الحاسوب والأنترنت خصوصية تميزه عن الإجراءات التقليدية تنبع من دقة التعامل مع الأجهزة والبرامج التي يتضمنها، لذا يجب على الجهات المعنية بإذن التفتيش اتخاذ إجراءات وتحرّيات دقيقة وفقا لما يلي:

- تحديد نوع النظام المراد تفتيشه.
- الاعداد الجيد لعملية التفتيش من خلال التقييم العام للوضع الشامل حتى لا يتم إفلات الدليل من التفتيش.
- يجب على الجهات القائمة بالتفتيش أخذ الاحتياطات اللازمة لقدرة المتهم على الدخول عن بعد إلى النظام عن بعد من خلال جهاز الاتصال الوسيط.

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

- التحكم في عملية الدخول إلى الأجهزة والولوج إلى الأنظمة المعلوماتية والحرص على عدم إتلاف الدليل والحفاظ عليه، مع الاستعانة بعمليات التصوير لتوثيق عمليات التفتيش الالكتروني[1].

و يتبين من خلال موضوع الدراسة أن المشرّع في جلّ القوانين التي نص فيها على إذن التفتيش حاول حماية خصوصية الأفراد بما فيها البيانات والمعلومات الشخصية وكذلك السجلات والدفاتر 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 ومجال حركتها غير محدد بمجموعة من الأشخاص، وتكون قابلة للتداول، فلا يمكن عندئذ الحديث عن الاعتداء عليها بالاطلاع عليها دون وجه حق[2].

المطلب الثاني: الضمانات القانونية لإجراء التفتيش الالكتروني

إن محل التفتيش يشمل كافة إجراءات التفتيش المنظومة المعلوماتية لكل ملف من الملفات المخزنة حتى وإن كان الإجراء يُحدِث مساساً بالحريات الشخصية لذا أحاطته التشريعات بضمانات، والهدف من ذلك تحقيق الموازنة بين مصلحة المجتمع في العقاب وبين حقوق الأفراد وحرياتهم، لذا أجاز خرق الخصوصية من خلال العمليات التفتيشية[3].

أحاط المشرع الجزائري إجراء التفتيش الالكتروني بجملة من الضوابط الصارمة لما يترتب عنه من مساس بحرية الأشخاص وكرامتهم وحرمة ممتلكاتهم[4]، وفقا لنص المادة 74 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

[1] – د/ علي حسن محمد الطوالبة، المرجع السابق، ص 59.

[2] – نجاة لوصيف، موسي مرمون، مبادئ وضوابط المعالجة الآلية للمعطيات الشخصية، مجلة العلوم الانسانية، جامعة بسكرة، المجلد 33، عدد 02 جوان 2022، ص 83.

[3] – د/ علي حسن الطوالبة، المرجع السابق، ص 46.

[4] – أ/ زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص 130.

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

يتضح لنا جليّا من نص المادة أن المشرّع يعاقب على كل انتهاك لهذه الحقوق والحريات وهذا ما تؤكده المادة 48 من التعديل الدستوري " تضمن الدولة عدم انتهاك حرمة المسكن. فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه. لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة". وهذا ما أكده المشرّع في المواد من 44 إلى 47 والمادة 64 إضافة إلى المادة 79 وما بعدها من قانون الإجراءات الجزائية، ولكن بالنظر لخطورة الجرائم المعلوماتية فان المشرّع الجزائري أجاز تقييد الحقوق الدستورية بموجب تعديلات قانون الإجراءات الجزائية والقانون رقم 04/09 حتى لا يتحكم الجاني في تغيير الدليل وتظليل جهات التحقيق.

أدخل المشرّع الجزائري تعديلا على قانون الإجراءات الجزائية بموجب القانون رقم 22/06 في المادة 45 الفقرة الخامسة منه، استغناؤه على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالَجة الآلية للمعطيات.

والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الالكتروني، 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]

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 الأنترنت وهي عبارة عن

[1] – أ/عائشة بن قارة مصطفى، حجّية الدليل الإلكتروني في مجال الإثبات الجنائي (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، 2009، ص 54.

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 الالكترونية عبر شبكات الحاسوب[1]، وفي أماكن بعيدة عن الموقع المادي للتفتيش، وإن أمكن 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 العالم تقريبا. وبالتالي فإن الحاسوب الذي يمكن أن ترتكب عليه أو بواسطته الجريمة المعلوماتية يخضع للقانون الإجرائي الخاص بتلك المنطقة.[2].

أجاز المشرّع الجزائري تمديد التفتيش وذلك في نص المادة 05 الفقرة الثانية من القانون 04/09 التي نصت بأنه" في حالة تفتيش منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

ما يجعلنا نرى هنا أن المشرّع الجزائري أخذ نفس مسار المشرّع 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".

[1] – هلالي عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، ط1، دار النهضة العربية، 2007، ص 76.

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

إن إجراء التفتيش في الجريمة المعلوماتية تحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش التقليدية، لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات الأجهزة وأماكن إخفاء المعلومات فيها، لأنه يسهل إتلافها كليا أو جزئيا، كما يصعب تحديد مكان الدليل[1]، يلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش والضبط 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، ويبعد الشك حول إمكانية إخفاء الدليل من قبل القائمين به ،ويقوم المفتش في إطار البحث عن الجرائم الماسة بأنظمة الإتصال والمعلوماتية.

وتجدر الإشارة هنا إلى أن مثل هذا المحل لا يكون قائما بذاته، وإنما يشمله مكان أو عقار ما أو يكون بصحبة مالكه أو حائزه ولذلك وجب على ضابط الشرطة القضائية عند استصداره الإذن بالتفتيش أن يحدد محل ذلك الإجراء تحديدا دقيقا وكذلك الغرض منه وإلا كان التفتيش باطلا[3].

و عليه يحدد التفتيش الالكتروني دقة الإجراءات فمن خلاله يتم نقل البرنامج الداخلي من الوسائط المتعددة وبذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما يتم في جرائم النسخ والتقليد حيث يتم ضبط الوسائط المتعددة المحمّلة بالبرامج المنسوخة والأجهزة المستخدمة في ذلك[4].

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

[1] – نبيلة هبة هروال، المرجع السابق، ص 234.

[2] – د/ خالد ممدوح إبراهيم، المرجع السابق، ص 228.

[3] – د/ عبد الفتاح بيومي حجازي، المرجع السابق، ص 378.

[4] – د/ كوثر سعيد عدنان خالد، حماية المستهلك الكتروني، دار الجامعة الجديدة، الاسكندرية، 2012، ص 114.

المتصلة بالحاسب الذي ارتكبت في نظامه الجريمة المعلوماتية، فهذا الفرض يؤكد أن إجراءات التفتيش والضبط 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 وعند القيام بتنفيذ إذن التفتيش، فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم، أو يمتد لأ كثر من جهاز في أماكان مختلفة أو تعدد المتهمين كأن يكو ن له شركاء في الأجهزة مما يتطلب الحصول على إذن آخر من وكيل الجهورية.

اشترط المشرّع الجزائري لصحة التفتيش أن يكون مسببا، باعتباره إجراء من إجراءات البحث والتحقيق ويهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقّق وقوعها بمكان أو شخص يتمتع بالحرمة، فلا تفتيش إلا بمقتضى القانون.

و الغرض من محل الجريمة هو الحصول على الدليل وحجزه وفقا للمقتضيات القانونية وهذا ما تؤكده المادة 06 من القانون رقم 04/09 "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية".

لنظم المعلوماتية خاصيات مميزة تجعل من إجراءات المتابعة أكثر دقة وموضوعية بالنظر لكونها عنصرا هاما في الكشف عن الأدلة، بحيث تتكون هذه الأخيرة من وحدات الإدخال والإخراج والذاكرة وأخرى غير معنوية وتتمثل في البرامج، البيانات والمعلومات ،ويعترض التفيش صعوبات ترتبط ببراعة الجاني في تغيير الأدلة محل التفتيش أو إذا كان

[1] – د/ عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، جامعة الوادي، الجزائر، عدد 4 , 2018، ص 60.

النظام يتمع بحماية فنية تحول دون الولوج إلى البيانات وتفتيشها، كما أن المشرّع يسعى من خلال هذا الإجراء إلى احترام الضمانات التي تكرسها القواعد الدستورية، لذا ضبطه بقيود.

المطلب الثالث: ضرورة التعاون الأمني والقضائي الدولي في مجال دعم التفتيش الالكتروني

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

الفرع الأول: ضمان فعالية التفتيش الالكتروني على المستوى الوطني

من الصعوبة تماما حصر الجريمة الالكترونية محل التفتيش إلا أن تصنيف قانون العقوبات الجزائري للجرائم المعلوماتية في تعديله بالقانون 21/14 المؤرخ في 28 ديسمبر 2021 فقد جاء في المادة 12 من هذا القانون المعدل والمتمم بالفصل الثالث من الباب الثامن 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 ثمان مواد جاء في المادة الأولى: 394 مكرر جريمة الدخول أو البقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

وفي المادة 394 مكرر 01 نص على جريمة إدخال معطيات في نظام للمعالجة الآلية للمعطيات، أو إزالة أو تعديل معطيات موجودة فيه، إذا كان ذلك عن طريق الغش.

[1] – د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 1998، ص 75.

وفي المادة 394 مكرر 02 نص على القيام عن طريق الغش بـ:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار 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 مكرر 03 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 مكرر 05 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 مكرر 06 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.[1]

[1] – د/ جميل عبد الباقي الصغير، المرجع السابق، ص 75.

- استحداث أو نشر أو الإتجار 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 المشرّع 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.

كما أطلق المشرّع الجزائري على الجرائم المعلوماتية مصطلحي: "جرائم المساس بأنظمة 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 الالكترونية[1].

و بالرغم من كل الأحكام القانونية الموضوعية والإجرائية فان إجراءات التفتيش الالكتروني لا تتم الا وفقا للضمانات القانونية إلا 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

[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 إلكترونية)، أنظر قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

يقضي بخلاف ذلك تخضع كل عملية معالجة معطيات ذات طابع شخصي لتصريح مسبق لدى السلطة الوطنية أو لترخص منها طبقا للأحكام المنصوص عليها في هذا القانون".

