جامعة محمد الصديق بن يحي –جيجل–

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة بعنوان:

الإطار القانوني للتفتيش في الجرائم الإلكترونية

مذكرة مكملة لنيل شهادة الماستر في الحقوق

تخصص: المهن القانونية والقضائية

إعداد الطالبة:

- حمدان شيماء

إشراف الأستاذة:

د. حايد سعاد

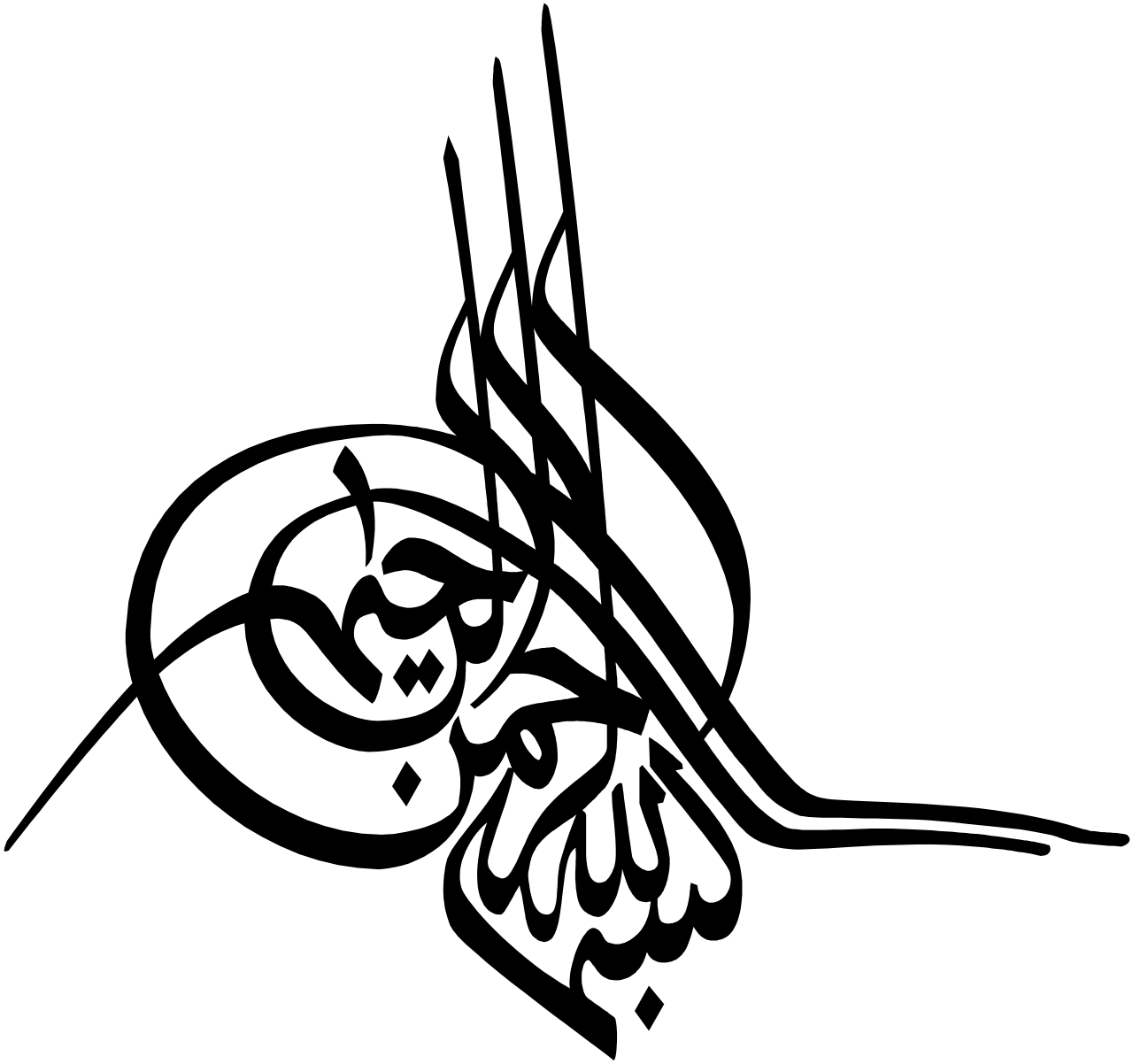
المشرف الميداني:

المحامية: مخلوف هناء

أعضاء لجنة المناقشة

اسم ولقب الأستاذ(ة)	الرتبة العلمية	الجامعة	الصفة
بوزبرة سهيلة	أستاذ محاضر –أ–	جامعة جيجل	رئيسا
حايد سعاد	أستاذ محاضر –أ–	جامعة جيجل	مشرفا ومقررا
عميور خديجة	أستاذ محاضر –ب–	جامعة جيجل	ممتحنا

السنة الجامعية 2023/2022


بسم الله الرحمن الرحيم

شكر وتقدير

بسم الله الرحمان الرحيم

إنطلاقا من قول الرسول صلى الله عليه وسلم:

"من لم يشكر الناس لم يشكر الله"

نشكر الله عز وجل أن أنعم علي بإتمام هذا العمل.

ومن ثم يقتضي مني واجب الشكر والإعتراف بالفضل أن أتقدم وبخالص الشكر والإمتنان للأستاذة المشرفة "**حايد سعاد**" على إشرافها ومتباعتها لهذه المذكرة وعلى توجيهاتها القيمة ونصائحها الهادفة للتوضيح لي ويسهل ما تعسر لي.

كما نتقدم بجزيل الشكر والتقدير والإمتنان إلى أعضاء المناقشة لقبولهم مناقشة هذا العمل (المذكرة).

كما أتوجه بالشكر والامتتنان إلى المشرف الميداني "**مخلوف هناء**" على مدها لي يد المساعدة في إنجاز هذا العمل العلمي.

كما أتوجه بالشكر إلى مديرية الأمن الولائي بجيجل.

"

إهداء:

الحمد لله الذي أعانني ووفقني على هذا الجهد.

أهدي هذا العمل المتواضع إلى كل أفراد العائلة الكريمة.

إلى والدي الكريمين نسأل الله أن يحفظهما ويرعاهما لنا.

وإلى منبع المحبة وسندي في الدنيا أختي الغالية وإخواني.

إلى كل الأهل والأقارب وجميع الأصدقاء والزملاء.

إلى كل من قدم يد المساعدة وساعدني في إنجاز هذا العمل

ولو بكلمة وبالأخص الأخت سعيدة

إلى كل هؤلاء أهدي هذا العمل المتواضع وثمرة جهدي.

"شيماء"

قائمة المختصرات:

ج ر: الجريدة الرسمية.

ق إ ج ج: قانون الإجراءات الجزائية الجزائري.

ص: الصفحة.

ص ص: من الصفحة إلى الصفحة.

د س ن: دون سنة نشر.

مقدمـــــــة

مقدمــة:

يستهدف التفتيش البحث والاستقصاء في محل 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.

ومن دون أي شك أن الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها قد تركت آثار إيجابية وشكلت قفزة نوعية في المجتمع ككل، وذلك نظرا لما تتميز به من عنصري السرعة والدقة في تجميع وتخزين ومعالجة المعلومات، ومن ثم نقلها وتبادلها بالصوت والصورة عبر أنحاء العالم.

لكن على الرغم من المزايا الهائلة التي حققتها تقنية المعلومات إلا أن هذا لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، بالإضافة إلى أن العلماء قاموا بتطوير شيء جديد يسمى بعلم الإجرام المعلوماتي الذي يعد من قبيل علم الإجرام الخفي الذي يرتكبه الجاني في الخفاء، وبالتالي يصعب الوصول إلى مرتكبيه أو القائم به.

ونظرا لخطورة هذا العلم الإجرامي ومساسه لمصالح المجتمع كالمساس بالحياة الخاصة للأفراد والمساس باعتبار وشرف الأشخاص، تسعى الدولة القانونية إلى إقامة حالة من التوازن بين حق المجتمع في إيقاع العقاب على من يقومون بجرائم الحاسوب والأنترنت، وبين المحافظة على حقوق الإنسان في مجال الإجراءات الجزائية، وأشد هذه الإجراءات التفتيش، لأنه يتصل بحرية الأفراد ومستودع سرهم وحرمة مساكنهم.

مقدمــة:

فالتفتيش في الجريمة الإلكترونية يعد من أصعب أنواع التحقيق، ويرجع ذلك إلى التطور المذهل في تكنولوجيا الإعلام والاتصال، وإن كان ذلك يخضع للقواعد المتعارف عليها في التفتيش طبقا لقانون الإجراءات الجزائية، إلا أنه يتميز بخصوصية معينة نظرا لطبيعة الجريمة المستهدفة وطبيعة مرتكبيها، فضلا عن مسرح الجريمة الذي هو عبارة عن بيئة افتراضية، وفي هذه الأطر تأتي هذه الدراسة كمحاولة لتسليط الضوء على إحدى هذه المشكلات وهي التفتيش على نظم الحاسوب والأنترنت.

وتكمن أهمية البحث في بيان الدور الذي يعهد به المشرع لضباط الشرطة القضائية في حالة التلبس بالجريمة أو الندب لمباشرة إجراء القبض والتفتيش وذلك الإجراء يمس الحريات الشخصية للأفراد خروجا عن الأصل المقرر من أن لكل شخص الحق في الحفاظ على أسراره، لكن الضرورة الإجرائية التي يسعى التفتيش إلى تحقيقها قد اقتضت الخروج من هذا الأصل.

ويعود سبب اختيار هذا الموضوع إلى الرغبة في دراسة هذه الجريمة المستحدثة وتبيان خصوصية التفتيش في هذا النوع من الجرائم، وهذا الموضوع لا يزال يستقطب اهتمام الباحثين والمختصين وذلك بسب انتشارها الواسع في الآونة الأخيرة.

أما بالنسبة للأسباب الموضوعية فهذا الموضوع يتميز بحداثته كون أن الجريمة الإلكترونية ظاهرة مستجدة نسبيا، ولهذا يتوجب على البشرية التنبه لأهمية وحجم المخاطر الناجمة عنها باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، فهذه الجرائم تحتاج إلى دقة وخبراء مختصين لإخراج هذه الأدلة الهامة أثناء التفتيش عن المعلومات الجنائية الإلكترونية.

وبهذا تسعى هذه الدراسة إلى تسليط الضوء على إجراءات التفتيش في الجرائم الإلكترونية من خلال الوقوف على النصوص والأحكام القانونية المنظمة لإجراء التفتيش الإلكتروني من خلال الكشف عن الأدلة التي ترتكب بها هذه الجريمة وكذا الوصول إلى مرتكبيها.

وعليه يمكن صياغة الإشكالية التالية:

مقدمــة:

ما مدى فعالية التفتيش الإلكتروني باعتباره إجراء للتحقيق في الكشف عن الجريمة الإلكترونية؟

وقد تمت معالجة هذه الإشكالية وفق المنهج الوصفي التحليلي من خلال وصف التفتيش الإلكتروني في الجريمة الإلكترونية، وتحليلي من خلال تحليل النصوص القانونية الواردة في قانون الإجراءات الجزائية الجزائري، ونصوص خاصة كالقانون رقم 09-04 التي تتعلق بتكنولوجيات الإعلام والاتصال، وكيفية استخدامها في التحقيق الجنائي.

ومن أجل دراسة هذه الإشكالية تم تقسيم هذا البحث إلى فصلين:

الفصل الأول بعنوان: ماهية التفتيش في الجريمة الإلكترونية، حيث عالجت مفهوم التفتيش في الجرائم الإلكترونية في المبحث الأول منه، أما المبحث الثاني من هذا الفصل تناولت فيه ضوابط التفتيش في الجريمة الإلكترونية.

الفصل الثاني بعنوان: إجراءات التفتيش في الجرائم الإلكترونية، بينت في المبحث الأول الآليات القانونية الخاصة بالتفتيش في الجرائم الإلكترونية، وفي المبحث الثاني لهذا الفصل تطرقت للآثار المترتبة عن إجراءات التفتيش في الجرائم الإلكترونية.

الفصل الأول: ماهية التفتيش في الجريمة الإلكترونية.

الفصل الأول: ماهية التفتيش في الجريمة الإلكترونية

من المعلوم أنه من حق الفرد أن يتمسك بمستودع أسراره باعتبارها حقوق تخصه وحده، وهي جزء مهم من حياته اليومية، سواء كان ذلك في مسكنه أو مراسلاته أو معلومة مخزنة في جهاز الحاسب الآلي الخاص به أو نظامه المعلوماتي، وهذا الحق يعتبر من الحقوق الدستورية التي لا يمكن لأحد انتهاكها دون سبب قانوني، ولكن قد يتطلب الأمر في بعض الأحيان الوصول إلى هذه الأسرار وكشفها بحثا عن الحقيقة التي يتطلبها القانون، ولا يكون ذلك إلا بموجب إجراء نصّ عليه القانون تحت اسم التفتيش.

فمحل التفتيش في الجرائم التقليدية قد يكون مسكنا أو شخصا، وقد يتعلق التفتيش بالمتهم سواء انصب على مسكنه أو شخصه، وقد ينصب على مسكن غير المتهم أو شخص غير المتهم، وهو في كل الأحوال تفتيش جائز بالشروط القانونية المقررة.

ولكن مع التطور التكنولوجي للاتصالات الذي يشهده العالم حاليا والذي استفاد منه عالم الإجرام، وجدت جرائم حديثة يطلق عليها مصطلح الجرائم الالكترونية والتي أثارت العديد من المشكلات في نطاق قانون الإجراءات الجزائية، حيث وضعت نصوص هذا القانون لتحكم الإجراءات المتعلقة بالجرائم التقليدية التي لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع إخضاعها لمبدأ حرية القاضي الجنائي في الاقتناع، وصولاً إلى الحقيقة الموضوعية بشأن الجريمة والمجرم، أما في الجرائم الالكترونية فيتسم إجراء التفتيش فيها بالعديد من المعوقات والصعوبات، نظرا لوقوع الجريمة الإلكترونية ضمن بيئة رقمية كامنة في أجهزة الحاسب الآلي ومختلف شبكاته.

من أجل كل هذا كان لا بد علينا من إبراز مفهوم التفتيش في الجريمة الإلكترونية (المبحث الأول) ثم ضوابطها (المبحث الثاني).

