الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة امحمد بوقرة – بومرداس -

كلية الحقوق – بودواو -

قسم القانون العام

التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر في الحقوق

تخصص : قانون عام

إعداد الطلاب :

- بومرداسي مروة
- زموري بدر الدين

إشراف الأستاذة:

العرفي فاطمة

لجنة المناقشة :

الاسم و اللقب	الرتبة	الجامعة	الصفة
أوصيف سعيد	أستاذ محاضر أ	امحمد بوقرة بومرداس	رئيسا
العرفي فاطمة	أستاذة محاضرة أ	امحمد بوقرة بومرداس	مشرفا و مقررا
حبيباتني بثينة	أستاذة مساعدة ب	امحمد بوقرة بومرداس	ممتحنا

السنة الجامعية 2023/2022

شكر وعرفان

نتقدم بجزيل الشكر للمشرفة الأستاذة " العرفي فاطمة " التي تابعت العمل منذ بدايته إلى نهايته و التي أحاطتنا بتوجيهاتها العلمية ، كما ساعدتنا على تخطي عقبات البحث .

لكي كل الشكر و الاحترام .

كما لا ننسى من كان لهم الفضل في تعليمنا في مشوارنا الدراسي منذ بدايته ، خاصة أساتذة قسم القانون العام .

و كما أشكر اللجنة المحترمة لتقييمها

مذكرتي

كل الإحترام و التقدير.

الإهداء

بسم الله الرحمان الرحيم.

الصلاة و السلام على أشرف المرسلين محمد عليه أفضل الصلاة و أزكى السلام.

و الحمد لله على هذا العمل و على إتمام مشواري الدراسي و على وصولي هذه المرحلة ، الحمد لله حمدا كثيرا على هذا التوفيق .

أما بعد :

أهدي هذا العمل المتواضع الى من أفضلها على نفسي و لم لا . فقد ضحت من أجلي و لم تدخر جهدا في سبيل سعادتي على الدوام ، إلى منبع الحب و الحنان ، غاليتي التي سهرت و كانت معي في أسوء حالاتي ، التي انتظرت بفارغ صبرها هذه اللحظة و انتظرتني لأصبح خريجة و ها اليوم تحقق بفضل الله ما انتظرته ، شكرا لكي .

ينير في دروب الحياة و يبقى من يسيطر على أذهاننا في كل مسلك نسلكه ، صاحب الوجه الطيب ، و الأفعال الحسنة ، فلم يبخل علي طيلة حياته ، الذي أعطاني كل شيء و أنار لي دربي والدي العزيز

أرجو من الله أن يمد في عمرهما (والديا)

إلى سر سعادتي إخوتي ، حبيبتي جميلة و روحي عبد الرحمان

كما أخص بالذكر من كانت سندا لي أختي و أمي الثانية غاليتي و عزيزتي يسرى.

إلى عائلتي الثانية ، خالتي وسيلة التي لطالما ساندتي و دعمتني منذ الصغر ، أخوالي الثلاثة أحمد ، عبد السلام و بالأخص خالي الصغير رحيم الغائب و ابنه كتري

إلى روحي الثاني جدي عمر الذي دعمني في كل مشواري الدراسي و انتظر لحظة تخرجي ، أدامك الله فوق رأسي و لك الشكر .

إلى من جمعني بهم القدر ، أجمل الصدف في حياتي أصدقائي أصحاب القلوب النقية و من جمعتني بهم أحلى الذكريات . و إلى كل قريب لقلبي .

أهديكم هذا العمل و أتمنى أن يحوز على رضاكم.

وصلت رحلتي الجامعية إلى نهايتها بعد تعب و مشقة و ها أنا أختم بحث تخرجي بكل هم و نشاط و توفيق من الله عز وجل

بومرداسي مروة

الإهداء

الحمد لله و الصلاة و السلام على من لا نبي بعده سيدنا المصطفى الأمين و نحمد الله الذي وفقنا في مشوارنا الدراسي .

أهدي هذه المذكرة إلى من سهرت ليال طويلة من أجل راحتي و من استيقظت فجرا من أجل الدعاء لي أمي الحبيبة

إلى أغلى ما في الكون ذلك الرجل الذي لم يعجز لحظة في مساعدتي و الوقوف بجانبي في أيام الشدائد أبي العزيز

الى روح جدتي الحنون التي لم يأتي مثلها أبدا و لم يعوض مكانها أحد رحمة الله عليك.

دون أن أنسى إخوتي و أخواتي الذين كانوا لي سندا في مشواري الدراسي و أهديها إلى أصدقائي الذين رافقوني طوال مسيرتي الدراسية و قاسموني لحظات حياتي .

و في الأخير أشكر جميع أسرة كلية الحقوق بودواو و من أساتذة و إداريين و عمال النظافة على سهرهم في راحة الطالب و كل من ساعدنا من قريب أو بعيد في انجاز هذه المذكرة .

زموري بدرالدين

مقدمة

مقدمة

لقد دخلت البشرية في بداية الألفية الثالثة مرحلة جديدة من التطور الفكري والمعرفي، وذلك بفضل الثورة العلمية التكنولوجية في مجال الإتصالات والمعلومات التي اقتحمت بقوة هذه المرحلة, ولا شك أن هذه الثورة المعلوماتية الهائلة قد انعكست بصورة إيجابية على كثير من جوانب الحياة المعاصرة، بسبب ماتوفره من الوقت والجهد والتكلفة عن الإنسان تجعل حياته اليومية أكثر سهولة ويسر، الأمر الذي أدى إلى تضاعف الطلب على التقنيات التي تقوم عليها هذه الثورة والمتمثلة في الحواسب الآلية والشبكات المعلوماتية، وتوسع ميادين استعمالها وازداد الاعتماد عليها بشكل مفرط في كل القطاعات العامة أوالخاصة، إلى حد يبدو من الصعب على هذه القطاعات أداء نشاطاتها دون الإستعانة بشكل أساسي على هذه التقنيات الحديثة، غير أن هذا بسبب تطور الانسان في شتى الميادين، خصوصا في مجال التقنية وظهور هذا الحاسوب الآلي وشبكة الأنترنت، وغزت هذه الوسيلتين جميع المجالات لماتتسم به من الدقة والسرعة، وأصبحت في متناول الجميع، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم، ونوع جديد من المجرمين، وهو الإنعكاس السلبي لهذه الثورة العلمية.

فالجريمة ظاهرة قديمة، عرفتها المجتمعات البشرية منذ القدم ، و ظهرت في هذه المجتمعات السلطة الحاكمة إنطلاقا من رب الأسرة إلى شيخ القبيلة، حيث وضعت بعض القيود على تصرفات الأفراد لاستتباب الأمن لدى الفرد والمجتمع، واعتبرت أن كل فعل يمس أمن الجماعة أو حياة الفرد أو ماله وسلامته الجسدية ، فعل مجرم يسحق العقاب عليه.

حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الإلكترونية، فهذه التقنية تسمح بنقل المعلومة صوتا و صورة عبر الأنترنت، وفي أي مكان من العالم مما يسمح للبعض استغلال هذه الشبكة في ارتكاب جرائمهم وهذا يعتبر خطر يهدد المجتمع والعالم ككل، وتختلف هذه الجرائم اختلافا كبيرا عن غيرها من الجرائم التقليدية

في وسائل ارتكابها وفي طبيعة الأشخاص الذين يقومون بها وكذلك تختلف عنها في مسرح الجريمة.

وبالتالي مشكلة البحث على الجريمة في البيئة الإلكترونية تنبع من طبيعة هذا النوع المستحدث من الإجرام فهي جريمة تتعلق ببيانات معالجة إلكترونيا وكيانات غير مادية يصعب الكشف عنها، ويصعب في غالب الأحيان جمع الأدلة بشأنها والتفتيش عنها بالطرق المألوفة في الجريمة التقليدية وتزداد المهمة صعوبة عندما يتعلق الأمر بتفتيش بيانات وأنظمة معلوماتية موجودة خارج النطاق الوطني, لأن الأمر قد يصطدم بسيادة دولة أخرى في الحالة التي يلجأ فيها بعض المجرمين إلى تخزين البيانات أو المعلومات المتعلقة بالجريمة بالخارج، كما يثير التفتيش في مجال أنظمة الإتصال الإلكترونية ضرورة وضع ضوابط إجرائية لها، تعمل على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد وبين تحقيق الفاعلية أثناء عملية التحقيق وكشف الجريمة وضبط فاعليها وتقديمهم للمحاكمة.

غير أن التفتيش هو إجراء من الإجراءات التي تهدف إلى البحث عن ملابسات الجريمة وهو اجراء يمس حقوق الانسان كونه يتعلق بخصوصيته وبسره، وهو الوسيلة التي يتم بموجبها كشف الحقيقة وضبط الأدلة الجنائية على الجريمة الإلكترونية وصحة إسنادها إلى الجاني.

وتنبع أهمية الدراسة من أهمية الموضوعات التي تعالجها وحداثها، فالتفتيش في الجرائم الإلكترونية وكيفية ضبط الأدلة الإلكترونية الرقمية وجمعها من الموضوعات المستجدة كما أن طبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية، لذلك تسلية التعامل القاضي مع الأدلة الرقمية تسلط هذه الدراسة الضوء على كيفية وزنه لها وتحديد قيمتها في الإثبات الجزائي.

وتنبع كذلك أهمية الدراسة من معالجاتها لجوانب النقص في النظام القانوني والعلمي وتطبيقي.

الإشكالية التي يمكن طرحها لهذا الموضوع ومن ثم معالجتها تتمثل في: **ما مدى فعالية التفتيش الإلكتروني باعتباره إجراء للتحقيق في الكشف عن الجريمة المعلوماتية ومرتكبيها؟**

حيث تتفرع هذه الإشكالية الرئيسية إلى جملة من التساؤلات الفرعية التي من شأنها أن تساهم في فهم وتحليل الموضوع وتندرج فيما يلي :

- ما المقصود بالتفتيش الإلكتروني؟
- ما هو دور التفتيش الإلكتروني بالنسبة للجرائم المعلوماتية؟
- فيما يكمن دور مسرح الجريمة بالنسبة للتفتيش الإلكتروني؟
- ماهو المحل الذي ينصب عليه التفتيش الإلكتروني في الجرائم المعلوماتية؟
- ما هي الضوابط الموضوعية والشكلية التي يخضع لها التفتيش الإلكتروني أثناء التحقيق في الجرائم المعلوماتية؟
- ما هي حجية الدليل الإلكتروني؟

ومن أسباب إختيار موضوع "التفتيش "الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية" يرجع في حقيقة الأمر إلى العديد من الأسباب بعضها ذاتية والأخرى موضوعية، فالأسباب الذاتية تكمن في إهتمامي بمجال المعلوماتية واجراء المتابعة في جريمة المعالجة الآلية للمعطيات التي تختلف كل الإختلاف عن إجراءات التحقيق والتفتيش التقليدية, وتجعل العقل يفكر في شكل مسرح الجريمة وطريقة التفتيش, وهذا ما أعطاني دافع للبحث وحب التعرف عليها باعتبارها متعلقة بالعالم الإفتراضي، أما الأسباب الموضوعية تتمثل في كون أن الجريمة الإلكترونية موضوع حديث يمس الواقع المعاش, كما أن الجريمة الإلكترونية تمس كل القطاعات ويساعد ذلك على إنتشار هذا النوع من الجرائم.

تسعى هذه الدراسة إلى أهداف منه الوقوف على النصوص والأحكام القانونية المنظمة لإجراء التفتيش الإلكتروني ومعرفة مدى فعاليتها في التصدي الجريمة المعلوماتية والحد من خطورتها المتزايدة من خلال الكشف عن الأدلة التي ترتكب بها هذه الجريمة وكذا الوصول الى مرتكبيها.

اعتمدنا في بحثنا على بعض الدراسات السابقة ذات الصلة بالموضوع فنذكر منها :

-عبد القادر كيحول مذكرة ضمن متطلبات نيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية كلية الحقوق والعلوم السياسية جامعة زيان عاشور الجلفة لسنة 2019- 2020 حيث تضمن ماهية التفتيش الإلكتروني والتحقيق في الجرائم المعلوماتية عن طريق التفتيش الإلكتروني وتناول التحقيق الإبتدائي وآليته وغيرها، وانطلقنا من هذه الدراسة أنه لم يركز على التفتيش كعنصر محدد وعدم ذكره لمسرح الجريمة الذي تناولناه في دراساتنا غير أنه توسع وذكر كل إجراءات التحقيق وهذا غير مطلوب وغير مهم في هذه الدراسة.

وهذا ما يدل على الصعوبات والمعوقات المتلقاه من خلال البحث والدراسة المقدمة وتكمن في؛ دور المشرع في محاولته للتماشي مع باقي التشريعات للتصدي لهذه الجرائم وتفتيشها، وكذا المعطيات والمعلومات الناقصة التي تسبح في العالم الافتراضي وقلة المراجع وصعوبة التنسيق نظرا لتقليص وصغر الموضوع وضبطه في عنصر واحد.

تعتمد الدراسة في سبيل مناقشة موضوعها على المنهج التحليلي وذلك من خلال تحليل النصوص والأحكام القانونية المنظمة لإجراء التفتيش الإلكتروني ومحاولة شرح مضمونها.

انطلاقا من هذا تم الاعتماد على خطة ثنائية مكونة من فصلين وهما:

الفصل الأول: مدخل مفاهيمي للتفتيش الإلكتروني في الجرائم المعلوماتية

المبحث الأول: ماهية الجرائم المعلوماتية

المبحث الثاني: ماهية التفتيش الإلكتروني

الفصل الثاني: ضوابط التفتيش الإلكتروني

المبحث الأول: شروط التفتيش الإلكتروني

المبحث الثاني: حجية الدليل الرقمي في إثبات الجريمة المعلوماتية

الفصل الأول :

مدخل مفاهيمي للتفتيش الإلكتروني في الجرائم المعلوماتية

الفصل الأول: مدخل مفاهيمي للتفتيش الإلكتروني في الجرائم المعلوماتية

لقد ظهر حديثا نمطا جديد من الجرائم، نظرا للتحولات الإقتصادية والإجتماعية والثقافية تجسد في الجرائم المعلوماتية وهي بذاتها أصبحت خطرا على الأفراد والمؤسسات وبياناتهم ولذلك أصبحت ترتكب جرائم بوسائل إلكترونية، و أصبحت تعاني المجتمعات الإلكترونية من إنتهاك لحقوقها وخصوصياتها الإلكترونية لسبب إنتشار الجريمة الإلكترونية، الأمر الذي دفع الدول إلى الحد من هذه الجرائم التي تلحق الضرر بالأفراد، ومن إجراءات مكافحتها والتعرف عليها لا بد من عملية إجراء التفتيش وهو التفتيش في منظومة معلوماتية، وهو من أهم وأخطر إجراءات التحقيق المقررة في الجرائم المعلوماتية وقد يفسر عنه من أدلة تؤدي إلى كشف الحقيقة عن الجريمة التي وقعت باستخدام النظام المعلوماتي، ولتحليلنا لهذه الدراسة لا بد من تقسيم هذا الفصل إلى مبحثين ولنخصص المبحث الأول إلى ماهية الجرائم المعلوماتية، والمبحث الثاني تحت عنوان ماهية التفتيش الإلكتروني.