كما قيد المشرّع والاتصال بضرورة مراعاة حرمة الحياة الخاصة بحيث منح المشرّع الجزائري للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته العديد من الامتيازات وقيده من جهة آخرى احتراما للضمانات الدستورية وهذا ما أكده المشرّع الجزائري في المادة 49 من القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"يمكن السلطة الوطنية القيام بالتحريات المطلوبة ومعاينة المحلات والاماكن التي تتم فيها المعالجة، باستثناء محلات السكن ويمكنها للقيام بمهامها الولوج للمعطيات المعالجة وجمع المعلومات والوثائق أيا كانت دعامتها".

وتظهر عدة عراقيل وصعوبات لجهات التحري في الكشف عن هذه الجرائم ومتابعة مرتكبيها بالنظر إلى اتساع نظام الشبكات المعلوماتية وتطور التقنيات الفنية للأنترنت، الأمر الذي دفع بالمشرّع 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 بأحكام الرقابة التي فعل المشرّع الجزائري ضوابطها القانونية.

ولدعم الإجراءات 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 با لمرسوم الرئاسي رقم 261/15[1]، وكلّفت الهيئة بتنشيط وتنسيق

[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 رقم 53، الصادرة في 08 أكتوبر سنة 2015 .

عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها[1]، بالإضافة إلى صدور المرسوم الرئاسي رقم 05/20 المؤرخ في 20 جانفي سنة 2020 بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، تدعم إجراءات التفتيش الالكتروني.

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

- 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 الو طنية لأمن الأنظمة المعلوماتية.

وعليه تتمثل مهام المجلس الوطني لأمن الأنظمة المعلوماتية:

- البث في عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.
- دارسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما.
- دارسة التقارير المتعلقة بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها.
- الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.
- الموافقة على تصنيف الأنظمة المعلوماتية.

[1] – نورة صرشي، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر، 2012، ص 65.

- يبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذو صلة بأمن الأنظمة المعلوماتية[1].

الفرع الثاني: الجهود المبذولة على المستوى االدولي

ظهرت الجهود الدولية في هذا المجال فيما يعرف 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، والاتفاقية العربية سنة 2010 واتفاقية الاتحاد الإفريقي للتعاون الدولي والقضائي لمكافحة الجريمة العابرة للحدود.

كما عملت الأجهزة 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[2]، الحرص على التصدي للاستخ دام غير المشروع للحاسبات وشبكات المعلومات، وذلك من خلال العديد من الجهود التي بذلت في هذا الشأن.

و تجلّت الاهتمامات الإقليمية للمجلس بالمعلوماتية بشكل عام وما يحيطها من مشكلات للتصدي للاستخدام غير المشروع للحواسيب وشبكة الأنترنت، وقد اتجه إلى 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 تضمّنت تلك الاتفاقية عدة مبادئ تمثلت في الحد الأدنى من الاحتياطات التي يجب أن تتضمّنها التشريعات الداخلية للدول أطراف المعاهدة لحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيا.[3]

[1] – منصورية بلعيد، النظام الإجرائي للجريمة المعلوماتية، مذكرة لنيل الماستر في تخصص القانون القضائي، جامعة بن باديس مستغانم، السنة الجامعية 2020، ص 95.

[2] – د/ محمد أمين الشوابكة ، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، بدون بلد نشر، 2007، ص 73.

[3] – د/ عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 82.

إن الجرائم الالكترونية من أخطر التحديات الأمنية التي تواجه أعضاء المجتمع الدولي، فهي جرائم معقدة تُرتكب بوسائل تقنية حديثة ومتطورة من قبل مجرمين على مستوى عال من الذكاء والخبرة مما يجعل الإثبات والتحقيق فيها صعباً، بحيث أن الصورة التقليدية لإجراءات التحقيق التي تقوم بها الجهات المكلّفة بالبحث والتحري عن الجريمة لا تتماشى وطبيعة الجرائم الالكترونية ويعد التفتيش الالكتروني من إجراءات التحقيق التي خلقت للتماشي مع الوضع فهوإجراء تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها، وفقا لشروط وضوابط قانونية حددها المشرّع الجزائري تضمن نسبة الجريمة إلى الجاني، وتعطي صلاحيات للجهات المختصة للقيام بعمليات التفتيش الالكتروني.

ضرورة التعاون الدولي يعد أحد ضمانات فعالية هذا الإجراء ويكون ذلك في إطـار اتفاقيات خاصة ثنائية أو متعددة الأطراف تجيز لامتداد والتنسيق بين الدول ودعم التعاون الشرطوي باستخدام تقنيات عالية التقدم لدعم التفتيش الالكتروني.

الفصل الثاني الأحكام الإجرائية للتفتيش الالكتروني

بما أن التفتيش الالكتروني يعتبر من بين الإجراءات التي تعنى بخصوصية جرائم المنظومة المعلوماتية كونه يركّز على محل جريمة تتميز ببيئة رقمية افتراضية، ولمشروعية هذا الأخير لا بد من وقوع جريمة من الجرائم المعلوماتية واتهام جهة معنية أو أفراد بارتكاب هذه الجريمة أو المشاركة فيها مع توفر الدلائل على وجود أجهزة معلوماتية بحوزة المتهم تفيد في كشف الحقيقة أو غيرها بمقتضى ضبط قواعد إجرائية خاصة من الناحية القانونية والعملية، والتي سنسلّط عليها ضوء المعالجة، ويعتبر التفتيش الالكتروني إحدى هذه الإجراءات التي حملها القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وباعتبار الفصل الأول قد تضمن التنظيم الموضوعي لإجراء التفتيش الالكتروني كان لابد من التطرق للأحكام الإجرائية للتفتيش الالكتروني على النحو التالي: (المبحث الاول) خصص للجهات المختصة بالتفتيش الالكتروني نوعيا و إقليميا أما (المبحث الثاني) فكان لآثار التفتيش الالكتروني وكيفية التعامل معها.

المبحث الأول: الجهات المختصة بإجراء التفتيش الالكتروني

إن الهدف من التفنيش الالكتروني تمكين جهات التحقيق من كشف الجريمة والتعرف على مرتكبيها، وهو الأمر الذي سعى المشرّع الجزائري إلى تجسيده من خلال استحداث نصوص قانونية جديدة أوجد بموجبها قواعد إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية لذا خصصنا (المطلب الاول) للاختصاص النوعي للتفتيش الالكترونية، و(المطلب الثاني) للاختصاص المكاني للتفتيش الالكتروني.

المطلب الأول: الاختصاص النوعي للتفتيش الالكتروني

تخوّل إجراءات التفتيش الالكتروني بتسهيل مكافحة الجرائم المعلوماتية، إذ الأثر المترتب على التفتيش المنصبّ 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 جرائم تقنية المعلومات خاصة المادتان 26 و27 المتعلقتان بتفتيش المعلومات المخزنة وضبطها.

الفرع الأول: السلطات المختصة بالتفتيش الالكتروني.

أن إجراءات التفتيش الالكتروني لا تعد صحيحة ومنتجة لآثارها 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]

[1] – الأمر 11/21 المؤرخ في 26 أوت 2021 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 65. أنظر د/ رضا هميسي، المرجع السابق، ص 162.

ومن الملاحظ أن المشرّع أجاز لوكيل الجمهورية ولقاضي التحقيق أو ضباط الشرطة القضائية في إجراءات التفتيش الالكتروني تسخير كل عون مؤهل له إلى المهارات الفنية التي تتطلبها الجريمة المعلوماتية فقد أجاز المشرّع الجزائري للسلطات المكلفة بالتفتيش الاستعانة بخبير له دراية بالمعلوماتية محل البحث أو التدابير المتخذة من أجل المحافظة على الدليل، طبقا لمقتضيات المادة 05 الفقرة الرابعة من الأمر رقم 04/09، وتقديم التوضيحات وكيفية التفتيش بطرق صحيحة عليه للطرق التقنية الحديثة.[1]

و بالنظر لخصوصية التفتيش الالكتروني فإنه يخضع من حيث الإجراءات والضبط للأحكام المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم المنصوص عليها على سبيل الحصر في المادة 03/47 من ق.إ.ج.ج، فتخضع لقواعد خاصة تختلف عن القواعد العامة المقررة في الفقرتين 01 و02 من المادة 45 من قانون الإجراءات الجزائية [2] وتتباين القواعد حسب حالتين:

أولا- الحالة الأولى تتعلق بالجرائم الخاصة:

إذا تعلق الأمر بالتحقيق التمهيدي في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، فإن ضابط الشرطة القضائية بموجب الفقرة الأخيرة من نفس المادة 45 لم يعد مقيدا عند إجراء تفتيش المساكن والمحلات لشرط المتعلق بضرورة حضور المشتبه فيه أو من ينوبه أو شاهدين إذا حصل التفتيش في مسكن المتهم وفقا للمادة 82 من نفس القانون "...غير انه يجوز له وحده في مواد الجنايات أن يقوم بتفتيش مسكن المتهم في غير الساعات المحددة في المادة 47 بشرط أن يباشر التفتيش

[1] – زيدان زبيحة، المرجع السابق، ص 160.

[2] – راجع المادة 45 الفقرتين الأولى والثانية من الأمر رقم 11/21 المؤرخ في 25 أوت 2021 المتعلق بقانون الإجراءات الجزائية الجزائري.

بنفسه وأن يكون ذلك بحضور وكيل الجمهورية "، ويختلف الأمر إذا حصل التفتيش في مسكن غير المتهم أو شخص آخر يشتبه فيه يحوز أوراقا أو أشياء لها علاقة بالجريمة.[1]

ثانيا- 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 أ جهزة 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 إذن بالتفتيش من الجهات القضائية، فتقوم بحكم موقعها الوظيفي بالبحث والتحري حول الجرائم المعلوماتية من خلال ما تكرسه شرطة الأنترنت من ضمانات عند توليها مباشرة الإجراءات في العالم الافتراضي، بشرط أن تكون الجهات القائمة التفتيش الالكتروني على كفاءة تدريبية في مجال الجرائم المعلوماتية.[2]

لذلك دعم المشرّع 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

[1] – نبيلة هبة هروال، المرجع السابق، ص 100.