الفصل الأول: ماهية التفتيش في الجريمة الإلكترونية

المبحث الأول: مفهوم التفتيش في الجريمة الالكترونية:

يعرف التفتيش بأنه إجراء من إجراءات التحقيق التي تستهدف البحث عن الحقيقة في مستودع السر من أجل كشفها، لأنه غالبا ما يصدر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم في محل يتمتع بحرمة المسكن أو الشخص، أما التفتيش في الجريمة الالكترونية فهو إجراء صعب بالنظر إلى طبيعة الدليل المتحصل منه، والذي يسهل إخفاءه وتدميره كونه يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الشرطة والمحققين، ولهذا سنتناول التعريف بالجرائم الالكترونية وأهم خصائصها والوسائل التقنية لارتكابها (المطلب الأول)، ثم نتطرق إلى التعريف بالتفيش الالكتروني والطبيعة القانونية لتفتيش المنظومة المعلوماتية ومدى قابلية مكونات الحاسوب للتفتيش (المطلب الثاني).

المطلب الأول: التعريف بالجريمة الالكترونية.

إن الحداثة النسبية للجريمة الإلكترونية وارتباطها بتقنيات الحاسوب وشبكة الأنترنت المتطورة باستمرار، استقطبت اهتمام المتخصصين في مجال المعلوماتية والفقهاء لوضع تعريف شامل لها، باعتبارها ظاهرة جديدة مازالت قيد البحث والدراسة من طرف القانونيين، والعديد من الفقهاء، وبالمثل لا يوجد تعريف محدد ومتفق عليه لهذا النوع المستحدث من الجرائم، حيث سنعرف الجريمة الالكترونية (الفرع الأول) ونذكر خصائصها (الفرع الثاني)، والوسائل التقنية الحديثة ارتكابها (الفرع الثالث).

الفرع الأول: تعريف الجريمة الإلكترونية.

تعتبر الجريمة الإلكترونية جريمة حديثة نظرا لارتباطها بتقنية متطورة في تكنولوجيا المعلومات والاتصالات، مما صعب من وضع تعريف جامع لها، لذا بذل الفقهاء جهودا مضنية في محاولتهم تعريفها، حيث برز اتجاهان هما: الاتجاه الأول يعرف بالاتجاه الضيق في تعريفه للجرائم الإلكترونية، ويعرف الثاني بالاتجاه الموسع لها.

أولا: الاتجاه الضيق لتعريف الجريمة الالكترونية.

يذهب أنصار هذا الاتجاه إلى حصر الجريمة الالكترونية في الحالات التي تتطلب قدرا من المعرفة التقنية لارتكابها، حيث تعد الجرائم التي لا تستدعي هذه المهارة جرائم تقليدية تخضع للنصوص العقابية التقليدية.[1]

ومن التعريفات الضيقة للجرائم الالكترونية التي استندت إلى وسيلة ارتكاب هذه الجريمة وموضوعها، التعريف الذي يرى " بأنها تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات." أو هي " كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومة المخزنة داخل الكمبيوتر، أو تلك التي يتم تحويلها عن طريقه.[2]

وعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا.[3]

أما بالنسبة للتعريفات التي تقوم على أساس صفات شخصية في مرتكب الفعل، فهناك من الفقهاء من عرفها بأنها: أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها، أو هي ما تعرف بأنها أية جريمة متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب.[4]

فرغم كل اجتهادات الفقهاء لإعطاء تعريف للجريمة الالكترونية وفق هذا الاتجاه، إلا أن هذا الأخير يتميز بالنقصان في تعريفه للجريمة الالكترونية والتضييق من مفهومها. إذ ركز بعض الفقهاء على موضوع الجريمة وركز البعض الآخر على وسيلة ارتكابها، في حين ركز

---

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، الجزائر 2012 / 2013، ص 27.

[2] عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، مصر، 2012، ص40.

[3] كان مكتب تقييم التكنولوجيا (OTA) أحد مكاتب الكونغرس الولايات المتحدة من عام 1972 إلى عام 1995 كان الغرض منه هو تزويد أعضاء الكونغرس ولجانه بتحليل موضوعي وموثوق للقضايا العلمية والتقنية المعقدة في أواخر. القرن العشرين أي تقييم التكنولوجيا.

[4] أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والأنترنت، مكتبة الوفاء القانونية، مصر، 2011، ص 66.

آخرون على فاعل الجريمة، بينما نجد بأن الجريمة الالكترونية قد تقع على الحاسب الآلي بشقيه المادي والمعنوي.[1]

ثانيا: الاتجاه الموسع لتعريف الجريمة الالكترونية.

على عكس الاتجاه السابق، يذهب فريق من الفقهاء إلى التوسع في مفهوم الجرائم الالكترونية، وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية، حيث تعرف بأنها " كل فعل إجرامي أو أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل".[2] أو هي " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، ويكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية.[3]

ومن بين أهم التعريفات الذي ذكرها الفقهاء أيضا " أنها سوء استخدام الحاسب الآلي ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذا الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق الكترونية وتزييف المكونات المادية والمعنوية للحاسب، وسرقة الحاسب الآلي في حد ذاته أو أي مكون من مكوناته ".[4]

وهناك من الفقهاء من يرون أن تعريف الجريمة الالكترونية هي " كل فعل أو امتناع عمدي، ينشأ من الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية، أو هي عمل أو امتناع يلحق أضرار بمكونات الحاسب، وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا ".[5]

---

[1] محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، الجريمة المعلوماتية، الإصدار الثاني، دار الثقافة، الأردن، 2007، ص09.

[2] حنان ريحان المبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2014، ص 26.

[3] أمير فرج يوسف، مرجع سابق، ص 67.

[4] حنان ريحان المبارك المضحكي، مرجع سابق، ص 28.

[5] أشرف عبد القادر قنديل، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة الحديدة، مصر، 2015، ص93.

ومن جانبنا تقترح التعريف الآتي " كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على تقنية المعلوماتية أيّا كان غرض الجاني ".

أما بالنسبة للتعريف القانوني، فإن المشرع الجزائري قد اصطلح على تسمية الجرائم الإلكترونية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة 02 من القانون 09-04 [1] " على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية ".

ومن خلال هذا التعريف نستنتج أن المشرع الجزائري قام بتبني معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر 7، وترك المجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية. [2]

الفرع الثاني: خصائص الجريمة الالكترونية.

من التعاريف السابقة يمكننا أن نستخلص بعض الخصائص التي تتميز بها الجرائم الالكترونية عن باقي الجرائم العادية التقليدية، لعل أبرزها ما يأتي:

أولا: جرائم عابرة للحدود.

من أهم الخصائص التي تميز الجريمة الالكترونية أنها جريمة تتخطى الحدود الجغرافية لاتصالها بعالم الأنترنت وتقنية المعلومات، حيث قد تتأثر دول كثيرة بهذه الجريمة في آن واحد، بسبب السرعة الهائلة في تنفيذها، يمكن أن تقع الجريمة من طرف الجاني في دولة

---

[1] القانون رقم 09 – 04 الصادر في 05 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، العدد 47، سنة 2009.

[2] القانون رقم 04-15 الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم156/66 الصادر في 8 جوان 1966، المتضمن قانون العقوبات، ج ر، العدد 71، سنة 2004.

والمجني عليه في دولة أخرى في وقت يسير جداً،[1] حيث يفصل بين الدول آلاف الأميال مما خلف مشكلات قانونية عديدة، كتحديد الدولة صاحبة الاختصاص القضائي، وكذا القانون الواجب التطبيق، إضافة إلى الإشكالات المتعلقة بإجراءات الملاحقة القضائية وصعوبة التعاون القضائي بين الدول نظرا لطبيعة هذه الجرائم.[2] وكمثال على ذلك قضية الإيذز.[3]

ثانيا: الصعوبة في اكتشاف هذا النوع من الجرائم وإثباتها.

تتميز الجريمة الإلكترونية بصعوبة متابعتها واكتشافها، فهي لا تترك أثراً نظراً لأنها مجرد أرقام تتغير في السجلات فهي تفتقر إلى الدليل المادي التقليدي كالبصمات.

وترجع صعوبة إثباتها إلى الأسباب التالية:

– أن هذا النوع من الجرائم المعلوماتية لا تترك أثارا مادية ملموسة في محيطها، بل ترتكب في الخفاء دون أي آثار كالجرائم التقليدية.

– مما لا شك فيه أن المجني عليه في الجرائم المعلوماتية عادة يتجنب الإبلاغ عن هذه الجرائم، وهذا لعدة أسباب منها عدم قدرته الفنية التي تمكنه من اكتشاف الجريمة أو خوفا من الإضرار بمصالحه، لا سيما إذا وقعت الجريمة على مؤسسات مالية ومصرفية أو تجارية كبيرة فربما يؤدي الإبلاغ عن الجريمة إلى تأثر المؤسسة أو مركزها المالي الى خسائر.[4]

– سهولة إزالة أدلة إدانة الجاني خلال فترة بسيطة وبالتالي اختفاء الأدلة بسهولة.

---

[1] باطلي غنية، الجريمة الإلكترونية، دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، 2015، ص 33.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 51.

[3] لقد كانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الأيدز) من القضايا التي لفتت الانتباه إلى البعد الدولي للجرائم المعلوماتية، وتتلخص وقائعها التي حدثت سنة 1989 في أن الجاني "جوزيف بوب" (الذي كان أول من حوكم بتهمة إعداد برنامج خبيث) قام بتوزيع عدد كبير من نسخ برنامج يحتوي على فيروس "حصان طروادة" على أنه يهدف إلى إعطاء بعض النصائح حول مرض نقص المناعة المكتسبة، حتى يتمكن من طلب مبلغ مالي من المجني عليه مقابل مضاد الفيروس. حيث وبعد أن تم القبض عليه في أوهايو الأمريكية لسنة 1990، طالبت المملكة المتحدة بتسليمه وتمت محاكمته وتوجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة. نهلا عبد القادر المومني، نفس المرجع، ص 52.

[4] محمد أحمد عياينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2006، ص37.

– قلة الخبرة الفنية، وذلك أن هذا النوع من الجرائم يتطلب خبرة فنية عالية وإلماماً واسعا باستخدام الحاسوب.

– أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها بما أن الجاني لا يعطي معلومات صحيحة في العالم الافتراضي.[1]

ثالثا: الجرائم الإلكترونية جرائم ناعمة.

تتميز الجرائم الإلكترونية بأنها جرائم ناعمة، لا تتطلب أي نوع من المجهودات العضلية مثل الجرائم التقليدية كالسرقة والاغتصاب والقتل، بل أنها تحتاج إلى القدرة الذهنية والعقلية للجاني وإلمامه الجيد بتقنيات الحاسوب، بحيث تمكنه هذه الميزات من ارتكاب الجريمة وخلال لحظات دون أن يترك أثراً.[2]

وهناك عدة خصائص يتميز بها المجرم المعلوماتي عن غيره من المجرمين العاديين، ويمكن حصر هذه الخصائص في الآتي:

–المجرم المعلوماتي هو شخص ذو مهارات فنية عالية متخصص في الاجرام المعلوماتي، قادر على استخدام خبراته في الاختراقات وتغيير المعلومات، وعلى تقليد البرامج أو تحويل الأموال، وغيرها، محترف في التعامل مع الوسائل التقنية والأنترنت، اجتماعي يمكنه التكيف مع الآخرين.[3]

–يمتاز بالمستوى المعرفي والذكاء في استعمال وسائل التكنولوجيا الحديثة.

[1] محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004، ص 166.

[2] أسامة أحمد المناعسة، جرائم الحاسب الآلي، دار وائل للنشر والتوزيع، عمان، 2001، ص107.

[3] أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، سنة 2021/2020، ص 29.

–يتميز المجرم المعلوماتي بأنه عائد للجريمة دائما فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات وقد لا يحقق الاختراق بهدف الإيذاء بل بهدف تطوير مهارته وقدرته على الاختراق.[1]

–يعتمد على القوة الفكرية لا العضلية، مما يرتب خسائر فادحة خاصة في الدول المتقدمة.

–استخدام المجرم المعلوماتي لوسائل الدفع الالكتروني يشكل خطرا يفوق ما يترتب عن الجرائم التقليدية.

–مجرم فضولي محترف يعمل على تطوير قدراته التقنية باستمرار.[2]

ومن حيث أنماط مجرمي المعلوماتية:

يمكن تصنيف مرتكبي الجرائم الالكترونية على أساس أغراض الاعتداء إلى الفئات التالية:

الفئة الأولى المخترقون وتضم نوعين من المتطفلين الهاكرز والكراكز، أما الفئة الثانية فتشمل المحترفين وتعد الأخطر من بين مجرمي التقنية، حيث تهدف اعتداءاتهم أساسا إلى تحقيق الكسب المادي، أو تحقيق أغراض سياسية.

أما الفئة الثالثة والمتمثلة في فئة الحاقدين لا يسعون إلى إثبات قدراتهم الفنية ولا إلى مكاسب مادية، فما يحرك نشاطهم سوى الرغبة بالانتقام والثأر من رب العمل.[3]

الفرع الثالث: الوسائل التقنية الحديثة لارتكاب الجريمة الإلكترونية:

يستعين المجرم المعلوماتي بجملة من الوسائل تختلف عن تلك المستخدمة في الجرائم التقليدية بغية تحقيق أهدافه الإجرامية التي ينشدها، ومن أهم هذه التقنيات المستخدمة لتدمير نظم المعلومات، فيروسات الحاسب الآلي، برامج الدودة والقنابل المنطقية أو الزمنية.

---

[1] أمير فرج يوسف، مرجع سابق، ص 11.

[2] أومدور رجاء، مرجع سابق، ص 30.

[3] أشرف عبد القادر قنديل، مرجع سابق، ص 118.

أولا: برنامج الفيروس:

يعرفه بعض المتخصصين في المجال المعلوماتي بأنه "برنامج يصممه بعض المتخصصين بهدف تخريبي، مع إعطائه القدرة على ربط نفسه ببرامج أخرى، ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدميره تماماً، لأن البرامج الفيروسية قادرة على الاختفاء داخل برنامج سليم مما يصعب اكتشافها، كما أنها قادرة على الانتشار بسرعة كبيرة داخل الذاكرة ثم اختيار المكان المناسب لنسخ نفسها وتدمير برامج أو تغيير معلومات،[1] وهي على عدة أنواع فيروس عام العدوى فيروس محدد العدوى وفيروس عام الهدف وفيروس محدد الهدف.