المبحث الأول: ماهية الجرائم المعلوماتية

أدت الثورة التكنولوجية في مجال الإعلام والاتصال إلى ظهور سلوكيات تنطوي على المساس والإعتداء والإستغلال في ارتكاب جرائم جديدة، مما صعب مهمة ملاحقة المجرمين عن طريق النصوص القانونية التقليدية وهذا ما استغله الجناة لارتكاب أفعال اعتداء عن التقنية والمتعاملين بها، وقد حاولت الكثير من التشريعات الداخلية والجهود الدولية لتوفير حماية جزائية لتكنولوجيا المعلومات غير أن هذه المحاولات اصطدمت بعدة عوائق منها عدم الإتفاق عن مفهوم محدد لما يدخل وما يعد من تكنولوجيا المعلومات أو لإدخالها.

وعليه سنقسم هذا المبحث إلى مطلبين، المطلب الأول مفهوم الجرائم المعلوماتية، أما المطلب الثاني أنواع الجرائم المعلوماتية.

المطلب الأول: مفهوم الجرائم المعلوماتية

تعد الجرائم المعلوماتية أو الإلكترونية من الجرائم المستحدثة التي ظهرت في عصرنا الحديث وهذا بسبب ارتباط هذه الجرائم بالوسائل الحديثة من كمبيوتر وشبكة الأنترنت ومواقع إلكترونية.

ومنه نحاول تقسيم هذا المطلب إلى فرعين (02) يخص الفرع الأول لتعريف الجرائم المعلوماتية، أما بخصوص الفرع الثاني سنتناول فيه خصائص الجرائم الإلكترونية.

الفرع الأول: تعريف الجرائم الإلكترونية

منذ ظهور هذه الجرائم حاولت التشريعات حول العالم إعطاء تعريف جامع ومانع لهذا النوع من الجرائم المعلوماتية ووضع الجزاء المناسب لها.

ورغم ذلك لا يوجد تعريف قانوني موحد حيث أن المشرع الجزائري لم يعطي تعريف للجريمة الإلكترونية وإنما تبنى للدلالة عن الجريمة بمصطلح المساس بأنظمة المعالجة الآلية

للمعطيات معتبرًا أنّ النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية هو محل للجريمة، فيما عرفها نظام مكافحة الجرائم المعلوماتية السعودي في المادة 1/8 أنها: "أي فعل يرتكب متضمنا إستخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[1] فيجب أولا استخدام الحاسوب أو الأنترنت في ارتكاب الجريمة وبهذا تبنى المفهوم الضيق للجريمة الإلكترونية.

كما عرفه المشرع القطري في المادة الأولى من قانون مكافحة الجرائم الإلكترونية رقم 14 لسنة 2014 أنه : "أي فعل ينطوي عن استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية بطريقة غير مشروعة بما يخالف أحكام القانون"[2] وبهذا التعريف أخذ المشرع الجزائري بالتعريف الموسع للجريمة الإلكترونية .

أما بالنسبة للتعريف الفقهي فقد بذلت جهود كبيرة للوصول إلى تعريف متفق عليه غير أنها باءت بالفشل فقد عرف البعض من الفقهاء هذه الجريمة بالاستناد إلى وسيلة ارتكاب هذه الجرائم حيث اسند هذا الاتجاه في تعريفه أنها: " كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي"[3]. أي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب. ويستخدم في اقترافه كأداة رئيسية.

غير أن هذا الاتجاه تم انتقاده حيث لا يمكن مجرد استخدام الحاسب الآلي جريمة إلكترونية. فيما يذهب أنصار الإتجاه الثاني إلى الإستناد إلى موضوعها حيث عرف مؤيدو هذه النظرية الجريمة الإلكترونية على أنها: " نشاط موجه لنسخ أو تغيير أو حذف أو الوصول إلى

[1] عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، كلية الحقوق جامعة مؤتة، الطبعة الأولى، 2017، ص40.

[2] المرجع نفسه، ص40.

[3] سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار شتات للنشر والبرمجيات، مصر، كلية الحقوق والعلوم السياسية، جامعة السليمانية، ص19.

المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه"[1]. أي هي كل سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الحاسوب. وتعرض هذا الإتجاه إلى النقد لإسناده على المعلومات محل الجريمة متجاهلا دور الحاسوب في وقوع هذه الجرائم أيضا .

فيما يرى أنصار الإتجاه الثالث أن الجريمة الإلكترونية لا تتم إلا بوجود معرفة فنية باستخدام الحاسوب حيث أوردو في هذا الخصوص عدة تعريفات وقد عرفوا الجريمة الإلكترونية بأنها: " أي فعل مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا"[2]. أي هي واقعة تتضمن تقنية الحاسوب ومجنى عليه يمكن أن يتكبد خسارة وفاعل يحصل عن قصد أو يمكنه الحصول على مكسب, حيث تعرض هذا الإتجاه كونه ضيق بنحو كبير من نطاق الجريمة الإلكترونية إضافة إلى أنه يمكن ارتكاب الجريمة دون الحاجة إلى معرفة فنية كبيرة بالحاسوب.

فيما تبنى البعض الآخر نظام أو معيار مزدوج للتعريف بالجرائم الإلكترونية واستندوا على أداة ارتكاب الجرائم وموضوعها حقا حيث عرفوها على أنها: " أي عمل ليس له في القانون أو العرف جزاء ويضرب بالأشخاص والأموال ويوجب ضد التقنية المتقدمة لنظم المعلومات"[3].

مع اختلاف التعريفات للجريمة الإلكترونية في تشريعات العالم والفقه إلا أنها جميعها تتفق على تجريمها ورغم التباين والاختلاف وهذا راجع إلى اختلاف المستوى الرقمي أو التكنولوجي بالنسبة للدول المتقدمة.

وسعى المشرع الجزائري لتجريم هذه الأعمال الماسة بأنظمة الحاسب الآلي وذلك لمواكبة التطور الهائل الحاصل في مجال الإتصال كل هذه التغيرات قادت المشرع إلى تعديل قانون

---

[1] سامي جلال فقي حسين، مرجع سابق , ص20.

[2] المرجع نفسه ، ص21.

[3] المرجع نفسه ، ص22.

العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وتضمن هذا القسم 8 مواد من المادة 394 إلى 394 مكرر ونذكر على سبيل المثال بعض المواد التي تضمن هذا القانون المادة 394 مكرر 2.[1] على أن يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.000دج إلى 5000.000دج كل من يقوم عمدا أو عن طريق الغش بما يأتي ، 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 إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.[2]

ومن خلال ما تقدم من تعريفات للجريمة الإلكترونية في التشريع الجزائري نستنتج أو موقف المشرع من هذه الجريمة، في أن تقدم التكنولوجي وانتشار وسائل الإتصال الحديثة أدى إلى بروز إجرام فني في أشكال مستجدة ، مما دعى إلى النص على معاقبة هذا النوع من الجرائم تسعى من خلالها إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تتدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها.

[1] الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 الذي يتضمن قانون العقوبات المعدل والمتمم.

[2] سعيدة بعرة، الجرمية الإلكترونية في التشريع الجزائري (دراسة مقارنة)، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة محمد خيضر بسكرة، سنة 2015-2016، ص62.

وهي في الأخير ورغم تجريم المشرع الجزائري وكل تشريعات العالم الجرائم الإلكترونية عن طريق قانون العقوبات والقوانين الخاصة بالإضافة إلى إقرار أجهزة خاصة لمتابعة ومكافحة هذه الجريمة لكنّها تتطور يوما بعد يوم مع تطور وسائل التكنولوجيا.

الفرع الثاني: خصائص الجرائم المعلوماتية

تختلف الجريمة الإلكترونية عن الجريمة العادية ويرجع هذا إلى مجموعة من الخصائص والمميزات التي تميز بعضها، وهذا بسبب إرتباطها بنظام المعلومات والتكنولوجية، وذلك جعلها تأخذ طابعا خاصا بمجموعة الخصائص وسيتم ذكرها في النقاط التالية:

أولا: الجريمة المعلوماتية جريمة عابرة للحدود

حيث عرف العالم الأنترنت وهي شبكة عالمية أو الشبكة العنكبوتية أو شبكة الشبكات تتعدى الحدود الدولية، وهذا يعني أن المجرم المعلوماتي قد يرتكب جريمة من مكان بعيد عن تواجد الضحية بأبعد مكان.[1] فلا مجال للتحدث عن الحدود الجغرافية للجريمة الإلكترونية.

ثانيا: صعوبة إكتشاف الجريمة الإلكترونية

بمجرد عدم ترك آثار مادية خارجية لهذه الجريمة، قد يصعب إكتشاف هذه الجريمة الإلكترونية، كما أنّ المجرم المعلوماتي بإمكانه أن يدمر دليل الإدانة في أقل من ثانية إضافة إلى أن الجريمة الإلكترونية تتم في عالم إفتراضي مما يجعلها تتم خفية لسبب التلاعب الإلكتروني[2].

ثالثا: سرعة التنفيذ

ويعني ذلك أن الجريمة الإلكترونية لا تتطلب وقتا طويلا لتنفيذها، بمجرد كبسة زر تتم ولهذا أطلق تسمية الجرائم السرعة الفائقة لتنفيذها وعدم اللجوء إلى العنف فيها.

---

[1] عيدة بلعايد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو، الأغواط، العدد السادس (06)، مارس 2021، ص134.

[2] المرجع نفسه ، ص135.

رابعا: صعوبة اثبات الجريمة المعلوماتية

تكمن صعوبة ذلك في بساطة وسهولة محو الدليل الرقمي و صعوبة إكتشاف الجريمة الإلكترونية، وسبب صعوبة إثباتها أيضا نقص الخبرة لدى المكلفين بالتحقيق وهذا سبب مباشر، ويؤدي ذلك بإفلات المجرم المعلوماتي من الجزاء.[1]

خامسا: الجريمة المعلوماتية جريمة منظمة

باعتبار الجريمة الإلكترونية جريمة منظمة تقوم بها عصابات متعددة ومنظمة، وهذا راجع إلى تتابع الاعتداءات على الشبكات الدولية المعلوماتية وأنظمة المعالجة الآلية للمعطيات فجعلها ذات حيز دولي ، كجريمة تبيض الأموال عن طريق الوسائط الإلكترونية، قرصنة المعلومات والحقوق الفكرية والفنية، الغش في البطاقات البنكية.[2]

المطلب الثاني: أنواع الجرائم المعلوماتية

أصبح إستعمال الأنظمة المعلوماتية مفرط وانتشر في مجالات مهمة فجعلها تحت مرصاد المجرمين، حيث نتج عن ذلك نشاط إجرامي الحاصل على البرمجيات الإلكترونية و ولد ذلك أنواع مختلفة من الجرائم.

ولتوضيح ذلك سنقسم هذا المطلب إلى فرعين (02)، الفرع الأول الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي أما الفرع الثاني للجرائم المعلوماتية الواقعة على النظام المعلوماتي.

الفرع الأول: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

حيث في هذه الجرائم محل الجريمة لا يكون النظام المعلوماتي محل الجريمة، فالوسيلة التي تسهل النتيجة الإجرامية تكون الحاسب الآلي باستخدام النظام المعلوماتي، فمن وراء ذلك يكون الهدف هو الربح بطريق غير مشروع، كالإعتداء على أموال الغير،الإعتداء على

---

2 عيدة بلعايد ، مرجع سابق ، ص135.

[2]المرجع نفسه ، ص135.

الأشخاص وسلامتهم وحياتهم الخاصة، أو في سمعتهم وشرفهم والاعتداء على أمن الدولة وأسرارها.[1]

أولا: الجرائم الواقعة على الأشخاص أو الجرائم ضد النفس

فهي التي تهدد بالخطر أو تنال بالإعتداء، حيث أن الشبكة المعلوماتية رغم ما جاءت به من الإيجابيات والفوائد والتسهيلات المقدمة للفرد، إلا أنها جعلته أكثر عرضة للإنتهاك، فهي كذلك الجرائم الإلكترونية التي تمس بسمعة الأشخاص وتضربهم ماديا ومعنويا، حيث أننا حاولنا تلخيص بعض الجرائم الإلكترونية التي تقع على الأشخاص الأكثر حدوثا فنذكر منها:

1. **جريمة التهديد:** أي أنه يضغط على إرادة الإنسان ويزرع الخوف في نفسه من أضرار ما ستلحقه أو ستلحق أشخاص له صلة، وهذا ما يسمى بالوعيد و يجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس أو مال الغير، فالتهديد قد يكون مصحوبا بأمر أو طلب من أجل القيام بفعل أو الإمتناع عن الفعل أو لمجرد الإنتقام، ولهذا أصبحت الأنترنت الوسيلة لارتكاب جرائم التهديد عن طريق البريد الإلكتروني، الويب...[2]
2. **انتحال الشخصية:** وهي أن يستخدم شخصية فرد من أجل الإستفادة من ماله أو سمعته أو مكانته، فعرفت بسرعة الإنتشار وخاصة في الأوساط التجارية، حيث تكون عن طريق جمع قد كبير من المعلومات الشخصية للفرد المراد انتحال شخصيته، فهذه المعلومات تساعده لارتكاب جرائمه ويستفيد منها ويتم هذا عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة كالاسم، العنوان الشخصي، رقم بطاقة الائتمان...،

[1] سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018، ص241.

[2] المرجع نفسه ، ص241.

من أجل أن يصل لماله أو سمعته... عن طريق الغش وسنذكر بعض الجرائم التي من الممكن انتحال الشخصية فيها.

1.2 **انتحال شخصية أحد المواقع:**أي أن يخترق أحد المواقع من أجل السيطرة عليه، ثم يقوم باستعمال برنامجه الخاص هناك، باسم الموقع المشهور.[1]

2.2 جرائم السب والقذف: قد تختلف التسميات إلا أن الضرر يعود ضررا واحدا، فالسب يقصد به الشتم أي إعتداء على الأشخاص باللفظ، وفي معناه القانوني فقد تناولنا المشرع الجزائري في القسم الخامس من تحت عنوان الإعتداء على شرف وإعتبار الأشخاص، من خلال المادة 297 من قانون العقوبات رقم 21-08 المعدل والمتمم.[2] " يعد سبا اكل تغيير مشين أو عبارة تتضمن تحقيرا أو لا ينطوي على إسناد واقعة ".

حيث عرف من خلال المادة 296 من نفس القانون ، القذف على أنه, يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف وإعتبار الأشخاص أو الهيئة المدعي عليها به أو إسنادها إليهم أو إلى تلك الهيئة. ويعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة " ، ويقوم المنتحل بذلك إلى السب والقذف عن طريق المطبوعات أو الرسوم تكون كتابيا عبر البريد الإلكتروني أو الصوتي، صفحات الويب بعبارات تمس الشرف، وبذلك ينشر المجرم معلومات خاطئة عن الضحية وبذلك تصل هذه المعلومات إلى عدد كبير من مستخدمي شبكة الأنترنت عن طريق نشرها من طرف المجرم.[3]

---

[1] سورية ديش، مرجع سابق، ص242.

[2] أمر رقم 21-08 مؤرخ في 27 شوال عام 1442 الموافق لـ 8 يونيو سنة 2021، يعدل ويتمم الأمر رقم 66-156 المؤرخ في18 صفر عام 1386 الموافق ل 8 يونيو 1966و المتضمن قانون العقوبات .

[3] سورية ديش، مرجع سابق، ص242.