[2] – راجع المادة 02 من الأمر رقم 11/21 المؤرخ في 25 أوت 2021 المتعلق بقانون الإجراءات الجزائية الجزائري.

التابعة للجهاز الأمني والمكلف بمكافحة الجرائم المعلوماتية، تابعة لسلك الأمن الوطني[1] ،بحث يوجد على مستوى 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 بوهرا ن.

الفرع الثاني: ضوابط التفتيش الالكتروني وفق مراحل التقصي

أولا- ضوابط التفتيش الالكتروني في مرحلة التحقيق الابتدائي:

استثناءا لا يطبق في التفتيش الالكتروني المرتبط بالجرائم المعلوماتية القيود المنصوص عليها في المادة 47 الفقرة الأولى من ق.إج.ج، وتؤكد الاستثناء الفقرة الثانية من نفس المادة المتعلقة بالميعاد القانون "غير أنه يجوز إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات النهار أو الليل في الجرائم المعاقب عليها في المواد 342 إلى 348 من قانون العقوبات...و عندما يتعلق الأمر بجرائم المعالجة الآلية للمعطيات ..."، و أسباب هذا الاستثناء تتمثل في:

- التفتيش الالكتروني يحتاج إلى جهات متخصصة في عمليات البحث الرقمي وكل ما يفيد في كشف الحقيقة مما تتلاشى معه مسألة احترام الزمن المحدد للتفتيش في الإجراءات العادية.
- الخروج عن الأحكام العامة في قانون الإجراءات مرده إلى قوة تدفق المعلومات وسهولة التحكم في المعطيات، مما يفسح المجال للجناة للتحكم في الدليل الجنائي.
- الخوف من تحكم الجناة في المعلومات وطمس الشاهد الالكتروني، لذا أجاز المشرّع التفتيش الالكتروني في المنظومة المعلوماتية عن بعد، لمواجهة آثار تغيير الدليل.

[1] – سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري، المجلد 7، كلية الحقوق جامعة الجزائر، العدد 01، جوان 2000، ص 281.

- احترام الميعاد القانون يؤدي إلى عدم جدوى التفتيش الالكتروني، ويفسح المجال للجناة للتلاعب بالأدلة.

ثانيا- ضوابط التفتيش الالكتروني في مرحلة التحقيق القضائي:

يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها وفقا للمادة 79 من قانون الإجراءات الجزائية الجدزائري ، 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 من نفس القانون في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا الحقيقة.

باستقراء المادة 83 من قانون الإجراءات الجزائية والتي تحيلنا إلى المادة 47 من نفس القانون والخاصة بميقات التفتيش القانون، وفي إطار وضع الأسس القانونية الكفيلة بمحاربة بعض الظواهر الإجرامية الحديثة، كجرائم الإرهاب والمخدرات والجريمة المنظمة عبر الوطن والجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والجرائم المتعلقة بالتشريع الخاص للصرف.

يقرّ قانون الإجراءات الجزائية لقاضي التحقيق دخول المساكن وتفتيشها في أي وقت خارج ميقات القانون 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.

يترتب على إجراءات التفتيش الالكتروني وصول جهات التحري إلى 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 وضمان 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 الأشياء والوثائق النافعة في إظهار الحقيقة أو التي قد يضر إفشاؤها بسير التحقيق، ويجوز لمن يعنيهم الأمر الحصول على نفقتهم ،وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تخل بمقتضيات التحقيق[1].

ثالثا: مقتضيات إجراء التفتيش الالكتروني

يعد التفتيش الالكتروني إجراء تحقيقي في الجرائم المعلوماتية، يستهدف ضبط أدلة الجريمة مثل البرامج الغير المشروعة والملفات المخزنة في الحواسيب والمعطيات 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.

1- الإذن بالتفتيش الالكتروني:

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

إن الإذن المسلّم 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

[1] – المادة رقم 84 من قانون الإجراءات الجزائية رقم (3) لسنة 2001م. أنظر د/ أحمد عبد الحكيم عثمان، تفتيش الأشخاص وحالات بطلانه، منشأة المعارف، الإسكندرية، 2002، ص 221.

[2] – رابح مباركية، المرجع السابق، ص 66.

الذين لهم حق على تلك الأماكن. فتنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص وفي حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة، وفقا للمقتضيات الآتية:

ضابط الشرطة القضائية مقيد أثناء قيامه لعمليات المحددة في المادة 65 مكرر 05 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.

ويشترط في الإذن أن يكون مكتوبا ومتضمنا لكافة العناصر الأساسية التي تسمح بالتعرف على الاتصالات المطلوب التقاطها كتحديد رقم الهاتف واسم المشترك، وتحديد الأماكن المقصودة سكنية أو غيرها، وتحديد نوع الجريمة التي تبرر اللجوء إلى هذه التدابير.[1] 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.

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 المذكورة في المادة 65 مكرر 05 .

يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات

[1] – د/محمد حزيط ، مذكرات في قانون الإجراءات الجزائية الجزائري، ط9، دار هومة، الجزائر ، 2014 ، ص 113.

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.

سعى المشرّع الجزائري إلى ضبط الجانب الاجرائي للتفتيش الالكتروني من خلال توزيع المهام وتكليف 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[1] وعليه يجب أن يحدد في الإذن الندب بالتفتيش المكاني والشخص والأشياء المراد تفتيشها وضبطها كتحديد الحاسوب، برامج الاختراق، برامج الفيروسات.

دعم المشرّع الجزائري الإذن بالتفتيش الالكتروني بتدخل الهيئة الوطنية للوقاية من الجرائم المتصل بتكنولوجيا الاعلام والاتصال ومكافحته بالنظر إلى الجوانب الفنية والتقنية التي يتميز بها التفتيش الالكتروني لذا لجأ إلى هذا الأسلوب سنة 2009 بموجب نص كل من المادتين 03 و04 الواردتين ضمن فصول القانون 04/09 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الهيئة المختصة بتنفيذ عمليات المراقبة الالكترونية للإتصالات.

و تم تعزيز ذلك من خلال إستحداث مديرية المراقبة الوقائية واليقظة الالكترونية التي يدخل في صميم إختصاصاتها القيام بمهام المراقبة الالكترونية للإتصالات من أجل الكشف عن الجرائم المعلوماتية بناء على رخصة مكتوبة من السلطة القضائية وتحت مراقبتها ، حسب ما تقره المادة 11 من المرسوم الرئاسي 261/15 كما منحها القانون حسب نص

[1] – أ/ رشيدة بوكر، المرجع السابق، ص 374.

المادة 21 من المرسوم السالف الذكر الصفة الحصرية لتولي مهام المراقبة الالكترونية في حال تصنيف الجريمة المعلوماتية ضمن الجرائم الإرهابية والتخريبية والماسة بأمن الدولة دون سواها من الهيئات الوطنية الأخرى وذلك تحت سلطة قاض مختص.

كما نصت المادة 10 من القانون رقم 04/09، التي توجب على مقدمي خدمة الأنترنت[1] 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

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

- طلب التحفظ المعجل على البيانات المخزنة ليتفادى المزود شطب التسجيلات والقضاء على الدليل.
- طلب تقديم بيانات معلوماتية خاصة بالمشترك.
- طلب اعتراض على الاتصالات الالكترونية.

نستنتج وفقا للمادة 12 من القانون 04/09 أن القانون قد سمح للسلطات المختصة بمتابعة الجرائم المعلوماتية حق طلب التحفظ على البيانات المخزنة لديها وكذلك حق تزويدها بالمعلومات الخاصة بالمشترك ونشاطه في إطار عملها المتعلق بأعمال البحث والتحري عن الجرائم المعلوماتية.

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 والخضوع لتعليمات وكيل الجمهورية أو قاضي التحقيق أو اختصاصا

[1] – 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

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.[1]

وتتمثل هذه الشروط في الشروط الشكلية للاذن بالتفتيش الالكتروني.

2- الحضور الضروري لبعض الأشخاص أثناء التفتيش في البيئة التقنية:

الأصل أن يتم التفتيش في حضور المتهم أو من ينوبه وفي حالة غيابه يعين شاهدين شرط أن لا يكونا من الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش ، إلا أن المشرّع الجزائري وبموجب الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية التي تنص على أنه " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف باستثناء الأحكام المتعلقة بالحفاظ على السر المهني ..."، استبعد هذا الشرط والعلّة 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 والتلاعب فيها مما يستدعي سرعة استخلاصها قبل فقدانها.[2]

3- الميقات الزمني لإجراء التفتيش في الجرائم المعلوماتية:

يقصد بضمانة الميقات الزمني في التفتيش أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرّع والعلّة في ذلك هو تضييق نطاق الاعتداء على الحريات الفردية وحرمة المسكن إلا أن هناك من التشريعات من تركت مسألة تحديد ميقات التفتيش للقائم به وبالتالي

[1] – د/خالد عياد الحلبي، المرجع السابق ، ص 197.

[2] – أ/نبيلة هبة هروال، المرجع نفسه، ص 252.

يجوز له القيام به ليلا أو نهارا ومن بين هذه التشريعات نجد التشريع الإجرائي المصري[1].
ذهب المشرّع الجزائري وكذا المشرّع الفرنسي إلى حظر تفتيش المنازل وما في حكمها في وقت معين، فقد حدد المشرّع 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 وهذا من خلال المادة 59 ق.إ.ج.ج.[2]

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

- حالة رضا صاحب المنزل رضاً حرّاً، وصريحا وعن علم بالسبب.
- حالة الضرورة والمتمثلة في الاستغاثة من داخل المنزل كالحريق مثلا.