ثانيا: برنامج الدودة

برنامج الدودة هو برنامج معلوماتي يمتاز بقدرته على التنقل عبر شبكات الانترنت بهدف تعطيلها والتشويش عليها، بشل قدرتها على التبادل والتخريب الفعلي للملفات والبرامج ونظم التشغيل، وذلك بشغل أي حيز ممكن من سعة الشبكة،[2] إذ تعتبر برامج مخصصة لاستغلال أية فجوات في نظم التشغيل، فتنتقل إلى الحاسبات الآلية وشبكات الاتصال عبر الوصلات التي تربطها، حيث أنها تتكاثر وتنتشر أثناء عملية انتقالها[3]. ولكي تحقق عملية الانتشار أهدافها فإنها تستعمل عادة البريد الالكتروني فالدودة المعلوماتية تنتشر أساسا عبر خطوط التوصيلة الإلكترونية وتصدر معلومات غير صحيحة تؤدي في الأخير إلى إغلاق النظام. ومن أشهر أنواع برامج الديدان دودة (Kood Face) و دودة (ConFicker).[4]

---

[1] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004، ص ص 84-85.

[2] محمد أمين الشوابكة، مرجع سابق، ص 240.

[3] محمد علي العريان، مرجع سابق، ص 37.

[4] نهلا عبد القادر المومني، مرجع سابق، ص 131.

ثالثا: القنابل المعلوماتية.

وتنقسم القنبلة المعلوماتية إلى قسمين:

أ- **القنبلة المنطقية:** وهي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة ويتم وضعه في شبكة المعلومات بهدف تحديد ظروف أو حالة النظام بغرض تسهيل تنفيذ عمل غير مشروع. ومن الأمثلة الواقعية على ذلك ما قام به أحد العاملين بإدارة المياه والطاقة في الولايات المتحدة الأمريكية، بوضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها، الأمر الذي أدى إلى تخريب هذا النظام.[1]

ب- القنبلة الزمنية أو الموقوتة: خلافا للقنبلة المنطقية التي تطلق لشروط محددة، القنبلة الزمنية تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة،[2] ومن أمثلة ذلك أن شخص يعمل في نظم المعلومات في فرنسا وضع قنبلة زمنية بدافع الانتقام بعد فصله بحيث تنفجر بعد ستة أشهر بعد رحيله و ترتب على ذلك إتلاف كل البيانات المتعلقة بها.[3]

المطلب الثاني: التعريف بالتفتيش الالكتروني.

يعد التفتيش من أهم إجراءات التحري والتحقيق في الجرائم، فهو إجراء تقليدي إلا أنه عرف عدة تطورات في تطبيقه، خاصة في ظل وجود جرائم تتسم بالطابع التقني الإلكتروني، لذا قرر المشرع الجزائري تقنين التفتيش الالكتروني باستعمال تكنولوجيا الإعلام والاتصال، وفي هذا السياق ستتطرق إلى تعريف التفتيش الالكتروني في (الفرع الأول) والطبيعة القانونية لتفتيش نظم الحاسوب في (الفرع الثاني) وأخيرا مدى قابلية نظام الحاسوب للتفتيش (الفرع الثالث).

---

[1] عمرو عيسى الفقى، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، مصر 2006، ص 53.

[2] محمد علي العريان، مرجع سابق، ص99.

[3] عمرو عيسى الفقى، مرجع سابق، ص 54.

الفصل الأول: ماهية التفتيش في الجريمة الإلكترونية

الفرع الأول: تعريف التفتيش الالكتروني.

يعد التفتيش الالكتروني إجراء مستحدث في الجرائم الالكترونية نظرا لحداثة هذه الجرائم لكن يبقى التفتيش إجراء معروف منذ القدم، ومن بين أهم التعريفات تلك التي أجمع عليها الفقه الجنائي: " أن التفتيش كإجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا.[1] كما عرف التفتيش أيضا على أنه البحث في مستودع سر المتهم، عن أشياء تفيد في كشف الحقيقة ونسبتها إليه أو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، ويستوي في ذلك أن يكون المحل مسكنا أو ما في حكمه أو أن يكون شخصاً.[2]

أما تعريف التفتيش الالكتروني أو التفتيش في البيئة الافتراضية فقد اختلف الفقه حول مصطلحه، حيث اعتبره البعض ينصب على أنظمة برامج أو مواقع صفحات إلكترونية، وبالتالي المصطلح الأدق هو الولوج أو النفاذ، في حين فضل اتجاه آخر بالإبقاء على مصطلح التفتيش كونه عام يشمل التفتيش التقليدي والتفتيش الإلكتروني.[3]

نستنتج في النهاية أنه يمكن تعريف التفتيش الالكتروني بأنه إجراء من إجراءات التحقيق، يهدف إلى الوصول إلى الأدلة المنبثقة من جناية أو جنحة، تحقق وقوعها فعلاً داخل نظام

---

[1] عبد الفتاح بيومي حجاري، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، 2006، ص 192.

[2] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2012، ص 115.

[3] مانع سلمى، "التفتيش كإجراء التحقيق في الجرائم المعلوماتية"، مجلة العلوم الانسانية، عدد 22، جامعة بسكرة، جوان 2011، ص 229.

المعالجة الآلية للمعطيات، لإثبات ارتكابها ونسبتها لمتهم معين[1]، وينبغي التعامل مع الأدلة المعلوماتية بحيطة وحذر لتفادي تلفها وضياعها.

الفرع الثاني: الطبيعة القانونية لتفتيش نظم الحاسوب.

إن الحديث عن الطبيعة القانونية للتفتيش في نظام الحاسوب والأنترنت، يقتضي الرجوع إلى القواعد العامة في القوانين الإجرائية، ومن ثم الولوج إلى مجال الحاسوب والانترنت، حيث تعددت آراء الفقهاء حول طبيعة التفتيش وظهرت أربعة اتجاهات مختلفة وهي:

الاتجاه الأول: ويأخذ أصحابه في تحديدهم للطبيعة القانونية للتفتيش بالهدف منه، وبحسب هذا الاتجاه فإن غاية الإجراء الحصول على الأدلة الجرمية وضبطها وكشف حقيقتها وإزالة الغموض الذي يحيط بها، وترجيح نسبتها إلى شخص معين، مثل ضبط برامج غير مشروعة على جهاز الحاسوب الخاص بالمتهم، وتقديمها كدليل اتهام ضده أمام المحكمة.[2]

الاتجاه الثاني: أخذ أنصار هذا الرأي بوقت التفتيش، فإذا كان التفتيش اتخذ قبل فتح التحقيق كان من أعمال الاستدلال بينما يعد عملاً من أعمال التحقيق الابتدائي إذا جرى بعد فتح التحقيق.[3]

غير أن تحديد الطبيعة القانونية وفقا لمفهوم أصحاب هذا الاتجاه ستواجه صعوبة في مجال الجرائم الواقعة على الحاسوب والانترنت أو بواسطتها، فقد تضطر السلطة المختصة بالتحقيق

---

[1] هميسي رضا، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، عدد 05، جامعة الوادي، جوان 2012، ص 164.

[2] هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي: دراسة مقارنة، دار النهضة العربية، القاهرة، 1997، ص 46.

[3] دلائدة يوسف، قانون الإجراءات الجزائية، دار هومة، الجزائر، 2001، ص 46.

إلى أن تقوم ببعض التحريات، كالتنصت والتجسس المعلوماتي، ولا تستطيع أن تقوم بإجراء التفتيش بالسرعة اللازمة لضبط الأدلة.[1]

الاتجاه الثالث: وينظر أنصار هذا الاتجاه إلى التفتيش من ناحية صفة القائم به، فيعتبر التفتيش من إجراءات التحقيق إذا قامت به سلطة التحقيق، غير أن هذا الاتجاه تم انتقاده على أساس أن المشرع لا يعتد بصفة القائم بالإجراء، خاصة في حالتي الندب والتلبس، حيث يقوم به عناصر الضبطية القضائية ورغم ذلك يبقى من أعمال التحقيق.[2]

الاتجاه الرابع: يأخذ هذا الاتجاه بالمعيار المختلط، فيعد التفتيش من إجراءات التحقيق متى اتخذته سلطة التحقيق بعد تحريك الدعوى الجزائية وباشرته بقصد الكشف عن الحقيقة.[3]

وبناء على ما تقدم أرى أن الطبيعة القانونية للتفتيش الواقع على نظم الحاسوب والإنترنت، يمكن أن يحدد في ضوء الاتجاه الرابع الذي اعتبر التفتيش عملاً من أعمال التحقيق الابتدائي، وبعد تحريك الدعوى الجزائية بهدف الكشف عن الحقيقة وبالتالي يتضمن الإجراء ثلاثة معايير: الهدف الوقت والقائم بالإجراءات.

الفرع الثالث: مدى قابلية نظام الحاسوب للتفتيش.

تتكون نظم الحاسوب من مكونات مادية ومكونات منطقية، كما أنه تربطه بغيره من الحاسبات شبكات اتصال بعدية على المستوى المحلي أو الدولي والتي سنتطرق إليها فيما يلي:

---

[1] على حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، عالم الكتب الحديث للنشر والتوزيع، الأردن، 2004، ص15.

[2] يوسف دلائدة، مرجع سابق، ص 47.

[3] على حسن محمد الطوالبة، مرجع سابق، ص 16.

أولا: تفتيش مكونات الحاسوب المادية.

ليس هناك خلاف على أن الولوج إلى المكونات المادية للحاسوب، بحثا عن شيء ما يتصل بجريمة معلوماتية وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات العادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات، وهل هو من الأماكن العامة أو من الأماكن الخاصة، حيث أن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته.[1]

ثانيا: تفتيش مكونات الحاسوب المعنوية.

كان هناك اختلاف بين الفقهاء حول جواز تفتيشها، فذهب رأي في الفقه إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى القوانين الإجرائية فعندما تنص على إصدار الإذن بضبط أي شيء، فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة.[2] بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على تفتيش الكمبيوتر، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد، تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب الآلي.[3]

في مقابل الرأيين أعلاه، فإن هذا الرأي قد نأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحاسبة الالكترونية أم لا، فذهب إلى أن النظرة في

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، مصر، 2009، ص 195.

[2] المرجع نفسه، ص197.

[3] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية: دراسة مقارنة، المكتب الجامعي الحديث، مصر، 2012، ص42.

ذلك يجب أن تستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسبة الالكترونية إذا اتخذت شكلاً ماديا.[1]

ثالثا: تفتيش الشبكات المتصلة بالحاسوب (التفتيش عن بعد).

إن طبيعة التكنولوجيا الرقمية عقدت التحدي أمام أعمال التفتيش والضبط، بسبب امتداد الأدلة الإلكترونية عبر شبكات الحاسوب في أماكن بعيدة عن الموقع المادي للتفتيش، وان كان من الممكن الوصول اليها 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.[2] وبالتالي فإن الحاسوب التي يمكن أن ترتكب عليه أو بواسطته الجريمة المعلوماتية يخضع للقانون الإجرائي الخاص بتلك المنطقة، ونستطيع أن نميز في هذه الصورة بين الاحتمالين التاليين:

الاحتمال الأول: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة:

قد أجازت بعض التشريعات للأشخاص القائمين على التفتيش امتداد هذا الأخير إلى سجلات البيانات المتصلة في النهاية الطرفية للحاسوب في منزل المتهم مع جهاز أو نهاية طرفية في مكان آخر، حيث أنه يمكن امتداد الحق في تفتيش المساكن إلى نظم المعلومات الموجودة في موقع آخر، حينما يهدف ذلك إلى إظهار الحقيقة دون وجوب صدور اذن مسبق من قاضي التحقيق، وذلك بشرطين هما:

- أن تكون النهاية الطرفية المتصلة بالحاسب الآلي موجودة داخل الدولة المعنية

---

[1] علي عدنان الفيل، مرجع سابق، ص43.

[2] بن طالب ليندا، صالتفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، عدد 16، جامعة مولود معمري، تيزي وزو، الجزائر، جوان 2017، ص 490.

– أن تتضمن النهاية الطرفية المتصلة بالحاسب الآلي بيانات مخزنة تستهدف إظهار الحقيقة.[1]

وبخصوص القانون الجزائري فقد تضمن في التعديل الجديد لسنة 2021 لقانون الإجراءات الجزائية في الباب السادس الخاص بالقطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال نصوص قانونية إجرائية فيما يخص توسيع بعض الصلاحيات في مجال المتابعة والتحقيق والحكم، ذلك في بعض الأنواع من الجرائم من بينها الجريمة المعلوماتية، إذ يمارس كل من وكيل الجمهورية وقاضي التحقيق ورئيس ذات القطب الخاصة بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال صلاحياتهم في كامل التراب الوطني. [2]

الاحتمال الثاني: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

من المشاكل التي تواجه سلطة الادعاء في جمع الأدلة، قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة، مستخدمين في ذلك شركة الاتصالات المعلوماتية مستهدفين عرقلة الادعاء في جمع الأدلة والتحقيقات، وفي هذه الحالة فإن هناك امتداد للاذن بالتفتيش إلى خارج الاقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن بالدخول في المجال الجغرافي لدولة ما، وهو ما يسمى بالولوج أو التفتيش عبر الحدود، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها.[3]

---

[1] فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2011/2010، ص 312 – 313.

[2] المواد من 211 مكرر 23 إلى 211 مكرر 24 من الأمر رقم 21–11 المؤرخ في 16 محرم عام 1443 الموافق لـ 25 أوت سنة 2021 يتمم الأمر رقم 66–155 المؤرخ في 18 جويلية سنة 1966 والمتضمن قانون الإجراءات الجزائية، سنة 2021، ج ر، عدد 65، سنة 2021.

[3] علي عدنان الفيل، مرجع سابق، ص 46.

لذا فإن جانب من الفقه يرى بأن التفتيش الالكتروني العابر للحدود لا بد أن يتم في اطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد تعقد بين الدول المعنية.[1]

فالمشرع الجزائري أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج الدولة وهذا ما نصت عليه المادة 05 فقرة 3 من القانون رقم 09 / 04.[2]

المبحث الثاني: ضوابط التفتيش في الجرائم الالكترونية.

يعتبر التفتيش من أخطر الحقوق التي منحت للمحقق، وذلك لمساسها بالحريات التي تكفلها الدساتير عادة، ولهذا نجد المشرع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أو تأذن فيها بمباشرته، والأحوال التي تجوز فيها مباشرته، وشروط اتخاذ هذا الإجراء مثل ضمانات الحرية الفردية أو حرمة المسكن، حيث هناك عدة ضوابط يجب توافرها لإجراء التفتيش منها ما هو موضوعي (المطلب الأول)، ومنها ما هو شكلي (المطلب الثاني).

المطلب الأول: الضوابط الشكلية للتفتيش في الجرائم الالكترونية.