3.2 **المواقع الإباحية والدعارة:**فقد توجد مواقع على الأنترنت تحرض على ممارسة الجنس للكبار والقصر، ويتم ذلك بنشر صور جنسية تحرض على ممارسة المحرمات والجرائم المخلة بالحياء عن طريق صور ومقاطع الفيديو المخلة بالآداب على مواقع الأنترنت من أجل أن يتداولها الشباب ويفسد بذلك أفكارهم وإضعاف إيمانهم فتسهل الشبكة القيام بالدعارة، عبر آلاف المواقع الإباحية وتسوق الدعارة وتستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.

3. التشهير وتشويه السمعة:ينشر من خلال ذلك المجرم معلومات مغلوطة وسرية عن الضحية، فيكون فردا أو مؤسسة تجارية أو سياسية، فهذا النوع من الجرائم تتعدد فيه الوسائل المستخدمة، ولكن من ضمن هذه الوسائل توجد في المقدمة وسيلة إنشاء موقع على الشبكة يتضمن المعلومات المطلوب نشرها.

وكذلك ترسل هذه المعلومات إلى أعداد كبيرة من المستخدمين عبر القوائم البريدية ، وهذه الجرائم تضم تشويه السمعة، الشائعات والأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية من أجل أن يشك الناس في مصداقية هؤلاء الأفراد ، فالهدف من ذلك قد يكون الإبتزاز.[1]

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كفلها القانون وفي مقدمته الدستور الجزائري حيث تنص المادة 40 من دستور 2016 المعدلة والمتممة في التعديل الدستوري الأخير لسنة 2020 بالمادة 39 حيث تنص: " تضمن الدولة عدم انتهاك حرمة الإنسان" [2].

[1]سورية ديش، مرجع سابق ، ص243.

[2]القانون رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر سنة 2020، في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية (ج، ر رقم 82 ل 30 ديسمبر 2020).

وعليه يمكن استخدام الشبكة المعلوماتية في الإعتداء على حرمة الفرد وحياته الخاصة وحرمته، والحريات العامة للأفراد، وهو مخالف للقانون ومعاقب عليه.

ثانيا: الجرائم الواقعة على الأموال

أصبحت المعاملات التجارية كالشراء، البيع والإيجار تتم عبر الشبكة المعلوماتية، وما انجز عليه من وسائل الدفع والوفاء ، فابتكرت معه طرق ووسائل للسطو على هذا التداول المالي بطريق غير مشروع كالتحويل الإلكتروني ، السرقة، القرصنة وغيرها.

وهذه الجرائم التي تنال بالإعتداء وتهدد بالخطر الحقوق ذات القيمة المالية، ومن أهم تطبيقات هذه الجرائم في نطاق الجرائم المعلوماتية وهي أنواع:

1. **السرقة الواقعة على البنوك:**يتم اختلاس البيانات والمعلومات الشخصية للمجني عليهم، وذلك يعد سرقة للمال بالطرق المعلوماتية ، ويستخدم شخصية الضحية ليقوم بعملية السرقة المتخفية، ومنه أيضا يستخدم الجاني الحاسب الآلي ليقوم بدخول إلى شبكة الأنترنت والوصول إلى المصارف والبنوك، ويحول الأموال الخاصة بالعملات إلى حسابات أخرى،[1] ويسمى بالتحويل البنكي للأموال الإلكتروني.
2. **تجارة المخدرات عبر الانترنت:**تتعلق بالترويج للمخدرات وبيعها، والتحريض على استخدامها، وصناعتها بمختلف أنواعها.
3. **غسيل الأموال:** تختلف تسمياتها وتتعدد بين غسيل الأموال أو تنظيفها، أو تبييضها أو تطهيرها، فتعددت كذلك التعريفات غير أن المعنى واحدة فيقصد بها مجموعة العمليات هذا الطبيعة الإقتصادية تغير صفة المال وتخفي طبيعته وتمويه مصدره الذي جاء من مصدر غير مشروع ليظهر وكأنه نشأ عن مصدر مشروع .

[1] سورية ديش، مرجع سابق، ص243.

حيث يعرفه البعض أنه فعل مرتكب غرضه ايجاد مبرر كاذب لمصدر الأموال الصادرة بصورة مباشرة أو غير مباشرة عن عمل غير مشروع.[1]

أي أن عملية غسيل الأموال تتم عن طريق أربعة عناصر مهمة ورئيسية لا تقوم الجريمة بدون أحدها، وتتمثل في: الأموال القذرة، مصدر زائف، الأنشطة، المخادعة وأطراف التنفيذ والذي هو الشخص أو الأشخاص الذين يقومون بعملية الغسل.[2]

فهي جريمة عابرة للحدود باعتبارها ظاهرة عالمية منتشرة تشمل عدة دول ولا ترتبط بنظام سياسي محدد، فهي كذلك جريمة لاحقة ومنظمة، كونها لاحقة لأنشطة جرمية سابقة، أولها ارتكاب جريمة حققت أرباح مالية ، وتليها مرحلة غسل الأموال أما منظمة كونها غير عادية مخططة ، دقيقة.

4. **الاستعمال غير الشرعي للبطاقات الإئتمائية:** في الوقت الحالي أصبحت البطاقة الائتمانية من الأشياء التي تستخدم بكثرة والمعروفة لدى أغلبية المجتمع، فهي تعرف على أنها يتم استيلاءها باعتبارها نقود إلكترونية، يقومون بسرقة أرقام البطاقات لبيع المعلومات للآخرين من خلال الحصول على كلمة السر المدرجة في أنظمة الحاسب الآلي للضحية عن طريق احتياله، أن يتحصل على ربح فيقدم للضحية معلومات تسهل للجاني من التصرف في ماله.[3]

وكذلك يقوم السارق باستعمال البطاقة للحصول على السلع والخدمات أو سحب مبالغ مالية من أجهزة توزيع الالي أو السحب باستخدام بطاقة ضرورة.

5. **القرصنة الإلكترونية:**فهي تخريب أو إلغاء أو تعديل محتوى أو سرقته والقيام بتحديد ضعف أو ثغرة ما متعلقة بأنظمة الكمبيوتر والشبكات فمثلا اختراق لكلمة المرور عبر

---

[1] هاجر بسمي، مفيدة بن ساسي، دور مسرح الجريمة الإلكترونية في الإثبات الجنائي، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر في القانون، تخصص قانون عام معمق، كلية الحقوق والعلوم السياسية 2020-2021، ص23.

2 المرجع نفسه ، ص23.

[3] سورية ديش، مرجع سابق، ص244.

خوارزميتها للوصول إلى النظام، ويقوم بذلك شخص أو أشخاص ذو خبرة والذين يطلق عليهم بالمقرصنين، من أجل تحقيق أهداف معينة. والوصول إلى معطيات ومعلومات مخزنة ولها أوجه عديدة كإختراق حواسيب الآخرين أو إختراق الشبكات أو السيطرة على نظام البرمجيات ، ويقوم بتحويل الأموال بطريقة غير مشروعة أو سرقة البيانات.[1] بحيث نص المشرع على القرصنة الإلكترونية في المادة 394 من قانون العقوبات رقم 21 – 08 المعدل والمتمم على أنه: " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50,000 دج إلى 80,000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة أو إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام تشغيل المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 إلى 300.000 دج ".[2]

ثالثا: الجرائم الواقعة على أمن الدولة

تقع هذه الجرائم باستعمال النظام المعلوماتي سواء لإفشاء الأسرار التي تخص مصالح الدولة ونظام الدفاع الوطني أو الإرهاب أو التجسس.

1. الإرهاب

حاليا تستخدم المجموعات الإرهابية تقنية المعلومات من أجل تسهيل الأشكال النمطية من الأعمال الإجرامية، فيستخدمون الإرهابيون الأنترنت من أجل استغلال من يؤيد أفكارهم من أجل جمع الأموال لتمويل برامجهم الإرهابية ، ويستولون على المواقع الحساسة وسرقة

[1] هاجر بسمي، مفيدة بن ساسي، مرجع سابق، ص25.

[2] أمر رقم 08/21 مؤرخ في 27 شوال عام 1442 الموافق لـ 8 يونيو سنة 2021، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

المعلومات وامتلاك القدرة على نشر الفيروسات ،ويعود ذلك إلى العدد المتزايد من برامج الكمبيوتر القوية وسهلة الاستخدام.[1]

2. التجسس :

فيقوم المجرمون بالتجسس على الدولة والمنظمات و الشخصيات والمؤسسات الوطنية أو الدولية .وتستهدف خاصة التجسس العسكري، السياسي، الإقتصادي، فيقوم بذلك استخدام التقنية المعلوماتية، تمارس هذه التقنية من قبل دولة على دولة، أو من شركة على شركة من أجل الإطلاع على المعلومات الخاصة المؤمنة في جهاز الآلي ويكون الإطلاع عليها غير مسموح أي هي من أسرار الدولة.[2]

الفرع الثاني: الجرائم المعلوماتية الواقعة على النظام المعلوماتي

فيكون الحاسب الآلي هو محل ارتكاب الجريمة، فيتضمن الدخول والبقاء في منظومة معلوماتية ،المساس بمنظومة معلوماتية، كما تضم أفعال إجرامية أخرى.

أولا: جريمة الدخول والبقاء غير المشروعان في منظومة معلوماتية

يعاقب كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك، فمنه العقوبة تضاعف إذا ولد عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي ، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء ، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محور أو تغيير في المعطيات الموجودة في النظام[3]. ولنوضح ذلك نذكر:

1. **فعل الدخول غير المشروع:**لا نعني هنا الدخول بالمعنى المادي أي الدخول إلى مكان معين كمنزل أو غيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها

[1]سورية ديش، مرجع سابق، ص245.

[2]المرجع نفسه ، ص246.

[3]عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أحمد دراية (أدرار)، سنة 2016-2017، ص27-28.

عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان ،أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات[1]، غير أن هذه الجريمة يحدث وقوعها لدى كل إنسان مهما كانت صفته أو كان يعمل أو لا يعمل في مجال المعلوماتية أو كان يستطيع الإستفادة من دخوله أو لا ، فهنا الجاني يكفي أن يكون ليس له الحق في الدخول إلى النظام وإن لم تكن له القدرة على تنفيذ العمليات على النظام غير أن الجريمة تتوافر رغم ذلك.

2. **فعل البقاء الغير مشروع:**ويعني ذلك من له الحق في السيطرة على النظام فيكون دخوله في نظام المعالجة الآلية للمعطيات قد تكون ضد إرادته ، فيكون البقاء معاقب عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول الى النظام بالصدفة أو كان عن طريق الخطأ ،فعلى المتدخل الإنسحاب من داخل النظام أو أن ينقطع وجوده، فإن بقي رغم ذلك يعاقب على جريمة البقاء غير المشروع وكذلك إذا سمح له الإطلاع على المعلومات حيث حين أنه يطبع فيها نسخة يكون البقاء جريمة سواء حصل الدخول مباشرة أو حصل عن بعد على الحاسوب.[2]

ثالثا.جريمة المساس بمنظومة المعلوماتية:نصت المادة 394 مكرر1 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات عن طريق استعمال الغش في أفعال الإدخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي توجد في نظام المعالجة الآلية للمعطيات سواء إضافة معلومات ومعطيات

[1] عائشة نايري ، مرجع سابق ، ص28.

[2] المرجع نفسه، ص29.

جديدة غير صحيحة ومحوها أو تعديل لمعطيات موجودة من قبل. فمثال ذلك ، إدخال فيروس المعلوماتية في البرامج الهدف من ذلك إتلافها.[1]

ثالثا: أفعال اجرامية اخرى

المادة 394 مكرر 2 حرمت الأعمال الآتية: تصميم ،بحث، تجميع أو توفير أو نشر أو الإيجار في معطيات أو معالجة مرسلة عن طريق منظومة معلوماتية[2] . فهذه الأعمال يمكن أن ترتكب بها احدى جرائم الغش المعلوماتي، وحرم المشرع كذلك بعض الأفعال المتحصلة من جرائم الغش وهي: الحيازة الإفشاء، النشر أو استعمال المعطيات لأي غرض.

ويستنتج من ذلك أن هذه الأنواع من الجرائم المعلوماتية قد تهدد كيان وسلامة وحرمة الفرد.

المبحث الثاني: ماهية التفتيش الإلكتروني

لكل فرد من أفراد المجتمع الحق بالتمسك بحق سرية حياته الخاصة سواء أكانت هذه السرية تتمثل في شخصه أو مسكنه أو مراسلته وله الحق بالتمتع بحماية القانون لهذا الحق، ولكن في بعض الأحيان يمكن إنتهاك هذا الحق وكشف هذه السرية في سبيل الوصول إلى الحقيقة الذي ينشدها القانون، وهذا الحق يكون بإجراء نص عليه القانون وهو التفتيش وبهذا فإن التفتيش هو إجراء قانوني يمس بحرمة الأشخاص ومساكنهم وله صور عديدة مثل: التفتيش القضائي، التفتيش العادي، الوقائي، التفتيش الإلكتروني، ومن هذا نتطرق إلى مفهوم التفتيش الإلكتروني في المطلب الأول، وبخصوص المطلب الثاني فحددناه إلى معاينة مسرح الجريمة الإلكترونية .

المطلب الأول: مفهوم التفتيش الالكتروني

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2011-2012، ص185.

[2] المرجع نفسه، ص185.

يعتبر التفتيش إجراء من إجراءات التحقيق يهدف إلى ضبط أدلة الجريمة موضوع التحقيق وكل ما يساعد للكشف عن الحقيقة عن طريق البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها أدت للمساس بحق المتهم في سرية حياته الخاصة وهذا من أجل إثبات وقوعها.[1] ومن خلال تحليلنا لهذا يمكن استخلاص تعريف التفتيش الإلكتروني في الفرع الأول ومحله في الفرع الثاني.

الفرع الأول: تعريف التفتيش الإلكتروني

يمكن استخلاص تعريف التفتيش على أنه' " إجراء من إجراءات التحقيق يهدف للبحث عن أدلة مادية وقعت في محل يتمتع بحرمة السكن أو تفتيش الشخص من أجل اثبات وقوعها وفق الإجراءات القانونية المحددة ".[2]

و يقصد أيضا على انه' " البحث في مستودع سر المتهم عن أشياء تفيد في كشف الحقيقة و نسبتها إليه، أو هو إجراء التحقيق الذي يهدف إلى التوصل إلى أدلة جريمة إرتكبت فعلا، وذلك بالبحث عن الأدلة في مستودع السر سواء أجري على شخص المتهم، أو في منزله دون توقف على إرادته".[3]

ومن خلال ذلك يمكننا القول بأن التفتيش بشكل عام أنه إجراء جنائي يتضمن اعتداء على حق الإنسان في الاحتفاظ بسره وحرمته مسكنه، ويحقق مصلحة المجتمع من أجل الوصول إلى أدلة الجريمة، والكشف عن الحقيقة.

ولا يختلف التفتيش لجرائم الحاسب الآلي عن التفتيش العادي بالنسبة لمدلوله القانوني فيمكننا إعطاء تعاريف للتفتيش الإلكتروني على أنه، " البحث في مستودع سر المتهم أو الإطلاع على محل منحه القانون حماية خاصة، يتمثل هذا المستودع وهذا المحل في جهاز

---

[1] سماح محمودي، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والأنترنت، المركز الجامعي بريكة، العدد 08 ج،01 جوان 2017، ص328.

[2] المرجع نفسه، ص328.

[3] المرجع نفسه، ص328.