و يلاحظ أن المشرّع الجزائري استثنى الميعاد القانون من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من حظر التفتيش ليلا، قد أدرك الطبيعة المميزة لهذه الجريمة وخصوصيتها من حيث إمكانية ارتكابها في أي وقت وأن أدلة الإدانة فيها سهلة المحو والتدمير وأنها غير مرئية وعليه فإن تأخير إجراء التفتيش قد يحفز على ارتكاب العديد من الجرائم ويعرقل السير الطبيعي لمجريات التحقيق، ومن جهة ثانية فإن هذه الضمانة بدأت أهميتها تتضاءل مع ظهور ما يعرف بالتفتيش عن بعد أو ما يطلق عليه في الفقه الفرنسي مصطلح التفتيش على المباشر والذي يمكن أن يتم في أي وقت.[3]

4- توافر متطلبات إجراء التفتيش الالكتروني للنظم المعلوماتية:

نص المشرّع الجزائري في المادة 05 من القانون رقم 04/09 على ضرورة توافر حالات على سبيل الحصر، تجيز للسلطات القضائية وضباط الشرطة القضائية القيام

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

[2] – 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

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

بتفتيش المنظومة المعلوماتية في إطار قانون الإجراءات الجزائية وهي الحالات المذكورة في المادة 04 منه حيث نصت المادة 05 منه" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

كما نص في المادة 05 منه" يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدبير المتخذة لحماية المعطيات التي تتضمنها. قصد مساعدتها و تزويدها بالمعلومات الضرورية لإنجاز المهمة".

المطلب الثاني: الاختصاص المكاني للتفتيش الالكتروني

يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في البحث والتحري الالكتروني عن الجريمة المعلوماتية، ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة وهو الاختصاص القضائي لنظر في الجرائم المعلوماتية والقانون الواجب تطبيقه على الفعل، وبالنظر 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 الأول: ضوابط الاختصاص المكاني للتفتيش الالكتروني.

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

مدّد المشرّع الجزائري من اختصاص ضباط الشرطة القضائية وجعله يشمل كامل الإقليم الوطني في إطار البحث ومعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بعدما

كان هذا الأمر مقتصرا في البداية على الجرائم المتعلقة بالإرهاب حسب التعديل الذي جاء به القانون 11/21 المتعلق بالإجراءات الجزائية وتم توسيع ذلك إلى جرائم أخرى منها الجريمة المعلوماتية، وفي هذه الحالة يعمل ضباط الشرطة القضائية تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات، ويرفع ضباط الشرطة القضائية أيديهم عن إجراءات التفتيش الالكتروني في حال وصول وكيل الجمهورية، ويقوم بإتمام جميع أعمال الضبط القضائي أو يكلف كل ضابط للشرطة القضائية بمتابعة إجراءات التفتيش وفقا لنص المادة 56 من ق.إ.ج.ج.

طبقا لأحكام المادة 40 مكرر 01 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 التنفيذي 348/06 المتعلق بتعيين وتحديد المحاكم ذات الاختصاص الإقليمي الموسع، وطبقا للمادة 40 مكرر 03 من ق.إ.ج.ج، فإنه للنائب العام التابعة له المحكمة المختصة المطالبة بالإجراءات في جميع مراحل الدعوى.

كما تنص المادة 35 من ق.إ.ج.ج على أنه" يمثل وكيل الجمهورية النائب العام لدى المحكمة بنفسه أو بواسطة أحد مساعديه وهو يباشر الدعوى العمومية في دائرة المحكمة التي بها مقر عمله" كما حددت المادة 36 من نفس القانون اختصاصات وكيل الجمهورية، وذكرت المادة 36 مكرر مهام وصلاحيات أخرى تندرج ضمن مهام وصلاحيات وكيل الجمهورية.

تجسد هذا التوسيع في الصلاحيات من خلال منح وكيل الجمهورية سلطة الإذن بالتفتيش، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور وهذا ما نصت عليه المادة 65 مكرر 05 من القانون 22/06، و يسمح الإذن المسلم بغرض وضع الترتيبات التقنية

بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن.[1]

كما نلاحظ توسيع الصلاحيات من خلال التعديلات التي جاء بها القانون رقم 11/21 صلاحيات قاضي التحقيق ومنحته صلاحيات إضافية لم يكن يتمتع بها من قبل ،وهذه الصلاحيات يمارسها عند التحقيق في نوع معين من الجرائم وردت على سبيل الحصر، منها اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وإجراء عملية التسرب الرقمي.*

يعد البعد الدولي من أهم مميزات الجريمة المعلوماتية لكونها جريمة عابرة للحدود ولا تعرف حدودا تمنع انتشارها فيمكن ارتكابها من عدة أفراد ينتمون لجنسيات مختلفة، كما يمكن أن يرتكب الفعل في بلد معين وتكون النتيجة في بلد أخر مما أثار خلافا فقهيا حول تحديد الجهات المختصة بعمليات التفتيش والفصل في النزاع القضائي، لإتاحة الفرصة للاطلاع على مدة التخزين في اقاليم متعددة، والسماح لمزودي الخدمات الاطلاع على محتوى الرسائل وتعاونهم مع رجال القضاء.[2]

فذهب فريق من الفقه إلى القول بأن 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 وبالتالي فهي فعلا مباحاً ولا يعاقب عليه القانون، وهذا ما دفع لظهور رأي أخر يرى بأن الاختصاص للنظر في هذه الجرائم يؤول لمكان تحقق النتيجة لاحتمال تعدد الدول التي تم فيها التحميل مما يؤدي إلى إفلات المجرم من

[1] – د/ عبد الله أوهايبية، ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي، الاستدلال، ط1، الديوان الوطني للأشغال التربوية، 2004، ص 300.

* – حدد المشرّع 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.

[2] – د/ غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والأنترنت وجرائم الاحتيال المنظم باستعمال شبكة الأنترنت، دار الفكر والقانون، المنصورة – مصر، 2010، ص 180.

العقاب، وهذا الرأي أيضا لاقى انتقاداً لكونه لم يأخذ بعين الاعتبار بأن مصلحة المتهم تقتضي تطبيق قانون الدولة الحامل لجنسيتها وليس قانون دولة أخرى.[1]

الفرع الثاني: تمديد الاختصاص الإقليمي لإجراء التفتيش الالكتروني:

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[2].

كذلك نظم المشرّع 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". كما تختص المحاكم الجزائرية بالنظر في الجرائم التي تقع كلها أو جزء منها على إقليمها أيا

[1] – د/ محمد عوض محمد، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، بحث مقدم في المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص 43 منشور على الرابط: https//:academia-araria.com وتصفحه بتاريخ 2024/04/21 على الساعة 22.18سا.

[2] – د/ محمد معمر الصغير، المرجع السابق، ص 22.

كانت صفة الشخص المتهم وبغض النظر عن جنسيته، ويرتبط قانون العقوبات في أية دولة ارتباطا وثيقا بسيادتها بل في الحقيقة يعتبر أهم مظهر للدولة على إقليمها، فيعد مبدأ إقليمية النص الجنائي معتمد في التشريعات الجنائية ومن مبادئ قوانين كل دول العالم.

وعليه تبنّى القانون الجزائري هذا المبدأ فنصّت المادة 03 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"*، كما نصت المادة 15 من القانون 04/09 "زيادة عن قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للإقتصاد الوطني".

أما في نطاق تطبيق مبدأ العينية للفعل المجرم بالنص الجنائي ليطبق على بعض الجرائم وبالعودة إلى صورة الجريمة الالكترونية وأركانها التي نص عليها المشرّع 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 أو عن طريق إدخال أو محو أو تعديل بيانات نظم المعالجة الآلية للمعطيات قد تمت بالجزائر[1].

و منه نستنتج أن إجراءات التفتيش الالكتروني تخضع لأعمال التحقيق باعتبارها من الأعمال الإجرائية لتنظيم القانون من حيث شروط صحتها وآثارها، وأي إجراء مخالف للقواعد الإجرائية يترتب عنه جزاء يتمثل في البطلان، ولا يقبل الدفع ببطلان التفتيش إلا ممن شرع

* – وهذا ما أكده المشرّع الجزائري في المادة 586 من القانون رقم 11/21 من قانون الإجراءات الجزائية المؤرخ في 25 أوت 2021.

[1] – أ/ نبيلة هبة هروال، المرجع السابق، ص 134.

البطلان لمصلحته، كحائز جهاز الحاسوب أو البرنامج الذي جرى تفتيشه، وإذا تعلق بطلان التفتيش بالنظام فيجوز الاحتجاج به في أية مرحلة من مراحل الدعوى الجزائية[1].

أولا- اختصاص تمديد التفتيش الالكتروني إلى منظومة معلوماتية أخرى:

انصبت اهتمامات المشرع الجزائري بالمنظومة المعلوماتية وإنشاء العديد من الأجهزة والهيئات الرقابية التي تساهم في مكافحة الجريمة الالكترونية، بالإضافة إلى اعتماد العديد من الضوابط التي تساهم في التصدي للإجرام الالكتروني من خلال متابعة الارتباط بين شبكات الحواسيب سواءا كانت شبكة محلية أو شبكات دولية الأمر الذي يستدعي سرعة متابعة الجناة، من خلال تمديد التفتيش إلى منظومة معلوماتية أخرى، ففي هذه الحالة يختص النائب العام لدى مجلس قضاء الجزائر بمنح النائب العام بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 من القانون 04/09، وفي غير هذه الحالة نطبق القواعد العامة التي رسمها قانون الإجراءات الجزائية يرجع الاختصاص لوكيل الجمهورية وقاضي التحقيق بمنح الإذن بالتفتيش.[2]

ثانيا- إختصاص تمديد الإنابات القضائية خارج الجزائر:

يقصد بالإنابة القضائية ذلك الإذن أو التكليف الصادر من الجهات المختصة من أو إنابة للقيام بالإجراء المطلوب فهو كل تصرف إجرائي يصدر ممن له سلطة التحقيق بموجبه يفوض أحد مأموري الضبط القضائي ليقوم بدلاً منه بإجراء[3]، وحدّد المشرّع الجزائري سبلاً في مجال ملاحقة الجرائم المعلوماتية من خلال تمديد الإنابات القضائية، والسماح لضباط الشرطة القضائية بتتبع المعلومات المخزنة في المنظومة المعلوماتية التي تقع خارج الإقليم الوطني في إطار المساعدة القضائية.[4]

---

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

[2] – المادة 13 من القانون 04/09، المرجع السابق.