الضوابط الشكلية هي تلك الإجراءات التي أوجب المشرع مراعاتها عند إجراء عملية التفتيش، والهدف من وضع هذه الشروط من قبل المشرع هو إحاطة عملية التفتيش بإجراءات وشكليات تضمن صحة ودقة النتائج التي يصل إليها القائم بالتفتيش، وإحاطة المتهم بضمانات كافية للحفاظ على حريته الفردية، فالشكلية في الإجراءات الجنائية هي ضمانة لعدم تعسف الجهات القائمة بالتفتيش،[3] لذلك سنتطرق إلى الحضور الضروري للأشخاص المعنيين أثناء

---

[1] خالد ممدوح إبراهيم، مرجع سابق، ص205.

[2] تنص المادة 05 الفقرة 03 من قانون رقم 09-04 السالف الذكر على أنه " 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 وفقا لمبدأ المعاملة بالمثل".

[3] عثماني عز الدين، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة دائرة البحوث والدراسات السياسية، مخبر المؤسسات النظم السياسية، عدد 04، جامعة تبسة، جانفي 2018، ص 57.

التفتيش (الفرع الأول)، ثم الميعاد الزمني لإجرائه (الفرع الثاني)، وأخيرا محضر التفتيش (الفرع الثالث).

الفرع الأول: الحضور الضروري للأشخاص المعنيين أثناء التفتيش.

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية وذلك لضمان الاطمئنان على سلامة الإجراء، وغني عن البيان أن التفتيش فيه اطلاع على أسرار الغير فبالنسبة لتفتيش الأشخاص لم تشترط التشريعات الإجرائية لصحته حضور شهود عند تفتيشهم.[1] أما فيما يتعلق بتفتيش المساكن ينص القانون الجزائري على وجوب حصول إجراء التفتيش المتعلق بالمساكن أو ملحقاتها بحضور المشتبه فيه أو المتهم عندما يتم تفتيش مسكنه، سواء من طرف قاضي التحقيق أو ضابط الشرطة القضائية، وإذا تعذر ذلك بامتناعه عن حضور التفتيش أو كان هاربا، يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة القائم بالتفتيش.[2]

ويلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب لقانون رقم 06-22 من المادة 45 منه. حيث استغنى على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،[3] 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.

---

[1] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2007، ص.108.

[2] بن طالب ليندا، مرجع سابق، ص493.

[3] قانون رقم 06-22 المؤرخ في 20 ديسمبر2006 يعدل ويتمم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية ج ر، عدد 84، سنة 2006.

الفرع الثاني: الميعاد الزمني لإجراء التفتيش في الجرائم الإلكترونية.

يقصد بشرط الميعاد الزمني في التفتيش أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع، وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن،[1] حيث حدد المشرع الجزائري أوقات التفتيش من الساعة الخامسة صباحا إلى الساعة الثامنة مساءًا، وقد نصت على ذلك في المادة 47 فقرة 01 من ق إ ج ج "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة صباحاً، ولا بعد الثامنة مساءً..."

إلا أنه وفي حالات استثنائية يجوز الخروج عن تلك القاعدة فعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الأموال والارهاب وكذلك الجرائم المتعلقة بالتشريع الخاص بالصرف، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل، وذلك بناء على إذن مسبق من وكيل الجمهورية المختص.[2]

ويتبين من النص أعلاه أن المشرع الجزائري أجاز إجراء التفتيش في أي وقت من أوقات النهار والليل في جرائم معينة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وبذلك يكون المشرع الجزائري قد أدرك فعلا ميزة هذه الجرائم من حيث قابلية الدليل الالكتروني فيها للمحو والتدمير في أقل من ثانية.[3]

الفرع الثالث: محضر التفتيش في الجرائم الإلكترونية.

باعتبار أن التفتيش من أعمال التحقيق لابد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة، والقانون لم يتطلب شكلاً خاصا وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تنص عليه القواعد العامة في المحاضر عموما، بأن يكون مكتوبا

[1] بن طالب ليندا، مرجع سابق، ص493.

[2] المادة 47 فقرة 3 من ق إ ج ج.

[3] أشرف عبد القادر قنديل، مرجع سابق، ص 153

باللغة الرسمية وأن يكون مؤرخا وموقعا عليه، ونفس الأمر بالنسبة لمحضر تفتيش نظم الحاسوب، فإنه يستلزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات.[1]

وإذا كانت مكونات المحاضر تتباين تبعا لنوع التحقيق وموضوع المحضر غير أن الهيكل العام والمكونات الرئيسية المشتركة تكاد توجد في كل المحاضر، وهذه المكونات نلاحظ أنها أكثر جلاء ووضوحا في محضر التحقيق الأولي، حيث يتضمن البنود التالية:

- البيانات الهامشية والمقدمة.
- التمهيد.
- المعاينات والإجراءات التحفظية.
- التحقيق.
- اختتام المحضر.[2]

ويستهدف المحضر نقل الوقائع التي تمت معاينتها بموضوعية لذلك فإن الأسلوب الذي يحرر به يجب أن يكون بلغة سليمة وأسلوب واضح ودقيق وينقل تسلسل الوقائع دون إسهاب ممل أو إيجاز مخل بحيث يتجنب المحرر كل العبارات أو الصيغ التي يكون مدلولها ظنيا يقبل عدة تأويلات وتفسيرات أو تلك المتضمنة لأحكام ذاتية أو تعاليق معبرة عن انطباعات المحرر الشخصية، إذ لا يجب أن يكون المحضر فيه حشو أو محو أو تداخل بين مكوناته وإلا تترتب على ذلك بطلان الإجراءات.[3]

ومن جهة أخرى لابد وأن يرافقه شخص متخصص في الحاسوب والأنترنت للاستعانة به في مجال الخبرة الفنية الضرورية، فوجود الخبير سوف يساعد في صياغة مسودة محضر

---

[1] عائشة بن قاره مصطفى، مرجع سابق، ص ص 112 – 113.

[2] غاي أحمد، الوجيز في تنظيم ومهام الشرطة القضائية، الطبعة 5، دار هومة للنشر والتوزيع، الجزائر، 2009، ص 192.

[3] المرجع نفسه، ص 188.

التحقيق، بحيث يتم تغطية كل الجوانب الفنية في عملية التفتيش والضبط، بالإضافة إلى المحافظة على الأدلة المتحصل عليها من كل تلف أو مسح أو تحريف.[1]

المطلب الثاني: الضوابط الموضوعية للتفتيش في الجرائم الالكترونية.

يقصد بهذه الضوابط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، حيث يشترط أن يتوافر في التفتيش سلطة مختصة به (الفرع الأول)، ثم سببه (الفرع الثاني)، وأخيرا محله (الفرع الثالث).

الفرع الأول: السلطة المختصة بالتفتيش في الجرائم الالكترونية.

يعد التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمس حقوق وحريات الأفراد، لذا حرص المشرع على إسنادها لجهة قضائية تكفل تلك الحقوق والحريات، وتتمثل هذه الجهة القضائية في قاضي التحقيق أو النيابة العامة باختلاف التشريعات كسلطة أصلية، أو استثناء رجال الضبط القضائي وهذا ما سنبينه تباعا.

أولاً: إجراء تفتيش النظم المعلوماتية بمعرفة سلطة التحقيق الأصلية.

جعل المشرع الجزائري سلطة التحقيق الأولية من اختصاص قاضي التحقيق[2] باعتباره مختص بإجراء كل التحقيقات بما فيها التفتيش، لكن في كل الحالات التي يقوم فيها بهذا الإجراء لابد من إخطار وكيل الجمهورية الذي له الحق في مرافقته،[3] واستثناءً يجوز لوكيل الجمهورية أن يقوم ببعض اجراءات التحقيق، لأن الاختصاص الأصيل بمباشرته يعود لقاضي التحقيق وحده دون سواه.[4]

---

[1] خالد ممدوح ابراهيم، مرجع سابق، ص 225.

[2] يجب الاشارة إلى أن قاضي التحقيق لا يختص بالقضية إلا بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بادعاء مدني. وذلك بعد أخذ بعين الاعتبار نص المواد 67 و73.

[3] المواد 79، 82 من ق إ ج ج.

[4] المادة 56-01 من ق إ ج ج.

قاضي التحقيق الذي يقوم بإجراء التفتيش لابد أن يكون مختصا من ناحية الاختصاص المكاني أو النوعي، فيتحدد اختصاص قاضي التحقيق محليا إما بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في ارتكابهم الجريمة أو بمحل القبض على هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.

كما يجوز تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم وذلك في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم المخدرات والجريمة المنظمة عبر الحدود وغيرها. [1] وبالنسبة للاختصاص النوعي لقاضي التحقيق نجده يتحدد بنوعية الجرائم، فنجد أن التحقيق الابتدائي وجوبي في مواد الجنايات وجوازي في مواد الجنح والمخالفات بالنسبة لقاضي التحقيق،[2] وبالنسبة للقانون الجزائري نجد أن قاضي التحقيق يختص بإجراءات التحقيق بما فيها التفتيش في الجنايات والجنح المتلبس بها.

ثانيا: إجراء تفتيش النظم المعلوماتية بمعرفة ضباط الشرطة القضائية:

يتحقق إجراء تفتيش نظم المعلوماتية بمعرفة ضباط الشرطة القضائية في الحالات التالية وهي:

أ. **التفتيش بناء على إذن قضائي بإجرائه:**

القاضي غير ملزم في كل الحالات بمباشرة التفتيش، إذ يجوز له أن يندب أحد ضباط الشرطة القضائية للقيام بهذا الإجراء، وهذا ما يسمى بالإنابة القضائية، لذلك فلا يجوز لضباط الشرطة القضائية القيام بإجراء التفتيش إلا بعد حصولهم على إذن من السلطة المختصة.[3]

وفي هذه الحالة يجب أن يحدد إذن التفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها (أجهزة الحاسوب – صور جنسية الكترونية خاصة بالأطفال، مصنفات

[1] المادة 40 من ق إ ج ج.
[2] المادة 66 من ق إ ج ج.
[3] المادة 44 من ق إ ج ج.

إلكترونية مقلدة...) ، والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي، بحيث لا يترك للمأذون بالتفتيش أي سلطة تقديرية في ذلك،[1] إلا أن هناك صعوبة في احترام هذا الشرط أثناء الممارسة العملية في تفتيش أجهزة الحاسوب، ويرجع ذلك إلى الطبيعة الخاصة لهذه الأخيرة، فجهاز الحاسوب يحتوي على عدد كبير من الملفات، بالإضافة إلى أن أسماء هذه الملفات لا تدل بالضرورة على ما تحتويها، خاصة وقد يعمد المتهم إلى وضع أسماء مستعارة لملفات تحتوي على مواد غير مشروعة.[2]

ب. التفتيش بناء على حالة التلبس بالجريمة:

لا يختلف التفتيش في حالة التلبس في نظم الحاسب الآلي عن الجريمة التقليدية، لذلك يجوز لضابط الشرطة القضائية المنتدب في أحوال التلبس بالجنايات و الجنح المعلوماتية تفتيش نظم الحاسب الآلي،[3] حيث أنه ومن المتعارف عليه في معظم التشريعات الإجرائية أن حالة التلبس تعتبر احدى الحالات التي تتسع فيها سلطات الضبطية القضائية، حيث تباشر اختصاصات هي أصلا من اختصاص سلطة التحقيق، ومنها تحديدا التفتيش بحثا عن أدلة الجريمة وتحديد فاعلها.[4]

ومن مظاهر التفتيش في حالة التلبس أن يكون رجل الضبط القضائي في إحدى مقاهي الانترنت يمارس هوايته في الابحار عبر شبكة الإنترنت ويلاحظ وجود شخصاً آخر يقوم بالإبحار في تلك الشبكة في المواقع الإباحية، ويقوم بطباعة الصور المتواجدة فيها بواسطة طابعة، ففي هذه الحالة تحقق شروط التلبس.[5]

---

[1] أشرف عبد القادر قنديل، مرجع سابق، ص 150.

[2] بن طالب ليندا، مرجع سابق، ص ص492 – 493.

[3] طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، مصر، د. س. ن، ص 437.

[4] عثماني عزالدين، مرجع سابق، ص 59.

[5] المرجع نفسه، ص 60.

ج. التفتيش بناء على موافقة المتهم:

يجب أن تكون الموافقة من طرف صاحب الشأن بالتفتيش صريحة ومكتوبة بخط يده، فإذا كان لا يعرف الكتابة يذكر ذلك في المحضر ويذكر فيه هذه الموافقة، أما بخصوص جرائم الحاسب الآلي فإنه لا توجد نصوص قانونية مشابهة تخص تفتيش نظم المعلوماتية بناء على موافقة المتهم، لذلك فإن هذا الفراغ يمكن تغطيته بالقواعد التقليدية.[1]

الفرع الثاني: سبب التفتيش في الجرائم الالكترونية.

إن سبب التفتيش في القواعد العامة بوصفه إجراء من إجراءات التحقيق، هو وقوع جناية أو جنحة، واتهام شخص أو عدة أشخاص بارتكابها أو المساهمة فيها، وتوافر إمارات قوية أو قرائن على وجود أشياء تفيد في كشف الحقيقة لدى المشتكى عليه أو غيره،[2] وسنبحث هذه الشروط المهمة كما يلي:

أولا: وقوع جريمة معلوماتية.

لا يجوز لهيئات التحقيق مباشرة إجراءات التفتيش الا بعد التأكد من الوقوع الفعلي لجريمة الكترونية نص عليها القانون في نصوص التجريم والعقاب، وأي تفتيش في جريمة محتملة الوقوع مستقبلا ولو أيقنت التحريات والدلائل الجدية على أنها ستقع بالفعل، يعد إجراء غير مشروع مآله البطلان، كما لا يكفي وقوع جريمة الكترونية للقول بمشروعية إجراء التفتيش طبقا للقواعد العامة، بل لا بد من وقوع جريمة معلوماتية مصنفة على أنها جناية أو جنحة مثلما هو الحال في القواعد الموضوعية التقليدية.[3]

كما أن القانون الجزائري حدد أن نكون بصدد جريمة ارتكبت باستخدام تكنولوجيا الإعلام والاتصال، ووقعت بالفعل، مثل جريمة القذف والسب، جريمة التهديد، فهذه الأفعال نص عليها

---

[1] هلالي عبد الله أحمد، مرجع سابق، ص 162.

[2] علي حسن محمد الطوالبة، مرجع سابق، ص 62.

[3] طرشي نورة، مرجع سابق، ص 130.