للمعلومات كالكمبيوتر أو أنظمة الأنترنت، وذلك للبحث عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إلى المتهم".[1]

حيث أنه كذلك: " إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها "[2].

ومنه الهدف من التفتيش هو كشف الغموض الذي يحيط بالجريمة وجمع الأدلة المتعلقة بها، والوصول إلى أشياء مادية تكشف الحقيقة.

وبالذهاب إلى المشرع الجزائري تجدر الإشارة إلى أنّ المشرع الجزائري لم يضع تعريفا تشريعيا للتفتيش الإلكتروني وهذا في القانون رقم 09/04 بل ترك ذلك للفقه واكتفى المشرع فقط بتنظيم أحكامه وضوابطه.

ونستخلص ذلك خلال المادة الخامسة من هذا القانون على أنه: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، الدخول بغرض التفتيش، ولو عن بعد إلى:

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

ب-منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة إذا كان هناك أسباب تدعو للإعتقاد بأجهزة المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات

[1] سماح محمودي، مرجع سابق، ص328.

[2] المرجع نفسه ، ص328.

يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

- إذا تبين مسبقا 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 للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.
- يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة حماية المعطيات والمعلوماتية التي تتضمنها قصد مساعدتها وتزويرها بكل المعلومات الضرورية لإنجاز مهمتها".[1]

ويستنتج من هذا أن المشرع الجزائري ذكر التفتيش في القانون 09-04 ولم يحدد تعريف دقيق له.

وانطلاقا من كل هذا أن التفتيش الإلكتروني هو إجراء من إجراءات التحقيق في الجريمة المعلوماتية وللبحث عن الأدلة للوصول إلى حقيقة تكشف خفايا وأشخاص هاربين من وجه العدالة، لجريمة معلوماتية تحقق وقوعها ويكون المحل المراد تفتيشه هو جهاز الحاسوب الآلي أو شبكة الأنترنت لسبب خبايا المعلومات المخزنة فيه وضبطها.

الفرع الثاني: محل التفتيش الإلكتروني

للتعرف ولتحليل محل التفتيش الإلكتروني يجب تفتيش مكونات الحاسوب الآلي والذي يتكون من مكونات مادية "Hard ware" ومكونات منطقية soft ware، كما انه يتكون من ألياف اتصال سلكية ولا سلكية وبما أن التفتيش الغاية منه ضبط الأدلة المادية من أجل الوصول

[1] قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

إلى الكشف عن الحقيقة.[1] والكشف عن المجرم والتفتيش في المكونات المادية للحاسب الآلي يدخل ضمن نطاق التفتيش الإلكتروني طالما تم وفقا للإجراءات القانونية المحددة مع الأخذ بعين الاعتبار حساسية هذه الأجهزة والحفاظ عليها من التلف إضافة إلى مراعاة المكان الموجود فيه سواءا للأماكن العامة أو الخاصة حيث للمكان أهمية خاصة في التفتيش.[2]

أولا: خضوع مكونات الحاسوب المعنوية للتفتيش

أثار موضوع التفتيش مكونات الحاسب المعنوية جدلا وخلافا كبيرا حيث يذهب رأي لجواز تفتيشها كون أن الغاية من التفتيش هي ضبط الأدلة المادية التي تؤدي للكشف عن الحقيقة وهذا مفهوم شامل يمتد إلى البيانات الإلكترونية بأنواعها.[3]

فيما يذهب الرأي الثاني للقول بأن غاية التفتيش جمع أدلة مادية التي تفيد في كشف الجريمة فإن هذا المفهوم لا ينطبق على بيانات الحاسب الآلي الغير محسوسة، واقترح هذا الرأي إضافة عبارة "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي"،[4] وبهذا يصبح التعريف الجديد أو الغاية الجديدة من التفتيش بعد التطور الكبير الحاصل في هذا الزمان هو البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب الآلي.

1. مدى خضوع شبكات الحاسب الآلي للتفتيش "التفتيش عن بعد"

مع التطور الهائل الحاصل في مجال الإتصال ومع ظهور شبكة الأنترنت والتي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية أي أجهزة الكمبيوتر متصلة بعضها ببعض بطريقة مركزية ويدخل فيها ملايين الكمبيوترات الموزعة في مختلف أنحاء

[1] ليندة بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، جوان 2016، ص489.
[2] المرجع نفسه، ص490.
[3] المرجع نفسه، ص490.
[4] المرجع نفسه، ص490.

العالم.[1] حيث عرفها البعض ونستخلص منها أنها مجموعة كبيرة من أجهزة الحاسوب المتصلة فيما بينها بحيث يمكن لمستخدميها مشاركة المعلومات فيما بينهم وبالإضافة إلى أجهزة الكمبيوتر هناك أجهزة تحكم أخرى التي تؤدي إلى نفس وظيفة الحاسوب وتستعرض بعض استخدامات شبكة الأنترنت لتبيان علاقتها لموضوع التفتيش مثل: البريد الإلكتروني email، شبكة العنكبوت web أو مجموعة الأخبار وغرفة المحادثة والدردشة "ميسنجر" ومن هذا يتضح أن مجال الاتصالات لم يعد يقتصر على إقليم الدولة بل امتد ليشمل كل أرجاء العالم مما صعب وعقد مهمة التفتيش والضبط. ومنه نستخلص فرضيتين:

الفرضية الأولى: اتصال حاسب المتهم بحاسب آخر موجود في مكان آخر داخل الدولة

حيث أجاز المشرع الجزائري في نص المادة 05 من الفقرة الثانية من قانون رقم 09/04 تمديد التفتيش حيث تنص المادة على: " في حال تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، إذا كانت هناك أسباب تدعو للإعتماد بأن المعطيات المبحوثة عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى ويجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة بذلك "

ونلاحظ من خلال هذه المادة أن المشرع الجزائري قيد سلطة التفتيش باستصدار إذن قضائي وهذا ما أقرته الإتفاقيات الأوروبية للجرائم الإلكترونية، وقد أضفى المشرع على البحث داخل المعلومات صفة الرسمية أي بعد إخطار السلطات المختصة[2].

[1] ليندة بن طالب ، مرجع سابق، ص490.

[2] المرجع نفسه ، ص491.

الفرضية الثانية: حالة ما يكون الكمبيوتر متصلا بجهاز آخر خارج الدولة

لا يمكن مباشرة الدولة المختصة بالتحقيق للقيام بأي إجراء خارج إقليمها كون ذلك يعد انتهاكا لسيادة الدولة الأخرى، وهذا ما يعيق الحصول على الدليل بشأن بعض الجرائم فتمسك الدولة بسيادتها يمنع الوصول للمشتبه فيه لكن يمكن اتخاذ إجراءات بهذا الشأن في حالة إذا كانت هناك اتفاقيات بين الدول، كاتفاقيات الإنابة القضائية[1].

بالعودة إلى المشرع الجزائري نصت المادة 05 من قانون رقم 04-09: " أنه يمكن للسلطات القضائية المختصة للدخول إلى المنظومة المعلوماتية حتى وإن تبين لها أن المعلومات محل البحث مخزنة في منظومة خارج إقليم التراب الوطني فهذا لا يمنعها من الوصول إليها بمساعدة السلطات الأجنبية المختصة في إطار الاتفاقيات المبرمة في مثل هكذا جرائم ".

ثانيا: المكونات المادية للحاسب الآلي

الكمبيوتر هو جهاز إلكتروني لمعالجة المعلومات أو البيانات وله القدرة على تخزين واسترجاع البيانات وبعد دراستنا للمكونات المعنوية له ومدى قابليتها للتفتيش، نقدم باستعراض المكونات المادية للحاسب الآلي ومدى قابلية التفتيش.

ونقصد بالمكونات المادية للحاسب الآلي تلك الوحدات المكونة له ولكل منهم وظيفة معينة وتتصل بعضها ببعض بشكل يجعلها تعمل كنظام واحد وهذه الوحدات هي:

1. **وحدات الإدخال:** وهي التي تمكن المستخدم من إدخال البيانات وهي الفأرة تستخدم للانتقال داخل نظام "مايكروسفت ويندوز" إضافة إلى لوحة المفاتيح ومشغل الأقراص.

[1] ليندة بن طالب، مرجع سابق، ص491.

2. **وحدة الذاكرة:**ويستخدمها المعالج في تخزين بعض البيانات الخاصة والمتكررة استخدامها ليسهل الرجوع إليها.
3. **وحدة الحساب والمنطق:**أي تكمن وظيفتها حساب العمليات المطلوبة.[1]
4. **وحدة التحكم:** أي التي تتحكم بأعمال الكمبيوتر ووحداتها وتنسق وتبدل البيانات.
5. **وحدة الذاكرة المساعدة:** تستعمل لتخزين كميات كبيرة من البيانات وبصورة دائمة أي أنها لا تفقد محتواها من قطاع الكهرباء ومن أهم وسائل التخزين المستخدمة هي الأقراص المرنة والصلبة والمضغوطة[2] ،ويمكن ضبط الأقراص المرنة عند إجراء التفتيش ولمن تحتاج إلى إجراءات فنية معينة.
6. **وحدات الإخراج:** تعمل على استقبال بيانات من الحاسوب الآلي، وتمريرها إلى المستخدم بالطريقة المناسبة[3] ،أي إخراج نتائج المعالجة ومن أمثلة أجهزة الإخراج: الشاشة، الطابعة .

ويستخلص من هذا أن المكونات المادية للحاسوب مسألة ضرورية من أجل مدى قابلية إجراء التفتيش عن المعلومات المتواجدة فيه، ولا غنى أيضا عن المكونات المعنوية له.

المطلب الثاني: معاينة مسرح الجريمة الإلكتروني

تعد معاينة مسرح الجريمة الإلكتروني من الإجراءات المادية للقواعد العامة لمتابعة الجريمة المعلوماتية، ولم يحدد المشرع المقصود بالمعاينة، لذلك فقد عرفت من قبل الفقه الجنائي، رؤية بالعين المكان أو شخص أو شيء لإثبات حالة وضبط كل ما يلزم لكشف الحقيقة.[1]

[1] سماح محمودي، مرجع سابق، ص333.
[2] المرجع نفسه ، ص333.
[3] المرجع نفسه ، ص334.

فتقتضي وجوبا الانتقال من طرف الضبط القضائي إلى محل الواقعة لمباشرتها، ومن أجل إثبات أي حالة أو أشياء أو أشخاص ذات الصلة بالحادث، قد تفيد في الكشف عن الحقيقة في الجريمة وهي المرحلة الأولى للاستدلال حول أية جريمة تتم من خلالها جمع ضباط الشرطة القضائية[2].

حيث تكمن أهمية المعاينة في أنها تنقل إلى جهة التحقيق والمحاكمة صورة مجملة لموقع الجريمة، فنظرا لتنوع الجرائم إلى الجرائم التقليدية والجرائم الحديثة فيختلف مسرح الجريمة بين التقليدي والحديث، فقد يكون مسرح الجريمة تقليدي كما قد يكون مسرح الجريمة جهاز كمبيوتر ومن خلال هذا سنقسم هذا المطلب إلى فرعين الفرع الأول سنعرف فيه مسرح الجريمة التقليدي، أما الفرع الثاني نتناول فيه تعريف مسرح الجريمة الإلكتروني.

الفرع الأول: تعريف مسرح الجريمة التقليدي

يعرف مسرح الجريمة التقليدي فقهيا أنه المكان الذي انتهت فيه أدوار النشاط الإجرامي للجاني ويبدأ منه نشاط القائم بالتحقيق قصد البحث عن الجاني من واقع الآثار التي خلفها.[3]

ويعرف كذلك أنه المكان الذي يحدث فيه تنفيذ الجريمة احتكاكا عنيف للجاني بمحتوى سطحه المادي سواء كان هذا المحتوى شخص أو شيئا، ويعرف أيضا المكان الذي يشمل معظم الأدلة.[4]

---

[1]عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي الإسكندرية، ط1، 2006، ص179.

[2]ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة الماستر في القانون، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي بن مهيدي، أم البواقي، سنة 2015-2016، ص7.

[3]هاجر بسمي، مفيدة بن ساسي، مرجع سابق، ص29.

[4]المرجع نفسه ، ص29.

ولجمع الأدلة في مسرح الجريمة يمكن أن يكون مسرح الجريمة مكان واحد كما قد يكون أماكن، ليستدل منها على آثار تكون ذات صلة بالجريمة.

أما في التعريف القانوني حيث المشرع الجزائري لم يعرف مسرح الجريمة ولم يأخذه كمصطلح حيث أخذ من قانون الإجراءات الجزائية عدة مواد لها صلة وتحمل دلالة على مسرح الجريمة، في المواد56،50،43،42، 79،62،60.[1]

- المادة 42 حيث ذكرت فيها: "يجب على ضابط الشرطة القضائية أن ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع التحريات اللازمة...."
- وكلمة بمكان الجناية دلالة على مسرح الجريمة الذي يتخذ منه الأدلة.
- المادة 43 ق03/82: "يخطر في مكان ارتكاب جناية... الأماكن التي وقعت فيها..."

حيث مكان ارتكاب الجريمة جناية، والأماكن التي وقعت فيها الجريمة هي مسرح الجريمة.

- المادة 50: ".... مبارحة مكان الجريمة...."
- المادة 56 و60 و62: "مكان الحادث" أي مكان وقوع الجريمة ويعني مسرح الجريمة.
- المادة 79 ق18-06: "أماكن وقوع الجريمة"

الفرع الثاني: تعريف مسرح الجريمة الإلكتروني

مسرح الجريمة الإلكتروني او المسرح الافتراضي وهو الذي يتم ويقع داخل بيئة الحاسوب ويتكون عادة من البيانات الرقمية التي توجد داخل الحاسوب في ذاكرة الأقراص الصلبة المتواجدة في داخله.[2]

[1] الأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[2] ابتسام بغو، مرجع سابق، ص9.

فقد يكون مكان أو مجموعة الأماكن الإلكترونية التي يتم فيها مرحلة تنفيذ الجريمة الإلكترونية و التي تنتج عن ارتكابها آثار إجرامية غير مادية، لأن مسرح الجريمة الإلكترونية يعتبر المكان غير المادي او غير الملموس الذي تنبثق منه الأدلة الرقمية المؤيدة للإتهام.

ونظرا لصعوبة إثبات الجريمة الإلكترونية باعتبارها متعددة الأبعاد لا ترتبط مكان خاص ومعين، لذلك أن مسرح الجريمة الإلكتروني في هذه الحالة يقع بين شبكات التواصل الإجتماعي، أي أنه يصعب تحديده ويعود سبب ذلك لسهولة التخلص منه.

حيث أن المعاينة في المسرح الافتراضي تتميز بالصعوبة وتتمثل في:

- قلة الآثار المادية التي تولد عن الجرائم التي تقع على أدوات المعلومات.
- لكون الجريمة المعلوماتية صعبة الإثبات واكتشاف من قام بها خاصة في مقاهي الأنترنت لتوافد عدد كبير جدا من الأشخاص الذين يترددون على مسرح الجريمة خلال مدة زمنية، وحتى يمكن لضابط الشرطة القضائية القيام بالمعاينة في العالم الافتراضي لابد عليه أن ينتقل للمعاينة من مكتبة أو اللجوء إلى مقهى الأنترنت أو إلى الخبراء وغيرها من الأماكن التي تساعده في ظهور الحقيقة.[1]

وتتميز المعاينة في جرائم الأنترنت والحاسوب المعلوماتية بأشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة، فهناك عدة طرق عامة تتماشى مع طبيعة الإتصال بالأنترنت أو الوسيلة المستخدمة مثلا: وسيلة تصوير شاشة الحاسوب impression de captures d'écran والتي تكون بواسطة آلة تصوير تقليدية أو عن طريق استخدام حاسوب مختصة

[1] ابتسام بغو، مرجع سابق، ص10.