[3] – د/ أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، دون بلد نشر، دون سنة، ص 507.

[4] – أ/ زيدان زبيحة، المرجع السابق، ص 144.

المبحث الثاني: آثار التفتيش الالكتروني وكيفية التعامل معها

إن الضبط الناتج عن عمليات التفتيش الالكتروني محله في مجال الجرائم الالكترونية، البيانات المعالجة إلكترونيا، فهنا أثير الجدل حول مدى صلاحية البيانات الالكترونية البيانات لأن يكون محلا للضبط ومدى حجية الدليل المستخلص من الوسائل الالكترونية بالتفتيش الالكتروني وهو محل الدراسة في هذا المبحث حيث نتطرق في المطلب الأول إلى آثار التفتيش الالكتروني والتعامل مع الدلة الرقمية وفي المطلب الثاني إلى حجية الدليل المستخلص من الوسائل الإلكترونية بالتفتيش الالكتروني.

المطلب الأول: آثار التفتيش الالكتروني والتعامل مع الأدلة الرقمية

بما أن الضبط بطبيعته القانونية لا يقع إلا على أشياء المادة المنقولة، وهذا لا خلاف في ضبطه أما النظام المعلوماتي فتفتيشه يتميز بالتعقيد لمعالجة الآلية للبيانات الرقمية، وهو يشتمل على وسائل الإدخال والإخراج وتخزين البيانات، وهذا قد يكون منفرداً أو متصلاً بمجموعة من الأجهزة المماثلة عن طريق شبكة إلكترونية متباينة الحدود الوطنية والدولية.

كل هذه المعطيات عقّدت إجراءات التفتيش الالكتروني، مما جعل المشرّع الجزائري يكرس إجراءات وقائية الغاية منها الحيلولة دون وقوع الجريمة الالكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة 03 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، من جهة أخرى يهدف التفتيش المنصب على المنظومة المعلوماتية إلى استخلاص الدليل الالكتروني، قبل قيام المجرم المعلوماتي بتدميره أو إخفائه للإفلات من العقوبة. [1]

الفرع الأول: ضبط الدليل الرقمي كأثر للتفتيش الالكتروني

الضبط هو الأثر المباشر للتفتيش الالكتروني، وباعتباره أحد إجراءات التحقيق فتنطبق عليه القواعد التي تنطبق على التفتيش فإذا بطل التفتيش بطل الضبط، والتفتيش

[1] – د/ حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية،(بدون بلد نشر)، 2000، ص 228.

يعتبر وسيلة تهدف للوصول إلى الحقيقة وليس غاية في حد ذاته، ولعل أن الاشكال الذي يتبادر إلى الذهن في هذه الحالة هو مدى قابلية النظم المعلوماتية للتفتيش باعتبارها بيانات مادية وكيفية التعامل معه.

أولا – جمع آثار التفتيش الالكتروني (الدليل الرقمي):

الخطوة الأولى في عملية التحقيق الجنائي هي تحديد مصدر الدليل الرقمي المتوقع حتى يتم الحصول عليه بصورة رقمية تمهيدية لفحصه وتحليل مصادر البيانات تختلف فقد تكون أقراص ويمكن القيام بهذه العملية عن طريق مقارنة توقيع الحاوية الأصلية والبيانات المنسوخة، بالإضافة إلى عمل نسخ أخرى من البيانات مع التأكد من سلامتها بنفس الخطوة السابقة وحفظها في مكان آمن في حالة حدوث أي عطب في البيانات المستخدمة.[1]

و للحصول على البيانات يجب المرور بعدد من الخطوات للتأكد من صحة الدليل، قبل وبعد تفتيش المنظومة و بتحديد 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.[2]

ثانيا– فحص البيانات الرقمية كأثر للتفتيش:

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

ثالثا– تحليل ومراجعة آثار التفتيش الالكتروني:

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 وربط

[1] – نعيم سعيداني، المرجع السابق، ص 124.

[2] – فاطمة الزهراء خبازي، الجريمة الالكترونية في ظل الجرائم المرتبطة بتكنولوجيات المعلومات، منشور على الرابط http://salahgardafi.eb2a.com.content تم التصفح بتاريخ 2024/04/22، على الساعة 19:08سا.

الأحداث المشتبه بهم ومن المستحسن أن يقوم بعملية التحليل أكثر من محقق حيث كل شخص قد يكون له طريقته الخاصة في البحث و التحليل وبالتالي الحصول على عدد أكبر من الأدلة لدعم ملف القضية، كما يقوم المحقق الجنائي بتدوين عملية التحقيق منذ البداية إلى غاية نهايتها، على محاضر وتقارير ترفق كملف مجمل لأجل إثبات الدليل الناتج عن عملية التفتيش الالكتروني الذي تم نقله من مصدر مسرح الجريمة المعلوماتية.[1]

الفرع الثاني: حجز المعطيات الرقمية محل التفتيش وحدود استعماله:

حجز المعطيات المعلوماتية يظل الهدف الأساس لعملية تفتيش المنظومة المعلوماتية، هو وضع اليد على الأدلة الرقمية لإدانة المجرم الالكتروني، 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 أن المشرّع 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".

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، ويتم الحجز عن طريق

[1] – حسني ثابت، الجريمة الالكترونية في ظل تطور تكنولوجيات المعلومات، منشور على الرابط http//:kenonaonline.com تاريخ التصفح: 2024/04/21، على الساعة 21.20سا

منع الوصول إليها حيث نص المشرّع الجزائري في المادة 07 من القانون رقم 04/09 " 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 المشرّع لم يحدد الأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه*، 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.

إن إجراء مراقبة الاتصالات الالكترونية يمس بحق الأشخاص في سرية المراسلات الالكترونية، وهو حق مكفول دستوريا، لذا نص المشرّع 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 يلى:

- الإسراع في الكشف يجب على المحقق السرعة في الانتقال إلى مسرح الجريمة؛

* – أما بالنسبة للمشروع قانون المعاملات الالكترونية، فقد تضمن تعريفات لعدد من المصطلحات، حيث عرف البيانات الالكترونية بأنها بيانات مماثلة أو حزمة إلكترونية سواء على شكل نص أو رمز أو صوت أو صور .... كما عرف السجل الالكتروني 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.

- اتباع الخطوات الأصولية المستحدثة في السيطرة على أجهزة والحواسيب المستخدمة في الجريمة؛
- الاستعانة بخبراء الحواسيب والبرامج لمنع فقدان أو تلف أو تلوث الأدلة؛
- الحفاظ على مسرح الجريمة وتأمينه ومنع العبث به.[1]

احتياطات الكشف عن الدليل الالكتروني وتشتمل على الإجراءات التالية التي ينبغي على فريق مسرح الجريمة من المحققين وأعضاء الضبط القضائي، ذوي الاختصاص من الخبراء والجنائيين وفق المواد (41 و42 و43، 44، 49، 52)، وعلى هذا الأساس يتم القيام بمايلي:

- فتح محضر الخاص بالمضبوطات الجرمية عند أول لحظة الوصول وعند المغادرة مسرح الجريمة؛
- تصوير مسرح الجريمة من قبل فريق الأدلة الجنائية قبل الدخول وبعد الخروج منها؛
- إجراء الكشف والمخطط على محل الحادث بشكل أصولي دقيق؛
- خبير بصمات يتولى رفع البصمات من مسرح الجريمة؛
- خبير الحواسيب الالكترونية وشبكات يتولى رفع وتحريز الأدلة الرقمية بالطرق الفنية مزودا ببرامج عرض الصور وبرامج فك الملفات المضغوطة مثل winzip, winrar؛
- الحفاظ على الأجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الأشياء التي يعتقد أن 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 الأنترنت يلعب دورا مهما في تحديد موقع ومكان المشتبه به؛

[1] – د/ طارق ابراهيم الدسوقي عطية، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية "الأنترنت"، بدون بلد نشر، 2014، ص 89.

- إثبات الطريقة التي تم بواسطتها إعداد 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، وإثبات حالة التوصيلات والكابلات المتصلة بمكونات النظام كله، وذلك لإجراء مقارنة لدى عرض الأمر على القضاء؛
- إنتداب خبير القضائي في مسائل الجرائم الالكترونية مع المحقق عند إجراء الكشف على مسرح الجريمة ورفع البصمات من خلال التعاون بين خبراء أدلة الجنائية من خلال إنشاء مكتب التنسيق بين المؤسسات المشار إليها آنفاً بصورة مستمرة ومتواصلة.[1]

أولا- الأصول القانونية للتعامل مع الدليل الرقمي أثناء التفتيش الالكتروني والحجز:

انقسم الفقه إلى اتجاهين:

1- الاتجاه الأول: الاتجاه المعارض لإمكانية خضوع مكونات الحاسوب المنطقية للتفتيش

يرى هذا الاتجاه ان تفتيش المنظومة المعلوماتية كما عرفت المادة 02/02 من القانون رقم 04/09 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] - نعيم سعيداني، المرجع السابق، ص 156.

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 ويستندون أنصار هذا الرأي إلى أن القوانين الإجرائية تنص على إصدار الإذن بضبط " أي شيء" فإن ذلك يفسر تفسيرا واسعا بحيث يشمل معلومات وبيانات الحاسب المحسوسة وغير محسوسة[1].

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

و على النقض من الرأي الأول فإن أنصار الرأي الثان 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 ويعتمد في رأيه على الواقع العم لي الذي يتطلب أن يقع الضبط على معلومات الحاسب الآلي إذا اتخذت شكلا ماديا، لذلك يرى أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره.[2]

[1] – أ/علي عدنان الفيل، المرجع السابق، ص 42

[2] – المرجع نفسه، ص 58.