المشرع من خلال نصوص التجريم والعقاب ونصوص قانون 09-04 طبقا لمبدأ شرعية الجرائم والعقوبات.[1]

ثانيا: نسبة الجريمة الالكترونية لشخص أو أشخاص معينين إما بصفتهم فاعلين أصليين أو شركاء في ارتكابها.

ينبغي أن تتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه ساهم في ارتكاب الجريمة المعلوماتية، سواء بصفته فاعلاً لها أو شريكا فيها، وفي مجال الجرائم الالكترونية يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة المظاهر أو الإمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة، وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة المعلوماتية إلى شخص معين سواء بوصفه فاعلاً أو شريكاً.[2]

ثالثا: توافر إمارات قوية أو قرائن توحي على وجود أشياء أو أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره.

التفتيش لا يتم إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة الالكترونية، أو أشياء متحصلة منها أو أية مستندات إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره.[3]

ويتم الحصول عادة على هذه القرائن والامارات من خلال مختلف التحريات الجدية التي تجريها سلطات الضبط في مرحلة الاستدلال، بعد ما يتم إخضاعها لتقدير السلطة المختصة

---

[1] تومي يحي، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيات الإعلام والاتصال، رسالة دكتوراه، تخصص قانون، كلية الحقوق جامعة الجزائر 01, 2018، ص ص 205، 206.

[2] على عدنان الفيل، مرجع سابق، ص 50.

[3] المرجع نفسه، ص51.

بإصدار الإذن بالتفتيش، التي تتأكد من مدى توفر هذه القرائن لمصداقية كافية تبرر اللجوء إلى إجراء التفتيش.[1]

الفرع الثالث: محل التفتيش في الجرائم الالكترونية.

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، فالسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة كالمسكن أو الشخص والرسائل، لكن في الجريمة الالكترونية فإن محل التفتيش يكون في كل مكونات الحاسوب سواء كانت مادية أو معنوية وكل شبكات الاتصال الخاصة به[2].

ولكي يتم التفتيش على هذه الحال ينبغي الإشارة إلى أن هذه الأخيرة لا تكون قائمة بذاتها بل تكون إما موضوعة في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو الهاتف النقال الذكي.[3]

[1] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، مصر، 2017، ص130.

[2] أشرف عبد القادر قنديل، مرجع سابق، ص149.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص104.

مما سبق نستنتج أن التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهم إجراءات التحقيق لإزالة الغموض عن الجريمة المرتكبة، لأنه غالبا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم، أما بخصوص التفتيش في مجال جرائم الأنترنت فيعرف بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة.

ولذا حرصت القوانين الإجرائية على إحاطة إجراء التفتيش بضوابط أساسية نظرا لما يمكن أن يحدثه من مساس بحق الإنسان في حريته الشخصية وهدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم.

الفصل الثاني: إجراءات التفتيش في الجرائم الإلكترونية.

الفصل الثاني: إجراءات التفتيش في الجرائم الإلكترونية

تعتبر الجريمة الإلكترونية من حيث طبيعتها جريمة فريدة من نوعها، كون تطبيق مبدأ الشرعية يقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها لكي يستطيع رجال الضبط القضائي ممارسة مهامهم وفقا لطبيعة الجرائم الإلكترونية.

ولا يمكن بأي حال من الأحوال البحث والتحري في هذه الجرائم بالأساليب التقليدية، لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة كافية لملفات الحاسوب ومكان إخفاء المعلومات فيها لأنه يمكن إتلافها بكل سهولة، وكذلك يصعب تحديد مكان الدليل في حالة ما إذا كان مخزن داخل النظام أم على دعامة خارجية، وقد تكون الملفات مشفرة لا يظهر محتواها إلا بفك التشفير، كما أن التحقيق بشكل عام يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة في إيجاد الأدلة والتنقيب عنها معتمدا في ذلك على مجموعة من الوسائل المخصصة في عملية البحث والتحري.

وبالرغم من كل ذلك قد تواجه ضباط الشرطة القضائية العديد من المشاكل والمعوقات التي تؤثر على سلامة مجريات التحقيق، مما حتم على المشرع الجزائري توفير أجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة الإلكترونية، وأول سبب هو حماية أفراد المجتمع من مخاطر هذه الجرائم والحد منها بالإضافة إلى ضبط الحصول على مختلف الأدلة الإلكترونية التي تساعد على إثبات الجريمة.

وباعتبار التفتيش إجراء من إجراءات التحقيق فهو كغيره من إجراءات التحقيق الأخرى يترتب عليه آثار أثناء تنفيذه فيسفر على أشياء لها علاقة، سواء استعملت لتحقيق العمل الإجرامي أو نتجت عنه أو أي شيء آخر يساعد سلطة التحقيق للوصول إلى الحقيقة وهو ما يطلق عليه بمصطلح الضبط، وأيضا من الآثار المترتبة عن إجراء التفتيش البطلان لأن مخالفة قواعد التفتيش بصفة خاصة هو إهدار للحقوق والحريات الشخصية للأفراد.

الفصل الثاني: إجراءات التفتيش في الجرائم الإلكترونية

من أجل كل هذا كان لابد علينا من إبراز الآليات القانونية الخاصة بالتفتيش في الجرائم الإلكترونية (المبحث الأول)، ثم الآثار القانونية المترتبة عن إجراءات التفتيش في الجرائم الإلكترونية (المبحث الثاني).

المبحث الأول: الآليات القانونية الخاصة بالتفتيش في الجرائم الإلكترونية.

إن ظهور الجرائم الإلكترونية أدى إلى إضفاء أعباء جديدة على أجهزة التحقيق لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها المحققون ولم يعتادوا عليها، مما أدى إلى ضرورة توفير الإمكانيات والمهارات المطلوبة في هذا المجال، أضف إلى ذلك طبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية، ولهذا سنتطرق إلى الأجهزة المكلفة بالتفتيش في الجرائم الإلكترونية (المطلب الأول)، ثم الإجراءات الخاصة بالتفتيش (المطلب الثاني).

المطلب الأول: الأجهزة المكلفة بالتفتيش في الجرائم الإلكترونية.

إن للتطور المستمر للجرائم الإلكترونية الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لمواكبة التطور الحاصل في مجال الجريمة، نتيجة لذلك قامت أغلب الدول باستحداث وحدات خاصة لمكافحة هذا النوع من الجرائم، كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي، أما في الجزائر فقد تم تسخير هيئات ووحدات أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ولهذا سنتطرق إلى الهيئات المكلفة بالتحقيق في الجرائم الإلكترونية (الفرع الأول)، والأعوان المكلفون بالتحري وجمع الأدلة في هذه الجرائم (الفرع الثاني).

الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم الإلكترونية.

وتنقسم هاته الهيئات إلى: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والهيئات القضائية الجزائية المتخصصة.

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

وقد استحدثها المشرع الجزائري بموجب قانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تحديدا في المادة 13 التي تنص على أنه: <<تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته>>.[1]

لكن تم تحديد وتنظيم عمل هذه الهيئة بموجب المرسوم الرئاسي رقم 19-172 المؤرخ في 06 يونيو 2019، وبموجب المرسوم توضع الهيئة التي هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، تحت سلطة وزارة الدفاع الوطني كما حدد مقرها بمدينة الجزائر مع إمكانية نقله إلى مكان آخر من التراب الوطني بموجب قرار من وزير الدفاع الوطني.[2]

أما مهام هذه الهيئة فنصت عليها المادة 14 من القانون 09-04 السالف الذكر كالتالي:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[1] المادة 13 من القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[2] المرسوم الرئاسي رقم 19-172 المؤرخ في 6 يونيو 20 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 37 في 2019/06/09.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

– تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وتحديد مكان تواجدهم.

ثانيا: الهيئات القضائية الجزائية المتخصصة.

يتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص وذلك من خلال استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004،[1] الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر وتصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف.[2]

الفرع الثاني: الأعوان المكلفون بالتحري وجمع الأدلة الإلكترونية.

لقد خصصت الدولة أشخاص على غرار باقي التشريعات للبحث والتحري وجمع الأدلة الإلكترونية، لما لها من كفاءات البحث عن الجريمة الإلكترونية.

وبالنظر إلى خصوصية الجريمة الإلكترونية وفر المشرع الجزائري موظفين ومنحهم صفة الضبطية القضائية يتولون التحقيق في تلك الجرائم، وذلك على مستوى الشرطة والدرك الوطني.

فعلى مستوى جهاز الشرطة فرض عليهم القانون واجبات من خلال البحث عن الجرائم ومرتكبيها وجمع مختلف الاستدلالات ومناقشة الشهود وقبول الشكاوي والبلاغات المقدمة إليهم

---

[1] القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الصادر بالجريدة الرسمية، عدد 71، بتاريخ 10 نوفمبر 2004.

[2] بوضياف اسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، المسيلة، سبتمبر 2018، ص 370.

والتفتيش والانتقال إلى مكان الجريمة، ضف إلى ذلك تحرير المحاضر وغيرها من الأساسيات التي تساعد في التحقيق، باعتبار أن أعمال الشرطة القضائية تعتبر إجراءات رادعة.[1]

أما على مستوى جهاز الدرك الوطني فإنه يوجد المعهد الوطني الخاص بالأدلة الجنائية وعلم الإجرام الذي يتكون من إحدى عشر دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.[2]

ومن خلال هذا كله سنبين صفة ضباط الشرطة القضائية في البحث والتحري وجمع الأدلة (أولا)، ثم الشروط الواجب توفرها في الأعوان المكلفين بالتحقيق (ثانيا)، ثم الوسائل المستخدمة في ذلك (ثالثا)، وصعوبات ومعوقات جمع الأدلة (رابعا).

أولا: صفة ضباط الشرطة القضائية في البحث والتحري وجمع الأدلة.

يتولى ضباط الشرطة القضائية مهمة البحث والتحري وجمع الأدلة عن كافة الجرائم المقررة في القانون، بما فيها الجرائم المعلوماتية، فلا يوجد أي مانع قانوني يحول دون ممارسة هؤلاء لمهامهم في مجال جرائم المعلوماتية، سوى أن يتوافر فيهم شرط الاختصاص النوعي والمتمثل في التمتع بصفة ضابط الشرطة القضائية.[3] وذلك طبقا للمادة 05 من نص القانون 09-04 المتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وسبل مكافحتها والتي تنص على أنه <<يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية... الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها...>>.

---

[1] مقابلة مع إطار في الشرطة بأمن ولاية جيجل.

[2] بوضياف إسمهان، مرجع سابق، ص 370.

[3] بركاني أحمد ياسين، عبادلي فاطمة الزهراء، وسائل وأدلة الإثبات في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الخاص، تخصص: قانون العقوبات والعلوم الجنائية، كلية الحقوق –تيجاني صدام–، جامعة الإخوة منتوري، قسنطينة –1–، 2017/2016، ص 72.

وبنا على ما تقدم فإن الأشخاص المخولين لهم مباشرة أعمال البحث وتنفيذ أوامر التحقيق في الجرائم المعلوماتية هم الأشخاص المذكورين في نص المادة 15 من قانون الإجراءات الجزائية الجزائري والتي تحدد قائمة خاصة للأشخاص الذين يتمتعون بصفة ضابط الشرطة القضائية.[1]

ثانيا: الشروط الواجب توفرها في الأعوان المكلفون بالتحقيق.

يتطلب للتحقيق في الجرائم قدرات فنية ومهارات لابد من توفرها للتعامل مع الجريمة لا تتوفر في باقي المحققين للتمكن من تقديم الأدلة الجنائية أمام الادعاء والمحاكم الجنائية وشرح أبعاد الجريمة وأساليب ارتكابها من اجل تحقيق العدالة.[2] وتتمثل هذه المهارات والشروط فيما يلي:

- الاطلاع على الجوانب الفنية والتقنية لأجهزة الحاسوب والأنترنت.
- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك.[3]

---

[1] تنص المادة 15 من قانون الإجراءات الجزائية الجزائري المعدلة بموجب أمر رقم 15-02 المؤرخ في 23 جويلية سنة 2015 على ما يلي: يتمتع بصفة ضابط الشرطة القضائية:

- رؤساء المجالس الشعبية البلدية.
- ضباط الدرك الوطني.
- الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني.
- ذو الرتب في الدرك، ورجال الدرك الذين أمضو في سلك الدرك الوطني ثلاث سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني، بعد موافقة لجنة خاصة.
- الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضو ثلاث سنوات على الأقل بهذه الصفة والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، بعد موافقة لجنة خاصة.
- ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل.

[2] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة للطباعة والنشر والتوزيع، مصر، 2008، ص 263.

[3] سعيداني نعيم، مرجع سابق، ص 116.

– يتوجب على ضابط الشرطة القضائية معرفة آلية عمل تشكيلات الحاسوب والأنترنت، مما يساعده على تصور كيفية ارتكاب الفعل الاجرامي في العالم الافتراضي، وكذا طرق اختراق البرامج المخزنة وكيفية الحصول على الأرقام والشفرات الفنية التي تمكنهم من الدخول إلى الحاسوب.[1]

– قدرة ضابط الشرطة القضائية في معرفة الأساليب الإجرامية المستخدمة في ارتكاب الجريمة الإلكترونية وتقنية الأمن المعلوماتي.[2]

– كذلك يجب أن يتمتعوا بالسرعة في القراءة والكتابة، وكذا تعلم الخريطة الذهنية لتلخيص المادة وأسلوب الأفكار، وهذا يساعدهم على التصرف الإلكتروني بكل نزاهة.[3]

– يجب أن يكون ضابط الشرطة القضائية كتوما لمجريات التحقيق ضمانا لسيره طبيعيا وعدم المساس بمصالح الخصوم بغير حق.

– يجب على ضابط الشرطة القضائية أن يكون على دراية بالأنظمة الضرورية لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة المعلوماتية وذلك من خلال الترتيب والدقة في الانتقال إلى مكان الحادثة ومعاينته في الوقت الملائم.[4]

ثالثا: الوسائل المستخدمة في التحري وجمع الأدلة.

يحتاج العون المكلف بالتحري والتحقيق في الجرائم الإلكترونية إلى مجموعة وسائل تمكنه من فحص الأدلة الجنائية التي تثبت وقوع الجريمة والوصول إلى الجاني وهذه الوسائل تختلف من وسائل مادية ووسائل إجرائية.

---

[1] سعيداني نعيم، مرجع سابق، ص 116.

[2] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006، ص 30.

[3] مصطفى محمد موسى، مرجع سابق، ص 263.