في أخذ صورة لما يظهر على الشاشة وهذا ما يصطلح عليه تجميد مخرجات الشاشة Frozen وغيرها.[1]

ونظرا مما درسنا سابقا لمسرح الجريمة والتطرق إلى مسرح الجريمة التقليدي والإلكتروني سندرج أهم الفوارق بينهما:

1. يقع مسرح الجريمة الإلكتروني في بيئة رقمية، ويكون إفتراضي، بينما مسرح الجريمة التقليدي يكون في العالم الواقعي الملموس.
2. الأدلة التي تأخذ من مسرح الجريمة التقليدي تكون مادية وتنتج أثر مادي كالشعر، بقع دموية، استعمال آلة وغيرها فيكون هذا الأثر المادي مصدر للدليل المادي بعد الفحص، أما في المسرح الحديث فتكون الأدلة عبارة عن معطيات رقمية وتقنية وتكون غير ملموسة أي افتراضية.
3. في المسرح التقليدي الآثار التي تم ايجادها تكون صعبة للتخلص منها، وسهلة للمحقق إيجادها ورصدها في متابعة تحقيقيه، بينما المسرح الإلكتروني من السهل محوها والتخلص منها ويصعب للمحقق ملاحظتها على الجهاز والنظام.[2]
4. عند ارتكاب الجرائم يستعمل في مسرح الجريمة الإلكترونية أدوات تقنية كأدوات مسح الترميز الرقمي، الطابعات، برامج نسخ المعلومات المخزنة في الحاسب الآلي، بينما في مسرح الجريمة التقليدي تستعمل مختلف الأسلحة المألوفة.
5. الجرائم التي تقع في مسرح الجريمة التقليدية تكون مرتبطة إلزاما بإقليم دولة الجاني والمجني عليه، أما الجرائم الواقعة في المسرح التقليدي لا تتطلب شرطا ذلك.

وهذا ما نستنتجه من مسرح الجريمة الإلكتروني والتقليدي بالنسبة للجريمة المعلوماتية.

---

[1] ابتسام بغو ، مرجع سابق ، ص10.

[2] هاجر بسمي، مفيدة بن ساسي، مرجع سابق، ص36-37.

خلاصة الفصل

من خلال دراستنا إلى مفهوم الجرائم الإلكترونية وأنواعها، وإلى ماهية التفتيش الإلكتروني في هذه الجرائم، نستخلص ان العالم شهد تطور كبير للجرائم الإلكترونية ومدى علاقتها بالتفتيش لأنه يعتبر إجراء للتحقيق فيها لمعرفة مرتكبيها ووقوعها، وهو إجراء صعب بالنظر إلى طبيعة الدليل المتحصل منه والذي يسهل إخفائه، كما أنه يسهل حصوله من مسرح الجريمة الإلكتروني الذي يعدّ من أهم وأول وسيلة لإيجاد الدليل الإلكتروني عبر المنظومة المعلوماتية.

الفصل الثاني :

ضوابط التفتيش الإلكتروني

الفصل الثاني: ضوابط التفتيش الالكتروني

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يقوم به موظف مختص، طبقا للإجراءات المقررة قانونا ، و في محل يتمتع بحرمته، بهدف الوصول إلى أدلة مادية لجناية وجنحة تحقق وقوعها ، لإثبات ارتكابها ونسبها إلى المتهم، وأحاط المشرع إجراء التفتيش لضوابط عديدة نظرا لمساسها بالحريات الخاصة للأفراد.

ومع التطور التكنولوجي الذي يشهده العالم الحالي،واستفاد منه عالم الإجرام وجدت جرائم حديثة وهي الجرائم المعلوماتية، وشهدت مشكلات عديدة في قانون الإجراءات الجنائي، حيث أن هذه النصوص تحكم الإجراءات المتعلقة بالجرائم التقليدية التي لا توجد صعوبات كبيرة في إثباتها وجمع الأدلة المتعلقة بها، غير أن في الجرائم المعلوماتية يتم إجراء التفتيش بصعوبات ومعوقات نظرا لوقوع الجريمة المعلوماتية ضمن بيئة رقمية في أجهزة الحاسب الآلي والشبكات المعلوماتية وبذلك يصعب إثبات دليل الجريمة.

فاستوجب علينا تفصيل المفاهيم في مبحثين، وذلك في المبحث الأول تحت عنوان شروط التفتيش الإلكتروني، أما في المبحث الثاني نبين فيه حجية الدليل الرقمي في إثبات الجريمة المعلوماتية .

المبحث الأول: شروط التفتيش الإلكتروني

يعد التفتيش الإلكتروني من أهم وأخطر إجراءات التحقيق، ومساسه الحرية الشخصية للفرد، فنظرا لذلك حرصت كافة التشريعات الإجرائية بما فيها التشريع الجزائري على ضرورة إحاطته بمجموعة من الضوابط الموضوعية والشكلية التي تعمل على خلق التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد، وتحقيق الفاعلية المطلوبة للأجهزة الأمنية وكشف غموض الجريمة وضبط مرتكبيها وتقديمهم للمحاكمة بعد التحقيق معهم من طرف سلطات التحقيق.

وعلى هذا الأساس سوف نتناول شروط التفتيش الإلكتروني في مطلبين، نتطرق إلى الشروط الموضوعية كمطلب أول والشروط الشكلية كمطلب ثاني.

المطلب الأول: الشروط الموضوعية للتفتيش الإلكتروني

يقصد بالشروط الموضوعية للتفتيش الإلكتروني تلك الإجراءات اللازمة لتفتيش صحيح في الجرائم المعلوماتية، فسنقوم بتقسيم هذا المطلب إلى ثلاثة فروع يخصص الفرع الأول لسبب التفتيش والفرع الثاني سنخصصه لمحل التفتيش والفرع الثالث سنبين فيه السلطة المختصة بالتفتيش.[1]

الفرع الأول: سبب التفتيش

المقصود بسبب التفتيش، الدافع المقتضي لإجرائه، ويتحقق هذا بوقوع جريمة معلوماتية، وارتكاب أشخاص معينين والإشتراك فيها واتهامهم بها، ووجود دلائل قوية على وجود محل الجريمة في المكان أو لدى الشخص المراد تفتيشه، ووجود غاية معينة من وراء إجراءه1، ولصحة التفتيش في العالم الإفتراضي لا بد لسببه أن تتوفر فيه الشروط الآتية:

[1] سامي جلال فقي حسين، مرجع سابق، ص117.

أولا: وقوع جريمة معلوماتية

لإجراء عملية تفتيش المنظومات المعلوماتية أن تكون الجرائم قد وقعت بالفعل، فلا يمكن إجراء التفتيش من أجل جريمة تكون محتملة الوقوع حتى ولو تكون مبررات على جدية إحتمال وقوعها [1] ،بمعنى أن تكون الجريمة وقعت فعلا من أجل أن نقوم بإجراء التفتيش، والسبب هو أن التفتيش من الإجراءات الخطيرة التي تمس حرمة الأشخاص وحرمة حياتهم، فلا يجوز انتهاكها.

فقد نص المشرع العراقي على أنه إذا لم يكن الشخص متهما بارتكاب جريمة، فلا يجوز تفتيش الأشخاص أو الأماكن.

ولم يحدد المشرع العراقي نوع الجريمة المرتكبة، جناية أو جنحة أو مخالفة[2]، فيعني ذلك أن التفتيش يكون جائز في جميع أنواع الجرائم. أما المشرع المصري فموقفه لم يتوافق مع موقف المشرع العراقي، بحيث لم يجز إجراء تفتيش المنازل إلا في جرائم الجنايات والجنح، تبعا لخطورة وتقدير هذا الإجراء والذي يمس حرية الأشخاص وحرمة منازلهم وبذلك حصرها في الجنايات والجنح فقط دون المخالفات لبساطة أهميتها بما أنها لا تتناسب مع تلك الجرائم.[3]

وفي مفهوم القانون الجزائري فإننا نكون بصدد جريمة معلوماتية، أو إحدى الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات

---

1 رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، ع (5)، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، جوان 2012، ص164.

2 سامي جلال فقي حسين، مرجع سابق، ص.118

3 المرجع نفسه ، ص119

الإلكترونية أو أية وسيلة اتصال أخرى كالهاتف النقال، أو آلة لتصوير رقمية أو جهاز تسجيل. وهذا نظرا للمادة 2 من ق 09/04.[1]

ثانيا: اتهام شخص أو أشخاص معينين بارتكاب جريمة معلوماتية والاشتراك فيها

يتعين للقيام بإجراء التفتيش إضافة إلى وقوع الجريمة أن يكون هناك اتهام موجه إلى شخص أو عدة أشخاص سواء صفته فاعلا أوشريك أو يكون حائزا لأشياء تتعلق بالجريمة من جرائم تكنولوجيا الإعلام والاتصال.

ويجب أن يكون الاتهام جديا ومبنيا على أدلة وقرائن قانونية وقوية و كافية تبين أنه ساهم في ارتكاب الجريمة المعلوماتية[2]. فالمقصود بالدلائل: "استنتاج واقعة مجهولة من أخرى معلومة، وهذا الاستنتاج يكون على سبيل الاحتمال والرجحان"[3] ، فالدلائل التي تكفي لإتهام شخص معين يتم الحصول عليها بناء على تحريات جدية تجرى عند ارتكاب جريمة معلوماتية، وعندما يتم الوصول إلى دلائل تكفي لإتهام شخص أو أشخاص معينين يمكن إصدار إذن بإجراء التفتيش بعد ذلك، فتجمع هذه التحريات من قبل مأموري الضبط القضائي أو معاونيه.

وعليه يتعين على الجهة التي تمنح الإذن بالتفتيش أن تراقب هذه الإجراءات. " فالتفتيش لا يجوز إجراءه قانونا إلا إذا كان هناك احتمال للعثور على دليل من ورائه"[4]. بذلك لا بد من توفر بعض الأدلة الجدية التي يعتقد بها وقوع جريمة معلوماتية ونسبتها إلى المتهم المراد تفتيش منظومته المعلوماتية أو نظام اتصالاته الإلكترونية، و يمكن تلخيص هذه الأجهزة أو

---

[1] قانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق لـ 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[2] رضا هميسي، مرجع سابق، ص165.

[3] سامي جلال قفي حسين، مرجع سابق، ص121.

[4] سامي حسني الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972، ص98.

المعدات التي ارتكبت بها الجريمة المعلوماتية كجهاز الحاسوب وما يحتويه من بيانات ومعلومات تؤدي إلى كشف الحقيقة للشخص المراد تفتيشه أو قد تكون موجودة في منزله، ويجب أن تكون دلائل جدية وقوية لتبرر التعرض لحرمة المكان وحرية الشخص المراد تفتيشه[1]. بمعنى أن تكون دلائل قوية في تلك الأجهزة من الضمانات المهمة التي تكفل عدم التعرض لحرية الشخص وحرمة مسكنه.

ثالثا: غاية التفتيش

الغاية الأساسية من إجراء التفتيش هي الحصول على الأدلة التي تساهم في كشف الحقيقة، فتختلف غاية التفتيش بين الجرائم التقليدية والجرائم المعلوماتية. في الجرائم التقليدية تكون غاية التفتيش في ضبط الأدلة المادية التي تؤدي إلى كشف الحقيقة، أما بالنسبة للجرائم المعلوماتية فغاية التفتيش هي عند الحصول على الأدلة المعلوماتية التي تساعد في كشف الحقيقة والوصول إليها في جريمة معلوماتية تكون قد وقعت وجار التحقيق فيها.

الفرع الثاني: محل التفتيش في الجرائم المعلوماتية

يقصد بمحل التفتيش بشكل عام هو مستوع سر الإنسان، فيختلف بين الجرائم التقليدية والجرائم الماسة بأنظمة الإتصال والمعلوماتية، بالنسبة للجرائم التقليدية فيكون هذا المستودع في محل له حرمة خاصة كالمسكن أو قد يكون الشخص أو رسائله، أما محل التفتيش في الجرائم المعلوماتية فهو الحاسوب بمكوناته المادية والمعلوماتية وشبكاته والذي يعتبر النافذة التي تطل بها الأنترنت على العالم[2]، أي يقع التفتيش دائما على مستودع السر الذي يحتفظ به المرء بالأشياء التي تتضمن سره، ويكون التفتيش إما للأشخاص و إما للمساكن التي توجد فيها تلك الأجهزة أو الشبكات المعلوماتية.

---

[1] سامي جلال قفي حسين، مرجع سابق، ص125.

[2] عز الدين عثماني، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، جامعة تبسة، جانفي 2018، ص58.

فمحل التفتيش يشمل المكونات المادية والمعنوية للنظم المعلوماتية ،وهو يمتد إلى البيانات والمعلومات والبرمجيات التي تكون مقرها في الحواسيب فضلا عن الأقراص والأشرطة، وغيره من وسائل الاتصال الحديثة، كالهواتف الذكية،والخلوية، وشرائح الهاتف"carte sim " وبطاقات الذاكرة، وآلات التصوير الرقمية، وكذلك يكون التفتيش أيضا على بطاقات فك التفشير الخاصة بالتلفزيون الرقمي[1]. أي ينبغي تحديد البيانات والمعلومات المراد البحث عنها وضبطها حسب القواعد الخاصة للتفتيش.

غير أن ذلك صعب جدا نظرا لصعوبة التوصل إلى هذه المعلومات أحيانا بسبب تداخل وتشابك الملفات الى تحوي هذه المعلومات وصعب الفصل بينها ولذلك يضطر أحيانا القائم بالتفتيش أن يقوم ببحث عام للوصول إلى هذا الدليل وهذا يخالف القواعد العامة للتفتيش في وجوب تحديد المحل المراد تفتيشه، فعيب البحث العام للملفات أنه يؤدي إلى الإطلاع على ملفات لا يشملها اذن التفتيش[2] ،فبذلك قد يكون انتهاك حق خصوصية الأشخاص.

الفرع الثالث: السلطة المختصة بالتفتيش

التفتيش الإلكتروني لا يعتبر صحيحا ولاينتج آثاره، إلا إذا قامت به الجهات أو الأشخاص الذين خولت لهم صلاحيات إجرائه قانونا، فقد جرى اختلاف حول ذلك في التشريعات الإجرائية، فمنهم من أسند هذه السلطة إلى المدعي العام وهناك من منحها إلى قاضي التحقيق أو ضباط الشرطة القضائية .

أما المشرع الجزائري فقد منح صلاحية إجراء التفتيش إلى السلطات القضائية الممثلة في النيابة أوالتحقيق وكذلك ضباط الشرطة القضائية وفقا لأحكام المادة05من القانون 04/09.[3]

---

[1] رضا هميسي، مرجع سابق، ص167.

[2] سامي جلال فقي، مرجع سابق، ص130.

[3] قانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق لـ 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

كما أن التفتيش عن الأدلة في جرائم الحاسوب يتطلب وجود مهارات فنية معينة في المحقق يجب أن يمتاز بها، حتى يسهل له العمل بسرعة للمحافظة على الأدلة من الإتلاف أو الشطب أو التعديل، ولذلك سرعة تغيير المعطيات الحاسوب[1].