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 أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الاشياء المادية الملموسة[1].

3- موقف المشرّع الجزائري:

إن إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة الالكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة 03 من القانون رقم 04/09، 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 القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش كالحجز داخل منظومة معلوماتية".

إلا أن المشرّع الجزائري ومن خلال القانون 04/09 المادة الخامسة منه، يتضح أنه سار في اتجاه الرأي الثاني الذي رأى بضرورة وجود قواعد خاصة تحكم التفتيش وهذا بالنظر إلى طبيعة المعلومات التي لا تتماشى والنصوص 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 ولو عن بعد إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظومة معلوماتية.

[1] – د/ عز الدين عثماني، المرجع السابق، ص ص 49 – 50.

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 وكذلك للبيانات المعلوماتية المخزنة فيه وعلى أرضه.
- لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية".[1]

ثانيا: الجزاء المترتب على عدم مراعاة أحكام وضوابط التفتيش الالكتروني.

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

وتثير مسألة البطلان إشكالات عديدة، فيما يتعلق بطبيعة البطلان إذا كان يتعلق بالنظام العام أم بمصلحة جوهرية للخصوم، وكذلك الشأن فيما يخص حالات البطلان فهل هذا يعني أن احترام تلك الضمانات واجب في التفتيش طبقا للقانون يترتب على مخالفتها البطلان أو 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 من 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.

ومن ثمة فإن وجود الدلائل والقرائن القوية يتوفق على جدية التحريات المرتبطة بإجراءات التفتيش الالكتروني وما ينتج عنها من أدلة تعد من المسائل الموضوعية التي تخضع لقاضي الموضوع، ومن ثم فإذا أراد المتهم الدفع ببطلان التفتيش لعدم جدية

[1] – أ.د/ هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، (دارسة مقارنة)، ط1، دار النهضة العربية، (بدون بلد النشر)، 1997، ص 180.

التحريات التي سبقته فهذا الدفع يقدم أمام محكمة الموضوع، ولا يجوز إثارته أمام المحكمة العليا باعتبارها محكمة قانون .

الفرع الثالث: الحصول على البيانات والتعامل مع الدليل الرقمي أثناء التفتيش.

عمل المشرّع الجزائري على وصف الافعال الاجرامية المعلوماتية بدقة الأفعال بدقة، حتى يضمن صحة الأدلة الناجمة عن عمليات التفتيش الالكتروني، وإيجاد حلول للمشتملات المتعلقة بالدليل الالكتروني من حيث الوسائل المستعملة في الحصول عليه ومدى تأثير مشتملات الدليل الالك ترون على الاقتناع الشخصي للقاضي.

أولا: الركائز القانونية للحصول على البيانات الرقمية

تباينت الآراء الفقهية حول مدى امكانية إجبار المشتبه فيه أو 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 ويستندون في ذلك إلى القاعدة العامة التي مفادها عدم جواز أو إمكانية إجبار المتهم على الإجابة على الأسئلة التي من شأنها أن تؤدي إلى إدانته، ولا يمكن أن يفسر سكوته أو صمته ضد مصلحته وهو ما يمكن استنتاجه من نص المادة 100 من ق.إ.ج.ج التي نص على أنه" يتحقق قاضي التحقيق حين مثول المتهم لديه لأول مرة من هويته ويحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه و ينبهه بأنه حرٌّ في عدم الإدلاء بأي إقرار وينوه عن ذلك التنبيه في المحضر".

و في المقابل يرى رأي آخر أنه وإن 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 وقد رد أنصار الرأي الأول

[1] – نوارة حسين، آليات تنظيم المشرّع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، منشور في مجلة الدراسات القانونية لأعمال ملتقى آليات مكافحة الجرائم الالكترونية، كلية الحقوق جامعة الجزائر، ص 107.

على ذلك أن كلمة السر وما في حكمها هي أمر معنوي (بخلاف المفتاح الذي يعد شيء مادي) تكتنفه عدة صعوبات كإدعاء المتهم نسيانها.[1]

إلا أن المشرّع 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، 11، 18، 19 من القانون رقم 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، 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".[2]

و من ثمة بين المشرّع الحل في الحالة التي يكون فيها النظام المعلوماتي مزود بحماية فنية ككلمة السر، فالمشرّع من خلال القانون المذكور أعلاه تناول إجراءات تحري خاصة والمتمثلة في المراقبة التقنية وحفظ المعطيات المتعلقة بحركة السير، ونظرا لخصوصية الجريمة المعلوماتية وسهولة تدمير الأدلة فإن المشرّع حدد ضمانات لسلامة التفتيش الالكتروني وصحة الحصول على الدليل الرقمي وحجزه.[3]

و في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم مساعدات إلى السلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوي

---

[1] – أ /رشيدة بوكر، المرجع السابق، ص ص 399 – 400.

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

[3] – أ/ عبد القادر عدو، الجريمة الالكترونية إجرائيا، ط2، دار هومة، الجزائر، 2016، ص 109.

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 والتعامل مع الدليل الرقمي أثناء 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 إلي ها باستعمال وسائل فنية وتقنية.
- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجودها.

بالإضافة إلى دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته في دعم الحصول على الدليل الرقمي، حيث تتشكل هذه الهيئة من لجنة مديرة يرأسها الوزير المكلف بالعدل وثلاثة 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 والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.[1]

[1] – نورة صرشي، المرجع السابق، ص 63.

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: أسس حجز البيانات وتحصيلها أثناء التفتيش الالكتروني

1- إجراءات حجز المعطيات المعلوماتية:

يرتب التفتيش الالكتروني أثر 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 المشرّع الجزائري في نص المادة 06 و07 من القانون 04/09.

وتتمثل شروط إجراء الحجز فيمايلي:

- 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.

[1] - أ/ يوسف مناصرة، جرائم المساس بأنظمة المعالجة الألية للمعطيات- دراسة مقارنة، دار الخلدونية للنشر والتوزيع، الجزائر، 2018، ص 115.

[2] - أ/عبد القادر عدو، المرجع السابق، ص 109.

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

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.

ويلاحظ أنه 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 تأمر 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]

2- إجراءات جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات:

نظم المشرّع الجزائري ضمن قانون 04/09 سابق الذكر، إجراء جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وجعله من التزامات مقدمي الخدمات في

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

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 وبوضع 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 المشرّع الجزائري هذا الإجراء 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 " الأنترنت" ما يلي:

أ. التدخل الفوري لسحب المحتويات 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.

3- جمع الأدلة من خلال اعتراض رسائل البريد الالكتروني:

وذلك من خلال الاستعانة ببرامج مصممة للبحث في مضمون الرسائل الالكترونية المتبأدلة 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 الأنترنت 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 وتنفيذ الإذن القضائي بالتفتيش، ولكن يبقى أمر استخلاص نتائجها

أمرا مرهونا بمدى التزام مقدم خدمة الأنترنت بمد يد العون لأجل تحديد مكان ارتكاب الجريمة وهوية مرتكبها.[1]

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

المطلب الثاني: 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 الأول: أنواع الأدلة الرقمية الناجمة عن التفتيش الالكتروني:

من بين الأشياء أو الأدلة التي تضبط وتحتفظ بها في الجرائم المتعلقة بالجريمة المعلوماتية[3]، والتي لها قيمة في إثبات تلك الجريمة وتنسبها إلى المتهم.

أولا- ضبط جهاز الكمبيوتر وملحقاته:

للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو أنها مرتبطة بالمكان أو الشخص الحائز على الجهاز[4] يجب ضبط جهاز الكمبيوتر وملحقاته، ولأجهزة الكمبيوتر أشكال وأنواع مختلفة الأمر الذي يتطلب على ضباط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه ومواصفاته بسرعة فائقة إما بنفسه أو بواسطة خبير.

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

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

[3] – د/ محمود إبراهيم غازي، الحماية الجنائية للصوصية والتجارة الالكترونية، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2013، ص 256.

[4] – د/ خالد عياد الحلبي، المرجع السابق، ص 176.

ملحقات الكمبيوتر (البرمجيات – software): إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بالتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

وسائل التخزين المتحركة: كالأقراص المدمجة "أقراص الليزر، والاقراص المرئية والأشرطة المغناطيسية وغيرها".

المودم: Modem: وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف.

ثانيا – 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 الوارد أو الصادر أو الحفظ أو المهملات أو ضبط الرسائل الالكترونية عن طريق تشغيل برامج البريد الالكتروني في جهاز المتهم ومراجعة قائمة الرسائل الجديدة ليلتقط الرسالة المطلوبة[1]، وتوجد جملة من الصعوبات التي تواجه المحقق في ضبط الدليل:

إن 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 أو 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.

ويلاحظ أن المشرّع 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

[1] – د/ نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان –الاردن، 2010، ص 42.

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 أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية".

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق يهدف إلى البحث عن الأدلة لإثبات وقوع جريمة ما في مكان معين، ونظرا لخطورته تشترط أغلب التشريعات الحصول على رخصة التفتيش من الجهة القضائية المختصة للحجز على المنظومة المعلوماتية، لأن نظم المعالجة في الجرائم الالكترونية تتميز بأنها معالجة الآلية تكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال متطورة، فيتم الحجز عن طريق التنفيذ والاستعانة بخبراء من أجل الحفاظ على الدليل الرقمي.[1]

و هذا ما أكده المشرّع الجزائري لتسهيل عمليات الضبط والحجز داخل المنظومة المعلوماتية بموجب القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال حيث قررها بضوابط خاصة منها: وفقا لنص المادة 06 منه "عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وقفا للقواعد المقررة في قانون الإجراءات الجزائية.

ثالثا: محضر التفتيش الالكتروني.

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

[1] – عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 04/09، مجلة معالم الدراسات القانونية والسياسية، كلية الحقوق والعموم السياسية، جامعة المدية، الجزائر، المجلد 04، العدد 01، 2020، ص 199.