[4] المرجع نفسه، ص 270.

أ- الوسائل المادية.

هي مختلف الأدوات الفنية التي تستخدم في بيئة نظم المعلومات، والتي تثبت ارتكاب الجريمة وتساعد على تحديد شخصية مرتكبيها، ومن أهم هذه الوسائل نجد عناوين الأنترنت IP، والبريد الإلكتروني، وبرامج المحادثة المسؤولة عن تراسل البيانات عبر الأنترنت وتوجيهها إلى الهدف المرجو منها، وكذلك نجد نظام البروكسي الذي يعمل كوسيط بين الشبكة ومستخدميها، بالإضافة إلى برامج التتبع التي تقوم بالتعرف على محاولات الاختراق والمسؤول عن اختراقها.[1]

بالإضافة إلى نظام جرة العسل "Money Pot" الذي صمم خصيصا لاعتراض أنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أي بيانات ذات أهمية ويعتمد على خداع من يقوم بالهجوم واعطائه انطباعا خاطئا بسهولة الاعتداء على النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة.[2]

زد على ذلك نجد نظام الاختراق والذي يرمز له اختصارا بالأحرف IDS والتي تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الأنترنت، وكذلك أدوات الضبط التي تساعد في ضبط الجريمة كبرامج الحماية وأدوات المراجعة وغيرها، دون أن ننسى أدوات فحص ومراقبة الشبكات التي تستخدم في فحص بروتوكول الأنترنت لمعرفة المشاكل التي تصيب الشبكات والمتمثلة في أداة (ARP) المحدد لمكان الحاسوب الفزيائي وغيرها من الأدوات.[3]

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص ص 205،206،207.

[2] المرجع نفسه، ص 209.

[3] علي عدنان الفيل، مرجع سابق، ص ص 71-75.

ب- الوسائل الإجرائية.

يعني بها مختلف الإجراءات المستعملة في تنفيذ طرق التحقيق الثابتة والمتغيرة والمحددة وغير المحددة، المتبعة لوقوع الجريمة والمحددة لشخصية مرتكبيها،[1] ومن تلك الوسائل الإجرائية نذكر:

- اقتفاء الأثر حيث يمكن اقتفاء الأثر بعدة طرق سواء بواسطة البريد الإلكتروني أو عن طريق تتبع أثر الجهاز المستخدم في عملية الاختراق نظرا لأهمية اقتفاء الأثر في الجريمة الإلكترونية، بالإضافة إلى الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته، والاستعانة بالذكاء الصناعي في جمع الأدلة الجنائية.

- يضاف على ذلك التأكد من وقوع الجريمة الإلكترونية وتحديد مكان وزمان وقوعها وطريقة ارتكابها.[2]

رابعا: صعوبات ومعوقات جمع الأدلة.

يعتبر التفتيش إجراء من إجراءات التحقيق الهدف منه البحث عن الأدلة لجريمة ثبت وقوعها، لكن على الرغم من أهميته في الكشف عن الحقيقة إلا أنه قد يصادفه مجموعة من العراقيل التي تأثر على عملية التحقيق والمتمثلة في:

- غياب نصوص تشريعية ضد مرتكبي جرائم الحاسوب بالرغم من خطورة الجريمة الإلكترونية مما يؤذي إلى صعوبة جمع الاستدلالات والأدلة للقضاء على الجريمة ومرتكبيها.[3]

- زيادة على ذلك نجد الصعوبات المتعلقة بالجهات القائمة بالتحقيق وذلك لنقص خبرتهم في مجال الحاسوب والتكنولوجيا، وعدم إلمامهم بمستجدات الحاسوب وقلة معرفة مصطلحات الحاسوب والأساليب المتبعة في ارتكاب هذه الجرائم.[4]

---

[1] خالد عياد الحلبي، مرجع سابق، ص 212.

[2] خالد عياد الحلبي، مرجع سابق، ص ص 212،215.

[3] خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكاتب الحديث، الجزائر، 2012، ص 10.

[4] المرجع نفسه، ص 11.

– سهولة محو الدليل وإزالته من أجهزة الكمبيوتر وتدميرها في وقت قصير، بحيث لا يمكن للسلطات من كشف الجريمة، وتبادل المعرفة الرقمية السريعة خارج نطاق الدولة.[1]

– ومن معوقات التحقيق نجد أيضا المتعلقة بالجريمة من خلال اختفاء أثر الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه وكذلك صعوبة الوصول إلى الدليل الإلكتروني لاحتوائه على كلمة سر تمنع الوصول إليها والاطلاع عليها واستنساخها،[2] فتظل الجريمة الإلكترونية مستمرة ما لم يتم الإبلاغ عنها.

– بالإضافة إلى مشكلة الأصالة في الدليل الإلكتروني الذي له طابع افتراضي لا يرتقي إلى مستوى الأصالة بالنسبة للدليل المادي، فهذه الأخيرة تعبير عن وضع مادي ملموس. في حين أن الدليل الرقمي عبارة عن تعداد غير محدود من أرقام ثنائية موحدة في الصفر والواحد.[3]

المطلب الثاني: الإجراءات الخاصة بالتفتيش في الجرائم الإلكترونية.

تعد إجراءات التفتيش والضبط من إجراءات التحقيق التي تختص بها سلطة التحقيق ويناط لضابط الشرطة القضائية القيام بهما في حالات استثنائية، ويلاحظ أنه في الحالات التي يجوز فيها لضابط الشرطة القضائية القيام بإجراء التفتيش والضبط، فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة. حيث يقوم المفتش في إطار البحث عن الجريمة الإلكترونية بإجراءات تخص المتهم (الفرع الأول)، وأخرى تخص غير المتهم (الفرع الثاني)، وأخيرا تطبيقات إجراءات تفتيش نظم الحاسبات الآلية الخاصة بالأشخاص (الفرع الثالث).

الفرع الأول: إجراءات تفتيش النظام المعلوماتي الخاص بالمتهم.

إذا كان محل ارتكاب الجريمة ينصب على نظام المعلومات الخاصة بالمتهم دون الحاجة إلى التدخل في نظام معلوماتي لشخص آخر، وفي هذا الفرض إذا كانت الشروط الإجرائية للتفتيش صحيحة وفقا لما نص عليه القانون،[4] فإن التفتيش وما يسفر عنه من ضبط أي من

---

[1] ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 120.

[2] عبد العال الدريبي، ومحمد صادق إسماعيل، مرجع سابق، ص ص 329،330.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص 252.

[4] عثماني عزالدين، مرجع سابق، ص 60.

الأدلة، سواء كانت هذه الأدلة أجهزة الكمبيوتر أم أحد الوسائط المتعددة يكون ذلك مشروعا، وتكثر هذه الحالات في جرائم التزوير والتزييف أين يتم التفتيش وملحقاته من طباعات ملونة أو أجهزة ماسح ضوئي.[1]

يتم نقل البرنامج الداخلي الذي يوجد عن طريق إتمام عملية التزوير أو التزييف في أي من الوسائط المتعددة مما يمكن من الحصول على دليل ارتكاب الجريمة، ونفس الأمر مع جرائم النسخ والتقليد حيث يتم ضبط الوسائط المتعددة والمحملة بالبرامج المنسوخة والأجهزة المستخدمة في ذلك.[2]

اعتمادا على ما سبق فإن التفتيش يكون مشروعا في قضايا الجرائم المعلوماتية حيث سنتطرق إلى ذكر مجموعة من الإحصائيات الملموسة الخاصة بالجرائم الإلكترونية لسنة 2022، فحسب نتائج محضر قضايا الجرائم المعلوماتية المسجلة على مستوى اختصاص أمن ولاية جيجل خلال سنة 2022، فإنه تم تسجيل 284 قضية خلال هذه السنة سنشير إليها كالتالي:

أولا: القضايا المسجلة حسب النوع.

وهي خمسة (5) تتمثل في:

- قضايا المساس بأنظمة المعالجة الآلية للمعطيات سجلت فيها 19 قضية.
- قضايا المساس بالأشخاص عن طريق الأنترنت سجلت فيها 134 قضية والمتمثلة في قضية القذف بـ 44 قضية، السب بـ 23 قضية، التهديد بـ 21 قضية، التهديد والابتزاز بـ 3 قضايا، وانتحال الهوية بـ 19 قضية، أما المساس بالحياة الخاصة بـ 24 قضية.
- النشر والترويج لمواد إباحية عبر الأنترنت سجلت فيها 12 قضية.
- أما النصب عن طريق الأنترنت سجلت فيها 78 قضية.
- وهناك جرائم أخرى عن طريق الأنترنت سجلت فيها 41 قضية.

---

[1] ، عثماني عزالدين، مرجع سابق، ص 60.

[2] خالد ممدوح إبراهيم، مرجع سابق، ص 229.

ثانيا: القضايا المسجلة حسب صفة المتورط والضحية.

قدر عدد المتورطين لسنة 2022 التي سجلت فيها 284 قضية بـ 214 متورط كلهم بالغين (لا يوجد قصر)، حيث اختلف الأشخاص المتورطين في ارتكاب هذه الجرائم من حيث الجنس. بالنسبة للذكور 207 متورط أما الإناث 7 متورطين.

أما عدد الضحايا لسنة 2022 التي سجلت فيها 284 قضية قدر بـ 231 ضحية تباينت أعمارهم ما بين البالغين بمجموع 229 ضحية منهم 157 ذكر و65 أنثى، أما بالنسبة للقصر فبلغ عدد الضحايا 9، منها 3 ذكور و6 إناث.[1]

الفرع الثاني: إجراءات تفتيش النظام المعلوماتي الخاص بغير المتهم.

يظهر هذا الفرض في الجرائم التي تستخدم الشبكات الإلكترونية في ارتكابها، بحيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الأخرى المرتبطة بالحاسب الذي ارتكبت في نظامه المعلوماتي الجريمة، وفي هذا الفرض فإن إجراءات التفتيش والضبط تتطلب الدخول في نظام معلوماتي لشخص آخر،[2] غير أن قانون الإجراءات الجزائية نص على أنه لا يجوز لرجال الشرطة القضائية الدخول في أي محل مسكون إلا في الأحوال التي بينها القانون بغاية حماية الخصوصية، وهو ما دعا المشرع إلى مد تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن، وكذلك السيارة الخاصة إذا كانت توجد في مسكن المتهم، أما إذا وجدت في الطريق العام فلها نفس حرمة الشخص بحيث لا يجوز تفتيشها إلا إذا جاز تفتيش الشخص قانونا.[3]

الفرع الثالث: تطبيقات إجراءات تفتيش نظم الحاسبات الآلية الخاصة بالأشخاص.

طبقا لمعيار الخصوصية التي يحميها المشرع يتبين أنه قد تناول المسكن والسيارة والمحل وكل ما يتعلق بالشخص ويمثل خصوصياته، ولذلك فإن نظام المعلومات وما يحويه من

---

[1] أنظر الملحق رقم 1.

[2] عثماني عزالدين، مرجع سابق، ص 61.

[3] خالد ممدوح إبراهيم، مرجع سابق، ص 229.

خصوصيات للأشخاص تخضع أيضا وبالتبعية لمعيار الخصوصية من حيث عدم جواز التدخل فيها بدون إذن من وكيل الجمهورية.[1]

ورغم أن المشرع وفي أغلب القوانين التي نصها حاول حماية خصوصية الأفراد بما فيها البيانات والمعلومات الشخصية وكذلك السجلات والدفاتر أو الحاسبات الآلية والملحقات السرية بعدم جواز الاطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون وذلك بموجب القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي.[2] باعتبار أن البيانات لها طابع مادي قابلة بأن تسجل وتخزن في وسائط متعددة يمكن قياسها. وهذا ما أكده أيضا امتداد الحق في التفتيش إلى سجلات البيانات التي تكون في موقع إلكتروني آخر عندما يكون التخزين الفعلي خارج المكان الذي يتم فيه التفتيش.[3]

وباعتبار أن البحث عن دليل ارتكاب الجريمة يعد وسيلة للإثبات ومحلا للإقناع وفقا لنظرية الإثبات الجنائي فيتطلب الأمر في هذه الحالة من حيث الإقرار بإمكانية أن تكون المعلومات محلا للتفتيش وضبط الأدلة المتحصل عليها، غير أنه 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 قد ارتكب جناية أو جنحة وقامت قرائن قوية على ارتكابه للجريمة،[4] وعند القيام بتنفيذ إذن التفتيش فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم، أو أن للمتهم أكثر من جهاز في أماكن مختلفة كأن يكون المتهم مالكا لجهاز في منزله وجهاز آخر في عمله، أو أن يكون الشخص له شريك في الأجهزة مما يتطلب الحصول على إذن من النيابة العامة، ويتم تحديد

---

[1] عثماني عزالدين، مرجع سابق، ص 61.

[2] قانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق لـ 10 جويلية سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، عدد 34، سنة 2018.

[3] عثماني عزالدين، مرجع سابق، ص 62.

[4] خاد ممدوح إبراهيم، مرجع سابق، ص 231.

كل هذا عن طريق تعيين مجال التفتيش وما يستبعه بالضرورة من تتبع لشبكات المعلومات ويخضع كل ذلك للسلطة التقديرية للقاضي من حيث توافر حالة الضرورة من عدمها.[1]

المبحث الثاني: الآثار المترتبة عن إجراءات التفتيش في الجرائم الالكترونية.

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فالضبط هو غاية التفتيش أو الأثر المباشر له، إذا ما توافرت له عناصره وشروطه القانونية، وبمعنى آخر إذا كان التفتيش قانونيا، أما إذا لم يكن كذلك فالأثر الإجرائي الذي يترتب عليه هو بطلانه وبطلان الضبط الناتج عنه، ومن خلال ذلك سنتناول ضبط الأدلة والمراسلات الإلكترونية (المطلب الأول)، ونتناول البطلان كجزاء لمخالفة إجراءات التفتيش (المطلب الثاني).

المطلب الأول: ضبط الأدلة والمراسلات الإلكترونية.

التفتيش القانوني في الجرائم الإلكترونية الذي يجري وفق ما رسمه القانون يعطي مشروعية قانونية لأهم آثاره وهو ضبط الأدلة الإلكترونية، لما لهذه الأدلة من صلة مباشرة في الكشف عن الحقيقة.

تنص المادة 81 من قانون إ.ج.ج " يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة".

وكذلك نصت المادة 05 السالفة الذكر من قانون مكافحة الجرائم الالكترونية على أن التفتيش يتم على المنظومة المعلوماتية أو منظومة تخزين معلوماتية. وهذان النصان حددا الغاية من التفتيش وهي البحث الأدلة.