فإن رجال الضابطة العدلية يساعدون النيابة العامة في إجراءات التفتيش للوصول إلى الأدلة المادية للجريمة، لأن التفتيش لا يعتبر غاية في حد ذاته، وإنما هو وسيلة تهدف للوصول إلى الأدلة الإجرامية التي تساهم في ضبط الأدلة.

وبما أن الموقع الرئيسي للتفتيش هو أجهزة الحاسوب المتواجدة في المنزل أو في المكاتب، فإن التفتيش قد يقع على الفرد بما يحمله من حاسوب محمول او قرص ليزري أو مرن أو أي جهاز آخر يكون موضوع الجريمة، أو يقع على المساكن التي يوجد بها الحاسوب والأقراص التي تحتوي على معطيات الحاسوب[2].

ولابد الاستعانة بالفنيين المختصين بالحاسوب والأنترنت حتى يتمكن المحقق من القيام بالتفتيش، فالنيابة العامة التي تعطي الإذن بالتفتيش والتحقيق، وعليه من الضروري أن تضم الضابطة العدلية المختصة بالتفتيش أعضاء مختصين بالحاسوب والانترنت، غير أن يقوم أفراد الضابطة العدلية بصلاحية التفتيش دون أخذ الإذن في النيابة العامة استثناءا في:[3]

1. الجرائم المشهودة: هي التي يشهد فيها الجاني حال ارتكابه للجريمة، حيث يسمح فيها القانون لرجال السلطة العامة وللمواطنين ضبط الأشياء التي يحملها الجاني فمن هذه الأشياء، الأقراص المرنة والليزرية أو أي شيء مخصص بتخزين معطيات الحاسوب أو الهواتف الخلوية التي تستطيع الارتباط مع الانترنت.

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، دار الثقافة للنشر والتوزيع عمان ،الطبعة الأولى، 2011م – 1432هـ، ص155.

[2] المرجع نفسه، ص156.

[3] المرجع نفسه ، ص157.

2. الجرائم الواقعة داخل المساكن: في هذه الجرائم تكون عند طلب صاحب المسكن من الشرطة أن يتدخلوا لأن الجناة قد استعملوا الحاسوب الذي يخصه بارتكاب جرائم ضد الغير، مثلا كإتلاف معطيات الحاسوب أو ارتكاب جرائم السب أو التحقير عبر الأنترنت أو التسلسل على الحسابات الشخصية لدى البنوك بهدف الاحتيال والنصب.

ويستنتج من ذلك أن إجراءات التفتيش الهدف منها البحث عن الأدلة لجناية أو جنحة تحقق وقوعها في محل تتمتع بحرمة المسكن أو تفتيش الشخص، لأن تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات الحاسوب ومجال إخفاء المعلومات فيها لأنه يسهل إتلافها جزئيا أو كليا، ولهذا لا بد من ضبطها بقواعد موضوعية.

المطلب الثاني: الشروط الشكلية للتفتيش الإلكتروني

يقصد بالشروط الشكلية " تلك الإجراءات التي أوجب المشرع مراعاتها عند إجراء عملية التفتيش والهدف من وضع هذه الشروط من قبل المشرع هي إحاطة عملية التفتيش بشكليات تضمن صحة ودقة النتائج التي يصل إليها القائم بالتفتيش وإحاطة المتهم بضمانات للحفاظ على حريته الفردية والشكلية في الإجراءات الجنائية هي ضمانات لعدم تعسف الجهات القائمة بالتفتيش"[1] ، وبالتالي باعتبار التفتيش اعتداء على حرمة وحرية الأشخاص والاطلاع على أسرارهم فقد أوجبت بعض التشريعات الالتزام بهذه الإجراءات الشكلية وذلك لضمان سلامة المتهم من تعسف الجهات الموكل لها بالتفتيش أو انحرافها واستغلالها للسلطة ،ومن هذا سوف نقسم هذا المطلب إلى أربعة (04) فروع، الفرع الأول الميعاد الزمني لإجراء التفتيش الإلكتروني، والفرع الثاني يخص الإذن بالتفتيش أما الفرع الثالث حضور أشخاص يحددهم القانون أثناء التفتيش والفرع الرابع والأخير وهو تحرير محضر التفتيش.

[1] سامي جلال فقي حسين، مرجع سابق، ص163.

الفرع الأول: الميعاد الزمني لإجراء التفتيش الإلكتروني

يعتبر الميعاد الزمني لإجراء التفتيش من الأمور المهمة التي تساعد في الحصول على الدليل الإلكتروني من عدمه كونه سهل إتلافه ومحوه من قبل المتهم قبل وصول السلطات المختصة إليه ومنه كلما كان الوصول للجريمة في وقت قصير كلما كانت فرصة الحصول على الدليل أكبر.

وقد حدد المشرع الجزائري الوقت القانوني الذي يجوز فيه الدخول للمساكن وتفتيشها وذلك بموجب المادة 47/1 من قانون الإجراءات الجزائية المعدل والمتمم والتي نصت على: "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة 5:00 صباحا ولا بعد 8:00 مساء.."[1] ، وبذلك حرص المشرع في هذا النص إلى الحفاظ على حرمة البيوت وساكنيه إضافة إلى صون الحرية الفردية للأفراد.

ويرد هذا النص استثناءا حيث أتاح المشرع للسلطات المخولة بالتفتيش القيام بعملها في أي ساعة من ساعات النهار أو الليل وذلك في الجرائم التي تصنف كجرائم معلوماتية حيث نصت المادة السالفة الذكر 47/1 من فقرتها 03 على: ".... وبذلك يكون المشرع قد غلب مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن باعتباره مستودع اسرارهم "[2]. وبالتالي فإن المشرع الجزائري قد أجاز التفتيش في أي وقت في مثل هكذا جرائم ولم يقيد القائمين بعملية التفتيش بميعاد محدد لطبيعة هذه الجرائم التي تتميز بسهولة محو الأدلة إضافة إلا أنه وضع مصلحة العامة فوق المصلحة الخاصة وهذا من أجل الحفاظ على المجتمع من هذه الجرائم.

---

[1] القانون رقم 03/82 المؤرخ في 1982/02/13 مستدرك (ج ر 1982/49) من قانون الإجراءات الجزائية المعجل والمتمم.

[2] سرور طالبي، مجلة جيل الأبحاث المعمقة ، مجلة علمية دولية ، محكمة تصدر دوريا عن مركز جيل البحث العلمي، العدد 34 يوليو 2019 ، ص114.

كما نرى أيضا في بعض التشريعات التي لم تحدد وقت معينا لإجراء التفتيش كالتشريع العراقي الذي أجاز القيام بالتفتيش وفي " أي وقت كان سواء بالليل أو النهار وهذا الإطلاق للوقت من قبل القانون العراقي يفيد في تنفيذ التفتيش في الجرائم المعلوماتية دون إتلاف أو محو الأدلة من قبل المتهم قبل وصول القائم بالتفتيش لها"[1]. وبالتالي فإن المشرع العراقي منح المكلف بالتفتيش كل الحرية في اختيار الوقت الذي يراه مناسبا للقيام بالتفتيش وذلك للحصول على أكبر عدد من الأدلة لإدانة المتهم والوصول قبل القيام بإتلافها.

الفرع الثاني: الإذن بالتفتيش

بالنظر في المادة 44 من قانون إجراءات الجزائية التي تنص على لا يجوز إجراء التفتيش لا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة[2]، أي عملية التفتيش تكون بعد الحصول على تصريح من السلطة المختصة قبل القيام بالعملية حيث يشرط المشرع وجوب إستظهار هذا الإذن قبل الدخول إلى مسكن المشتبه به وأن يتضمن بيان وصف الجريمة وموضوعها وعنوان الأماكن التي سيقوم بتفتيشها.

لكن بالرجوع إلى قانون 04/09 وتحديدا في مادته 05 و الذي جاء فيها' " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04: " الدخول بغرض التفتيش ولوعن بعد....."[3] وبالتالي ورغم أن المشرع لم ينص صراحة على وجوب استصدار إذن بتفتيش المنظومة المعلوماتية من قبل ضباط الشرط القضائية ،إلا أن هذا لا يعني عدم الحصول على إذن بل بشرط لمباشرته ضرورة الحصول على إذن من قبل الجهات المختصة.

---

[1] سامي جلال فقي حسين، مرجع سابق، ص163.

[2] سرور طالبي، مرجع سابق، ص113.

[3] قانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق لـ 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثالث: حضور اشخاص يحددهم القانون أثناء التفتيش

يعتبر حضور الأشخاص المعينون أثناء عملية التفتيش من الضمانات المهمة التي تضمن إجراءه بشكل صحيح وذلك يبعد الشك حول إمكانية إخفاء الدليل من قبل القائمين به إضافة إلى أنه يضمن سلامة المتهم والحيلولة دون تعسف الجهة القائمة بالتفتيش.[1]

ولقد نص المشرع الجزائري بموجب المادة 45/1 من قانون الإجراءات الجزائية ضرورة حصول إجراء التفتيش المتعلق بالسكن وملحقاته بحضور المشتبه فيه عندما يتم تفتيش مسكنه وأن تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكفله بتعيين ممثل له[2]. وبالتالي فلا يمكن للجهات المختصة بحسب هذه المادة القيام بعملية التفتيش دون حضور صاحب المسكن أوالمشتبه فيه وحالة غيابه تقوم السلطات المختصة بتعيين من ينوب عنه وذلك حفاظا حرية وحرمة المسكن.

غير أنه يرد لاستثناء في الجرائم الماسة بأنظمة المعالجة وهذا لخصوصية هذه الجرائم ومدى صعوبة جمع الأدلة، بالإضافة إلى سرعة إتلاف الدليل لذلك أوجب المشرع الجزائري في المادة السالفة الذكر في فقرتها الأخيرة، حيث استبعد من خلالها المشرع تطبيق هذا الضابط عند إجراء التفتيش الإلكتروني حيث بإمكانه القيام بعملية التفتيش دون حضور المشتبه فيه أو من ينوب عنه أو حتى الشهود[3].

الفرع الرابع: تحرير محضر التفتيش

عند الانتهاء من عملية التفتيش على القائم بالتفتيش تحرير محضر يدون فيه تفاصيل عملية التفتيش سواءا كان قد نجم عنه الحصول على دليل أو لم يتم الحصول عليه، ولا يقيد القانون بكتابة المحضر بشكل معين لصحته بل يجب أن يكون مكتوب باللغة الرسمية وأن

---

[1] سرور طالبي، مرجع سابق، ص112.

[2] القانون رقم 03/82، مرجع سابق.

[3] سرور طالبي، مرجع سابق، ص112.

يحمل تاريخ تحريره وتوقيع الشخص أو الجهة المكلفة بالتفتيش وبالتالي يستوجب توفره على أسس العامة لصحته.

وهذا ما يقره المشرع الجزائري عند تحرير محضر من طرف ضابط الشرطة القضائية حيث يخضع للقاعدة العامة ويختلف عند إجرائه من طرف قاضي التحقيق الذي يشرط أن يكون مصحوبا بكاتب يتولى تحرير المحضر وتدوين ما تعرضه من الإجراءات والتأثير عليه تحت طائلة البطلان.[1] وبالتالي فإن المشرع الجزائري قد ميز بين المحضر المحرر المنجز من طرف ضابط الشرطة وبين المحضر المنجز من طرف قاضي التحقيق الذي قيده بوجود كاتب يتولى تحرير المحضر.

إضافة لذلك أوجب المشرع إحاطة القائم بالتفتيش في الجرائم المعلوماتية باستعانته بأهل الخبرة الفنية والإختصاص في هذا المجال لمساعدته في إنجاز محضر لتغطية جميع الجوانب الفنية وذلك لخصوصية هذه الجرائم.

وبالنظر إلى التشريعات الأخرى فقد أوجب المشرع العراقي عند تحرير محضر التفتيش على "... وينظم القائمين بالتفتيش محضر يدون فيه إجراءات و زمان التفتيش و مكانه والأشياء المضبوطة وأسماء الأشخاص الموجودين في المحل وملاحظات المتهم وذوي العلاقة بشأن كل ذلك وأسماء الشهود ويوقع عليه المتهم وصاحب المكان..."[2]. وبالتالي فإن معظم التشريعات حول العالم تنتهج طريقة واحدة و موحدة وعامة في تحرير المحاضر مع إلزاميات ذكر الإجراءات داخل المحضر ومكان وزمان التفتيش إضافة إلى تدوين أسماء الموجودين والأشياء المضبوطة في مكان التفتيش.

[1] سرور طالبي، مرجع سابق ، ص113.

[2] سامي جلال فقي حسين، مرجع سابق، ص171.

وفي الأخير وعلى ضوء ما درسنا نستنتج أن التفتيش الإلكتروني يخضع لقواعد شكلية يفرضها المشرع من أجل الحفاظ على حق المشتبه فيه، وضمان حرمة بيته وأسراره ولتقييد المكلف بالتفتيش لعدم تعسفه في استخدام سلطته وبالنظر إلى المشرع الجزائري فقد أعطى الجرائم المعلوماتية خصوصية مما جعله يقوم ببعض الاستثناءات التي تخرج عن القواعد والأسس المألوفة في التفتيش التقليدي ويترتب على عدم مراعاة هذه الضوابط المحددة قانونا بطلان هذا الإجراء.

المبحث الثاني: حجية الدليل الرقمي في إثبات الجريمة المعلوماتية

موضوع الدليل الرقمي قد شغل فقهاء القانون الجنائي والمشرعين، وهذا فيما يخص الإثبات الجنائي رغم اختلاف نظمه، ونتيجة ذلك أن الدليل الرقمي يعتبر دليلا مستحدثا و طبيعته صعبة و معقدة. و هو من أبرز تطورات العصر الحديث في كافة النظم القانونية وتطور مع ذلك الفكر الإجرامي، فظهر نوع جديد من الجرائم تعرف بالجرائم المعلوماتية، فهو بذلك الوسيلة الرئيسة لإثبات هذا النوع من الجرائم.

وعليه سوف نتناول في هذا المبحث مطلبين، خصصنا في المطلب الأول ماهية الدليل الرقمي في إثبات الجريمة المعلوماتية، أما في المطلب الثاني فخصصناه للطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي.

المطلب الأول: ماهية الدليل الرقمي في إثبات الجريمة المعلوماتية

يقصد بالدليل قانونا " إقامة البرهان والحجة على الشخص أمام القضاء ووفقا لأحكام القانون على واقعة قانونية متنازع عليها بين الخصوم"[1]. وهذا يخص مفهوم الدليل بشكل عام، أما الدليل الرقمي فإنه مختلف عن الدليل الجنائي في المضمون رغم أنه متشابها معه في

[1] نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد الحادي عشر، جوان 2017، ص911.

الغاية. وبهذا قسمنا المطلب إلى فرعين (02) الفرع الأول يخص التعريف و الخصائص، أما الفرع الثاني نبين فيه جمع الدليل الإلكتروني الرقمي من مسرح الجريمة الإلكترونية.

الفرع الأول: مفهوم و خصائص الدليل الرقمي الإلكتروني

أولا: تعريف الدليل الرقمي الإلكتروني

اختلفت تعريفات الدليل الرقمي وتعددت، فنجد تعريف الدليل الرقمي على أنه: " الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيات خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم وذلك من أجل اعتماده أمام أجهزة إنقاذ وتطبيق القانون"[1].

- فيما عرفته المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 على أنه: "المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية"[2].