1- 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 القانون والتكييف القانون 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.*

ويكتب الرقم القضائي بمداد مغايِر لِلَون المداد المسطّر 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.

2- عنوان المحضر التفتيش الالكتروني:

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

3- 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.

4- 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

* – 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.

اسم كاتب التحقيق، سواء كان كاتب النيابة أو آخر انتدبه المحقق بعد أداء اليمين، مع إثبات الحلف على ما سبق بيانه.*

5-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.

6- مقدمة المحضر:

هي عبارة عن ملخص 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.

7- 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.[1]

ويمكن تقسيم هذه الإجراءات إلى قسمين:

- الإجراءات التي قام بها المحقق ويطلق عليها الأدلة المحسوسة أو المادية.
- الإجراءات المتعلقة بأطراف الواقعة.

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

[1] – د/عبد الفتاح بيومي الحجازي، المرجع السابق، ص 74.

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 الالكترونية منها.*

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، المجني 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 بالأدلة التي تم العثور عليها بمسرح الجريمة أو في حيازته.
- يجب أن يحدد المحقق مدى تعارض وتناقض واختلاف أقول المتهم ويقوم بمواجهته بهذا التناقض[1].

8- 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.

* – تتمثل الضوابط في كل ما يتوصل إليه المحقق من الحجج والبراهين والأدلة التي يتركها الجاني في محل الجريمة المعلوماتية.

[1] – أ /عفيفي كامل عفيفي، جرائم الكمبيوتر، بدون دار نشر، الإسكندرية، 2000، ص 154.

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

يترتب عمليات التفتيش آثار متعددة اهمها حجز كل المنظومة ويتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهما على دعامة تخزين الكترونية تكون قابلة للوضع والحجز 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.[1]

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- شروط صحة الدليل المستخلص من التفتيش الالكتروني:

ومن ثمة لابد من التعرف على الشروط الواجب توافرها في الدليل الرقمي حتى يقال بأنه دليل مشروع وحتى يمكن للقاضي الأخذ به، وطالما أن التفتيش هو إجراء مطلوب من النيابة العامة[2] 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

[1] – د/ الشحات إبراهيم محمد منصور، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية، دار الفكر الجامعي الاسكندرية، 2011، ص 197.

[2] – د/ غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والأنترنت، دار الفكر والقانون المنصورة (بدون بلد نشر)، 2010، ص 211.

يجوز التعدي على تلك الحرمات فلا يتعرض لها إلا وفقا لما تقتضيه القوانين، وهذا يقود إلى نتيجة مفادها إن ا لحصول على الدليل الرقمي لابد أن يتم ضمن إجراء صحيح، فلابد للتفتيش أن يتم وفقا لشروط التفتيش، وإلا اعتبر التفتيش باطلا، كاستخدام التدليس والخداع للحصول على الدليل المستخلص من الوسائل الالكترونية ويرى الباحثون أن المشرّع استجاب للمتطلبات العملية عندما سن قوانين تواجه جرائم أنظمة المعلومات، من حيث تجريم التعدي على حريات الأفراد المتوافرة في الحواسيب والأنترنت، محيط هذه الحريات بالحماية وكما أحاط التفتيش الالكتروني بضمانات قانونية وقضائية.[1]

- أن يكون الدليل المستخلص من الوسائل الالكترونية يقينيا ومفاد ذلك أن لا يكون الدليل قابلاً للشك، وإذا 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.

2- خضوع الدليل المستخلص من التفتيش الالكتروني للمناقشة:

إن 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 وإظهار واستجلاء جوانب الدليل بحد ذاته والإجراء المستخلص من خلاله إجراءات 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 الالكتروني، ويمتد الأمر إلى أن المحكمة التي لم تستمع

[1] - أ.د/ عبد الإله هلالي أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، (دارسة مقارنة)، ط1، دار النهضة العربية، مصر، 1997، ص 180.

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 المشرّع الجزائري الحصول على الدليل الرقمي بصورة مشروعة فلا يجوز للقاضي الجنائي أن يسند في حكمه إلا على دليل تم الحصول عليه قانونية، ولابد أن يكون الدليل صحيحا لا يشوبه بطلان يتقرر بمخالفة إجراءات القانونية، لأن مشروعية الخصومة الأدلة تعتبر حدّاً لا يمكن للقاضي أن يتجاوزه، نظرا لما تقوم عليه الخصومة الجنائية من تعزيز لقرينة البراءة ومن جهة أخرى مراعاة حرية القاضي في الإثبات باعتباره ممثلا لسلطة الدولة في العقاب.[2]

أما بالنسبة لموقف المشرع الجزائري من الدليل الالكتروني في ظل التشريع الجزائري نصت المادة 212 من ق.إ.ج.ج الفقرة الأولى "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص في القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"، والقاضي الجزائري عند الفصل في النزاع المتعلق بالجريمة المعلوماتية يجد بين يديه المحضر الخاص بالتفتيش الالكتروني، هذا الأخير يرجع للسلطة التقديرية للقاضي الجنائي للأخذ به داعما هذه السلطة ببقية الأدلة المقدمة، بالإضافة إلى السلطات التي منحها له المشرّع في مجال التحقيق القضائي.[3]

[1] – د/ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الكترونية، مطابع الشرطة القاهرة، 2008، ص 259.

[2] – آمال قارة، المرجع السابق، ص 196.

[3] – راجع المادة 307 من الأمر رقم 11/21 المؤرخ في 25 أوت 2021 المتعلق بقانون الإجراءات الجزائية الجزائري.

لما كانت الضبطية القضائية مقيدة في الدعوى الجزائية بمبدأ الشرعية الجنائية والإجرائية، فإن هذه الأخيرة لا يمكنها اتخاذ إجراء 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 الأساس 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 الالكترونية يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الشرطة والمحققين والقضاة.

و عليه ساير المشرّع الجزائري في ذلك المجتمع الدولي من أجل مكافحة الجريمة المعلوماتية حيث بادر إلى وضع استراتيجية شملت استحداث نصوص قانونية خاصة بمقتضى القانون 04/09 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 الإجراءات ضبط ما استعمل في ارتكاب الجريمة أو نتج عنها.

الخاتمة

أصبحت جميع القطاعات تعتمد في آداء عملها على استخدام الأنظمة الالكترونية مما وسّع في مجال الإجرام المعلوماتي ليمسّ الجرائم الواقعة على الأشخاص، الجرائم الواقعة على الاموال، الجرائم الماسة بأمن الدولة.

و على هذا الأساس حدد المشرّع الجزائري القواعد الإجرائية التي تتناسب ومتطلبات الحماية القضائية للحقوق محل الاعتداء متابعة للجرائم لمعلوماتية، وتجسيد التفتيش الالكتروني كمتطلب لضبط الدليل الرقمي، من خلال الانضمام إلى العديد من الاتفاقيات الدولية، بالإضافة لاستحداث إجراءات خاصة 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.

أهم النتائج التي تم استخلاصها في موضوع دراستنالإجراء التفتيش الالكتروني عدم تناسب أحكام قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم الجرائم التقليدية، وعدم توافقه مع أحكام الجرائم المعلوماتية المستحدثة لتميزها بالمرونة لذا استحدث المشرّع القانون رقم 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها إلا أن الإشكالات الإجرائية في مجال المتابعات تعد أول عائق في غياب التأهيل الفني لجهات التحقيق الذي يؤدي إلى اتلاف الدليل وإفلات مرتكبي هذه الجرائم من العقاب، وبالنظر إلى أن التفتيش الالكتروني لم يعد قادرا على استيعاب كافة الجرائم المعلوماتية لاستخدامها اساليب متطورة ومتحولة، مما ساهم في خلق إشكالات على صعيد الملاحقة الجنائية في إطار القوانين والدولية مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانون 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 والأهداف بعد المصادقة على المعاهدات الدولية.

لاحظنا من النتائج أعلاه أن المشرّع الجزائري قد عمل جاهداً على سن نصوص عقابية موضوعية وإجرائية لمكافحة الجريمة المعلوماتية مواكبا بذلك التشريعات المتطورة، إلا أنه تبقى العديد من الثغرات التي تحول دون التطبيق الجيد للنصوص والمراسيم التي استحدثها المشرّع وفي الختام وتأسيساً على المعطيات السابقة ارتأينا الخروج بالاقتراحات التالية:

– إجراء تعديلات في الأحكام المتعلقة بالتفتيش الالكتروني حتى يصل المشرّع إلى مكافحة أكثر فعالية لهذا النوع المستحدث والمتطور من الإجرام المعلوماتي وتقديم المقترحات والحلول البديلة لتتناسب والوسائل الاجرامية الحديثة.

– إصدار تشريع خاص ومستقل للجرائم الالكترونية بوضع إجراءات جنائية تنسجم مع طبيعة هذا النمط من الجرائم، وتحديد ضوابط التفتيش الالكتروني وأحكامه الإجرائية المختلفة.

– النص على ضرورة حضور المتهم أو محاميه إجراءات الإطلاع على نتائج التفتيش الالكتروني لتأكيد سلامة الإجراء وضمان حقوق الدفاع أيضا، واحترام الضم انات التي يكرسها الدستور والقوانين الإجرائية.

–عقد دورات مكثفة للإطارات العاملة في حقل التحري الشرط وي والتحقيق في مجال جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب،

– الاستفادة من تجارب أو خبرات الدول المتطورة في مجال التفتيش الالكتروني واستغلال الإجراءات الوقائية لمنع وقوع الجريمة،

– ضرورة مواكبة القوانين للتطورات واستيعابها للتطور المتلاحق في مجال تقنية المعلومات والاتصالات وما يقابله من استغلال الجناة لهذه التقنية المتطورة بابتكار أساليب جديدة لارتكاب الجرائم الالكترونية،

– استحداث شعبة خاصة لمكافحة الجرائم الالكترونية،

– خلق إخصائيين تقنيين في مجال تسهيل عمليات التفتيش الالكتروني،

– ضرورة إزالة العقبات فيما يتعلق بموضوع الجرائم الالكترونية من خلال الإنضمام إلى الاتفاقيات الجماعية ذات العلاقة بالجرائم الالكترونية أو 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، ومتابعة الجرائم الالكترونية،

– سن قانون مستقل جديد كامل، يبين فيه جميع الآليات الموضوعية و الإجرائية الخاصة بالجرائم الالكترونية،

– إنشاء وحدات متخصصة على المستوى الدولي والعربي، تهتم بالتنسيق بين الدول في مجال متابعة ومعاقبة مرتكبي الجرائم الالكترونية.