[1] خاد ممدوح إبراهيم، مرجع سابق، ص 232.

الفرع الأول: ضبط الأدلة الإلكترونية:

سنتناول في هذا الفرع تعريف ضبط الأدلة (أولاً)، ثم الأدلة القابلة للضبط (ثانيا) ومدى قابلية جرائم الحاسوب لضبط أدلتها (ثالثا).

أولاً: تعريف ضبط الأدلة:

ويقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في الكشف عن الحقيقة وعن مرتكبيها[1] أما الضبط في المجال المعلوماتي فيقصد به وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية تلك المتصلة بالجريمة.[2] ولا يرد محل التفتيش إلا على الأشياء المادية لا غير، لأن الأشياء المعنوية لا تصلح لأن تكون محلا لوضع اليد عليها.[3]

ثانيا: الأدلة القابلة للضبط.

توجد العديد من أدلة الاثبات القابلة للضبط في مجال الجرائم المعلوماتية ومن أهمها نذكر ما يلي:

- المخرجات الورقية والمستندات التي تفيد في الكشف عن الحقيقة.
- أجهزة الحاسب الآلي وملحقاتها مثل وحدات المعالجة المركزية أجهزة لوحة المفاتيح وغيرها.
- الأقراص المرنة وأقراص الليزر أو الشرائط الممغنطة والتي قد تحتوي معلومات تفيد في مجريات التحقيق.[4]
- أجهزة المودم وهي الوسائل التي تمكن الحواسيب من الاتصال ببعضها.

---

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دار الفكر الجامعي، مصر، 2007، ص264.

[2] عادل عبد الله خميس المعمري، "التفتيش في الجرائم المعلوماتية"، مجلة الفكر الشرطي، المجلد 22، العدد 86، الإمارات، 2013، ص 267.

[3] نبيلة هبة هروال، مرجع سابق. ص 264.

[4] علي عدنان الفيل، مرجع سابق، ص ص 55-56.

– مختلف برامج الحاسوب حيث تعتبر الأدوات الأساسية التي يستعملها الجاني في تنفيذ جرائمه.

– البطاقات الممغنطة وبطاقات الائتمان والمواد المستعملة في إعدادها حيث تعتبر من قرائن الإثبات.[1]

ثالثا: مدى قابلية جرائم الحاسوب لضبط أدلتها.

ونفرق في ذلك بين حالتين:

أ– ضبط الأدلة المادية للحاسوب:

إن لتحصيل الأدلة في الجرائم الالكترونية يرتبط بعناصر الحاسوب وملحقاته الرئيسية والفرعية والمقصود بذلك الأشياء المنقولة التي يمكن تحريزها أما العقارات التي تحتوي على أجهزة الحاسوب وملحقاته فيتم الحفاظ على ما تشتمل عليه من آثار الجريمة المعلوماتية أو أشياء يصعب نقلها عن طريق وضع الأختام على الأماكن وغلقها وتعيين حراس عليها لمواجهة آثار الجريمة.[2]

والجدير بالإشارة إليه إلى أن وضع أختام وتعيين الحراس على المكان هو رخصة لضابط الشرطة القضائية المسؤولة عن التفتيش وليس واجبا إلا إذا قدر أهميتها في كشف الحقيقة.[3]

ب– ضبط الأدلة المعنوية للحاسوب:

بالنسبة للمكونات المعنوية للحاسوب لقد فرض الواقع ضرورة تفتيشها بالإضافة إلى إباحة إجراء ضبط هذه المكونات، لكن هذا الإجراء لا يكون بالكيفية المنصوص عليها بموجب النصوص التقليدية وذلك لانتفاء الطابع المادي عن هذه البيانات.[4]

---

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 401.

[2] علي حسن محمد الطوالبة، مرجع سابق، ص 142.

[3] المرجع نفسه، ص 143.

[4] بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي: دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي ورو، 2019، ص 66.

ولهذا فقد نظم المشرع الجزائري القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون رقم (09-04) تحت تسمية حجز المعطيات المعلوماتية حيث قضت المادة 06 من نفس القانون على نسخ المعطيات محل البحث، وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية التي تكتشفها السلطات المختصة عند القيام بالتفتيش في المنظومة المعلوماتية وتكون هذه المعطيات تفيد إظهار الحقيقة وقابلة للحجز، وتوضع في الأحراز مع وجوب قيام السلطة المختصة بحماية سلامة المعطيات المخزنة في المنظومة المعلوماتية، كما يجوز استخدام الوسائل التقنية وفقا لما يستهدفه التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتوى المعطيات.[1]

الفرع الثاني: ضبط مراسلات البريد الالكتروني:

يقصد بالمراسلات مختلف الرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات والمحادثات السلكية واللاسلكية وانتهاك حرمتها بضبطها والاطلاع عليها متى كان لذلك فائدة في إظهار الحقيقة.[2]

أما البريد الالكتروني هو إحدى الخدمات المتاحة على شبكة الإنترنت والتي تسمح لأي شخص بإنشاء بريد إلكتروني له يستقبل فيه رسائله الخاصة، وتتم هذه الخدمة في الغالب مجانًا، وهو ما يتميز عن البريد العادي بأن المراسلة تتم في بضع ثوانٍ، بينما البريد العادي يستغرق عدة أيام، فلم يعد فقط وسيلة لتبادل المعلومات والمراسلات، وإنما أصبح وسيلة لإبرام العقود الإلكترونية.[3]

أما فيما يتعلق بالمحافظة على سرية البريد الالكتروني، فقد عالجت نظم البريد الالكتروني هذا الموضوع بابتكار برامج تشفير خاصة بحيث لا يمكن الاطلاع على أية رسالة الا ممن

---

[1] المادة 6 من القانون (09-04)، مرجع سابق.

[2] علي حسن محمد الطوالبة، مرجع سابق، ص 149.

[3] إيهاب فوري السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة للنشر، مصر، 2008، ص 41.

يعرف تلك الشفرة، وهذا ساعد على ظهور ما يسمى بالتوقيع الالكتروني في تيسير عملية التراسل عبر البريد الالكتروني[1]، فالتوقيع الإلكتروني يقوم بعملية محددة ويمنح مصداقية للوثيقة أو المحرر الالكتروني بحيث يمكن من خلال هذا إكساب الوثيقة مصداقية لدى الغير أو الطرف الآخر مستقبل هذا المحرر أو الوثيقة.[2]

أما التعامل مع الرسالة الإلكترونية لا يختلف عن التعامل مع الرسالة الورقية. إذ بمقدور المستخدم أن يطرحها جانبا أو يرد عليها أو ينقلها إلى شخص آخر أو يحفظها في ملف خاص، وكذلك بمقدور المستخدم أن يحفظ بريده الإلكتروني بأحد الطرق التالية الحفظ في صناديق بريد خاصة أو الحفظ في ملفات أو طباعة الرسائل وحفظها في ملفات خاصة مع البريد الورقي التقليدي.[3]

ولكي يتم ضبط الرسائل الالكترونية المشكوك فيها فعلى المحقق اختيار صندوق البريد الخاص بالمتهم محل التفتيش، فإذا كان ذلك الأخير يريد ضبط الرسائل الإلكترونية الواصلة، كان عليه أن يختار خانة الرسائل الواردة، وإذا كان يريد ضبط الرسائل التي أرسلها المتهم كان عليه أن يختار خانة الرسائل الصادرة. وفي حالة ما إذا كان بريد ضبط رسالة كان قد ألغاها المتهم من قبل فعليه اختيار ملفات الحفظ أو سلة المهملات، وفي جميع الحالات المذكورة عليه طباعة تلك الرسالة.[4]

المطلب الثاني: البطلان كجزاء لمخالفة إجراءات التفتيش.

إن التفتيش الذي يجرى دون مراعاة الضمانات القانونية إجراءاته تعد باطلة، وبالتالي يفقد القدرة على إنتاج آثاره التي تنجم عندما يكون صحيحا وهذا ما يصطلح عليه قانونا

---

[1] علي حسن محمد الطوالبة، مرجع سابق، ص 150.

[2] مخلوفي عبد الوهاب، التجارة الالكترونية عبر الأنترنت أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2011، ص 196.

[3] نبيلة هبة هروال، مرجع سابق، ص 277.

[4] المرجع نفسه، ص 278.

بالبطلان، ولذلك سوف يتم تعريف البطلان (الفرع الأول)، وبيان طبيعة بطلان التفتيش (الفرع الثاني) وأخيرا أنواعه (الفرع الثالث).

الفرع الأول: تعريف البطلان.

البطلان وصف يلحق عملاً معينا لمخالفته للقانون مخالفة تؤدي إلى عدم إنتاج الآثار التي يرتبها القانون على هذا العمل لو لم يكن معيبا[1]. كما يعرف الأستاذ أحمد الشافعي البطلان "بأنه جزاء يلحق إجراء نتيجة مخالفته أو إغفاله لقاعدة جوهرية في الإجراءات يترتب عنه عدم إنتاجه لأي أثر قانوني".[2]

فالبطلان جزاء يترتب على مخالفة القاعدة الإجرائية، يحول دون الاعتداد بالأثار القانونية عند مخالفتها، ولهذا فالإجراء يكون باطلا إما بسبب عدم توفره على العناصر اللازمة لصحته، أو لأن من قام به لا يملك الصفة و الاختصاص والسلطة القانونية لمباشرته، أو أن إجراءً جوهريا قد تم إغفاله أولم يتم القيام به حسب الشروط التي فرضها القانون أو أقرها القضاء.[3]

الفرع الثاني: طبيعة بطلان التفتيش.

أما بخصوص طبيعة بطلان التفتيش في القانون الجزائري وبالرجوع إلى المادة 48 من قانون الإجراءات الجزائية. نجدها تنص صراحة على أنه لا بد من مراعاة أحكام المادتين 45 و47 وإلا ترتب عنها البطلان.

كما تنص المادة 44 من ذات القانون على أنه لا يجوز لضابط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقاً أو أشياء

---

[1] المعجم القانوني: أول معجم شامل بكل مصطلحات القانون المتداولة وتعريفاتها، الجزء الأول: من حرف الألف إلى حرف السين، النعمان رياض، دار أسامة للنشر والتوزيع، الأردن، 2013، ص 277.

[2] الشافعي أحمد، البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الديوان الوطني للأشغال التربوية، الجزائر،2004، ص10.

[3] المرجع نفسه، ص 12.

لها علاقة بالأعمال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهاره قبل الدخول إلى المنزل والشروع في التفتيش. إذ لا بد أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها وذلك تحت طائلة البطلان.

نستنتج من خلال هذه المواد أن أي تفتيش يقوم به ضابط الشرطة القضائية ويكون مخالفاً لأحكام المواد 44، 45، 47 يقع باطلا، لأن أي إجراء متعلق بالتفتيش يكون مخالفا للقيود المتعلقة بالإذن والحضور والميقات القانوني من السلطة القضائية المختصة يترتب عليه البطلان وبالتالي فإن ما بني على باطل فهو باطل.

الفرع الثالث: أنواع بطلان التفتيش.

إذا تعلق الأمر بالمصلحة العامة أو النظام العام وصف على أنه بطلان مطلق أما إذا تعلق بمصلحة الخصوم فيعتبر بطلانا نسبيا، وفكرة النظام العام والمصلحة العامة قد يستعصي تعريفه فقها لا سيما أن المشرع الجزائري لم يعط له تعريفا[1]، غير أنه بالرغم من ذلك فالبعض يرى أن الأشكال التي تمس بالنظام العام في الإجراءات التي لا تحمي فحسب مصالح أطراف الدعوى وإنما تتعلق بالمصالح العليا للتنظيم القضائي.[2]

باعتبار قواعد الإجراءات الجزائية قواعد آمرة وليست مكملة ومتعلقة بالنظام العام لا يجوز مخالفتها وإلا ترتب عنها البطلان ويجوز الاحتجاج به في أي مرحلة كانت عليها الدعوى الجزائية، كما يجوز الدفع به لأول مرة أمام محكمة النقض.[3]

ويكون البطلان نسبيا إذا تعلق بمصلحة الخصوم، وذلك عند مخالفة تنفيذ قاعدة إجرائية، إذ لا يقبل الدفع بالبطلان النسبي إلا لمن تقرر البطلان لمصلحته، كما يجوز له التنازل عنه

---

[1] قدواري ابراهيم، التفتيش في قانون الإجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016/2015، ص 66.

[2] بوسقيعة أحسن، التحقيق القضائي، الديوان الوطني للأشغال التربوية، الجزائر، 2003، ص 193.

[3] علي حسن محمد الطوالبة، مرجع سابق، ص 177.

صراحة أو ضمنيا ويمكن أن يصحح برضائهم وليس للمحكمة الدفع بالبطلان من تلقاء نفسها، إلا إذا تمسك صاحب الشأن أمامها، كما يجوز الدفع بالبطلان أمام محكمة الموضوع ولا يجوز الدفع به لأول مرة أمام محكمة النقض.[1]

[1] قدواري إبراهيم، مرجع سابق، ص67.

نستنتج أن دراسة إجراءات التفتيش في جرائم الحاسوب والانترنت تعتبر بلا أدنى شك من الموضوعات المهمة التي وجب دراستها بصورة جيدة ومتأنية وذلك من خلال وضع وإنشاء أجهزة مكلفة بالتحقيق والتفتيش في المنظومة المعلوماتية، بالإضافة إلى ذلك فإن الجرائم الإلكترونية محطة اهتمام كل من العاملين والباحثين والدارسين القانونيين، ولهذا وجب على الأشخاص المكلفين بالتحري وجمع الأدلة و هم رجال الضبطية القضائية أن يقوموا بالإحالة وإلا لمام بكل الوسائل التقنية التي يحتاجونها للقيام بعملهم بكل احترافية وذلك على الرغم من كل المعيقات التي تواجههم نظرا لخصوصية هذا النوع من الجرائم.

وباعتبار أن إجراءات التفتيش والضبط التي تقوم بها أجهزة الضبط القضائي سواء في الجرائم العادية أو الجرائم الواقعة على الحاسوب تمس حقوق الناس وحرياتهم، ولذا وجب أن تتم هذه الإجراءات بصورة صحيحة وقانونية، لأن اللجوء إلى الطرق الغير مشروعة يؤدي إلى بطلان الإجراءات.