فيما ذهب بعض الدكاترة مثل الدكتور عمر محمد بن يونس إلى القول بأنه: " الدليل الذي يجد له أساس في العالم الافتراضي ويقود إلى الجريمة"[3].

ويمكن من خلال التعريفات السابقة القول بأن الدليل الجنائي هو دليل ينشأ في بيئة رقمية ويستخرج على شكل مادي يقدم أمام القضاء.

ثانيا: خصائص الدليل الرقمي الإلكتروني

نظرا للطبيعة الخاصة لجرائم الحاسوب والأنترنت فيمكن إثباتها جنائيا بعدة خصائص لتميزه عن الدليل الجنائي التقليدي وهي على النحو التالي:

---

[1] نور الهدى محمودي، مرجع سابق، 911.

[2] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، القاهرة، مطابع الشرطة، 1430هـ-2009م، ص213.

[3] خالد عياد الحلبي، مرجع سابق، ص229.

1. الدليل الإلكتروني بطبيعته يحتوي على عدة بيانات ومعلومات لها صفة إلكترونية ولا تدرك بالحواس العادية أي غير ملموسة، فإدراكها يتطلب الإستعانة بالحاسوب والأجهزة الإلكترونية خاصة بذلك.
2. الدليل الإلكتروني ليس دليلا ماديا فإنه تلك المجالات المغناطسية أو الكهربائية، فإخراج الدليل الإلكتروني في شكل مادي ملموس فهذا لا يعني أنه دليل، فهذا يعتبر نقل تلك المجالات من الطبيعة الإلكترونية إلى الشكل الذي يمكن استعماله كدليل على معلومة معينة.[1]
3. يختلف الدليل الإلكتروني عن الدليل التقليدي، في أنه يمكن استخراج نسخ من الدليل الإلكتروني تكون مطابقة للأصل ولها نفس القيمة العلمية والحجية، فهذا يشكل ضمانة فعالة من أجل الحفاظ على الدليل من الفقدان والتلف والتغيير، فهذا لا يتوافر في الدليل التقليدي.
4. عند محو الأدلة الإلكترونية يمكن استرجاعها وإظهارها بعد اخفائها، هذا يؤدي إلى صعوبة التخلص منها، ويمكن كذلك إخضاعه لعدة برامج من أجل التعرف ما إذا تعرض إلى التحريف والعبث فيه.[2]
5. الدليل الإلكتروني ذو طبيعة ديناميكية فائقة السرعة. فينتقل من مكان إلى آخر عبر شبكات الإتصال.
6. البحث الجنائي في الدليل الإلكتروني قد يكون بسهولة أيسر من الدليل التقليدي في إيجاده، من خلال تسجيل تحركات الفرد وسلوكياته.[3]

[1] خالد عياد االحلبي ، مرجع سابق ، ص232.
[2] المرجع نفسه ، ص232.
[3] المرجع نفسه ، ص233.

الفرع الثاني: جمع الدليل الإلكتروني الرقمي من مسرح الجريمة

يتطلب جمع الأدلة الإلكترونية مجموعة من الإجراءات وتتمثل في المعاينة وهذه الأخيرة لها دور مهم في كشف غموض مسرح الجريمة، فيكمن دورها في أن تكشف خبايا مسرح الجريمة المعلوماتية وأن تضبط المعلومات التي تفيد إثبات وقوع وارتكاب الجريمة، من أجل أن لا يقع في بعض المشكلات الآتية:

- إخفاء الدليل الإلكتروني ويعود ذلك إلى تعديله أو محوه في ثوان قليلة.
- يمكن للجاني أن يتلاعب بالبيانات أو محوها عن بعد عن طريق التدخل من وحدة ظرفية.[1]
- الجرائم الإلكترونية عند ارتكابها تخلف آثارا مادية تتمثل في بيانات غير مرئية.
- يتردد العديد من الأشخاص كونهم على مسرح الجريمة بين ارتكابها واكتشافها، يفتح المجال لحدوث إتلاف أو تغيير للآثار المادية، ونتيجة ذلك قد يدخل شك على الدليل المأخوذ من المعاينة.

وعليه فتساهم جمع الأدلة الإلكترونية الرقمية فيما يأتي'

- الكشف عن الدليل الرقمي، وتحديد خصائصه الفريدة.
- ضرورة إجراء إختبارات تكنولوجية وعملية على الدليل المأخوذ من أجل التحقق من مصدره وأصالته، حتى يمكن تقديمه كدليل لأجهزة تطبيق القانون.[2]
- إعادة إصلاح وتجميع الدليل من المكونات المادية للكمبيوتر HARD DRIVE
- ضرورة طبع نسخة أصلية منه من أجل التأكد من عدم وجود معلومات مفقودة عند عملية إخراج الدليل.

[1] رشيد بن فريحة، يوسف ميهوب، التحري الجنائي في مسرح الجريمة الإلكترونية، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد الثاني والأربعون (1)، صفر 2017، ص55.

[2] مصطفى محمد موسى، مرجع سابق، ص218.

- للتأكد من أن الدليل لم يتم العبث فيه أوتعديله، لا بد من استعمال خوارزميات Algorithm، والتي هي التعليمات يمكن أن تتبع لإنجاز عمل ما محدد عبر تجزئة المسألة البرمجية المراد حلها إلى أجزاء صغيرة بسيطة يمكن التوصل إلى حل صحيح من خلالها.[1]

وعادة ما توجد هذه الأدلة في' مخرجات الطابعة والتقارير والرسوم وأجهزة الكمبيوتر[2]، جيوب المتهم، واجهة أو شاشة الحاسب الآلي، المفكرة الإلكترونية والتي هي: (من أهم الأدلة التي يجب الحفاظ عليها، لأنها تحتوي على أسماء وأرقام وهواتف وعناوين بريد إلكتروني وتواريخ مهمة)، وتعود إلى سهولة القيام بالتحريات اللازمة.[3]

وغير أن المشرع الجزائري فقد أخذ بنظام الفصل بين سلطتي الاتهام للنيابة العامة والتحقيق يقوم به قاضي التحقيق، أما الشخص المكلف بجمع الأدلة الرقمية هو الخبير المتخصص والمدرب على أن يعالج جميع أنواع الأدلة وفحصها وتحليلها من أجل إثبات الجرائم المعلوماتية. ويعود ذلك لأنها معقدة ومحل الجريمة فيها غير مادي، وأسلوب ارتكابها سريع، وبذلك لا يمكن اكتشافها إلا من متخصص في هذا المجال، من خلال الخبرة التقنية التي هي أقوى مظاهر التعامل القانوني أو القضائي مع ظاهرة الأنترنت والتكنولوجيا.[4]

ومن خلال هذا يستخلص أن عملية الإثبات الجنائي تستند في جرائم الحاسوب والأنترنت على الدليل الإلكتروني باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم الحديثة العهد، وتبين أماكن تواجدها وإثباتها وإنبثاقها.

---

[1] مصطفى محمد موسى ، مرجع سابق، ص219.

[2] المرجع نفسه ، ص219.

[3] رشيد بن فريحة، يوسف ميهوب، مرجع سابق، ص56.

[4] المرجع نفسه، ص56.

المطلب الثاني: الطبيعة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي

إن الحصول على الدليل الإلكتروني وتقديمه للقضاء غير كافي لاعتماده كدليل موجه للقضاء، غير أن الطبيعة الفنية الخاصة للدليل الإلكتروني تمكن من العبث بموضوعه على نحو يحرف الحقيقة دون أن تكون قدرة الشخص غير المتخصص أن يدرك ذلك العبث، فإن نسبة الخطأ في عملية الحصول على دليل صادق في بيان الحقيقة قد تبدو عالية في مثل هذه الأدلة، ولذلك يدخل الشك في مصداقيتها كأدلة للإثبات الجنائي[1]. ولتبيان ذلك سنقسم هذا المطلب إلى فرعين (02)، سنخصص الفرع الأول لحجية الدليل الإلكتروني أمام القاضي الجنائي، أما الفرع الثاني نبين فيه سلطة القاضي الجنائي في قبول الدليل الرقمي.

الفرع الأول: حجية الدليل الإلكتروني أمام القاضي الجنائي

لا يكفي الحصول على الدليل الإلكتروني وتقديمه للقضاء كوكيل إدانة، بل يجب لقبوله توفر شروط معينة حيث يتمتع القاضي بسلطة واسعة في تقدير الدليل حتى وإن كان علمي وتكمن هذه الشروط في:

أولا: مشروعية الدليل الرقمي

حتى يكون الدليل الإلكتروني ذات قيمة قانونية أمام القاضي الجنائي يجب أن تكون الطريقة التي تم التوصل بها إلى الدليل تمت بطريقة مشروعة بعيدة عن أي زيف أو خداع، الأمر الذي يحتم عن من أسند إليهم أمر تحصيل الدليل الإلكتروني اتباع طرق قانونية ومشروعة تكون الغاية من ورائها إدانة المتهم من جهة ومن جهة أخرى قبول الدليل من طرف القاضي الجنائي.

وتعتبر مشروعية الدليل الإلكتروني أحد أهم ما أوصى به المؤتمر الخامس عسر للجمعية الدولية لقانون العقوبات والذي عقد في عاصمة البرازيل في الفترة ما بين 4-9 ، 1994

[1] خالد عياد الحلبي، مرجع سابق، ص246.

ولقد نص في التوصية رقم 18 على' "كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي والأدلة الناتجة عنه تكون باطلة ولا يمكن التمسك بها.[1]

ثانيا: بلوغ اقتناع القاضي درجة اليقين

لا بد لإثبات الدليل الإلكتروني توفره على شرط اليقين حيث يعتبر هذا الشرط عاما سواء كانت هذه الأدلة تقليدية أو حديثة وعليه يجب أن يكون الدليل الإلكتروني غير قابل للشك إذ أن هذا الأخير يفسر المصلحة المتهم، حيث أن الجزم بوقوع الجريمة الإلكترونية بجناح من القاضي نوعا آخر من المعرفة العلمية بالأمور المعلوماتية، إذ أن هذا الجهل بهذه الأمور يؤدي للتشكيك في قيمة الدليل وبالتالي يغض بالحكم بالبراءة ويستفيد المتهم من هذا الشك.[2]

ويشك في سلامة الدليل الإلكتروني من ناحيتين:

- بخصوص الناحية الأولى فإن الدليل الإلكتروني من الممكن خضوعه للعبث للخروج به على نحو يخالف الحقيقة وذلك دون أن يكون في إستطاعة الشخص غير المتخصص إدراك ذلك العبث.
- أما الناحية الثانية إذا كانت نسبة الخطأ الفني في الحصول على الدليل الإلكتروني نادرة إلا أنها تبقى ممكنة ويرجع الخطأ في الحصول على الدليل الإلكتروني لسببين هما:[3]

1. الخطأ في استخدام الأداة المناسبة للحصول على الدليل الإلكتروني كحصول خلل في الشفرة المستخدمة أو استخدام مواصفات خاطئة.
2. الخطا في استخلاص من الدليل، وذلك عن طريق استخدام أداة تقل نسبة صوابها 10% ويحدث هذا غالبا في سبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية.

---

[1] بن فردية محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، كلية الحقوق والعلوم السياسية، جامعة بجاية 06000، بجاية، الجزائر، ص278.

[2] المرجع نفسه، ص278.

[3] خالد عياد الحلبي، المرجع السابق، ص248.

ثالثا: مناقشة الدليل الرقمي

لا يبني القاضي حكمه إلا على أدلة تطرح أمام الجلسة أي أن يكون الدليل الرقمي ثابت أوراق الدعوى ويمكن للخصوم الإطلاع عليه ومناقشته حيث قضت المادة 212/2 من قانون الإجراءات الجزائية على: "لا يسوغ للقاضي أن يبني قراره إلا من الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة حضوريا أمامه"[1]. وهذا ما ينطبق على الدليل الرقمي أيا كان شكله.

وتقوم مناقشة الدليل على إتاحة الفرصة للخصوم من اجل الإطلاع على الدليل الرقمي والرد عليه لاستفاء حقهم في الرد و مواجهة هذه الدلائل، إضافة إلى إلزام وجود الدليل الرقمي في أوراق الدعوى حتى يكون اقتناع القاضي مبني على أساس.[2]

الفرع الثاني: سلطة القاضي الجنائي في قبول الدليل الرقمي

تتحدد سلطة القاضي الجنائي في قبول الدليل الرقمي حسب طبيعة نظام الإثبات السائد وتنقسم هذه الأنظمة إلى:

أولا النظام: اللاتيني

إن خصوصية مشروعية الدليل الإلكتروني في القوانين ذات الصيغة اللاتينية فإنها تترك للقاضي كامل الحرية في انتقاء الدليل وبأي وسيلة يراها مناسبة للوصول إلى الحقيقة، إلا أنه في المقابل يقيده من حيث الوسيلة التي يستعين بها حيث يجب أن تكون مطابقة للقانون يطلق على هذا النوع من الأنظمة بنظام الأدلة أو نظام الإثبات الحر ومن هذه التشريعات نجد كلا من الفرنسي والجزائري والمصري حيث أن المشرع الجزائري كرس المبدأ في المادة 212 من قانون الإجراءات الجزائية الجزائري.

[1] قانون رقم 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[2] بن فردية محمد، مرجع سابق، ص281.

ومع ظهور الدليل الرقمي أصبح القاضي في هذا النظام يتعامل مع الأدلة المستحدثة بغية إكشاف الجرائم ونتيجة لذلك أصبح القاضي غير مقيد بالأدلة التي يقدمها الأطراف لأن له الحق في المبادرة بنفسه باتخاذ جميع الإجراءات للبحث عن الأدلة اللازمة لتكوين قناعته وعلى سبيل ذلك له الحق في أن يأمر بتفتيش الحاسب الآلي وإختراق النظام والولوج إليه والإفصاح عن الكلمات السرية والشفرات الخاصة كما يحق للقاضي وفق هذه التشريعات أن يتأكد أولا من قبول الدليل ومدى مصداقيته وصحته.[1]

ثانيا: النظام الأنجلوسكسوني

إن مشروعية الدليل الإلكتروني في القوانين ذات الصيغة الأنجلوسكسونية تختلف كل الإختلاف عن المشروعية التي يتمتع بها الدليل في القوانين اللاتينية فهو نظام يطلق عليه بنظام الإثبات المحدد أو نظام الأدلة القانونية حيث يتم فيه المشرع بتحديد الأدلة مسبقا ولا يجوز للقاضي الخروج عليها وفي حالة وجود الدليل على شروط حددها وقيدها المشرع يلزم القاضي ببناء حكمه وفقه حتى اذ لم يكن مقتنعا به ومن الدول التي أخذت بهذا النظام، الولايات المتحدة و انجلترا وجنوب إفريقيا.[2] ويبنى الدليل في هذا النظام على قاعدتين أساسيتين هما:

1. **قاعدة الدليل الأفضل:** والمقصود به المستند الأصلي، فالقاعدة هي وجوب تقديم الأصل في الثبات أي من أجل إثبات محتويات سجل أو صورة فإن أصل الكتابة أو السجل أو الصورة يكون مطلوبا غير أن هذا العنصر يحتوي على استثناءات ترد عليه في القانون الأمريكي، ويرد على ذلك استثناءات أحدهما قبول الإحتجاج بالصورة إذا لم يتمكن من يريد الإحتجاج بها من الحصول على الأصل أو لأنها ليس لها وجود أساسا، أما الآخر فيمكن قبول الملخص لإثبات بدلا من الأصل.