قائمة المصادر والمراجع:

أولا: النصوص القانونية

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات محررة بالقاهرة في 2010/12/21 صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في 2014/09/08، الجريدة الرسمية رقم 57، الصادرة بتاريخ 2014/09/28.
- المرسوم الرئاسي 251/20 المؤرخ في 15 سبتمبر سنة 2020 المتضمن التعديل الدستوري، الجريدة الرسمية رقم 98.
- القانون 01/06 المؤرخ في 20 فيفري سنة 2006، المتعلق بالوقاية من الفساد ومكافحة الجريدة الرسمية رقم 37.
- القانون 04/09 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47.
- القانون رقم 07/18 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي المؤرخ في 10 جوان 2018 الجريدة الرسمية عدد 50.
- الأمر 11/21 المؤرخ في 26 أوت 2021 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 65.
- 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، الصادرة في 08 أكتوبر سنة 2015.

- المرسوم التنفيذي 348/06 المؤرخ في 5 أكتوبر سنة 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق الجريدة الرسمية رقم 13.

القرارات القضائية.

- قرار المحكمة العليا بتاريخ 1997/07/30، ملف رقم 165609، المجلة القضائية لسنة 1997 العدد 02.

ثانيا: الكتب

الكتب العامة:

- أحسن بوسقيعة، التحقيق القضائي، ط2، دار هومه، الجزائر، 2012.
- أحمد السيد عفيفي، الأحكام العامة للعلانية في قانون العقوبات (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2002.
- أحمد المهدي، القبض والتفتيش والتلبّس، ط1، دار العدالة، القاهرة، 2007.
- أحمد عبد الحكيم عثمان، تفتيش الأشخاص وحالات بطلانه، منشأة المعارف، الإسكندرية، 2002.
- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994.
- يوسف دلاندة، قانون الإجراءات الجزائية، دار هومه، الجزائر، 2001.

الكتب المتخصصة:

- أمال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، الهيئة المصرية العامة للكتاب، القاهرة، 1991.
- الشحات إبراهيم محمد منصور، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية، دار الفكر الجامعي، الاسكندرية، 2011.

- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن، دار الفكر الجامعي، الإسكندرية 2008.
- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، (بدون بلد نشر)، 2000
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، عمان – الأردن، 2011.
- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012.
- زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.
- سامي الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، دار النهضة العربية، القاهرة، 1980.
- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي (دراسة مقارنة)، دار الجامعة الجديدة، الإسكندرية، 2009.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2009.
- عبد الله أوهايبية، ضمانات الحرية الشخصية أثناء مرحلة البحث التمهيدي، الاستدلال، ط1، الديوان الوطني للأشغال التربوية، 2004.
- عبد الله بن سعود محمد السران، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني، جامعة نايف العربية للعلوم الأمنية، ب ط، 2011.
- عفيفي كامل عفيفي، جرائم الكمبيوتر، بدون دار نشر، الإسكندرية، 2000.
- علي إبراهيم توفيق، دور المحقق في الجرائم الالكترونية، ط3، دار المدى للنشر والتوزيع، العراق، 2000.

- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت (دراسة مقارنة)، عالم الكتاب الحديث، إربد، الأردن، 2004.
- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث، العراق، 2011.
- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والأنترنت وجرائم الاحتيال المنظم باستعمال شبكة الأنترنت، دار الفكر والقانون، المنصورة، مصر، 2010.
- فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الأردن والمقارن، ج2، دار الفارابي، عمان، 1980.
- كوثر سعيد عدنان خالد، حماية المستهلك إلكتروني، دار الجامعة الجديدة، الاسكندرية، 2012.
- محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، ط1، دار الثقافة ،عمان – الأردن، 2004.
- محمود إبراهيم غازي، الحماية الجنائية للصوصية والتجارة الالكترونية، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2013.
- مصطفى محمد موسى، التحقيق الجنائي في الجرائم إلكترونية، مطابع الشرطة القاهرة، 2008.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان – الأردن، طبعة 2010.
- هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، ط1، دار النهضة العربية، القاهرة، مصر، طبعة 1992.
- هلالي عبد الإله أحمد حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، القاهرة. بدون سنة نشر.

- هلالي عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، ط1، دار النهضة العربية، 2007.
- هلالي عبد الإله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، (دراسة مقارنة)، ط1، دار النهضة العربية، بدون دار النشر، 1997.
- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الألية للمعطيات- دراسة مقارنة، دار الخلدونية للنشر والتوزيع، الجزائر، 2018.

ثالثا: الرسائل والمذكرات

مذكرات الماجستير

- نعيم سعيدان، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة باتنة، السنة الجامعية 2012.
- قارة أمال، الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، 2002.
- نورة صرشي، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2012.

مذكرات الماستر:

- منصورية بلعيد، النظام الإجرائي للجريمة المعلوماتية، مذكرة لنيل الماستر في تخصص القانون القضائي، جامعة بن باديس مستغانم، السنة الجامعية 2020.
- رابح مباركية، إجراءات التحري والتحقيق في الجريمة الالكترونية، مذكرة لنيل الماستر في تخصص قانون الإعلام الآلي والأنترنت، جامعة محمد الإبراهيمي، جامعة برج بوعريريج، السنة الجامعية 2022/2021.

رابعا: المجلات العلمية

- عز الدين عثمان، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، جامعة الوادي، الجزائر، عدد 4، 2018.

- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، عدد 05، 2012.

- نجاة لوصيف، موسي مرمون، مبادئ وضوابط المعالجة الآلية للمعطيات الشخصية، مجلة العلوم الانسانية، جامعة بسكرة، المجلد 33، عدد 02 جوان 2022.

- سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري، المجلد 7، كلية الحقوق جامعة الجزائر، العدد 01، جوان 2000.

- نوارة حسين، آليات تنظيم المشرّع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، منشور في مجلة الدراسات القانونية لأعمال ملتقى آليات مكافحة الجرائم الالكترونية، كلية الحقوق جامعة الجزائر.

- عبد الصديق شيخ، الوقاية من الجرائم الالكترونية في ظل القانون رقم 04/09، مجلة معالم الدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة المدية، الجزائر، المجلد 04، العدد 01، 2020.

خامساً: الملتقيات والأعمال الدراسية

الملتقيات:

- حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، مجلة الحقوق كلية الحقوق جامعة بسكرة، العدد 33، طبعة 2016.

سادسا: 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.

سابعا: مواقع الأنترنت

- http://nidhaltechnologie.own0.com/t60-topic

−http://www.uobabylon.edu.iq/uobColeges/service_showrest.aspx?fid

−http://salahgardafi.eb2a.com.content.

http//:kenonaonline.com

فهرس المحتويات:

الفصل الثاني الأحكام الإجرائية للتفتيش الالكتروني

ملخص:

عرف العالم الحديث طفرة جد كبيرة في ميدان تكنولوجيات الإعلام والاتصال، ولِما يتجلى من انتشار واسع للأنرتنت حمل في طياته أنواع شتى من الجرائم المعلوماتية الناجمة عن الاستغلال غير المشروع لهاته التكنولوجيا، وأمام التجلي الواسع لهذه الظاهرة وجد المشرع نفسه ملزماً بمواجهة هذا الانتشار الخطير للجريمة المعلوماتية، وذلك بإقرار نصوص قانونية تنظم ضوابط التفتيش الالكتروني بقصد مواجهة الجرائم التي تهدد الأمن المعلوماتي، مع استحداث أجهزة من أجل مكافحة الجريمة المعلوماتية، كما نجد أن المشرع الجزائري أقر التفتيش الالكتروني بالاستناد إلى العديد من الأنظمة الموضوعية والإجرائية للكشف عن الأدلة الرقمية محل كشف حقيقة نتيجة الاستخدام الواسع للتقنيات الرقمية بمختلف أنواعها والتي من شأنها تفعيل النصوص والضوابط القانونية المعتمدة للتصدي لظاهرة الجريمة المعلوماتية، حيث تتجلى إرادة المشرع الجزائري للتصدي لهذه الظاهرة في سعيه دوليا إلى إبرام العديد من الاتفاقيات الدولية لوضع قواعد قانونية دولية واستراتيجيات متكاملة تخدمه لتطوير تقنياته في التفتيش الالكتروني و تكييف القوانين بما يجاري التطور الحاصل في ميدان تكنولوجيا الاعلام والاتصال وما ترتب عنها من جرائم معلوماتية.

الكلمات المفتاحية:

التفتيش – الإلكتروني

Abstract:

The modern world has seen a very significant breakthrough in the field of information and communication technologies. In view of the widespread dissemination of the Internet, various types of information crimes resulting from the illicit exploitation of such technologies have been introduced. In the face of the widespread manifestation of this phenomenon, the legislature has found itself obliged to deal with this dangerous proliferation of information crime by adopting legal provisions regulating electronic inspection controls with a view to countering crimes that threaten information security. The Algerian legislature has also adopted electronic inspections on the basis of a number of objective and procedural regulations for the detection of digital evidence. This is the result of the extensive use of digital technologies of various kinds, which would give effect to the legal provisions and controls adopted to deal with the phenomenon of information crime. The Algerian legislature will to combat this phenomenon is reflected in its international efforts to establish international legal norms and integrated strategies for the development of its electronic inspection techniques and the adaptation of laws in order to keep pace with the development of information and communication technologies and the resulting information crimes.

Keywords:

Electronic - inspection.