الخاتمـــــــــــة

الخاتمــة

يعد التفتيش أشد إجراءات التحقيق أثرا على الحرية الشخصية، وذلك يكون بصورة تتلاءم مع خصوصية الجريمة الالكترونية، ومن خلال دراسة موضوع "الإطار القانوني للتفتيش في الجرائم الإلكترونية" تم التوصل إلى مجموعة من النتائج:

- الجريمة الإلكترونية هي الأفعال المخالفة للقانون التي ترتكب بواسطة الكمبيوتر من خلال شبكة الأنترنت.
- لم تتضمن التشريعات تعريفا للتفتيش لذلك تعددت التعريفات التي صاغها الفقه وجميعها لا تخرج على أنه إجراء من إجراءات التحقيق يهدف إلى البحث عن أدلة مادية لجناية أو جنحة في محل يتمتع بحرمة المسكن أو الشخص، وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المقررة.
- من البحث في مفهوم التفتيش في الجرائم الإلكترونية، اتضح أن التفتيش الواقع مع مكونات الحاسوب المادية لا توجد فيه مشكلة في التنفيذ لسهولة ضبط المكونات المادية فيه، لكن المشكلة تكمن في تفتيش وضبط مكونات الحاسوب المعنوية كون البيانات والمعلومات فيها غير ملموسة.
- طبيعة التكنولوجيا الرقمية عقدت التحدي أمام أعمال التفتيش والضبط بسبب امتداد الأدلة الإلكترونية عبر شبكات الحاسوب في أماكن بعيدة عن الموقع المادي للتفتيش، فإن من الممكن الوصول إليها من خلال الحاسوب بعد أخذ إذن تفتيشه.
- القواعد الشكلية الخاصة بالتفتيش لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، وإنما تقيم بالإضافة إلى مقتضيات الإجراء سياجا يحمي الحريات الفردية.
- إن ضرورة حضور المتهم المعلوماتي عند إجراء التفتيش، وفي حالة غيابه حضور الشهود الذي نص عليهم القانون، ذلك لقابلية نظام الحاسوب للتغيير والتبديل والاتلاف، وبالتالي إمكانية الطعن بسلامة التفتيش وبطلانه، الأمر الذي يترتب عليه الإضرار بمصلحة المشتكى عليه وحرمانه من حقه في الدفاع.

الخاتمــة

- قد أحسن المشرع الجزائري في عدم تحديده لوقت معين إجراء التفتيش في الجرائم الإلكترونية لأنها تكثر أثناء ساعات الليل.
- استحدث المشرع الجزائري نصوص قانونية جديدة أوجد بموجبها قواعد إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية، ويعتبر التفتيش الإلكتروني إحدى هذه الإجراءات التي حملها القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- نقص الخبرة لدى المحققين ورجال الضبط القضائي في مجال الكشف عن المعلومات.
- من بين الوسائل التي تساعد المحقق في الجرائم الإلكترونية هي عناوين الأنترنت كبرتوكول الأنترنت (IP) الموجود بكل جهاز مرتبط بالأنترنت، والذي يساعد على تحديد مكان الحاسب الآلي.
- صعوبة تفتيش أجهزة الحاسب الآلي المرتبطة بجهاز المتهم الذي يحتوي على المعلومات والأدلة الخاصة بالتفتيش.
- يجوز أن يصدر إذن التفتيش مقتصرا على تفتيش الكمبيوتر، فإذا كان الأخير متواجدا في أحد المساكن يتعين توفر شروط تفتيش المساكن، أما إذا كان الكمبيوتر في حيازة شخص خارج مسكنه أو كان في سيارته خارج مسكنه، فإنه يكفي توافر شروط تفتيش الشخص.
- إذا أسفر التفتيش عن ضبط البيانات المتواجدة في نظام المعالجة الآلية فيمكن ضبطها دون ضبط النظام كله، وذلك بأخذ نسخة من البيانات الموجودة، وتلتزم الضبطية القضائية بالتحفظ عليها بشكل يمنع العبث بها وفي حالة مخالفة ذلك يترتب بطلان الإجراءات.
- جواز ضبط البيانات الإلكترونية بمختلف أشكالها ويستند هذا الرأي في ذلك إلى القوانين الإجرائية، فعندما تنص على إصدار الإذن بضبط أي شيء فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة.

الخاتمـة

- إمكانية تطبيق القواعد العامة للبطلان عند مخالفة إجراءات تفتيش نظم الحاسوب والأنترنت.
- إن الدليل المتأتي من عملية التفتيش الالكتروني عبارة عن معلومة أو بيانات خاصة تسجل في أرضيات رقمية وبالتالي يتم التحفظ عليها وتسجيلها على دعائم إلكترونية كوضعها في قرص صلب ليسمح بتقديمه مع ملف الدعوى لقاضي الموضوع.

وبالاعتماد على الدراسة والنتائج السابقة نعرض بعض الاقتراحات المتمثلة في:

- تطوير التشريعات العقابية وإصدار تشريعات جديدة لمواجهة الجرائم المستجدة التي ترتكب عبر الحاسوب وشبكة الأنترنت بسن نصوص تشريعية في قانون العقوبات تجرم هذه الأفعال، بيان كل جريمة ووضع العقوبة المقررة لها خاصة المتعلقة بالتفتيش وضوابطه بما يتناسب وأحكام القانون 09-04 في هذا المجال من أجل إثراء نصوصه.
- الاهتمام أكثر بتكوين ضباط وأفراد الشرطة وأعضاء النيابة العامة والقضاة لمعرفة كيفية التعامل مع إجراءات التحقيق في الجرائم الإلكترونية.
- تزويد الأشخاص المنوط لهم عملية التحقيق بالتقنيات الحديثة للكشف عن المجرم المعلوماتي.
- توسيع وزيادة المصالح في كافة مراكز الشرطة من أجل ضمن السير الحسن لإجراءات التحقيق.
- نشر الوعي لدى الهيئات والشركات وحتى المواطنين الذين قد تتعرض أنظمتهم المعلوماتية للانتهاك، وهذا عن طريق التبليغ عن هاته الجرائم والكشف عنها.

الملاحـــق

الملحق رقم: 1

قضايا الجرائم المعلوماتية المسجلة على مستوى إختصاص أمن ولاية جيجل خلال سنة 2022

01/ القضايا المسجلة حسب النوع:

	نوع القضية		عدد القضايا المسجلة سنة 2022	
1	المساس بأنظمة المعالجة الآلية للمعطيات		19	
2	المساس بالأشخاص عن طريق الأنترنت	القذف	44	134
		السب	23	
		التهديد	21	
		التهديد و الإبتزاز	3	
		إنتحال الهوية	19	
		المساس بالحياة الخاصة	24	
3	النشر و الترويج لمواد إباحية عبر الأنترنت		12	
4	النصب عن طريق الأنترنت		78	
5	جرائم أخرى عن طريق الأنترنت		11	
	المجموع		284	

02/القضايا المسجلة حسب صفة المتورط و الضحية:

السنة	عدد القضايا المسجلة	عدد المتورطين				المجموع	عدد الضحايا				المجموع
		بالغين		قصر			بالغين		قصر		
		ذكور	إناث	ذكور	إناث		ذكور	إناث	ذكور	إناث	
سنة 2022	284	207	7	0	0	214	157	65	3	6	231

قائمــة المراجـــــع

قائمة المصادر والمراجع

أولا: المصادر.

1- المعجم القانوني: أول معجم شامل بكل مصطلحات القانون المتداولة وتعريفاتها، الجزء الأول: من حرف الألف إلى حرف السين، النعمان رياض، دار أسامة للنشر والتوزيع، الأردن، 2013.

ثانيا: المراجع.

1/ الكتب:

1- أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والأنترنت، مكتبة الوفاء القانونية، مصر، 2011.

2- أسامة أحمد المناعسة، جرائم الحاسب الآلي، دار وائل للنشر والتوزيع، عمان، 2001.

3- أشرف عبد القادر قنديل، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة الحديدة، مصر، 2015.

4- إيهاب فوري السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة للنشر، مصر، 2008.

5- الشافعي أحمد، البطلان في قانون الإجراءات الجزائية، دراسة مقارنة، الديوان الوطني للأشغال التربوية، الجزائر، 2004.

6- بوسقيعة أحسن، التحقيق القضائي، الديوان الوطني للأشغال التربوية، الجزائر، 2003.

7- باطلي غنية، الجريمة الإلكترونية، دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، 2015.

8- دلائدة يوسف، قانون الإجراءات الجزائية، دار هومة، الجزائر، 2001.

قائمة المصادر والمراجع

9- هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي: دراسة مقارنة، دار النهضة العربية، القاهرة، 1997.

10- حنان ريحان المبارك المضحكي، الجرائم المعلوماتية: دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2014.

11- طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، مصر، د. س. ن.

12- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت، الجريمة المعلوماتية، الإصدار الثاني، دار الثقافة، الأردن، 2007.

13- محمد أحمد عياينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2006.

14-محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004.

15- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004.

16- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.

17- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة للطباعة والنشر والتوزيع، مصر، 2008.

18- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، مصر، 2007.

19- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن 2010.

20- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2007.

21- عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، مصر، 2012.

22- عبد الفتاح بيومي حجاري، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، 2006.

23- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة، عالم الكتب الحديث للنشر والتوزيع، الأردن، 2004.

24- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية: دراسة مقارنة، المكتب الجامعي الحديث، مصر، 2012.

25- عمرو عيسى الفقى، الجرائم المعلوماتية: جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، مصر، 2006.

26- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، مصر، 2017.

27- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، مصر، 2009.

28- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2011.

29- خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكاتب الحديث، الجزائر، 2012.

30- غاي أحمد، الوجيز في تنظيم ومهام الشرطة القضائية، الطبعة 5، دار هومة للنشر والتوزيع، الجزائر، 2009.

2/ الرسائل والمذكرات الجامعية:

أ- الرسائل:

1- أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، سنة 2021/2020.

2- بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي: دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2019.

3- مخلوفي عبد الوهاب، التجارة الالكترونية عبر الأنترنت أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لحضر، باتنة، 2011.

4- فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2011/2010.

5- تومي يحي، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيات الإعلام والاتصال، رسالة دكتوراه، تخصص قانون، كلية الحقوق جامعة الجزائر 01، 2018.

ب- المذكرات:

- **مذكرات ماجستير:**

1- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر1، 2012.

2- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لحضر، الجزائر، 2012 / 2013.

- **مذكرات ماستر:**

1- بركاني أحمد ياسين، عبادلي فاطمة الزهراء، وسائل وأدلة الإثبات في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في القانون الخاص، تخصص: قانون العقوبات والعلوم الجنائية، كلية الحقوق –تيجاني صدام-، جامعة الإخوة منتوري، قسنطينة -1-، 2017/2016.

2- قدواري ابراهيم، التفتيش في قانون الإجراءات الجزائية الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص: قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016/2015.

3/ المقالات:

1- بوضياف اسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، جامعة محمد بوضياف، المسيلة، سبتمبر 2018.

2- بن طالب ليندا، "التفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، عدد 16، جامعة مولود معمري، تيزي وزو، الجزائر، جوان 2017.

3- هميسي رضا، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، عدد 05، جامعة الوادي، جوان 2012.

4- مانع سلمى، "التفتيش كإجراء التحقيق في الجرائم المعلوماتية"، مجلة العلوم الانسانية، عدد 22، جامعة بسكرة، جوان 2011.

5- عادل عبد الله خميس المعمري، "التفتيش في الجرائم المعلوماتية"، مجلة الفكر الشرطي، المجلد 22، العدد 86، الإمارات، 2013.

6- عثماني عز الدين، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة دائرة البحوث والدراسات السياسية، مخبر المؤسسات النظم السياسية، عدد 04، جامعة تبسة، جانفي 2018.

4/ المقابلات:

1- مقابلة مع إطار في مديرية الأمن الوطني لولاية جيجل، الإحصائيات الملموسة الخاصة بالجرائم الإلكترونية لسنة 2022 على مستوى اختصاص فرقة مكافحة الجرائم الإلكترونية، ولاية جيجل، 2022.

5/ النصوص القانونية:

أ- نصوص تشريعية:

1- القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية الصادر بالجريدة الرسمية، عدد 71، بتاريخ 10 نوفمبر 2004.

2- القانون رقم 04-15 الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم156/66 الصادر في 8 جوان 1966، المتضمن قانون العقوبات، ج ر، العدد 71، سنة 2004.

3- قانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية ج ر، عدد 84، سنة 2006.

4- القانون رقم 09 - 04 الصادر في 05 أوت 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، العدد 47، سنة 2009.

5- الأمر رقم 15-02 المؤرخ في 23 جويلية سنة 2015 يعدل ويتمم الأمر رقم 155/66 المؤرخ في 08 يونيو، سنة 1966 المتضمن قانون الإجراءات الجزائية الجزائري، ج ر، عدد 40، سنة 2015.

6- قانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق لـ 10 جويلية سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، عدد 34، سنة 2018.

7- الأمر رقم 21-11 المؤرخ في 16 محرم عام 1443 الموافق لـ 25 أوت سنة 2021 يتمم الأمر رقم 66-155 المؤرخ في 18 جويلية سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ر، عدد 65، سنة 2021.

ب- نصوص تنظيمية:

1- المرسوم الرئاسي رقم 19-172 المؤرخ في 6 يونيو 20 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 37 في 2019/06/09.

الفهـــــــرس

الفهرس

الفهرس

الفهرس

الفهرس

الملخـــــــص

ملخص المذكرة:

يعد التفتيش في الجريمة الإلكترونية من أهم إجراءات التحقيق، كونه يهدف إلى البحث في مستودع سر المتهم عن أشياء مادية ومعنوية تفيد في الكشف عن الجريمة، ولذا حرص المشرع الجزائري على وضع ضوابط إجرائية خاصة بالتفتيش تعمل على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد وبين تحقيق الفاعلية المطلوبة للأجهزة الأمنية وسلطات التحقيق في كشف غموض الجريمة وضبط فاعليها، والتحقيق معهم، وتقديمهم للمحكمة دون الخروج عن الإجراءات القانونية التي يتطلبها القانون وإلّا ترتب عن ذلك البطلان.

Abstract :

Inspection in cybercrime is considered as one of the most important investigation procedures, as it aims to search the accused's secret repository for tangible and intangible things that are useful in detecting the crime. Therefore, the Algerian legislator was keen to establish procedural controls for inspection that work to establish a balance between individual freedom and the sanctity of the private life of individuals. And between achieving the required effectiveness of the security services and the investigation authorities in uncovering the mystery of the crime and apprehending its perpetrators, investigating them, and bringing them to court without deviating from the legal procedures required by the law, otherwise that would result nullity.