[1] بن فردية محمد ، مرجع سابق، ص282.

[2] المرجع نفسه ، ص282.

أما بالنظر إلى القانون الانجليزي فإنه لا يجوز تقديم الصورة لإثبات محتوى الأصل إلا إذا كان الطرف الذي يحتج بالصورة لم يستطع تقديم الأصل ويرد على هذه القاعدة استثناء وهو قبول الصورة في حال إثبات الخصم إستحالة الحصول على الأصل.[1]

2. **قاعدة استبعاد سماع الشهود:** لا تقبل شهادة الشاهد طبقا لمبدأ الشهادة الحضورية في النظام الأنجلوسكسوني لا تقبل إلا إذا كانت صادرة عن ذلك الذي يعلم بصفة شخصية الوقائع والمعلومات المراد إثباتها فهو في الواقع الشخص الوحيد الذي يخضع لإختبار حضوري.[2]

وينتج عن ذلك اعتبار أي شهادة ليست حضورية ومباشرة تعتبر في القانون الأنجلوسكسوني شهادة بالتسامح ومن ثم لا تقبل أمام المحاكم كدليل إثبات.

فإذا ما قدم أحد مخرجات الحاسب كدليل إثبات أمام المحاكم فإن قبوله يتوقف حسب قاعدة عدم جواز الشهادة السماعية على شهادة من صدر عنه المسند حضوريا أمام القاضي على صحة المعلومات التي يتضمنها الوسيط الإلكتروني الصادر عن الحاسب تتم على أكثر مزيد.

بتطور التكنولوجيا الحديثة أصبح الدليل الالكتروني يحتل مكانة كبيرة في مجال الإثبات الجنائي ولا يتصور انقضاء في الجرائم المعلوماتية دون الإعتداء به إذ أنه قد يستطيع تقييد سلطة القاضي الجنائي عند الأخذ به في حالة ما إذا توافرت شروطه وأصبح يقينا.

فإن اثبات المواد الجزائية نحو النتيجة التي تتحقق باستعمال وسائله وطرقه المختلفة للوصول إلى الدليل الذي يستعين به القاضي لاستخلاص حقيقة الوقائع المعروضة عليه وإعمال حكم القانون عليه، ويعني ذلك أن موضوع الإثبات هو الوقائع وليس القانون وبالتالي فإن الإثبات الجزائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة دليل على وقوعها

[1] بن فردية محمد، ص283.

[2] المرجع نفسه، ص282.

و التأكد من أن المتهم هو مرتكب الجريمة بالفعل و وجود الدليل على ذلك، و يعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها الى المتهم.[1]

ويتبين موقف المشرع الجزائري من خلال حسمه لأنظمة الإثبات الجنائي بشكل واضح من خلال نص المادتين 212و307 من قانون الإجراءات الجزائية. حيث نصت المادة 212 على' "أنه يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص عليها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لإقتناعه الشخصي"، أما بالنسبة للمادة 307 تنص على أن "القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها وقد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما"، ولكنه يأمرهم أن يسألوا أنفسهم في صمت و تدبر، و يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: "هل لديكم اقتناع الشخصي"

فالنظر إلى نص هاتين المادتين يتضح جليا أن المشرع الجزائري تبني كأصل عام نظام الإثبات الحر أو الإقتناع الشخصي للقاضي الجزائي، والذي منح من خلاله للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لقناعته الذاتية، وفتح أمامه باب الإثبات على مصراعيه كي يستلمهم عقيدته من أي موطن يراه، دون أن يطالبه بتقديم مبرر لذلك.[2]

وفي الوقت نفسه وعلى سبيل الاستثناء نجده أخذ بنظام الإثبات المقيد أو ما يدعى كذلك بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا

[1] رابح مباركية ،إجراءات التحري و التحقيق في الجريمة الإلكترونية، مذكرة مقدمة لإستكمال متطلبات شهادة ماستر مهني في الحقوق،تخصص قانون الإعلام الآلي و الأنترنت، كلية الحقوق و العلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2022/2021،ص99.

[2] المرجع نفسه ،ص100

على سبيل الحصر كما هو الشأن بخصوص جريمة الزنا المنصوص عليها في المادة 339 من قانون العقوبات"[1]

وما يعزز توجه المشرع الجزائري إلى هذا الإتجاه هو عدم منعه نصوصا تملي على القاضي الجزائي مقدما بقبول أو عدم القبول أي دليل من الأدلة المطروحة عليه في الدعوى أو ترسم له طرقا محددة لإثبات يتقيد بها، إنما فسح له المجال لكي يختار بحرية بكل طرقه ما يراه مفيدا وموصلا إلى الكشف عن الحقيقة ويستلهم عقيدته من أية وسيلة أو دليل يطمئن إليه ويرتاح إليه ضميره، ولو تعلق الأمر من الأدلة الإلكترونية،[2] خاصة أنه لم يتضمن قانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها أية استثناءات خاصة بهذا الصدد، مما يوحي بأن الدليل الإلكتروني مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والاثبات في مجال الجرائم الإعتداء على النظم المعالجة الآلية بصفة خاصة ويمثل مظهرا من مظاهر اعتناق المشرع لمبدأ حرية الاثبات.

ولم يكتفي المشرع الجزائري بالنصوص المذكورة التي أطلقت حرية قاضي الموضوع في حرية بما فيها الإلكترونية، وتجميعها عن طريق وضع الترتيبات اللازمة لذلك.[3] وكذا تجميعها وصولا إلى الحقيقة التي سوف تبرر وفقها الإتهام وتؤسس عليها الأوامر التي يصدرها أبناء التحقيق. إضافة إلى إمكانية الإستعانة بكل شخص مؤهل أو لديه علم أو خبرة في الواقعة المراد اتخاذ الإجراء بشأنها.

وفي مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وضع المشرع الجزائري على عاتق مقدمي خدمات الأنترنت عددا من الإلتزامات لمساعدة السلطات المختصة بالتحري والتحقيق.

---

[1] رابح مباركية ، مرجع سابق ، ص100

[2]، المرجع نفسه ، ص101.

[3]المرجع نفسه، ص101.

لما من شأنه تسجيل وحفظ المعطيات المتعلقة بمحتوى الإتصال او المراسلة في حينها، كالمعطيات التي تسمح بالتعرف على مستعملي الخدمة، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال، خصائصها التقنية، وكذا تاريخ ووقت مدة الإتصال، والمعطيات التي تسمح بالتعرف على مرسل الإتصال والمرسل إليه وكذا العناوين الموقع المطلع عليها.[1]

وكل ذلك يعد إخبارا صريحا على أن المشرع الجزائري قد سار على نهج نظام الإثبات الحر وهناك أسباب أخرى عديدة تبرر أخذ المشرع الجزائري بنظام الإثبات و الإقتناع الحر، ولعل أهمها ظهور وتفشي الأدلة العلمية بمختلف أنواعها كذلك مستمدة من الطب الشرعي والتحاليل العلمية الدقيقة كالبصمات الشخصية والبصمة الوراثية، والأدلة الإلكترونية الرقمية، والتي لا تقبل بطبيعتها إخضاع القاضي لأية قيود بشأنها، بل بالعكس وهي تفرض أن يترك الأمر تقديرها لمحض إرادة واقتناع القاضي الجزائي.

ومن النتائج التي يمكن استخلاصها من خلال دراستنا السابقة ما يلي:

- إن التطور العلمي التكنولوجي خلق جرائم جديدة وبالتالي كان إثباتها هو الآخر نوعا جديدا وهو ما يطلق عليه بالدليل الرقمي.
- يتميز هذا الدليل بصعوبة الحصول عليه كونه غير مرئي وسهل الإتلاف، وبالرغم من ذلك أوجد التطور التقني طرقا لاسترجاع الأدلة المتلفة.
- يتم قبول الدليل الإلكتروني أمام القضاء في حالة توفره على شروط متفق عليها قضائيا أهمها: مشروعية الدليل ويقينه.

[1] رابح مباركية، مرجع سابق، ص102.

خلاصة الفصل

ما يمكن استخلاصه مما تم عرضه في هذا الفصل، أن مشكلة البحث عن الجريمة في البيئة الإلكترونية تنبع من طبيعة النوع المستحدث من الإجرام فهي جريمة متعلقة ببيانات معالجة إلكترونيا ومعلومات غير مادية يصعب الكشف عنها، ومن الصعب في بعض الأحيان جمع الأدلة والتفتيش عنها، فتزداد العملية صعوبة عندما يتعلق الأمر بتفتيش أنظمة معلوماتية، ومن هذا يثير التفتيش الإلكتروني ضرورة وضع ضوابط إجرائية للجريمة والكشف عنها وضبط فاعليها وتقديمهم للمحاكمة.

غير أن الدليل الإلكتروني التقليدي أصبح لا يتفق بشكل كامل مع طبيعة الوسط الذي ارتكبت فيه الجريمة حتى يستطيع القاضي أن يبني القناعة الكاملة في الإثبات، ولهذا ظهرت الأدلة الجديدة الجنائية تتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهو الدليل الإلكتروني الذي يستطيع القاضي بموجبه أن يبني قناعته ويصدر قراره.

خاتمة

خاتمة

بعد دراستنا لموضوع التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية وعرضنا مختلف أبعاده، ووضحنا بعض المفاهيم في عالم الجرائم الإلكترونية وأنواعها، ووضحنا أيضا التفتيش الإلكتروني واختلافه مع التفتيش العادي، و دور مسرح الجريمة بالنسبة له واختلافه أيضا مع المسرح التقليدي، وكذلك مفهوم الدليل الإلكتروني وقيمته الثبوتية، اتضح لنا جليا مدى التحول الذي مس مجالات البحث في العلوم الجنائية، ومدى التطور التكنولوجي الذي أثر على ذلك.

لقد بينا من خلال ما تقدم التفتيش كإجراء تحقيق في العالم الافتراضي ورأينا صلاحية جرائم الحاسوب لتكون محلا للتفتيش، مع مراعاة بعض الإجراءات والإحتياطات التي ترجع للطبيعة الإلكترونية، ورأينا أيضا أن التفتيش يمكن أن ينصب على المكونات المادية لجهاز الحاسوب وملحقاته باعتبارها أدلة مادية، كما يمكن أن ينصب أيضا على المكونات غير المادية من بيانات و معلومات معالجة آليا، يمكن الإحتجاج بها في الإثبات الجنائي مع مراعاة التعامل معها من قبل مختصين.

وتوصلنا إلى أن التفتيش المعلوماتي فعال و له ضرورة، و شأنه في ذلك شأن التفتيش التقليدي يخضع لنفس الأحكام العامة التي تضمن حقوق وحريات الأفراد ، و هو الامر الذي سعى المشرع الجزائري إلى تجسيده من خلال استحداث نصوص قانونية جديدة أوجد بموجبها قواعد إجرائية تتفق مع الطبيعة التقنية للجريمة المعلوماتية ، ويعتبر التفتيش الإلكتروني إحدى هذه الإجراءات التي حملها القانون رقم 04/09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإتصال ومكافحتها.

ونستنتج ومن خلال هذا البحث أن التحقيق الإلكتروني، يعاني من فراغ تشريعي وعدم توفر في النظام القانوني لتعليمات وإرشادات أو إجراءات تبين كيفية ضبط الأدلة الإلكترونية ، لم يعالج قانون الإجراءات الجزائية التفتيش عن بيانات الحاسوب ، فلا يوجد حتى الآن نصوص قانونية تتناول خصوصية الفضاء الإلكتروني .

التوصيات والإقتراحات:

1. ندعو المشرع إلى إصدار تشريع خاص ومستقل للجرائم الإلكترونية، و وضع عقوبات خاصة لهذه الجريمة.
2. إنشاء هيئة متخصصة تتكون من محققين من ذوي الإختصاص في مجال تقنية المعلومات للتحقيق في الجرائم الإلكترونية.
3. وضع تشريع يحدد طبيعة وكيفية و مفهوم محدد ومخصص للتفتيش الإلكتروني.
4. وجوب استخدام وسائل من خلالها يتم الحصول على الأدلة الإلكترونية في مجال الإثبات الجنائي لتسهيل العملية.

قائمة المصادر و المراجع

قائمة المصادر والمراجع

أولا: النصوص القانونية

1. رقم 20-442 المؤرخ في 15 جمادى الأول عام 1442 الموافق ل 30 ديسمبر سنة 2020. يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية (ج. رقم 82 ل30 ديسمبر 2020).
2. الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 الذي يتضمن قانون العقوبات المعدل والمتمم.
3. أمر رقم 08/21 مؤرخ في 27 شوال عام 1442 الموافق لـ 8 يونيو سنة 2021، يعدل ويتمم الأمر رقم 66-156 .
4. القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.
5. القانون رقم 03/82 المؤرخ في 1982/02/13 مستدرك (ج ر 1982/49) من قانون الإجراءات الجزائية المعجل والمتمم.

ثانيا: الكتب

1. عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر والتوزيع، كلية الحقوق جامعة مؤتة، الطبعة الأولى، 2017.
2. سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار شتات للنشر والبرمجيات، مصر، كلية الحقوق والعلوم السياسية، جامعة السليمانية.
3. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي الإسكندرية، ط1، 2006.
4[1].خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، 2011م.

4. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، القاهرة، مطابع الشرطة، 1430هـ-2009م.

5. سامي حسنيي الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972.

ثالثا: المذكرات

1. سعيدة بعرة، الجريمة الإلكترونية في التشريع الجزائري (دراسة مقارنة)، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة محمد خيضر، بسكرة، سنة 2015-2016.

2. هاجر بسمي، مفيدة بن ساسي، دور مسرح الجريمة الإلكترونية في الإثبات الجنائي، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر في القانون، تخصص قانون عام معمق، كلية الحقوق والعلوم السياسية 2020-2021.

3. عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أحمد دراية (أدرار)، سنة 2016-2017.

4. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجيستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر باتنة، 2011-2012.

5. ابتسام بغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة الماستر في القانون، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي بن مهيدي، ام البواقي، سنة 2015- 2016.

6. رابح مباركية، إجراءات التحري والتحقيق في الجريمة الإلكترونية، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر مهني في الحقوق تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشري الإبراهيمي، برج بوعريريج، 2021-2022.

رابعا: المقالات العلمية

1. عيدة بلعايد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بأفلو، الأغواط، العدد السادس (06)، مارس 2021.
2. سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018.
3. سماح محمودي، مشكلات التفتيش الجنائي في المعلومات في الكمبيوتر والأنترنت، المركز الجامعي بريكة، العدد 08، ج01، جوان 2017.
4. ليندة بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، جوان 2016.
5. رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، ع (5)، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، جوان 2012.
6. عز الدين عثماني، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، جامعة تبسة، جانفي 2018.
7. نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد الحادي عشر، جوان 2017.
8. رشيد بن فريحة، يوسف ميهوب، التحري الجنائي في مسرح الجريمة الإلكترونية، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد الثاني والأربعون (1)، صفر 2017.
9. بن فردية محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي (دراسة مقارنة)، كلية الحقوق والعلوم السياسية، جامعة بجاية 06000، بجاية، الجزائر.
10. سرور طالبي، مجلة جيل الأبحاث المعمقة، مجلة علمية دولية محكمة تصدر بيانا دوريا عن مركز جيل البحث العلمي، العدد 34 يوليو 2019.

فهرس المحتويات

فهرس المحتويات